# Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

## Σχολή Τεχνολογικών Εφαρμογών

## Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων


## Πτυχιακή Εργασία

# Ψηφιακό βιβλίο. Μελέτη και ανάπτυξη προτύπου σχολικού ψηφιακού βιβλίου


**Μιχάλης Λιοντάκης ΑΜ: 1701**

**Επιβλέπων Καθηγητής: Αθανάσιος Μαλάμος**

# Ευχαριστίες

Θα ήθελα να ευχαριστήσω την οικογένεια μου για την αμέριστη συμπαράσταση και υπομονή που έχουν δείξει όλα αυτά τα χρόνια της πορείας μου. Αλλά και τη φίλη μου Daria για όλη την υπομονή, ανεκτικότητα και την παρότρυνση να συνεχίσω την ολοκλήρωση της πτυχιακής μου εργασίας.

Τέλος, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου Αθανάσιο Μαλάμο για την καθοδήγηση του καθ' όλη την διάρκεια συγγραφής της πτυχιακής μου εργασίας.

# Περίληψη

Η παρούσα εργασία έχει ως σκοπό την περιγραφή και ανάλυση των ηλεκτρονικών βιβλίων. Ποία πρότυπα ηλεκτρονικών βιβλίων υπάρχουν αυτή την στιγμή και με ποιές ηλεκτρονικές συσκευές μπορούμε να τα διαβάσουμε. Επιπλέον, υπάρχει και αναλυτικός οδηγός ανάπτυξης ενός απλού ηλεκτρονικού βιβλίου.

Στην συνέχεια, γίνεται αναφορά στα συστήματα ασφάλειας των ψηφιακών δικαιωμάτων που προστατεύουν τα διάφορα έργα και τους δημιουργούς τους.

Τέλος, υπάρχει παράρτημα μου περιγράφει την τεχνολογία της κρυπτογραφίας μαζί με τις κυριότερες κρυπτογραφικές μεθόδους.

# Abstract

The purpose of this thesis is to describe and analyze the current state of eBooks. It refers to the ebook formats currently being used in markets and their corresponding electrical devices (eReaders), which read them. There is a written guide on how to create a simple eBook without any specific knowledge.

Also presented in this thesis are the systems for digital rights management which protect digital content and it's creators.

Finally, there is an appendix describing the technology of cryptography and the methods that are being used today to thwart various attacks.

# Κατάλογος Περιεχομένων

# Κατάλογος Εικόνων

# Κατάλογος Πινάκων

# Εισαγωγή

## 1.1 Κίνητρο για τη διεξαγωγή της εργασίας

Με την τεχνολογία να αναπτύσσεται καθημερινά και τα ηλεκτρονικά βιβλία να μπαίνουν ολοένα και περισσότερο στην καθημερινότητα μας, ήταν εύκολα να κινήσει το ενδιαφέρον της δημιουργίας ενός ηλεκτρονικού βιβλίου αλλά και η μελέτη των διάφορων προτύπων που υπάρχουν. Το ενδιαφέρον μεγαλώνει ακόμα περισσότερο όταν πρέπει να μελετήσεις την τεχνολογία όλων αυτών των προτύπων και τα συστήματα ασφάλειας πνευματικών δικαιωμάτων ώστε να διαλέξεις το καταλληλότερο για το η-βιβλίο σου.

## 1.2 Σκοπός της εργασίας

Η μελέτη έχει ως σκοπό την ανάλυση του τρόπου σχεδιασμού και την ανάπτυξη ενός ηλεκτρονικού βιβλίου .Σημαντικός στόχος της πτυχιακής, είναι ν' αποτελέσει ένα εμπεριστατωμένο οδηγό για τον οποιοδήποτε που ενδιαφέρεται να μάθει σχετικά με τα ηλεκτρονικά βιβλία, τους ηλεκτρονικούς αναγνώστες, τα ψηφιακά πνευματικά δικαιώματα αλλά και τα βασικότερα στοιχεία της κρυπτογράφησης. Επιδιώκοντας μέσα από πίνακες σύγκρισης αλλά και παραδείγματα να γίνει όσο πιο κατανοητά για τον οποιοδήποτε.

## 1.3 Ανάλυση κεφαλαίων

Το κεφάλαιο δύο ξεκινάει με κάποια γενικά για τα ηλεκτρονικά βιβλία όπως την ιστορία τους και την σχέση τους με διάφορες οντότητες. Επίσης, γίνεται μία εισαγωγή στα ψηφιακά δικαιώματα που υπάρχουν και τέλος τα πλεονεκτήματα και μειονεκτήματα των eBook.

Στο κεφάλαιο τρία γίνεται μία λεπτομερής ανάλυση των υπαρχόντων προτύπων που υπάρχουν για τα ηλεκτρονικά βιβλία. Και στο κεφάλαιο τέσσερα αναφέρονται τα θετικά και αρνητικά των προτύπων και διαφορές παρατηρήσεις για το καθένα ξεχωριστά που θα βοηθήσει τον ενδιαφερόμενο να καταλήξει πιο πρότυπο θα ακολουθήσει.

Το κεφάλαιο πέντε και έξι μιλάει αποκλειστικά για της συσκευές ανάγνωσης ηλεκτρονικών βιβλίων ή αλλιώς ηλεκτρονικούς αναγνώστες. Στο κεφάλαιο πέντε αναφέρονται γενικά θέματα, όπως σύγκριση των ηλεκτρονικών συσκευών με τα παραδοσιακά βιβλία αλλά και η τεχνολογία κατασκευής των οθονών. Στο έξι γίνεται μια λεπτομερή ανάλυση των νεώτερων ηλεκτρονικών αναγνωστών που υπάρχουν στην αγορά. Αναφέροντας τα χαρακτηριστικά τους. Όπου και στο τέλος υπάρχει συγκριτικός πίνακας, όπου αναφέρονται και τα θετικά και τα αρνητικά κάθε συσκευής ώστε να κάνει ακόμα πιο εύκολη την επιλογή του αναγνώστη.

Έπειτα, στο κεφάλαιο επτά γίνεται μία γενική ανάλυση των Digital Rights Management(DRM). Τι είναι η προστασία πνευματικών δικαιωμάτων και ποιούς στόχους έχουν.

Στο κεφάλαιο οκτώ γίνεται παρουσιάζονται τα πιο βασικά συστήματα προστασίας ψηφιακών πνευματικών δικαιωμάτων για διάφορες ψηφιακά μέσα, όπως eBooks, εικόνες, μουσική και τηλεόραση.

Στο κεφάλαιο εννέα γίνεται αναφορά στα creative commons, ένα νέο σύστημα προστασίας των πνευματικών δικαιωμάτων, που για πολλούς πιστεύετε ότι θα είναι το μέλλον των DRM.

Στην συνέχεια ακολουθεί το κεφάλαιο δέκα όπου υπάρχει ένας συνοπτικός οδηγός, σχεδιασμού και ανάπτυξης ενός απλού ePUB ηλεκτρονικού βιβλίου με την βοήθεια της εφαρμογής InDesign.

Τέλος, υπάρχει το παράρτημα Α' όπου γίνεται λεπτομερής ανάλυση της κρυπτογράφησης και των βασικότερων αλγορίθμων της, μέσω την βοήθεια εικόνων και πινάκων.

# ΚΕΦΑΛΑΙΟ 2

## Τα Ηλεκτρονικά Βιβλία

### 2.1 Τί είναι το ηλεκτρονικό βιβλίο

Ηλεκτρονικό ονομάζουμε το βιβλίο το οποίο βρίσκεται σε ηλεκτρονική μορφή και του οποίου το πλήρες κείμενο μπορεί να διαβαστεί με τη βοήθεια ενός ηλεκτρονικού υπολογιστή ή άλλης ειδικής συσκευή ανάγνωσης(e-book readers) ή ακόμα και από μερικά κινητά τηλέφωνα.

Ένα ηλεκτρονικό βιβλίο (η- βιβλίο) μπορεί να παραχθεί εξ αρχής σε ηλεκτρονική μορφή ή να προϋπάρχει σε έντυπη μορφή και να ψηφιοποιηθεί αργότερα.

Ψηφιοποίηση γίνεται κυρίως σε παλιά και σπάνια βιβλία, προκειμένου να διασωθεί το περιεχόμενο τους αλλά και για να δοθεί η δυνατότητα πολλαπλής και ταυτόχρονης εξ αποστάσεως ανάγνωσης τους από πολλούς ενδιαφερόμενους, χωρίς μάλιστα να υπάρχει ο κίνδυνος περαιτέρω φυσικής τους φθοράς.

Μετατροπή ενός έντυπου βιβλίου σε ψηφιακό γίνεται και για άλλους πιο εξειδικευμένους λόγους, όπως π.χ. ια να γίνει δυνατή η μελέτη ενός βιβλίου από άτομα με προβλήματα όρασης, αφού οι χαρακτήρες του βιβλίου στη νέα ηλεκτρονική του μορφή, μπορούν να διαβαστούν μέσω ειδικών μηχανημάτων(e-book readers) ακόμα και από τυφλούς χρήστες.

### 2.2 Ιστορία των ηλεκτρονικών βιβλίων

Μεταξύ των πρώτων ηλεκτρονικών βιβλίων ήταν εκείνα του προγράμματος Gutenberg, το 1971. Μία πρόωρη εφαρμογή του ηλεκτρονικού βιβλίου ήταν το desktop prototype για ένα προτεινόμενο φορητό υπολογιστή, το Dynabook

Τα πρώτα ηλεκτρονικά βιβλία ήταν γενικά γραμμένα για περιορισμένο κοινό. Το περιεχόμενο των εν λόγω ηλεκτρονικών βιβλίων περιείχε τεχνικά εγχειρίδια σχετικά με το hardware, την κατασκευή τεχνικών και άλλων θεμάτων. Στη δεκαετία του 1990,η έξαρση του Διαδικτύου έκανε τη μεταφορά ηλεκτρονικών αρχείων πολύ πιο εύκολο, συμπεριλαμβανομένων των ηλεκτρονικών βιβλίων.

Πολυάριθμα format ηλεκτρονικών βιβλίων προέκυψαν, μερικά υποστηρίχτηκαν από μεγάλες εταιρείες λογισμικού όπως το Adobe με την μορφή PDF, και άλλα που υποστηρίχτηκαν από ανεξάρτητους προγραμματιστές ανοιχτού κώδικα. Πολλοί αναγνώστες ακολούθησαν πολλά format, οι περισσότεροι όμως από αυτούς έδειξαν ενδιαφέρον σε ένα μόνο format, και κατά συνέπεια συντέλεσαν στον κατακερματισμό της αγοράς ηλεκτρονικών βιβλίων ακόμα περισσότερο. Λόγω της αποκλειστικότητας, το περιορισμένο αναγνωστικό κοινό και η έλλειψη συνεννόησης για ένα κοινό format μεταξύ των ανεξάρτητων δημιουργών επέφερε την μείωση στις πωλήσεις των ηλεκτρονικών τους βιβλίων.

Το 2010, τα η-βιβλία συνέχισαν να κερδίζουν μεγάλο μερίδιο στις πωλήσεις βιβλίων. .Πολλοί εκδότες ηλεκτρονικών βιβλίων άρχισαν να μετατρέπουν και διανέμουν τα βιβλία που ήδη βρισκόταν στην παραδοσιακή μορφή. Την ίδια στιγμή, οι συγγραφείς με βιβλία που δεν έγιναν δεκτές από εκδότες, "ανέβασαν" τα βιβλία τους στο ιντερνέτ ώστε να γίνουν γνωστά στο ευρύ κοινό . Ανεπίσημα (και ενίοτε χωρίς άδεια) κατάλογοι των βιβλίων υπήρχαν διαθέσιμοι μέσω του web, καθώς και ιστοσελίδες που είναι αφιερωμένες στο e-βιβλία άρχισαν να διαδίδουν πληροφορίες σχετικά η-βιβλία στο κοινό.

Το 1998 οι ΗΠΑ βιβλιοθήκες άρχισαν να παρέχουν δωρεάν e-books για το κοινό από τις ιστοσελίδες τους, όμως τα η-βιβλία ήταν κυρίως επιστημονικά, τεχνικής ή επαγγελματικής φύσης, και δεν μπορούσαν να τα "κατεβάσουν" στο υπολογιστή τους. Το 2003, οι βιβλιοθήκες άρχισε να προσφέρει δωρεάν υπηρεσίες όπου μπορούσαν να κατεβάσουν η-βιβλία λογοτεχνίας για το κοινό, προωθώντας ένα μοντέλο δανεισμού η-βιβλίο το οποίο είχε πολύ μεγάλη απήχηση πολύ μεγαλύτερη επιτυχία για τις δημόσιες βιβλιοθήκες. Ο αριθμός των βιβλιοθηκών που διάνεμαν e-book συνέχισαν να αυξάνονται κατά τα προσεχή έτη. Το 2010, διαπιστώθηκε ότι 66% των δημοσίων βιβλιοθηκών στις

ΗΠΑ είχαν προσφέρει e-books, επίσης αρκετές βιβλιοθήκες άρχισαν να σκέφτονται και να εξετάζουν σχετικά με το δανεισμό των η-βιβλίων και στην περαιτέρω εξέταση πάνω στα η-βιβλία.

### 2.3 Η παγκόσμια αγορά των ηλεκτρονικών βιβλίων και τα οικονομικά μοντέλα (business models) για τις βιβλιοθήκες

Αν και η παραγωγή ηλεκτρονικών βιβλίων έχει αυξηθεί εμφανώς κατά τη διάρκεια των τελευταίων δύο δεκαετιών, με μια ετήσια αύξηση του 20%, τα ηλεκτρονικά βιβλία αποτελούν μέχρι τώρα μόνο μια μικρή μερίδα της συνολικής αγοράς βιβλίων (Just, 2007). Ο Hook (2007) αναφέρει πως «τα ηλεκτρονικά βιβλία αν και αποτελούν ακόμη ένα μικρό μέρος της συνολικής έκδοσης στην αγορά, οι πωλήσεις τους αυξάνονται, και πολλοί αναμένουν εξελίξεις όσον αφορά τη μορφή τους στο άμεσο μέλλον».

Ακριβείς αριθμοί πωλήσεων των ηλεκτρονικών βιβλίων στην Ευρώπη δεν υπάρχουν λόγω του χαμηλού επιπέδου των πωλήσεών τους (European Commission, 2005). Στις Ηνωμένες Πολιτείες, το International Digital Publishing Forum (πρώην Open E-book Forum) συλλέγει ανά τρίμηνο τα στατιστικά για τις λιανικές πωλήσεις των ηλεκτρονικών βιβλίων σε συνεργασία με την Association of American Publishers (AAP). Σύμφωνα με τα πρώτα στατιστικά στοιχεία που παρήχθησαν το 2002, οι πωλήσεις των ηλεκτρονικών βιβλίων ήταν περίπου 6 εκατομμύρια US Dollars. Το 2006, οι πωλήσεις έφτασαν τα US$20 εκατομμύρια, ενώ το 2007 υπήρξε μια αύξηση του 23.6% φτάνοντας τα US$31.7 εκατομμύρια (IDPF, 2008). Εντούτοις, η μελέτη του 2007 έχει τους περιορισμούς της και παρέχει μόνο μέρος των συνολικών δεδομένων. Στοιχεία έχουν υποβληθεί από περίπου 12 έως 15 αμερικανικούς εμπορικούς εκδότες. Συνεπώς, οι στατιστικές υποτιμούν το πραγματικό μέγεθος των ηλεκτρονικών βιβλίων της αμερικανικής αγοράς. Ωστόσο, οι στατιστικές παρουσιάζουν γενική αύξηση αν και το μέγεθός τους είναι ακόμα χαμηλό, εάν λάβουμε υπόψη ότι τα καθαρά έσοδα όλων των εκδοτών το 2007 έφθασαν τα US$37.26 δισεκατομμύρια (BISG, 2007).

Η αύξηση των πωλήσεων των ηλεκτρονικών βιβλίων εμφανίζεται υψηλότερη στην Ασία. Σύμφωνα με έκθεση αγοράς που δημοσιεύτηκε από την China Book Business Report και την www.du8.com, οι πωλήσεις στην Κίνα έφτασαν τους 660.000 τίτλους το 2007 με μια άνοδο των 24.5% και 14% το 2008 (Xinhua News Agency, 2008). Οι αναγνώστες των ηλεκτρονικών βιβλίων αυξήθηκαν επίσης το 2007, φτάνοντας τα 59 εκατομμύρια, σημειώνοντας άνοδο του 37% (Xinhua News Agency, 2008). Επιπλέον, η ιαπωνική αγορά ηλεκτρονικών βιβλίων αυξήθηκε κατά το διπλάσιο το 2004 φτάνοντας τα US$40.9 εκατομμύρια (Suzuki, 2006), ενώ οι πωλήσεις μυθιστορημάτων σε κινητά τηλέφωνα έφθασαν τα US$82 εκατομμύρια το 2007 (The Economist, 2007). Στη Νότια Κορέα οι πωλήσεις άγγιξαν τα US$59 εκατομμύρια το 2005 και τα US$144εκατομμύρια το 2006 (Asia news, 2007).

Για πολλά έτη, οι βιβλιοθήκες έχουν συνεργαστεί με προμηθευτές των ηλεκτρονικών εκδοτών (Moghaddam και Moballeghi, 2007). Τα οικονομικά μοντέλα (business models) που διατίθενται στο εμπόριο όσον αφορά τα ηλεκτρονικά βιβλία παρουσιάζουν μεγάλη ποικιλία. Η έρευνα της Ebrary το 2007 με τίτλο “ebrary’s global eBook survey” αναφέρει ότι το 80% των ακαδημαϊκών βιβλιοθηκονόμων που συμμετείχαν στην έρευνα υποστηρίζουν πως δεν είναι εξοικειωμένοι με τα οικονομικά μοντέλα της αγοράς όσον αφορά τα ηλεκτρονικά βιβλία. Σύμφωνα με την ίδια μελέτη το 55% προτιμούν το μοντέλο αγοράς (purchase model) ενώ το 59% το μοντέλο συνδρομής (subscription model).

Το μοντέλο αγοράς (purchase model) προσφέρει τη δυνατότητα σε μια βιβλιοθήκη να αγοράσει ένα αντίγραφο άμεσα από έναν εκδότη ή ένα διαθέτη. Σε αυτήν την περίπτωση ο αριθμός προσβάσεων διαπραγματεύεται ετήσια π.χ. η Dawsonera επιτρέπει 400 χρήσεις. Μια τρέχουσα αμοιβή πρόσβασης, απαιτείται συνήθως προκειμένου να διατηρηθεί η πρόσβαση στο περιεχόμενο. Η Taylor & Ο Francis και η NetLibrary παρέχουν επίσης αυτό το μοντέλο. Το δεύτερο μοντέλο που προτιμάται από τις βιβλιοθήκες, είναι το μοντέλο συνδρομής (subscription model). Η πληρωμή μιας ετήσιας συνδρομής στον εκδότη ή το διαθέτη είναι απαραίτητη για την πρόσβαση σε μια συλλογή ή θεματικές ενότητες μιας συλλογής. Η Ebrary και η Taylor & Francis παρέχουν αυτή την επιλογή χορήγησης αδειών. Η τρίτη επιλογή που παρέχεται από κάποιους προμηθευτές είναι το μοντέλο ενοικίασης τίτλων (rental model). Οι τίτλοι αυτοί μπορούν να ενοικιαστούν για ένα περιορισμένο χρόνο ως εναλλακτική λύση των διαδανισμών μεταξύ βιβλιοθηκών.

## 2.4 Χρήστες και χαρακτηριστικά των ηλεκτρονικών βιβλίων

Οι περισσότεροι προμηθευτές παρέχουν χαρακτηριστικά όπως: αναζήτηση κειμένου σε συγκεκριμένο τίτλο βιβλίου ή σε συλλογή βιβλίων, σελιδοδείκτες, επισημάνσεις, και σημειώσεις. Δυνατότητες εκτύπωσης και αντιγραφής κειμένου παρέχονται από κάποιες εταιρίες όπως τη Sage e-reference και την Ebrary. Αξίζει να σημειωθεί ότι διάφοροι περιορισμοί επιβάλλονται όσον αφορά στην αντιγραφή και μεταφορά κειμένου. Η Cambridge University Press επιτρέπει την εκτύπωση 20 σελίδων και την αντιγραφή 5 σελίδων μέσα σε μια περίοδο 30 ημερών. Ωστόσο, κάποιες εταιρίες όπως οι Safari Books Online, EBL, NetLibrary και RSC Publishing επιτρέπουν τη «μεταφόρτωση» (downloading) των ηλεκτρονικών βιβλίων τους σε ηλεκτρονικούς υπολογιστές και αυτόνομες φορητές συσκευές (όπως Dedicated Reading Devices και eBook Readers) για offline εργασία.

Κάποιοι προμηθευτές παρέχουν βιβλιογραφικές αναφορές σε περισσότερα από ένα πρότυπα. Οι χρήστες του MyiLbrary για παράδειγμα μπορούν να εξαγάγουν βιβλιογραφικές αναφορές στο RefWorks αλλά και στο Endnote, ενώ η Wiley Interscience επιτρέπει την εξαγωγή στο Endnote. Η Sage Reference προσφέρει βιβλιογραφικές αναφορές σε τρία πρότυπα: APA, MLA, και Chicago. Εκτός από τις στατικές εικόνες, εργαλεία πολυμέσων μπορούν να ενσωματωθούν σε διάφορες συλλογές. Για παράδειγμα, η Credo Reference (η πρώην xreferplus) έχει ενσωματώσει απεικονίσεις κινουμένων σχεδίων (animation) και βιντεοκλίπ (video clips), διαλογικούς χάρτες και εργαλείο που βοηθά στην προφορά λέξεων. Η EBL έχει ενσωματώσει σε όλους τους τίτλους της μια λειτουργία η οποία διαβάζει μεγαλοφώνως το κείμενο και επίσης προσφέρει υπερσυνδέσεις στη μεταφραστική υπηρεσία Babel Fish. Επιπλέον, κάποιες συλλογές διαθέτουν ενσωματωμένα λεξικά, θησαυρούς, και εγκυκλοπαίδειες.

Πολύ λίγοι προμηθευτές παρέχουν τους τίτλους τους σε πολλαπλές γλώσσες αλλά δυστυχώς όχι στα ελληνικά. Η NetLibrary παρέχει τίτλους στα αγγλικά, κινέζικα, γαλλικά και ισπανικά, ενώ η CredoReference διαθέτει δίγλωσσα λεξικά στα γαλλικά, γερμανικά, ιταλικά, πορτογαλικά, ισπανικά και λατινικά. Διάφοροι προμηθευτές όπως οι παρακάτω: Taylor & Francis, EBL, Springer, Thieme, Wiley Interscience, Questia, Springer, και Elsevier παρέχουν πολλαπλή σύγχρονη πρόσβαση, έτσι ώστε διάφοροι χρήστες να μπορούν να χρησιμοποιήσουν το ίδιο περιεχόμενο ταυτόχρονα.

Τα ηλεκτρονικά βιβλία διατίθενται σε διάφορες μορφές (formats). Κάποιες εταιρίες προσφέρουν το υλικό τους σε περισσότερες από μία μορφές. Για παράδειγμα η Springer παρέχει τους τίτλους της σε PDF και HTML, ενώ η Taylor & Francis σε τέσσερις μορφές: DX Reader, MobiPocket, Microsoft Reader και Adobe eBook. Διάφορα εργαλεία προσφέρονται επίσης από τους περισσότερους προμηθευτές προκειμένου να βοηθήσουν τους πελάτες τους στη χρήση των προϊόντων τους και να τους ενημερώσουν για τις νέες υπηρεσίες. Η Ebrary μέσω της ιστοσελίδας της δίνει πρόσβαση σε διάφορα εκπαιδευτικά videos (training videos) καθώς και σε brochures και οδηγούς χρήσης (guides) σε διάφορες γλώσσες.

## 2.5 Ηλεκτρονικά βιβλία και Ψηφιακά δικαιώματα

Τα ψηφιακά δικαιώματα(DRM) όπως εφαρμόζονται σε ένα eBook είναι ένας κωδικός ο οποίος πρέπει να υπάρχει προκειμένου ο ηλεκτρονικός αναγνώστης να μπορεί να ανοίξει ένα η-βιβλίο. Ο κωδικός μπορεί να είναι αποθηκευμένος στην συσκευή , ή μπορεί να είναι κλειδωμένος σε κάποιο server ώστε να μπορεί να χρησιμοποιηθεί από πολλαπλές συσκευές. Με άλλα λόγια είναι κλειδωμένος για το χρήστη.

Το DRM χρησιμοποιείται για να προστατέψει το συγγραφέα και τον εκδότη ενός βιβλίου από την πειρατεία και άλλες παράνομες δραστηριότητες. Μερικοί αντίπαλοι των DRM, υποστηρίζουν ότι το μέτρο αυτό ξεπερνάει τις παράνομες δραστηριότητες και περιορίζει αντικείμενα τα οποία είναι νόμιμα. Κάποια πρότυπα η-βιβλίων δεν χρησιμοποιούν DRM και ακόμα και αν το πρότυπο το υποστηρίζει κάποια η-βιβλία αυτού του πρότυπου δεν ελέγχονται από το DRM.

Το DRM χρησιμοποιείται συχνά από τις βιβλιοθήκες που δανείζουν η-βιβλία και με αυτό τον τρόπο εξασφαλίζουν ότι το βιβλίο θα μπορεί να ανοιχτεί και να διαβαστεί μόνο από το άτομο που το δανείστηκε ή τουλάχιστον μόνο από τον ηλεκτρονικό αναγνώστη του δανειστή. Η Βιβλιοθήκη ελέγχει τον αριθμό της άδειας που αγοράστηκε το βιβλίο και όταν τελειώσει η χρονική περίοδος ενοικίασης

σταματάει την άδεια όπως ένα κανονικό βιβλίο απλά με στην περίπτωση του η-βιβλίου δεν χρειάζεται να επιστραφεί πίσω. Πρότυπα που υποστηρίζουν αυτή την τεχνική είναι τα PDF, ePUB και MOBI.

### 2.6 Γενικά πλεονέκτημα και μειονεκτήματα των ηλεκτρονικών βιβλίων.

Πολλά από τα πλεονεκτήματα των ηλεκτρονικών βιβλίων έχουν άμεση σχέση με τα χαρακτηριστικά των ηλεκτρονικών συσκευών που χρησιμοποιούνται για την καταγραφή ή τη μεταφόρτωσή τους και αφορούν σε λειτουργίες που δεν διαθέτει το έντυπο βιβλίο, όπως: η δυνατότητα άμεσης διάθεσης του περιεχομένου του ηλεκτρονικού βιβλίου, οι αυξημένες δυνατότητες του υλικού (αναζήτηση ευρείας κλίμακας στο ηλεκτρονικό κείμενο, διαδραστικό λεξικό, δυνατότητες εμφάνισης πολυμέσων κ.λπ.), η δυνατότητα επικαιροποίησης του εκπαιδευτικού υλικού, οι εκπαιδευτικές εφαρμογές, η εύκολη πρόσβαση σε πηγές πληροφόρησης, το φιλικό περιβάλλον διεπαφής (interface), η δυνατότητα βελτίωσης του επιπέδου της εγγραμματοσύνης -αλλά και της εκπαίδευσης γενικότερα- στις λιγότερο ανεπτυγμένες χώρες, καθώς και η βελτίωση του επιπέδου εγγραμματοσύνης σε εθνικό επίπεδο με γνώμονα τα εκπαιδευτικά πρότυπα.

Συγκεκριμένα, στα ιδιαίτερα χαρακτηριστικά του ηλεκτρονικού βιβλίου συμπεριλαμβάνονται τα εξής:

- Δυνατότητα επικαιροποίησης του περιεχομένου.
- Δυνατότητα επικοινωνίας των εμπλεκομένων στην εκπαιδευτική διαδικασία.
- Δυνατότητα αμφίδρομης επικοινωνίας μεταξύ εκπαιδευτικών και γονέων μέσα στο περιβάλλον λειτουργίας του περιεχομένου.
- Δυνατότητα συνεργατικής μάθησης μεταξύ των μαθητών.
- Παράθεση των διδακτικών στόχων στην αρχή του μαθήματος.
- Πρόσβαση σε εξωτερικές πηγές πληροφοριών (κείμενα, ήχους, εικόνες κ.λπ.) μέσω υπερσυνδέσεων (Hyperlinks) και δυνατότητα εκτέλεσης
- σύνθετων εργασιών (project).
- Δυνατότητα αποθήκευσης πολλαπλών πηγών.
- Αρχεία ήχου με σημαντικές παρατηρήσεις για το μάθημα ή επιπλέον ηχητικό υλικό.
- Ενσωμάτωση ολιγόλεπτων βίντεο, κινούμενων εικόνων (animation) καθώς και πολυμεσικού περιεχομένου (multimedia clips).
- Ενσωμάτωση ποικίλων δραστηριοτήτων με τη μορφή μαθησιακών αντικειμένων και δυνατότητα επιλογής των κατάλληλων δραστηριοτήτων από τον δάσκαλο ανάλογα με το μαθησιακό επίπεδο
- του μαθητή (εξατομικευμένη διδασκαλία).
- Δυνατότητα χρήσης μηχανής αναζήτησης με λέξεις-κλειδιά σε κείμενα, στοιχείο που διευκολύνει την πραγματοποίηση σύνθετων εργασιών.
- Εμφάνιση/απόκρυψη μέρους της πληροφορίας προκειμένου να εστιαστεί η προσοχή σε συγκεκριμένα σημεία.
- Δυνατότητα υπερφόρτισης (highlighter) και υπογράμμισης (underliner).
- Δυνατότητα καταγραφής σημειώσεων πάνω στην οθόνη καθώς και δυνατότητα αναίρεσής τους.
- Ειδικά διαμορφωμένο περιβάλλον διεπαφής, το οποίο βασίζεται στην πρόσφατη ερευνητική εμπειρία.
- Δυνατότητα εμφάνισης βοήθειας για κάθε κουμπί της επιφάνειας διεπαφής.
- Δυνατότητα εκφώνησης των κειμένων.
- Δυνατότητα μεγέθυνσης χαρακτήρων και εικόνων, απομόνωσης μέρους ενός κειμένου και αποστολής του σε κειμενογράφο για περαιτέρω επεξεργασία ή σχολιασμό.
- Μεταφορά σημειώσεων από υπολογιστή σε υπολογιστή αλλά και από το ένα λειτουργικό σύστημα στο άλλο.
- Εισαγωγή κειμένου text με συμβατικό τρόπο (πληκτρολόγιο) ή με τη χρήση εικονικού πληκτρολογίου.
- Δυνατότητες εκτύπωσης.
- Διαλειτουργικότητα (λειτουργία σε διάφορα λειτουργικά συστήματα).

- Δυνατότητα DC \u955 λειτουργίας και σε συμβατικούς υπολογιστές.

Στα μειονεκτήματα του ηλεκτρονικού βιβλίου συγκαταλέγονται προβλήματα ως προς:

- Τις ταχύτατες τεχνολογικές αλλαγές που καθιστούν έναν Η/Υ μη λειτουργικό μέσα σε μια πενταετία.
- Την αντοχή της συσκευής στον χρόνο (και στην κακή μεταχείριση)
- Την επιβάρυνση του περιβάλλοντος από τα ηλεκτρονικά απόβλητα που προκύπτουν μετά από μια πενταετία χρήσης.
- Το κόστος αγοράς και συντήρησης ενός ηλεκτρονικού υπολογιστή.
- Τις αυξημένες ανάγκες συντήρησης των συσκευών και τις ανάγκες σε ειδικευμένο προσωπικό.
- Την εξάρτηση των Η/Υ από την ηλεκτρική παροχή σε περίπτωση που ο ενσωματωμένος συσσωρευτής ρεύματος του φορητού Η/Υ εξασθενίσει.
- Την τεχνοφοβία, η οποία μπορεί να αποτελέσει ανασταλτικό παράγοντα στην ενσωμάτωση του μοντέλου στη σχολική τάξη.

# ΚΕΦΑΛΑΙΟ 3

## Τα Πρότυπα ηλεκτρονικών βιβλίων

Αν και η-βιλία δεν θα αντικαταστήσουν πλήρως τα παραδοσιακά βιβλία, υπάρχουν σημαντικές προβλέψεις για την επιτυχία τους. Ωστόσο, παρά τα πλεονεκτήματα και την αποδοχή του η τεχνολογική τους ανάπτυξη είναι αργή λόγω πολλών εμποδίων. Το σημαντικότερο πρόβλημα είναι η έλλειψη ενός μοναδιαίου πρότυπου για την δημιουργία των η-βιβλίων. Με το να μην υπάρχει κάποιο στάνταρ format και με την κάθε μεγάλη εταιρία να χρησιμοποιεί το δικό της κάποιες συσκευές ανάγνωσης για η-βιβλία μπορεί να μην είναι σε θέση να διαβάσουν βιβλία που έχουν δημιουργηθεί στα πρότυπα άλλων συσκευών. Συνεπώς, υπάρχει το ενδεχόμενο να οι αναγνώστες πολλές φορές να μην μπορούν να βρουν κάποιο βιβλίο που τους ενδιαφέρει στην μορφή προτύπου ο ηλεκτρονικός αναγνώστης τους μπορεί να διαβάσει.

### 3.1 HTML

Τα αρχικά **HTML** προέρχονται από τις λέξεις **Hypertext Markup Language**. Η html δεν είναι μια γλώσσα προγραμματισμού. Είναι μια γλώσσα σήμανσης (*markup language*), δηλαδή ένας ειδικός τρόπος γραφής κειμένου. Ο καθένας μπορεί να δημιουργήσει ένα αρχείο HTML χρησιμοποιώντας απλώς έναν επεξεργαστή κειμένου. Αποτελεί υποσύνολο της γλώσσας SGML (Standard Generalized Markup Language) που επινοήθηκε από την IBM προκειμένου να λυθεί το πρόβλημα της μη τυποποιημένης εμφάνισης κειμένων στα διάφορα υπολογιστικά συστήματα. Ο browser αναγνωρίζει αυτόν τον τρόπο γραφής και εκτελεί τις εντολές που περιέχονται σε αυτόν. Αξίζει να σημειωθεί ότι η html είναι η πρώτη και πιο διαδεδομένη γλώσσα περιγραφής της δομής μιας ιστοσελίδας. Η html χρησιμοποιεί τις ειδικές ετικέτες (τα tags) να δώσει τις απαραίτητες οδηγίες στον browser. Τα tags είναι εντολές που συνήθως ορίζουν την αρχή ή το τέλος μιας λειτουργίας.

Τα η-βιβλία που χρησιμοποιούν HTML μπορούν να διαβαστούν από έναν οποιοδήποτε web browser. Όμως η HTML από μόνη της δεν είναι και το πιο αποτελεσματικό πρότυπο για την δημιουργία κάποιου η-βιβλίου. Ο αποθηκευτικός χώρος που χρειάζεται είναι πολύ περισσότερος από τα υπόλοιπα πρότυπα. Παρόλα αυτά, διάφορα e-books όπως το Amazon Kindle, Open eBook, Compressed HM, MobiPocket και ePub χρησιμοποιούν HTML για να αποθηκεύουν τις ενότητες των βιβλίων και στην συνέχεια χρησιμοποιώντας το πρότυπο συμπίεσης ZIP για να συμπιέσουν το HTML αρχείο μαζί με τις εικόνες τα μετά-δεδομένα και τις προτιμήσεις των Style sheets μέσα σε ένα αρκετά μικρότερο αρχείο.

### 3.2 Kindle (AZW)

Το AZW, πιθανότατα αντιπροσωπεύει τις λέξεις "Amazon Whispernet", είναι ένα πρότυπο που χρησιμοποιείται αποκλειστικά από το ηλεκτρονικό αναγνώστη Amazon Kindle και μερικά προγράμματα για Υ/Π ή iPhones της εταιρία Amazon. Το AZW είναι βασισμένο πάνω στο MOBI πρότυπο χρησιμοποιώντας την μέγιστη συμπίεση που μπορεί να επιτευχτεί.

Η Amazon υποστηρίζει αρκετά το πρότυπο της έτσι έχει δημιουργήσει μία online βιβλιοθήκη όπου κάποιος μπορεί να έχει πρόσβαση σε αυτήν μέσω της ιστοσελίδα της. Επίσης, μπορεί να κάποιος να την επισπευτεί μέσω του Kindle reader του ή του iPhone.

Επίσης, η Amazon προσφέρει την υπηρεσία σε άτομα που έχουν κάποιο έγγραφο ή βιβλίο σε κάποια άλλη μορφή του εκτός .azw, να στείλουν τα έγγραφα αυτά στην Amazon και αυτή θα αναλάβει να τα μετατρέψει σε .azw μορφή ώστε οι Kindle αναγνώστες τους να μπορούν να τα διαβάσουν.

#### *3.2.1 AZW και Ψηφιακά δικαιώματα (DRM)*

Το DRM στο AZW είναι κλειδωμένο στο σειριακό κωδικό της Kindle συσκευή η οποία έχει ήδη δηλωθεί στην Amazon όταν αγοράστηκε. Οπότε. όταν κάποιος αγοράζει ένα .azw η-βιβλίο από

την Amazon μόνο από τον ηλεκτρονικό αναγνώστη που αγοράστηκε μπορεί να ανοιχτεί και να διαβαστεί. Επιπλέον, υπάρχει και η επιλογή κάποιος να έχει δηλώσει πάνω από έναν ηλεκτρονικούς αναγνώστες στο λογαριασμό του στην Amazon. Το όριο είναι μέχρι έξι e-readers, έτσι μία οικογένεια μπορεί να μοιραστεί ένα αγορασμένο βιβλίο.

### 3.3 Fiction Book

Το FictionBook δημοσιεύεται σαν .fb2 είναι βασισμένο στα πρότυπα XML από W3C, και τα έγγραφα FictionBook είναι καλοσχηματισμένα έγγραφα XML, που προσαρμόζονται στα πρότυπα που έχει ορίσει το FictionBook.

Η συνολική δομή είναι απλή και μοιάζει με αυτή της HTML. Όμως, ο βασικός στόχος είναι να δημιουργηθεί ένα XML κείμενο το οποίο θα επικεντρώνεται στην λογική δομή του κειμένου και όχι τόσο στα εμφανισιακά χαρακτηριστικά του. Ένα ουσιώδες χαρακτηριστικό του πρότυπου είναι ότι διακρίνει ρητά τη δομή και το περιεχόμενο του κειμένου.

#### *3.3.1 Περιγραφή του προτύπου FictionBook*

Το κυρίως μέρος του FictionBook αρχείου είναι το "**σώμα**"(body) το οποίο περιέχει το κείμενο του "πραγματικού" βιβλίου. Υπό ενότητες του body μπορούν να χρησιμοποιηθούν για να αποθηκευτούν υποσημειώσεις, σχόλια και αλλά αντικείμενα τα οποία δεν ανήκουν στην πραγματική ροή του κειμένου. Το body χωρίζεται σε δύο τμήματα. Το ένα περιέχει άλλα υποτιμήματα και το άλλο τους παραγράφους των κειμένων. Κάθε τμήμα μπορεί να έχει μία προαιρετική επικεφαλίδα για τα εξής: τίτλο, επιγραφή, εικόνα και σχόλια. Μετά από αυτά πρέπει οπωσδήποτε να υπάρχει τουλάχιστον ένα αντικείμενο(element) για το κείμενο.

Τα αντικείμενα που καθορίζουν την εμφάνιση του βιβλίου βρίσκονται μέσα σε tags τα οποία ανάλογα με το χαρακτηριστικό τους καθορίζουν και το MIME τύπο του stylesheet.

### 3.4 Plain Text

Το Plain Text πρότυπο είναι το γνωστό .txt μου χρησιμοποιείται για την δημιουργία κειμένων. Δεν χρησιμοποιείται καμία συμπίεση και το άνοιγμα του γίνεται από έναν οποιοδήποτε αναγνώστη κειμένου.

### 3.5 PalmDOC

ΕΙΚΟΝΑ 1:ΛΟΓΟΤΗΠΟ ΤΟΥ PALMDOC

Το 1996, Rick Bram ανέπτυξε μία μέθοδο ώστε να συμπιέζει .txt αρχεία για το Palm λειτουργικό. Ονόμασε το πρότυπο αυτό "Palm Doc". Το 1997, η εταιρία Aportis Technologies Corporation αγόρασε τα δικαιώματα του PalmDOC και το μετονόμασε σε AportisDoc. Μέχρι το Δεκέμβριο του 2002, όπου η Aportis έπαψε να λειτουργεί. Από τότε το πρότυπο είναι γνωστό ως PalmDOC. Τα PalmDOC αρχεία έχουν την κατάληξη .pdb αλλά μπορεί και να τα βρείτε και ως .prc.

### *3.5.1 Συμπίεση PalmDOC*

Το PalmDOC χρησιμοποιεί LZ77 συμπίεση και τα αρχεία DOC μπορούν να περιέχουν μονό συμπιεσμένο κείμενο. Το πρότυπο δεν επιτρέπει καθόλου μορφή κειμένου. Με αυτό τον τρόπο κρατάει το μέγεθος των κειμένων μικρό, σύμφωνα με την φιλοσοφία της Palm. Παρόλα αυτά μπορεί να χρησιμοποιηθούν ετικέτες HTML ή PML για να προσθέσουν τμήματα κειμένου.

Ο LZ77 αλγόριθμος επιτυγχάνει συμπίεση με την αντικατάσταση τμημάτων πληροφορίας με αναφορές που αντιστοιχούν σε κομμάτια πληροφορίας τα οποία έχουν ήδη υποστεί κωδικοποίηση και αποκωδικοποίηση. Ένα ζεύγος αναφοράς και πληροφορίας είναι κωδικοποιημένο από ένα ζευγάρι αριθμούς που ονομάζεται "ζευγάρι length-distance".

Το PalmDOC υποστηρίζει bookmarks. Αυτοί οι δείκτης αναφέρονται σε μία θέση μέσα στο αρχείο. Αν το αρχείο επεξεργαστεί αυτοί οι σελιδοδείκτες ίσως να μην δείχνουν πια στην σωστή θέση. Μερικά προγράμματα επιτρέπουν στο χρήστη να επεξεργαστεί τους σελιδοδείκτες ενώ αλλά τα αναγνωρίζουν σαν πίνακα περιεχομένων. Άλλα τα αγνοούν τελείως. Οι σελιδοδείκτες είναι αποθηκευμένοι στο τέλος του αρχείου έτσι όλο το αρχείο χρειάζεται να αναζητηθεί για να βρεθούν.

## 3.6 ANSI/NISO (DAISY)

Το Digital Accessible Information System ή αλλιώς DAISY Talking Book (DTB) είναι ένα μέσω για την δημιουργία ψηφιακών ομιλούμενων βιβλίων για άτομα που επιθυμούν να ακούνε το γραμμένο περιεχόμενο των βιβλίων σε ακουστική μορφή. Πολλοί από τους ακροατές αυτών των βιβλίων έχουν προβλήματα ανάγνωσης λόγω τύφλωσης, μειωμένης όρασης δυσλεξίας ή άλλων προβλημάτων.

Το DAISY βοηθάει άτομα που, για διαφορετικούς λόγους, έχουν πρόβλημα να χρησιμοποιήσουν κανονικό εικονογραφημένο υλικό. Τα DAISY βιβλία έχουν τα ίδια πλεονεκτήματα με τα απλά audiobooks, αλλά υπερτερούν έναντι αυτών επειδή στα DAISY έχουν ενσωματωθεί επίπεδα πλοήγησης ώστε να γίνεται πιο αντιληπτό το περιεχόμενο από τον ακροατή (π.χ. εικόνες, γραφήματα κ.α.). Σαν αποτέλεσμα τα DAISY βιβλία επιτρέπουν σε τυφλούς να μπορούν να εξερευνήσουν μία εγκυκλοπαίδεια το οποίο με άλλα διαφορετικά ακουστικά μέσα είναι αδύνατο αφού χρησιμοποιούν γραμμική ηχογράφηση. Επίσης, διαβάζοντας κάποιος ένα DAISY book μπορεί να μεταφερθεί στην προηγούμενη ή επόμενη σελίδα ή πρόταση του κειμένου.

Το DAISY 2.0 συστάθηκε το 1998 και αναθεωρήθηκε τελευταία φορά το 2001 με την έκδοση DAISY 2.02 και δημιουργήθηκε πάνω στα πρότυπα του World Wide Web(W3C). Το DAISY 2.02 χρησιμοποιεί HTML, XHTML και SMIL για την δημιουργία του. Αυτή την στιγμή έχει κυκλοφορήσει το DAISY 3 το οποίο είναι βασισμένο πάνω στο πρότυπο XML και είναι αναγνωρισμένο σαν ANSI/NISO Z39.86-2005.

Υπάρχουν τρείς τύποι DAISY DTBs, όλοι προσφέρουν βελτιωμένη πρόσβαση στο περιεχόμενο των βιβλίων. Οι τρείς τύποι είναι:

- **Ήχος με NCX**:DTB με δομή. Το NCX είναι ένα σύστημα πλοήγησης του βιβλίου, ένα αρχείο περιέχει όλα τα σημεία του βιβλίου που μπορεί ο χρήστης να επισπευτεί. Το XML αρχείο, αν υπάρχει , περιέχει μία δομή του βιβλίου και μπορεί να περιέχει και συνδέσμους σε διάφορα χαρακτηριστικά όπως υποσημειώσεις κ.α. Μερικά DAISY βιβλία αυτού του τύπου μπορεί να περιέχουν στοιχεία κειμένου όπως περιεχόμενα ή λεξιλόγια ή ακόμα και αναζήτηση λέξεων.
- **Ήχος και κείμενο**:DTB δομή και ολοκληρωμένο ήχο και κείμενο. Αυτός ο τύπος είναι ο πιο ολοκληρωμένος και προφέρει την περισσότερη, multimedia εμπειρία διαβάσματος. Το XML περιέχει τη δομή και ολόκληρο το κείμενο του βιβλίου. Ο ήχος είναι συγχρονισμένος μαζί με το κείμενο.
- **Κείμενο χωρίς ήχο**: Το XML για το κείμενο περιέχει μία δομή για ολόκληρο το κείμενο του κειμένου. Δεν υπάρχουν αρχεία ήχου.

### *3.6.1 Σχέση DAISY Book και ePub*

Ένα ePub αρχείο μπορεί να μετατραπεί και να ακολουθήσει τα στάνταρ ενός DAISY Book αν το ePub είναι:

1. Καλά αναπτυγμένο σε XML αρχείο και
2. Πρέπει να είναι κωδικοποιημένο σε UTF-8 ή UTF-16 και
3. Πρέπει να είναι έγκυρο XML έγγραφο, σύμφωνα με το DTB DTD και
4. Πρέπει να περιέχει ένα MIME τύπο της εφαρμογής " application/x-dtbook+xml".

### 3.7 DJVU


ΕΙΚΟΝΑ 2: ΛΟΓΟΤΗΠΟ ΤΟΥ DJVU

Το DjVu αρχικά σχεδιάστηκε για να αποθηκεύει σαρωμένα αρχεία, ειδικά εκείνα που περιείχαν ένα συνδυασμό κειμένου και φωτογραφίες. Χρησιμοποιεί τεχνολογίες όπως:

- Χώρισμα της εικόνας από το κείμενο και το φόντο.
- Προοδευτική Φόρτωση
- Αριθμητική Κωδικοποίηση
- Συμπίεση με απώλειες για μονόχρωμες φωτογραφίες. Αυτό επιτρέπει μεγάλες σε ανάλυση φωτογραφίες να αποθηκευτούν στο μικρότερο δυνατό χώρο ώστε να μπορούν να δημοσιοποιηθούν στο ιντερνέτ.

Το DjVu είχε προταθεί ως εναλλακτικό του PDF, υπόσχεται μικρότερα αρχεία από ότι το PDF για τα περισσότερα σαρωμένα κείμενα.

DjVu διαιρεί μία εικόνα σε μικρότερες, έπειτα τις συμπιέζει καθεμία ξεχωριστά. Όταν δημιουργείται έναν DjVu αρχείο, η αρχική εικόνα του σαρωμένου αρχείου διαιρείται σε τρείς διαφορετικές εικόνες: "background" εικόνα, "foreground" εικόνα και μία mask εικόνα. Οι "background" και "foreground" εικόνες είναι μικρότερης ανάλυσης(π.χ. 100dpi) ενώ η "mask" είναι υψηλής ανάλυσης εικόνα(π.χ. 300dpi) και τυπικά είναι η εικόνα όπου το κείμενο αποθηκεύεται. Οι "background" και "foreground" εικόνες έπειτα συμπιέζονται χρησιμοποιώντας "wavelet" συμπίεσης αλγόριθμο γνωστό ως IW44. Η εικόνα "mask" είναι συμπιεσμένη χρησιμοποιώντας την μέθοδο JB2.

### 3.8 Microsoft Compiled HTML Help

Το Microsoft compiled HTML help είναι ένα ιδιόκτητο πρότυπο για τα online help αρχεία, αναπτύχθηκε από την Microsoft και πρωτοεμφανίστηκε το 1997 σαν ένας διάδοχος του Microsoft WinHelp πρότυπου. Πρώτη φορά παρουσιάστηκε με την κυκλοφορία του Windows 98 και συνεχίζει ακόμα να υποστηρίζεται και να διανέμεται μέσω των Windows XP, Vista και windows 7 λειτουργικών.

Το .CHM αποτελείται από ένα σετ ιστοσελίδων γραμμένες σε ένα υποσύνολο της HTML και έναν πίνακα περιεχομένων. Το .CHM προσφέρετε προς ανάγνωση αφού τα αρχεία του είναι αρκετά ταξινομημένα. Όλα τα αρχεία είναι συμπιεσμένα με LZX συμπίεση.

### 3.9 Microsoft .LIT

Το πρότυπο Microsoft .LIT είναι βασικά μια τροποποίηση του πρότυπου HTML Help CHM(.chm) χρησιμοποιώντας σχεδόν όλα τα χαρακτηριστικά του όπως την συμπίεση LZX, δυαδική αναπαράσταση των περιεχομένων και προαιρετικά δεδομένα σχετικά με το κάθε περιεχόμενο του η-βιβλίου. Το κείμενο του βιβλίου είναι ένας αυθαίρετος αριθμός από OEBPS 1.0 ακολουθίες σημάνσεις και μερικά υποσύνολα από OEBPS 1.0 CSS.

### 3.10 BBeB

Το BBeB(Broad Band eBook) είναι ένα ιδιόκτητο πρότυπο ανεπτυγμένο από τις εταιρίες Sony και Canon.Το BBeB μπορεί να έχει τις ακόλουθες καταλήξεις: LRS και LRF ή LRX.

Τα LRS είναι XML αρχεία τα οποία μπορεί να επεξεργαστούν και να ακολουθήσουν τα BBeB Xylog XML προδιαγραφές. Αυτά αντιπροσωπεύουν το πηγαίο κώδικα του κάθε BBeB eBook. Τα LRF (αποκρυπτογραφημένα αρχεία) και τα LRX (κρυπτογραφημένα για DRM λόγους) αρχεία συμπιεσμένα LRS αρχεία. Καθώς τα LRS αρχεία είναι ανοιχτά προς το κοινό, τα LRF και LRX δεν είναι και παραμένουν ιδιόκτητα. Η μετατροπή από LRS σε LRF μπορεί να γίνει χρησιμοποιώντας συγκεκριμένο εργαλείο.

### 3.11 TomeRaider .TR

ΕΙΚΟΝΑ 3: ΛΟΓΟΤΗΠΟ ΤΟΥ TOMERAIDER

Το πρότυπο TR χρησιμοποιείται από τον ηλεκτρονικό αναγνώστη Tome Raider. Το πρότυπο χρησιμοποιεί υψηλή συμπίεση και την πιο κατάλληλη για μεγάλα κείμενα. Τα περισσότερα αρχεία είναι κρυπτογραφημένα και χρειάζονται ένα DRM κλειδί για να ανοιχτούν. Το TR δημιουργήθηκε από την αγγλική εταιρία yadabyte ( http://www.yadabyte.com). Η πρώτη έκδοση του αναπτύχθηκε το 1999 και τώρα ήδη βρίσκεται στην TR3 έκδοση του. Η τελευταία του έκδοση TR3 περιλαμβάνει υποστηρίξει για κατηγορίες εικόνων, αναζήτησης και συμπίεσης. Το TomeRaider πρότυπο επιτυγχάνει συμπιέσεις 45%-60% του αρχικού μεγέθους. Επιπλέον, σε σύγκριση με άλλα πρότυπα το TR επιτυγχάνει πολύ γρήγορες αναζητήσεις, κατηγοριοποιήσεις και συμπιέσεις.

Το πρότυπο χρησιμοποιεί HTML για την δημιουργία του αλλά μερικά από τα html "tags" έχουν οριστεί με τέτοιο τρόπο για την αποκλειστική χρήση αυτού του πρότυπου. Κάποια από αυτά είναι τα εξής:

1. <new> δηλώνει την νέα ενότητα ενός βιβλίου.
2. <CATDEF> ... </CATDEF> δηλώνει το όνομα μίας κατηγορίας
3. <META> ... </META> δηλώνει όλα τα μετά-δεδομένα που χρησιμοποιήθηκαν
4. <EXPMSG> είναι ένα tag το οποίο εμφανίζει ένα μήνυμα όταν το αρχείο έχει τελειώσει.
5. <DIEMSG> αυτό το tag κάνει ακριβώς την ίδια δουλεία με το EXPMSG.
6. <ENGMSG> δημιουργεί ένα μήνυμα το οποίο εμφανίζεται για κρυπτογραφημένες σελίδες. Αν ο χρήστης προσπαθήσει να διαβάσει κρυπτογραφημένες σελίδες χωρίς το έγγραφο να είναι ξεκλειδωμένο θα εμφανιστεί αυτό το μήνυμα.
7. <catset>. </catset> παραθέτει ονόματα κατηγοριών σε κάθε αντικείμενο.

### 3.12 MobiPocket

ΕΙΚΟΝΑ 4: ΛΟΓΟΤΗΠΟ ΤΟΥ MOBIPOCKET

Το Mobi είναι ένα πρότυπο το οποίο χρησιμοποιείται από MobiPocket ηλεκτρονικούς αναγνώστες. Μπορεί να έχει την κατάληξη .mobi ή .prc. Η .prc κατάληξη χρησιμοποιείται για τις

συσκευές PalmOS αφού αναγνωρίζουν μόνο .prc ή .pdb αρχεία. Τα mobi αρχεία μπορεί να είναι DRM προστατευμένα ή όχι.

### 3.12.1 Περιγραφή πρότυπου

Το πρότυπο mobi αρχικά ήτανε μια επέκταση του PalmDOC, χρησιμοποιώντας παραπάνω ορισμένες HTML ετικέτες. Πολλά από τα MOBI αρχεία χρησιμοποιούν ακόμα αυτό τον τρόπο δημιουργίας. Όμως, υπάρχει επίσης και μία υψηλής συμπίεσης μορφή που συμπιέζει τα δεδομένα σε μεγαλύτερο βαθμό για ιδιόκτητους λόγους. Υπάρχουν μερικοί ηλεκτρονικοί αναγνώστες που μπορούν να διαβάσουν MOBI βιβλία στην κανονική τους μορφή, αλλά υπάρχουν ελάχιστα τα οποία μπορούν να διαβάσουν η-βιβλια με την υψηλότερη συμπίεση.

Το MobiPocket πρότυπο είναι βασισμένο στα στάνταρ του Open eBook χρησιμοποιώντας XHTML και μπορεί να συμπεριλάβει και JavaScript και frames. Μπορεί επίσης να χρησιμοποιήσει SQL queries για να χρησιμοποιηθούν με ενσωματωμένες database.

### *3.12.2 Γιατί είναι το πρότυπο MobiPocket προσαρμοσμένο για τα eBooks*

Τα MobiPocket η-βιβλία είναι σχεδιασμένα να διαβάζονται από πολλούς ηλεκτρονικούς αναγνώστες και όχι μόνο από Desktop PCs. Το πρότυπο αυτό προοριζόταν να λύσει αρκετά προβλήματα που είχαν δημιουργηθεί όταν κάποιος προσπαθούσε να προβάλει κάποιο περιεχόμενο σε συσκευές με διαφορετικά χαρακτηριστικά. Ειδικότερα, το πρότυπο λύνει τα εξής ζητήματα:

- Το περιεχόμενο διαμορφώνεται ανάλογα το μέγεθος της εικόνας.
- Ο χρήστης διαλέγει την γραμματοσειρά, το μέγεθος της, την απόσταση μεταξύ των γραμμών κ.α. ώστε να κάνει το διάβασμα ευκολότερο.
- Οι εικόνες προσαρμόζονται ανάλογα με την ανάλυση της εικόνας.
- Το MobiPocket μπορεί να διαβαστεί από οποιοδήποτε η-αναγνώστη.
- Το MobiPocket συμμορφώνεται με τα στάνταρντ όπως IDPF και XHTML.

### *3.12.3 MOBI DRM*

Το DRM, στο πρότυπο MOBI, όταν αγοράζεται ένα η-βιβλίο αποθηκεύεται στο αρχείο μέσα και είναι κλειδωμένο στην συσκευή από όπου αγοράστηκε. Επιτρέπεται κάποιος χρήστης να έχει μέχρι και τέσσερις συσκευές στην άδεια του. Σε αυτή τη περίπτωση ο server χρειάζεται να ξέρει όλων των συσκευών τους σειριακούς αριθμούς. Αν κάποιος προσθέσει μία νέα συσκευή πρέπει να πει το server όπου έχει προσθέσει τις ήδη υπάρχοντες συσκευές του και έπειτα να ξανακατεβάσει το βιβλίο.

Ένας δεύτερος, ευκολότερος τρόπος, μόνο χρειάζεται να ξέρει κάποιος τα στοιχεία του λογαριασμού του (login name και password) που χρησιμοποίησε για να αγοράσει το η-βιβλίο. Όταν θα θελήσει να ξανά αγοράσει κάποιο βιβλίο χρειάζεται να κάνει είναι να ξανά δώσει τα στοιχεία του λογαριασμού του αφού αυτά απαιτούνται μόνο μία φορά. Μερικοί ηλεκτρονικοί αναγνώστες δεν υποστηρίζουν αυτόν το τρόπο.

Ένας τρίτος τρόπος είναι η χρήση ενός γενικού MOBI κλειδιού. Αυτό σημαίνει ότι το MOBI η-βιβλίο μπορεί να διαβαστεί από όλους MobiPocket Readers αλλά από καμία συσκευή που δεν είναι της εταιρίας MobiPocket.

## 3.13 Portable Document Format (PDF)


ΕΙΚΟΝΑ 54: ΛΟΓΟΤΗΠΟ ΤΟΥ ADOBE PDF

Το PDF δημιουργήθηκε το 1993 από την Adobe για την ανταλλαγή των κειμένων. Αρχικά το PDF σχεδιάστηκε σαν ένα πρότυπο εκτύπωσης παρόμοιο με το PostScript και μέχρι και τώρα χρησιμοποιείται για την ανταλλαγή πληροφοριών όπου πρόκειται να εκτυπωθούν.

Το περιεχόμενο ενός PDF αρχείου μπορεί να περιέχει διάφορους τύπους από πληροφορίες. Σε αυτές περιλαμβάνονται κείμενο, γραφικά και μετά-δεδομένα. Υπάρχουν PDF αρχεία που δεν περιέχουν όλα αυτούς τους τύπους δεδομένων και μερικά είναι διαφορετικά από ότι φαίνονται. Για παράδειγμα ένα PDF αρχείο μπορεί να μοιάζει ότι έχει ένα κείμενο αλλά τελικά απλά να απεικονίζει μία εικόνα η οποία περιέχει κείμενο

Ένα PDF μπορεί να περιέχει ένα πίνακα αλλά συνήθως δεν υπάρχει λογική στην κατασκευή ενός πίνακα. Είναι φτιαγμένο από κάποιο κείμενο στοιχισμένο σε κάποια στοιχεία και με μερικές γραμμές. Μοιάζει σαν πίνακας στον χρήστη αλλά δεν μπορεί να αφαιρεθεί σαν πίνακας. Επίσης, ένας πίνακας μπορεί να παρουσιαστεί και μέσα σε μία εικόνα.

Ένα PDF περιέχει τις σελίδες που πρόκειται να παρουσιαστούν η να εκτυπωθούν. Το μέγεθος των σελίδων αναγνωρίζεται όταν δημιουργούνται αν και μπορεί να αλλάξει από σελίδα σε σελίδα. Επίσης, υπάρχει και η δυνατότητα μεγέθυνσης η σμίκρυνσης.

Το κείμενο σε ένα PDF είναι αναφερόμενο σε συγκεκριμένη γραμματοσειρά και στο μέγεθος της. Οι γραμματοσειρές βρίσκονται ή αποθηκευμένες μαζί με το αρχείο αλλιώς χρησιμοποιούνται οι εξωτερικές γραμματοσειρές οι οποίες πρέπει να υπάρχουν για να γίνει σωστά η παρουσίαση.

Οι εικόνες μπορεί να είναι είτε σε μορφή "raster" ή "vector" . Οι raster εικόνες είναι συχνά σαρωμένες εικόνες. η ανάλυση της εικόνας προσδιορίζεται όταν το αρχείο δημιουργείται αλλά μπορεί να είναι μεγαλύτερη από ότι απαιτείται ώστε να δίνει ένα σωστό αποτέλεσμα κατά την μεγέθυνση. Οι vector εικόνες δημιουργούνται με γραμμές και μαθηματικές καμπύλες. Αυτός ο τύπος εικόνας μπορεί να μεγεθυνθεί χωρίς να υπάρξουν απώλειες στην ποιότητα της.

Το κείμενο μπορεί να έχει ή όχι ετικέτες (tags) σε ένα PDF αρχείο. Οι ετικέτες είναι Μέτα-δεδομένα τα οποία προσδίδουν "νοημοσύνη" σχετικά με το κείμενο. Οι ετικέτες βασικά επιτρέπον στο πρόγραμμα ανάγνωσης του PDF να μετακινήσει ή να αλλάξει το μέγεθος της πληροφορίας με έναν έξυπνο τρόπο όπου το περιεχόμενο δεν θα χαθεί. Οι ετικέτες κανονικά τοποθετούνται στην βάση δεδομένων όταν το αρχείο μετατρέπετε σε PDF αλλά υπάρχουν τρόποι να τους προσθέσεις και μετά.

### *3.13.1 PDF's Reflow*

Το να μπορούμε να αναδιατάξουμε το κείμενο ονομάζεται Reflow και επιτρέπει ένα pdf σχεδιασμένο για full size χαρτί να μπορεί εύκολα να διαβαστεί από μικρότερες συσκευές όπως PDA ή eBook Reader. Οι ετικέτες χρησιμοποιούνται για να διευκολύνουν στο Reflow.

Το ότι υπάρχουν ετικέτες δεν σημαίνει ότι το πρόγραμμα παρουσίασης είναι ικανό να τις χρησιμοποιήσει. Στην πραγματικότητα οι περισσότεροι readers οι οποίοι δεν ανήκουν στην Adobe δεν μπορούν να αναδιατάξουν το κείμενο. Όμως, υπάρχουν και προγράμματα που επιτρέπουν ακόμα και αν τα κείμενα δεν έχουν ετικέτες. Η adobe έχει ανάπτυξη μία εφαρμογή την Adobe Digital Editions (ADE) το οποίο μπορεί να κάνει αναδιάταξη του σε pdf αρχεία. Οι περισσότερα ηλεκτρονικοί αναγνώστες που κυκλοφορούν τελευταία υποστηρίζουν την έκδοση ADE. Η

αναδιάταξη συσχετίζεται με την σμίκρυνση υπό την έννοια ότι το μέγεθος του κειμένου αλλάζει στο κανονικό μέγεθος ακόμα και αν η σελίδα είναι μικρότερη. Μία καλή χρήση του Reflow είναι ότι μπορούμε να προβάλουμε ένα κείμενο πολλών σελίδων σε μία μόνο στήλη το οποίο βοηθάει να διαβαστεί σε ηλεκτρονικούς αναγνώστες όπου δεν μπορούν να εμφανίσουν μία ολόκληρη σελίδα στην οθόνη τους.

Με την ανάπτυξη του ADE, όπου δεν χρειάζεται η χρήση ετικετών, υπάρχουν τρία επίπεδα Reflow

- Reflow γραμμής: Το μικρότερο επίπεδο, μπορεί να "πιέσει" τις γραμμές του κειμένου σε μικρότερη οθόνη όμως κάθε γραμμή είναι ανεξάρτητη και συμπεριφέρεται σαν μία διαφορετική παράγραφο. Επιτρέπει το διάβασμα αλλά η σελίδα δεν εμφανίζεται κανονικά των πολύ μικρών γραμμών.
- Reflow παραγράφου: Αυτό το επίπεδο ανιχνεύει τα όρια της παραγράφου μέσα στο κείμενο και πιέζει ολόκληρη την παράγραφο τόσο ώστε να είναι το ίδιο μέγεθος με την σελίδα του αρχικού κειμένου.
- Full Reflow: Αυτό το επίπεδο τυπικά δεν υποστηρίζεται από το ADE. Αγνοεί τα όρια του αρχικού κειμένου και το πιέζει βασισμένο στους παραγράφους. Προσφέρει την καλύτερη παρουσίαση του κειμένου με βελτιωμένη απόλαυση στο διάβασμα όπου οι παράγραφοι δεν χωρίζουν. Για να γίνει αυτό οπωσδήποτε πρέπει να χρησιμοποιηθούν ετικέτες.

### *3.13.2 Άλλα χαρακτηριστικά του PDF*

Τα PDF αρχεία μπορούν να περιέχουν συνδέσμους προς άλλες τοποθεσίες του αρχείου ή συνδέσμους σε αντικείμενο εκτός του αρχείου. Επιπλέον, ένα PDF μπορεί να περιέχει έναν πίνακα περιεχομένων ή ένα ευρετήριο με συνδέσμους προς διάφορα αντικείμενα ή πληροφορίες μέσα στο αρχείο. Αν και μερικοί ηλεκτρονικοί αναγνώστες δεν υποστηρίζουν αυτά τα χαρακτηριστικά και μερικοί επεξεργαστές PDF αρχείων δεν είναι ικανοί να προσθέσουν τέτοιου τύπου στοιχεία. Μερικά κείμενα υποστηρίζουν και σχόλια.

### 3.13.3 Δυνατότητες των PDF στους ηλεκτρονικούς αναγνώστες

Ο παρακάτω πίνακας δείχνει τις δυνατότητες των PDF αρχείων πάνω στους η-αναγνώστες.

| Capability | Description |
|---|---|
| Full Page View | Each page is shown on the screen full size. |
| Landscape View | Portrait pages are shown as several landscape screens. Left and right margins are often cropped. |
| Continuous View | There are no gaps between pages, so parts of two pages can be on the screen. |
| Two Column View | One column fills the screen, at the bottom of the page the 2nd column is started. |
| Manual Crop Margins | Zoom (magnify) in small increments to crop margins, i.e. reader customizable cropping. |
| Autocrop Margins | Zoom to remove whitespace in margins. Can be defeated by headers and footers and by scan artifacts. |
| Fixed Zoom | Zooming to fixed parts of the page via a menu. |
| Arbitrary Zoom | Zoom to any reader-specified part of the page. |
| Single Page Reflow | Reflow the text on a page. Number of font sizes allowed is typically 3 to 8. |
| Entire Document Reflow | Reflow the text across page boundaries. Number of font sizes allowed is typically 3 to 8. |
| Zoom Images in Reflow | Reflow "magnifies" text, so also magnify the images. |
| Passwords | PDFs with passwords can be opened. |
| Table of Contents | The table of contents, if any, is available for navigation. |
| Hyperlinks | Hyperlinks within the document can be followed and there is a "go back" option to unwind links. |
| Text to Speech | The text in the PDF, if any, can be read aloud. |
| Text Search | The text in the PDF, if any, can be searched. |
| Dictionary Lookup | Words in the PDF, if any, can be looked-up in a dictionary. |

ΕΙΚΌΝΑ 6: ΔΥΝΑΤΟΤΗΤΕΣ PDF

### 3.14 ePUB


ΕΙΚΟΝΑ 7: ΛΟΓΟΤΗΠΟ ΤΟΥ ΤΟ EPUB

Μια πρότυπη μορφή (format) ψηφιακών βιβλίων, που υποστηρίζεται από το International Digital Publishing Forum (IDPF http://www.idpf.org). Στον οργανισμό αυτό συμμετέχουν πολλές εταιρείες, οργανισμοί και πανεπιστήμια. Στη σχετική λίστα των μελών διακρίνουμε ονόματα όπως Sony, Adobe, National Geographic, μεγάλα πανεπιστήμια αλλά και ηλεκτρονικά βιβλιοπωλεία όπως τα Amazon (www.Amazon.com) και Barnes & Noble (www.barnesandnoble.com). Ο δικτυακός τόπος του IDPF αναφέρει: "το '.epub' επιτρέπει στους εκδότες να παράγουν και να διανέμουν ένα μόνο ψηφιακό αρχείο και να προσφέρουν στους καταναλωτές λειτουργικότητα μεταξύ λογισμικού/υλικού σε μη κρυπτογραφημένα ψηφιακά βιβλία αυτόματης σελιδοποίησης κατά το άνοιγμα (reflow able) και άλλες δημοσιεύσεις".

Το epub έγινε επίσημο πρότυπο του International Digital Publishing Forum τον Σεπτέμβριο του 2007, που αντικατέστησε το παλαιότερο πρότυπο Open e-Book. Τον Αύγουστο του 2009, η IDPF ανακοίνωσε ότι θα αρχίσει εργασίες συντήρησης του προτύπου epub. Η ομάδα που είχαν καθορίσει είχε ως σκοπό να κρατήσει το πρότυπο ενημερωμένο και να είναι έτοιμο για δημοσίευση έως το 2010. Στις 6 Απριλίου 2010, αναγγέλθηκε ότι η αναπροσαρμογή θα ολοκληρωθεί τον Απριλίου 2010. Το αποτέλεσμα επρόκειτο να είναι μια δευτερεύουσα αναθεώρηση σε EPUB 2.0.1 που «διορθώνει τα λάθη και τις ασυνέπειες και δεν αλλάζει τη λειτουργία». Στις 2 Ιουλίου 2010, τα σχέδια των προτύπων έκδοσης 2.0.1 εμφανίστηκαν στην ιστοσελίδα της IDPF.

#### 3.14.1 Η δομή του Epub

Το EPUB καθιερώθηκε ως επίσημο πρότυπο το 2007. Οι προδιαγραφές του καθορίζονται ουσιαστικά από τρία διαφορετικά αρχεία, τα OPS (Open Publication Structure), OPF (Open Packaging Format) και OCF (Open Container Format). Αυτό συμβαίνει γιατί το EPUB είναι βασισμένο σε XHTML. Έτσι, υπάρχουν αρχεία HTML με CSS, το οποίο καθορίζει τη μορφοποίηση του κειμένου, και αρχεία XML για το manifest, τα μετά-δεδομένα και τον πίνακα περιεχομένων ή και αρχεία εικόνας. Όλα μαζί είναι τοποθετημένα σε ένα αρχείο ZIP. Η λογική είναι παρόμοια με τα XML αρχεία του Microsoft Office 2007 (DOCX, XLSX κ.λπ.). Αυτό απλώς σημαίνει ότι μπορείτε να αλλάξετε την κατάληξη σε ένα μη κρυπτογραφημένο αρχείο από EPUB σε ZIP και στη συνέχεια να ανοίξετε τα αρχεία HTML. Το τελικό αρχείο μπορεί να έχει κατάληξη EPUB ή OCF.

Ένα **Epub** ή **OCF** είναι ένα συμπιεσμένο αρχείο που συνήθως περιέχει τα εξής:

```
mimetype
META-INF/
   container.xml
   [manifest.xml]
   [metadata.xml]
   [signatures.xml]
   [encryption.xml]
   [rights.xml]
OEBPS/
   Great Expectations.opf
   cover.html
   chapters/
      chapter01.html
      chapter02.html
      … other HTML files for the remaining chapters …
```

ΕΙΚΟΝΑ 8: ΠΑΡΑΔΕΙΓΜΑ ΠΕΡΙΧΟΜΕΝΩΝ ΕΝΟΣ OCF ΑΡΧΕΙΟΥ

Το **Open Publication Structure 2.0** (OPS) είναι ένα πρότυπο το οποίο χρησιμοποιείται για την παρουσίαση του περιεχομένου των ηλεκτρονικών βιβλίων.
Συγκεκριμένα:

- Το πρότυπο προορίζεται να δώσει τους προμηθευτές (π.χ. εκδότες, συντάκτες, και άλλους που έχουν περιεχόμενο να επιδείξουν), τις ελάχιστες και κοινές οδηγίες που εξασφαλίζουν την ακρίβεια, τη δυνατότητα πρόσβασης, και την επαρκή παρουσίαση του ηλεκτρονικού περιεχομένου σε διαφορετικούς αναγνώστες(e-readers).
- Ο στόχος αυτού του πρότυπου είναι η δυνατότητα δημοσιοποίησης του ηλεκτρονικού περιεχομένου και την βέλτιστη παρουσίαση από πολλαπλούς ηλεκτρονικούς αναγνώστες.

Το **Open Packaging Format** (OPF) πρότυπο καθορίζει τους μηχανισμούς, που περιέχονται σε μία προσθήκη OPS, και τον τρόπο λειτουργίας τους ώστε να προσθέσουν την δομή και τη σημασιολογία κατά την ηλεκτρονική δημοσίευση.
Συγκριμένα το OPF:

- Περιγράφει και αναφέρει όλα τα συστατικά της ηλεκτρονικής δημοσίευσης (π.χ. αρχεία σήμανσης, εικόνες, δομές πλοήγησης).
- Παρέχει τα μετά-δεδομένα.
- Διευκρινίζει την γραμμική σειρά ανάγνωσης του κειμένου.
- Παρέχει έναν μηχανισμό για να δημιουργήσει έναν δηλωτικό πίνακα περιεχομένων.
- Μπορεί παρέχει τους σελιδοδείκτες για πρόσθετα προαιρετικά στοιχεία όπως οι embedded fonts.

**Mime type** είναι ένα ASCII αρχείο. Το mime type είναι το αρχείο που λέει στο λειτουργικό μας σύστημα τι δομή έχει το ηλεκτρονικό μας βιβλίο (MIME type).

**Container.xml** είναι ένα συγκεκριμένο αρχείο με συγκεκριμένο όνομα. Πρέπει να βρίσκεται μέσα στο META-INF φάκελο. Όλα τα υπόλοιπα αρχεία είναι προαιρετικά δεν έχει σημασία τι όνομα θα έχουν. Το container.xml περιέχει τις πληροφορίες που δείχνουν το όνομα και την τοποθεσία του OPF αρχείου.

### *3.14.2 Εργαλεία που υποστηρίζουν το EPUB και την επικύρωση*

Λόγω του ανοιχτού κώδικα του πρότυπου EPUB, εργαλεία και εφαρμογές είναι διαθέσιμα από ποικίλες επιχειρήσεις και οργανώσεις. Συγκεκριμένα υπάρχει ένα εργαλείο, ανεπτυγμένο εν μέρη από την εταιρία Adobe, επικύρωσης των ePub. Ο σκοπός του εργαλείου είναι να δοθεί στους εκδότες και στους συγγραφείς η-βίβλιων ένας τρόπος να ελεγχθεί το περιεχόμενό τους για να βοηθήσει να εξασφαλίσει ότι τα EPUB αρχεία τους είναι πληρούν τις προδιαγραφές του IDPF. Τα επικυρωμένα EPUB είναι πολύ λιγότερο πιθανό να έχουν προβλήματα σε σημερινά και το μελλοντικά eBook

hardware and software. Το συγκεκριμένο εργαλείο επικύρωσης EPUB μπορείτε να το βρείτε στο http://code.google.com/p/epubcheck.

### *3.14.3 Προσβασιμότητα και ePub*

Το ePUB υποστηρίζεται από δύο πρότυπα κώδικα: XHTML και DTBook. Το DTBook είναι πρότυπο του οργανισμού Information and Standards Organization (NISO) το οποίο καθορίζει το σχήμα και το περιεχόμενο ενός ηλεκτρονικού αρχείου περιλαμβάνοντας τα και δημιουργώντας ένα ψηφιακό ηχογραφημένο βιβλίο (DTB). Το DTBs έχει ως σκοπό να καταστήσει το υλικό των η-βιβλίων προσιτό σε ατόμων με ειδικές ανάγκες.

Το K-12 (http://en.wikipedia.org/wiki/K%E2%80%9312_(education) ) μπορεί να δημιουργήσει ένα ePub η-βιβλίο χρησιμοποιώντας την τεχνική του DTBook, με κάποιες επιπλέον πληροφορίες, ώστε να δημιουργήσει ένα προς πώληση η-βιβλίο που επίσης θα πληροί τα πρότυπα του National Instructional Materials Accessibility (NIMAS).

### *3.14.4 Τα πλεονεκτήματα των ePUB και PDF.*

Το Adobe Digital Editions υποστηρίζει ePub και PDF αρχεία λόγω των πλεονεκτημάτων και τα δύο πρότυπα προσφέρουν. PDF αντιπροσωπεύει μία προσαρμοσμένη εικόνα και δίνει στον εκδότη τον έλεγχο πάνω στο σχεδιάγραμμα και στην παρουσίαση της σελίδας. Έτσι, ο αναγνώστης απολαμβάνει το κείμενο όπως ακριβώς ο εκδότης το προόριζε.

Το ePUB επιτρέπει στα ψηφιακά κείμενα να αναπροσαρμοστούν σύμφωνα με το μέγεθος, έτσι μπορούμε να προβάλουμε το ePUB αρχείο σε ηλεκτρονικούς αναγνώστες διαφορετικών μέγεθος εικόνων. Επίσης, το ePUB υποστηρίζει την χρήση διαδραστικών αντικειμένων ώστε να μπορεί να γίνει καλύτερη η ανάγνωση των ψηφιακών εκδόσεων οι οποίες μπορούν να διαβαστούν μέσω Η/Υ ή από διάφορους ηλεκτρονικούς αναγνώστες. Σε ένα ePUB αρχείο μπορεί να προσθέτουν βίντεο, γραφικά και animations ώστε να δημιουργηθεί μία ευχάριστη ψηφιακή δημοσίευση.

## ΚΕΦΑΛΑΙΟ 4

### 4.1 Σύγκριση των προτύπων των ηλεκτρονικών βιβλίων

Σε αυτό το κεφάλαιο θα γίνει μία προσπάθεια να προσδιορίσουμε και να συγκρίνουμε αν όχι όλα αλλά τα περισσότερα από τα πρότυπα των ηλεκτρονικών βιβλίων. Με την μεγάλη αύξηση των προτύπων ένας χρήστης μπορεί εύκολα να μπερδευτεί. Τα πιο σημαντικά πρότυπα είναι εκείνα που δουλεύουν πάνω σε φορητές συσκευές αλλά τα σημαντικότερα εκείνα που οι εκδότες χρησιμοποιούν για τις εκδόσεις βιβλίων τους ή σε πιο πρότυπο είναι δημοσιευμένα τα ήδη υπάρχοντα η-βιβλία. Σήμερα, αυτά τα πρότυπα είναι κυρίως τα AZW της Amazon, το MOBI της MobiPocket, το PalmDOC της Palm Reader και το ePUB. Ένα άλλο πολύ διάσημο πρότυπο είναι και το PDF από την Adobe. Όμως, δεν δουλεύει πολύ καλά σε φορητές συσκευές λόγω του μεγέθους της οθόνης. Χρησιμοποιείται πολύ καλύτερα πάνω στους υπολογιστές αφού μπορούν να προβάλουν "full size" σελίδες

**Portable Document Format**

**Πλεονεκτήματα:** Ένα μεγάλο πλεονέκτημα του Adobe Acrobat PDF πρότυπου είναι ότι μπορεί να διαβαστεί από πολλά διαφορετικά λειτουργικά συστήματα, και θα φανεί γενικά σχεδόν το ίδιο αποτέλεσμα στο καθένα από αυτά. Το αρχείο μπορεί να περιέχει εικόνες, και υπάρχει ακόμη και κάποια περιορισμένη υποστήριξη για τον ήχο ή τα βιντεοκλίπ. Σύνδεσμοι (links) μπορούν να προστεθούν για κομμάτια μέσα στο έγγραφο και από το έγγραφο στο World Wide Web. Υπάρχει επιλογή αναζήτησης μέσα στο κείμενο. Ο εκδότης μπορεί να προσθέσει σελιδοδείκτες (bookmarks) αλλά και ο χρήστης μπορεί να χρησιμοποιήσει και να προσθέσει τους δικούς του. Το μέγεθος των σελίδων μπορεί να αλλάξει ανάλογα το μέγεθος της εικόνας, έτσι μπορεί κάποιος να προβάλει τις εικόνες όσο μεγάλες χρειάζεται για να έχει ένα καλό αποτέλεσμα. Το μόνο που χρειάζεται για να προβάλει κάποιος PDF αρχεία είναι ο Adobe Acrobat Reader που είναι διαθέσιμος για Windows. Macintosh και Linux/Unix συστήματα. Επίσης, πολύ web browser έχουν ενσωματωμένο reader για προβολή των pdf αρχείων.

**Μειονεκτήματα:** Αν το αρχείο είναι φτωχά μορφοποιημένο, μπορεί να χρειαστεί ένα μην εμφανίζεται ολόκληρο το κείμενο στην οθόνη και θα πρέπει να μετακινήσουμε(scroll) το κείμενο οριζόντια για να μπορέσουμε να συνεχίσουμε να διαβάζουμε. Παρόμοιο πρόβλημα αντιμετωπίζουμε και όταν προσπαθούμε να διαβάσουμε PDF αρχεία στον Adobe eBook reader. Επίσης, τα αρχεία συνήθως είναι μεγαλύτερα σε μέγεθος από ότι τα αρχεία παρόμοιων προτύπων, ειδικά όταν οι εικόνες δεν είναι σωστά βελτιωμένες εκ των προτέρων. Το μεγαλύτερο όμως πρόβλημα αυτού του πρότυπου για τους συγγραφείς είναι το κόστος του λειτουργικού Acrobat από την Adobe, αν και υπάρχουν φτηνότερες λύσεις που κάποιος μπορεί να χρησιμοποιήσει αλλά είναι λιγότερο ευέλικτες.

**Παρατηρήσεις:** Τα μέτρα ασφάλειας που μπορεί να πάρει κάποιος εκδότης για τις εκδόσεις του συμβάλουν στο να αποτρέψουν τυχόν παραβιάσεις. Αν και αυτό έχει προκαλέσει κάποιες αντιπαραθέσεις, ειδικά όταν προσθέτουν DRMs σε η-βιβλία που είναι προς δημόσια χρήση. Υπήρξε κάποιο πρόγραμμα που μπορούσε να "σπάσει" τις ρυθμίσεις ασφαλείας. Το πρόγραμμα αυτό δεν είναι εύκολο να βρεθεί αφού ο προγραμματιστής του συνελήφθηκε και κατηγορήθηκε από τον νόμο, αλλά το πρόγραμμα εξακολουθεί να υπάρχει και να χρησιμοποιείται σποραδικά από διάφορους χρήστες.

**Hiebook**

**Πλεονεκτήματα:** Εύκολο στην χρήση. Μπορούμε να προσθέσουμε σελιδοδείκτες που θα δείχνουν σε μία τοποθεσία μέσα στο κείμενο. Και επίσης μπορούν να διαβαστούν από τον Hiebook η-αναγνώστη ή από Windows PC. Το πρότυπο αυτό υποστηρίζει μουσική στην μορφή mp3. παιχνίδια και διάφορους άλλους ήχους. Υπάρχουν δωρεάν η-αναγνώστες για τα Windows.

**Μειονεκτήματα**: Για να προσθέσει κάποιος βιβλία πρότυπου Hiebook στον η-αναγνώστη πρέπει να γίνει μέσω κάποιου Windows PC, το οποίο μειώνει αρκετά την ελευθερία του προτύπου.

**Παρατηρήσεις:** Επίσης, υπάρχει το πρόγραμμα Hibuilder για την δημιουργία η-βιβλίων σε Hiebook πρότυπο, το λογισμικό είναι δωρεάν και μπορεί να χρησιμοποιηθεί για εμπορικούς σκοπούς,

**HTML**

**Πλεονεκτήματα:** Λόγω του World Wide web (W3C), αυτό το πρότυπο έγινε παγκόσμια γνωστό. με πολλές επιλογές μορφοποίησης. Ανάλογα στο browser που χρησιμοποιείται για την προβολή των HTML αρχείων μπορεί να υποστηρίξει γραφικά, animations, ήχο, java, flash και άλλα multimedia χαρακτηριστικά. Ένα δυνατό πλεονέκτημα του HTML πρότυπου είναι οι σύνδεσμοι προς άλλα κείμενα ή άλλα sites. Βασικά, τα HTML βιβλία είναι σαν ιστοσελίδες αποθηκευμένα σε ένα CD ή στο σκληρό δίσκο.

**Μειονεκτήματα**: Δεν υπάρχουν χαρακτηριστικά για ασφάλεια για το πρότυπο HTML, έτσι κάποιος μπορεί να αντιγράψει ένα οποιοδήποτε HTML eBook και να το παρουσιάσει σαν δικό του.

**Παρατηρήσεις:** Γενικά είναι ένα αρκετά καλό πρότυπο για δημιουργία φτηνών η-βιβλία που προορίζονται για το όλους τους χρήστες.

**MobiPocket**

**Πλεονεκτήματα:** Το πρότυπο MobiPocket σχεδιάστηκε για να δουλεύει πάνω σε φορητές συσκευές αλλά μπορεί να χρησιμοποιηθεί και σε Windows PC. Το πρότυπο προσφέρει την αλλαγή της γραμματοσειράς και την πρόσθεση σημειώσεων. Επίσης, υπάρχει μία μπάρα προόδου (progress bar) για να δείχνει σε πιο σημείο του κειμένου βρισκόμαστε. Υπάρχει επιλογή αναζήτησης του κειμένου και όταν το η-βιβλίο κλείνει θα ξανά ανοίξει από το σημείο όπου κλίστηκε.

**Μειονεκτήματα**: Το πρότυπο αυτό δεν υποστηρίζει εκτύπωση. Επίσης, δεν υπάρχει ακόμα κάποιος η-αναγνώστης για MobiPocket πρότυπα για τα λειτουργικά Macintosh και Unix/Linux.

**Παρατηρήσεις:** Το λειτουργικό για την δημιουργία του πρότυπο είναι λίγο ακριβό, η βασική έκδοση ξεκινάει από τα $150 και φτάνει μέχρι τα $1000 η Professional έκδοση, αν και μία τσάμπα έκδοση υπάρχει για προσωπική χρήση.

**DjVu**

**Πλεονεκτήματα:** Το πρότυπο DjVu είναι ένα πρότυπο συγκεκριμένο για να αποθηκεύει σαρωμένα αρχεία. Περιέχει αρκετά ανεπτυγμένους συμπιεστές για εικόνες με κείμενο. Η κάθε σαρωμένη εικόνα χωρίζεται σε επίπεδα, κάθε επίπεδο είναι συμπιεσμένο με την καλύτερη υπάρχουσα συμπίεση. Το πρότυπο είναι σχεδιασμένο να αποσυμπιέζει και να διαβάζει τα αρχεία του παρά πολύ γρήγορα σε σχέση με άλλα πρότυπα. Επίσης, στο DjVu υπάρχει η δυνατότητα οι σαρωμένες εικόνες να είναι 300-400 DPI που είναι αρκετά υψηλής ανάλυσης, αρκετά καλή για εκτυπώσεις, κάθε σάρωση μπορεί να αποθηκευτεί με μέγεθος του ένα megabyte.

**Μειονεκτήματα**: Στο πρότυπο DjVu τα αρχεία δεν μπορούν αναδιαταχθούν έτσι η προβολή σε φορητούς υπολογιστές δεν είναι καλή. Επίσης δεν μπορούν να χρησιμοποιηθούν multimedia στοιχεία ούτε σύνδεσμοι στο να βοηθήσουν στην καλύτερη ανάγνωση του η-βιβλίου.

**Παρατηρήσεις:** Αρκετά καλό πρότυπο για εκτυπώσεις και ασπρόμαυρα κείμενα αλλά δεν είναι ιδανικό για κείμενα με εικόνες και άλλα multimedia στοιχεία. Επίσης, η προβολή των DjVu η-βιβλίων σε φορητούς υπολογιστές είναι αρκετά δύσκολη λόγω της μικρής οθόνης και το ότι το κείμενα βρίσκεται μέσα σε μία εικόνα.

**ePUB**

**Πλεονεκτήματα:** Το ePUB είναι ένα από τα πιο γρήγορα ανεπτυγμένα πρότυπα. Το ePUB προσφέρει ότι ακριβώς και το PDF αλλά και ακόμα περισσότερα. Προσφέρει αναδιάταξη στην σελίδα και υποστηρίζει την προσθήκη multimedia στοιχείων όπως εικόνα, ήχο ακόμα και βίντεο. Σύνδεσμοι (links) μπορούν να προστεθούν για κομμάτια μέσα στο έγγραφο και από το έγγραφο στο World Wide Web. Όμως ένα από τα δυνατά του στοιχεία είναι ότι υποστηρίζεται από παρά πολλούς ηλεκτρονικούς αναγνώστες.

**Μειονεκτήματα:** Το κυριότερο μειονέκτημα είναι ότι για την δημιουργία κάποιου πλήρους ePUB η-βιβλίου απαιτείται αρκετά καλή γνώση της γλώσσας XML και XHTML 1.1. Παρόλα αυτά

υπάρχουν προγράμματα για την δημιουργία ePUB μέσω γραφικού περιβάλλουν χωρίς καμία γνώση πάνω στην XML

**Παρατηρήσεις:** Ένα πρότυπο που θα κυριαρχήσει τα επόμενα χρόνια λόγω της απόλαυσης που δίνει στο διάβασμα ενός ηλεκτρονικού βιβλίου.

**Plain Text**

**Πλεονεκτήματα:** Το πιο γνωστό πρότυπο, τα ηλεκτρονικά βιβλία αυτού του πρότυπου μπορούν να διαβαστούν από όλους τους αναγνώστες κειμένων από όλους τους υπολογιστές.

**Μειονεκτήματα**: Δεν υπάρχει ασφάλεια σε αυτό το πρότυπο, οπότε τα βιβλία μπορούν να αντιγραφτούν ή να αλλαχτούν από τον οποιοδήποτε χρήστη χωρίς να έχουν πάρει την συγκατάθεση του συγγραφέα. Επίσης δεν υπάρχει ποικιλία στις γραμματοσειρές , στο μέγεθος των γραμματοσειρών και δεν υπάρχει υποστήριξη ήχου ή εικόνας.

**Παρατηρήσεις:** Χρήσιμο μόνο για την δημιουργία απλών ασπρόμαυρων κειμένων.

**Microsoft Reader**

**Πλεονεκτήματα:** Το πρότυπο αυτό μπορεί να διαβαστεί πάνω σε οποιοδήποτε Windows PC. Windows Tablet και Pocket PC συσκευές. Είναι εύκολο στην χρήση του, υποστηρίζει "ClearType" γραμματοσειρές οι οποίες βοηθούν στο καλύτερο διάβασμα. Υποστηρίζει αναζήτηση κειμένου, σελιδοδείκτες για να δείχνουν σε διάφορα σημεία του κειμένου, σημειώσεις, αλλαγή του μεγέθους της γραμματοσειράς και ηχογραφημένα κείμενα. Επίσης, το πρόγραμμα ανάγνωσης τέτοιου τύπου η-βιβλίων είναι δωρεάν.

**Μειονεκτήματα**: Αυτό το format δεν υποστηρίζει εκτύπωση και δουλεύει μόνο σε Windows λειτουργικά.

**Παρατηρήσεις:** Υπάρχουν αρκετά προγράμματα για την δημιουργία τέτοιων προτύπων άλλα με λιγότερα και άλλα με περισσότερα χαρακτηριστικά.

**PalmDOC**

**Πλεονεκτήματα:** Αν και τα χαρακτηριστικά αυτού του πρότυπου διαφέρουν ανάλογα τον ηλεκτρονικό αναγνώστη, τα PalmDOCs είναι βασικά κείμενα συμπιεσμένα για να έχουν μικρότερο μέγεθος, με την προσθήκη δεικτών, έτσι μπορούν να διαβαστούν από μία πολύ μεγάλη γκάμα συσκευών. Επίσης. η περισσότεροι PalmCOC αναγνώστες υποστηρίζουν την αλλαγή γραμματοσειράς.

**Μειονεκτήματα**: Δεν υποστηρίζει διαφοροποίηση κειμένου όπως "bold", "italic" και "underline" κείμενα.

**Παρατηρήσεις:** Υπάρχουν αρκετά προγράμματα που μπορούν να τρέξουν PalmDOC στα Windows και φυσικά πάρα πολλοί PalmOS προγράμματα που μπορούν να τρέξουν PalmDOCs.

**Amazon Kindle (.azw)**

**Πλεονεκτήματα:** Το πρότυπο της Amazon βασίζεται στο πρότυπο MobiPocket. Το πρότυπο προσφέρει την αλλαγή της γραμματοσειράς και την πρόσθεση σημειώσεων. Υπάρχει επιλογή αναζήτησης του κειμένου και όταν το η-βιβλίο κλείνει θα ξανά ανοίξει από το σημείο όπου κλίστηκε. Το πρότυπο χρησιμοποιεί δικό του DRM σύστημα επειδή τα ηλεκτρονικά βιβλία αγοράζονται μόνο online. Επίσης το Kindle πρότυπο είναι διαθέσιμο σε αρκετά λειτουργικά συστήματα

**Μειονεκτήματα**: Δεν υποστηρίζει εκτύπωση.

**Παρατηρήσεις:** Δεν μπορεί κάποιος να δημιουργήσει ένα βιβλίο τέτοιου προτύπου. Πρέπει το βιβλίο να σταλεί στην Amazon και έπειτα αυτή θα το εκδώσει στο πρότυπο της.

### 4.2 Συγκρίσεις των προτύπων μέσω πινάκων και εικόνων.

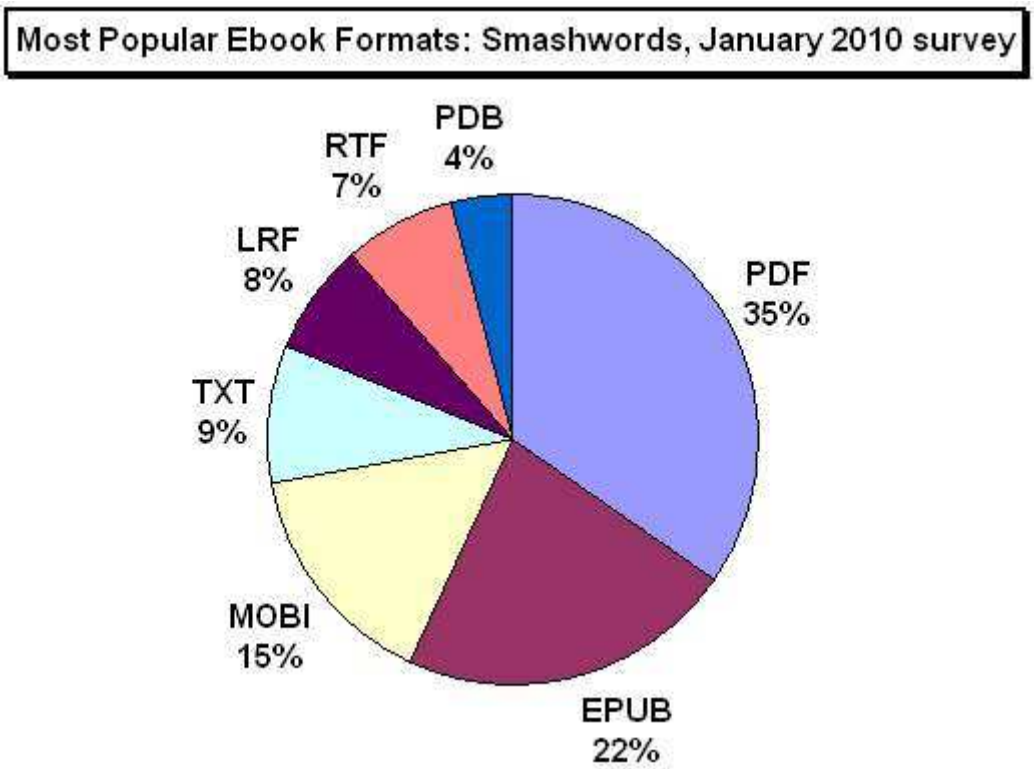
Στο παρακάτω πίνακα και εικόνα φαίνονται τα χαρακτηριστικά του κάθε format και με ποίες συσκευές είναι συμβατά

Πίνακας1: Σύγκριση προτύπων eBook

| **Πρότυπο** | Κατάληξη αρχείου | Υποστήριξη DRM | Υποστήριξη Εικόνας | Υποστήριξη Πινάκων | Υποστήριξη Ήχου | Υποστήριξη Multimedia | Υποστήριξη Συμπίεσης Κειμένου | Ανοιχτού κώδικα πρότυπο | Υποστήριξη Σχόλιων | Υποστήριξη Δεικτών |
|---|---|---|---|---|---|---|---|---|---|---|
| **Plain Text** | .txt | OXI | OXI | OXI | OXI | OXI | NAI | NAI | OXI | OXI |
| **HTML** | .html | OXI | NAI | NAI | OXI | OXI | NAI | NAI | OXI | OXI |
| **PDF** | .pdf | NAI | NAI | NAI | NAI | NAI | OXI | NAI | NAI | NAI |
| **DjVu** | .DjVu | ? | NAI | NAI | OXI | OXI | OXI | NAI | NAI | NAI |
| **ePUB** | .epub | NAI | NAI | NAI | NAI | NAI | NAI | NAI | NAI | NAI |
| **Kindle** | .azw | NAI | NAI | NAI | NAI | OXI | NAI | OXI | NAI | NAI |
| **PalmDOC** | .pdb | NAI | NAI | ? | OXI | OXI | NAI | OXI | NAI | NAI |
| **Hiebook** | .hie | NAI | NAI | NAI | NAI | OXI | OXI | OXI | OXI | NAI |
| **Microsoft Reader** | .lit | NAI | NAI | ? | OXI | OXI | NAI | OXI | ? | NAI |
| **Mobi** | .mobi | NAI | NAI | NAI | OXI | OXI | NAI | NAI | NAI | NAI |

| | **Adobe ePub** | **Adobe PDF** | **Mobipocket** | **B&N ePub** | **Apple ePub** | **Kindle** | **Microsoft Lit** | **PalmDOC** |
|---|---|---|---|---|---|---|---|---|
| **Windows PC** | Ναι | Ναι | Ναι | Ναι | Ναι | Ναι | Ναι | Ναι |
| **Sony** | Ναι | Ναι | Όχι | Όχι | Όχι | Όχι | Όχι | Όχι |
| **Nook** | Ναι | Ναι | Όχι | Ναι | Όχι | Όχι | Όχι | Ναι |
| **Mac** | Ναι | Ναι | Όχι | Ναι | Όχι | Ναι | Όχι | Ναι |
| **Kobo** | Ναι | Ναι | Όχι | Όχι | Όχι | Όχι | Όχι | Όχι |
| **Kindle** | Όχι | Ναι (Αν είναι χωρίς DRM) | Ναι (Αν είναι χωρίς DRM) | Όχι | Όχι | Ναι | Όχι | Όχι |
| **iPhone** | Ναι (Μέσω των εφαρμογ-ών Bluefire & Txtr) | Ναι(Με την εφαρμογή Bluefire για DRM αρχεία και με το Goodreader για χωρίς DRM) | Όχι | Ναι(Με την εφαρμογή του Nook ή την eReader) | Ναι για όλα τα iPhone με λειτουργ ικό iOS | Ναι | Όχι | Ναι |
| **iPad** | Ναι (Μέσω των εφαρμογ-ών Bluefire & Txtr) | Ναι(Με την εφαρμογή Bluefire για DRM αρχεία και με το Goodreader για χωρίς DRM | Όχι | Ναι(Με την εφαρμογή του Nook) | Ναι(Με την εφαρμογ ή iBooks) | Ναι | Όχι | Ναι |
| **Cybook** | Ναι | Ναι | Ναι αν γίνει αλλαγή firmware αλλά μετά δεν θα υποστηρίζει της adobe το DRM | Όχι | Όχι | Όχι | Όχι | Όχι |
| **Blackberry** | Όχι | Όχι | Ναι | Ναι | Όχι | Ναι | Όχι | Ναι |

Πίνακας2: Τι πρότυπα υποστηρίζουν διάφοροι η-αναγνώστες.




ΕΙΚΟΝΑ 9: ΤΑ ΠΙΟ ΔΙΑΣΗΜΑ ΠΡΟΤΥΠΑ EBOOK ΓΙΑ ΤΟ 2010[1]

[1] Η εικόνα είναι διαθέσιμη στο http://1.bp.blogspot.com/_d_yxMc3N2xs/S3MtZpEx_YI/AAAAAAAAAcs/B_nrAH4dF5M/s1600-h/mostpopular+ebook+formats+2010.jpg

# ΚΕΦΑΛΑΙΟ 5

## Οι ηλεκτρονικοί αναγνώστες

### 5.1 Γενικά για τους ηλεκτρονικούς αναγνώστες

Ο ηλεκτρονικός αναγνώστης βιβλίων (e-book reader) μετασχηματίζει τον παραδοσιακό τρόπο ανάγνωσης βιβλίων στην εκπαίδευση δίνοντας την δυνατότητα στους μαθητές, σπουδαστές ή φοιτητές να διαβάσουν πληθώρα ηλεκτρονικών βιβλίων και σημειώσεων με εύκολο τρόπο σε οποιοδήποτε σημείο . Ένας ηλεκτρονικός αναγνώστης μπορεί να υποστηρίξει περισσότερες από είκοσι μορφές αρχείων κειμένου. Οι ηλεκτρονικοί αναγνώστες βιβλίων είναι φορητές ηλεκτρονικές συσκευές στο φυσικό μέγεθος ενός παραδοσιακού βιβλίου, που εκτός από τις άλλες εργασίες που κάνουν ως υπολογιστές, αποτελούν μια πλατφόρμα για να διαβάσουμε βιβλία.

Οι ηλεκτρονικοί αναγνώστες έχουν περάσει από δύο κύματα ενδιαφέροντος και προσαρμογής. Το πρώτο κύμα εμφανίστηκε ανάμεσα στο 1998 και 2000 όπου διάφοροι η-λεκτρονικοι αναγνώστες εισήλθαν στην αγορά. αυτές οι συσκευές δέχτηκαν ανάμεικτα συναισθήματα και αρκετό ενθουσιασμό από ένα κείνο το οποίο ήταν συνηθισμένο με τα ψηφιακά κείμενα σε ηλεκτρονικούς υπολογιστές. Πολλοί σκέφτηκαν τότε ότι ήταν απίθανο τότε οι η-αναγνώστες να αντικαθιστούσαν τα παραδοσιακά βιβλία για διάβασμα, αλλά πίστευαν ότι ήταν φτιαγμένα για μαθητές και επίσης ήταν μία τέλεια λύση για επαγγελματίες που θα χρειαζόντουσαν να συμβουλευτούν κάποια εγχειρίδια. Ως το 2001 υπήρχαν 20 διαφορετικές ηλεκτρονικές συσκευές ανάγνωσης στην αγορά των Η.Π.Α. Όμως, λίγες από αυτές επέζησαν μετά την κατάρρευση του Dot-com bubble το 2001. Με τον καιρό ανάκτησε ο τομέας της υψηλής τεχνολογίας, το ενδιαφέρον για τις καταναλωτικές συσκευές μετατοπίστηκε από τους ηλεκτρονικούς αναγνώστες προς τα πολύ χρηστικά κινητά σε αυτό συνέβαλε και το όλο και πιο διαδραστικό ιντερνέτ. Παρόλα αυτά, το ενδιαφέρον για τα ηλεκτρονικά βιβλία και την δημοσίευση τους παρέμεινε δυνατό. Κυρίως τμήματα πανεπιστημίων επιστημονικές δημοσιεύσεις συνέχισαν να χρησιμοποιούν η-βιβλία σε μία προσπάθεια να μην ξεχαστούν.

Το δεύτερο κύμα ενδιαφέροντος για τους ηλεκτρονικούς αναγνώστες εμφανίστηκε με την είσοδο της εταιρίας Amazon στην αγορά το 2007. Ενώ οι πιο πρώτη κατασκευαστές η-αναγνωστών όπως η Sony, είχαν εστιάσει πάνω σε τεχνολογικά θέματα, η Amazon βασικός της στόχος ήταν η διανομή του η-αναγνώστη τους Kindle. Ως αποτέλεσμα είχε η είσοδο του Kindle να αλλάξει τα μέχρι τώρα δεδομένα. Το Kindle από συσκευή ανάγνωσης περισσότερο χρησιμοποιούταν για την αγορά τους. Αυτή η αλλαγή επηρέασε και τους τότε η-αναγνώστες Nook και Kobo, οι οποίοι υποστήριζαν τους δικούς τους πωλητές βιβλίων.

Έτσι, οι αναγνώστες των η-βιβλίων τπ πιο πιθανόν να έχουν το μέλλον τον κινητών τηλεφώνων. Το ποιός απ' όλους θα είναι ο καλύτερος θα κριθεί από τα αγαθά και τις υπηρεσίες που κάθε συσκευή θα προσφέρει. Παρά τις αλλαγές στις τεχνολογίες και τις υπηρεσίες που συνδέονται με τους ηλεκτρονικούς αναγνώστες, υπάρχουν αρκετά μειονεκτήματα με τους τρόπους με τους οποίους η εμπειρία ανάγνωσης eBook διαμορφώνεται από την εμπειρία του αναγνώστη των παραδοσιακών βιβλίων.

### 5.2 Αντικαταστάτης του βιβλίου;

Μία βασική απορία / αγωνία όσων εξετάζουν το ενδεχόμενο αγοράς ενός eBook Reader αφορά την αντικατάσταση του παραδοσιακού χάρτινου βιβλίου από το ηλεκτρονικό. Οι συγκεκριμένες συσκευές δεν έρχονται με σκοπό να αντικαταστήσουν το βιβλίο, αλλά αφενός να συμβάλλουν στην ευκολία μεταφοράς εγγράφων και βιβλίων και την εν συνεχεία προβολή τους με τρόπο χρήσιμο και ξεκούραστο στους χρήστες, αφετέρου δε, να ανοίξουν μία νέα αγορά για το ψηφιακό/ ψηφιοποιημένο περιεχόμενο: ένα βιβλίο δεν είναι ούτε οι σελίδες του, ούτε τα γράμματα, τα σύμβολα ή οι εικόνες που βρίσκονται τυπωμένες εκεί. Ένα βιβλίο είναι ένας τρόπος διάδοσης ιδεών και γνώσεων, ένα μέσο επικοινωνίας και μάθησης, ένα εργαλείο μεταφοράς: το αν θα είναι χάρτινο, πλαστικό, ηλεκτρονικό ή άλλο, είναι ένα ζήτημα που άπτεται περισσότερο της συνήθειας και της ευκολίας, παρά κάποιας ιδεολογίας ή αξιακού πλαισίου. Επίσης, το “βιβλίο” ουσιαστικά είναι άυλο,

και το χαρτί, η μελάνη και τα υπόλοιπα στοιχεία που το υλοποιούν στα μάτια μας είναι απλώς εργαλεία που τα αξιοποιούμε για αυτό το σκοπό.

### 5.3 Στόχοι δημιουργίας

Ο ηλεκτρονικός αναγνώστης είναι ένα μέσο ενσωμάτωσης τεχνολογιών στην εκπαίδευση. Στόχος είναι η δημιουργία μίας κατάλληλης συσκευής, η οποία θα συνδυάζει αρμονία μορφής και λειτουργίας, θα είναι ιδιαίτερα εύκαμπτη, και ανθεκτική, δεν θα περιέχει χημικά και θα είναι ιδιαίτερα χαμηλού κόστους. Η αποτελεσματική ενεργειακά μηχανή θα έχει δυνατότητες εφάμιλλες με εκείνες ενός σύγχρονου αναγνώστη βιβλίου ώστε κάθε παιδί να μπορεί να έχει πρόσβαση στη γνώση και στη νέα τεχνολογία. Μερικά από τα θετικά χαρακτηριστικά τα οποία θα παρέχει η συνδυασμένη χρήση των ηλεκτρονικών βιβλίων και των συσκευών ηλεκτρονικού βιβλίου θα είναι:

- Η προώθηση της ανάγνωσης, καθώς οι άνθρωποι, και κυρίως οι νέοι, ξοδεύουν τον περισσότερο χρόνο τους μπροστά από οθόνες
- Η δυνατότητα παραγωγής βιβλίων για τρέχοντα ζητήματα και γεγονότα μέσω ενός γρηγορότερου μέσου.
- Η διευκόλυνση της ενημέρωσής τους, για τη διόρθωση των λαθών και προσθήκη πληροφοριών.
- Η φορητότητά τους, καθώς μια ολόκληρη βιβλιοθήκη χωράει σε ένα DVD.
- Η διευκόλυνση της ανάγνωσης που μπορεί να γίνει προσιτή σε άτομα με ειδικές ανάγκες, καθώς το μέγεθος του κειμένου και της γραμματοσειράς μπορούν να αυξηθούν για άτομα με προβλήματα όρασης.

### 5.4 Προϊόντα για ηλεκτρονικούς αναγνώστες και Προμηθευτές

#### *5.4.1 Εκδότες*

Η παραγωγή των προϊόντων για τους ηλεκτρονικούς αναγνώστες αυξάνεται καθημερινά. Μεγάλη αποταμίευση γίνεται μέσω της ψηφιακής διανομής παρά της κλασικής μορφής εκτύπωσης, σε αυτό καθοριστικό ρόλο παίζει η αποστολή και η πώληση όπου μπορούν να γίνουν πάρα πολύ εύκολα στην περίπτωση της ψηφιακής διανομής.

Οι εκδότες κερδίζουν αρκετά χρήματα με την χρήση των η-βλίων επειδή συνήθως δεν επιτρέπεται να γυρίσουν τα παραδοσιακά βιβλία που δεν έχουν πουληθεί. Συχνά αυτό το μοντέλο συνεπάγει ότι οι εκδότες επιλέγουν μόνο συγγραφείς που είναι σίγουροι ότι το βιβλίο τους θα έχει επιτυχία.

Ένα νέο μοντέλο το οποίο θα επιτρέπει την μεταφορά γραμμένων κειμένων σε μία ηλεκτρονική πλατφόρμα, μπορεί να βοηθήσει εκδότες αλλά και τους λιγότερα γνωστούς συγγραφείς. Επίσης, το να αγοράσει κάποιος ένα η-βιβλίο είναι αρκετά πιο εύκολο.

Αλλά οι εκδότες ανησυχούν με το μοντέλο της Amazon, αφού αυτοί έχουν τον πλήρη έλεγχο επικοινωνίας με το τελικό χρήστη και μπορούν να επηρεάσουν τις τιμές προς όφελος τους. Αφού, οι ηλεκτρονικοί αναγνώστες της Amazon επίσης έχουν την δυνατότητα να προβάλουν εφημερίδες, βιβλία και περιοδικά, οι εκδότες έχουν πρόβλημα με το ότι δεν μπορούν να προβάλουν διαφημίσεις κάτι που είναι αντίθετο με άλλους η-αναγνώστες.

#### *5.4.2 Βιβλιοπωλεία και Βιβλιοθήκες*

Υπάρχουν αρκετά Βιβλιοπωλεία στον ιντερνέτ όπου κάποιος μπορεί να επισπευτεί. Η Amazon έχει δικό της online βιβλιοπωλείο για να πουλήσει και να παραδώσει τα η-βιβλία για τους δικούς της η-αναγνώστη. Το κανονικά βιβλιοπωλεία ίσως να επηρεαστούν απ' όλα αυτά και να πρέπει να προσφέρουν βιβλία διαθέσιμα προς κατέβασμα μέσω του ιντερνέτ αν θέλουν να παραμείνουν ανταγωνιστικά.

Οι εταιρίες που έχουν σχεδιάσει τους η-αναγνώστες μάλλον δεν θεωρούν τις βιβλιοθήκες σαν κερδοφόρα δουλειά και έτσι οι ηλεκτρονικοί αναγνώστες δεν είναι ανεπτυγμένοι για να χρησιμοποιούνται σε βιβλιοθήκες.

Αυτή η κατάσταση κάνει το δανεισμό ηλεκτρονικών βιβλίων και αναγνωστών αρκετά δύσκολη, και ίσως τελικά να καταλήξουμε στην περίπτωση όπου ηλεκτρονικά βιβλία θα μπορούν να διαβαστούν μόνο στο χώρο των βιβλιοθηκών. Οι βιβλιοθήκες θα έπρεπε επίσης να μπορούν να δανείσουν βιβλία τα οποία δεν υπάρχουν στην παραδοσιακή χάρτινη μορφή ή είναι πολύ μοναδικά στο να τα δανειστούν. Το να μπορούν να δανείζουν ηλεκτρονικούς αναγνώστες με ήδη εγκατεστημένα βιβλία θα κάνει το διάβασμα ευκολότερο αφού το διάβασμα από υπολογιστή μπορεί να είναι κουραστικό.

Άλλη ερώτηση είναι πως οι βιβλιοθήκες θα μοιάζουν οι βιβλιοθήκες όταν όλοι οι αναγνώστες θα μπορούν να κατεβάζουν τα βιβλία τόσο εύκολα όπως γίνεται σήμερα με την μουσική.

### *5.4.3 Περιεχόμενα Ηλεκτρονικών Αναγνωστών*

Τα αντικείμενα που μπορούμε να προβάλουμε σε ηλεκτρονικούς αναγνώστες μπορεί να είναι βιβλία, άρθρα, περιοδικά και εφημερίδες. Τα βιβλία έρχονται στην μορφή των ηλεκτρονικών βιβλίων. Παλαιότερα τα η-βιβλία προσφέρονταν κυρίως από τους Η/Υ, αλλά αυτή υ λύση δεν ήταν επιτυχής. Τα η-βιβλία συνήθως έχουν το δικό τους interface(γραφικό περιβάλλον) για την παρουσίαση του περιεχομένου τους.

Το πρόβλημα με την παρουσίαση των περιεχομένων των ηλεκτρονικών βιβλίων είναι ότι αλλάζει ανάλογα με το πρότυπο που είναι φτιαγμένο το βιβλίο.

Οι διάφοροι ηλεκτρονικοί αναγνώστες δεν υποστηρίζουν όλα τα πρότυπα. Η επόμενη λίστα είναι ένα γρήγορο overview(επισκόπηση) των πιο γνωστών προτύπων που χρησιμοποιούνται και δίνουν ένα σωστό αποτέλεσμα παρουσίασης.

- PDF
- Html
- Kindle
- BBeB
- ePUB
- Mobi

## 5.5 Ηλεκτρονικοί αναγνώστες εναντίων Παραδοσιακών βιβλίων

Μπορεί να βλέπουμε το η-αναγνώστη σαν ένα υποκατάστατο των παραδοσιακών βιβλίων. Πλεονεκτήματα και αδυναμίες των η-αναγνωστών μπορούν να συνοψιστούν όπως τα παρακάτω:

- Έναν ηλεκτρονικός αναγνώστης ζυγίζει λιγότερο από ότι ένα κανονικό βιβλίο, αφού περιέχει πολλά διαφορετικά βιβλία.
- Είναι θετικά προς το περιβάλλον αφού αποφεύγουμε την χρήση χαρτιού.
- Οι περισσότεροι υποστηρίζουν αναζήτηση λέξεων μέσα στο κείμενο.
- Πολύ μπορούν να χρησιμοποιήσουν Wi-Fi ή GSM δίκτυα για να συνδεθούν με το ιντερνέτ.

Μειονεκτήματα:

- Αρκετά ακριβό.
- Η τεχνολογία τους δεν έχει αναπτυχθεί αρκετά. Για παράδειγμα η αλλαγή των σελίδων γίνεται κάπως αργά.
- Μαθητές μοιράζονται βιβλία μεταξύ τους, αλλά με την χρήση η-αναγνωστών δεν είναι εύκολο.
- Δεν μπορεί κάποιος να τα ξεφυλλίσει όπως ένα κανονικό βιβλίο.
- Δεν είναι εύκολη η διαχείριση πολλών βιβλίων ένας χρήστης έχει αγοράσει, μεταξύ υπολογιστή και ηλεκτρονικού αναγνώστη.

## 5.5 Τεχνολογία

Οι ερευνητές δουλεύουν εδώ και χρόνια ώστε να αναπτύξουν μία οθόνη για τους ηλεκτρονικούς αναγνώστες βασισμένη στην τεχνολογία LCD, αλλά χωρίς μεγάλη επιτυχία.

Τελευταία έχουν εμφανιστεί κάποιοι η-αναγνώστες με LCD οθόνες αλλά μειονεκτούν αρκετά σε σχέση με της άλλες που κυκλοφορούν.

Με την εμφάνιση του "electronic paper" η Sony, Amazon και άλλες εταιρίες χρησιμοποίησαν αυτό το υλικό για την ανάπτυξη των ηλεκτρονικών τους αναγνωστών. Αυτή η νέα τεχνολογία έχει βελτιώσει την ποιότητα του διαβάσματος αρκετά.

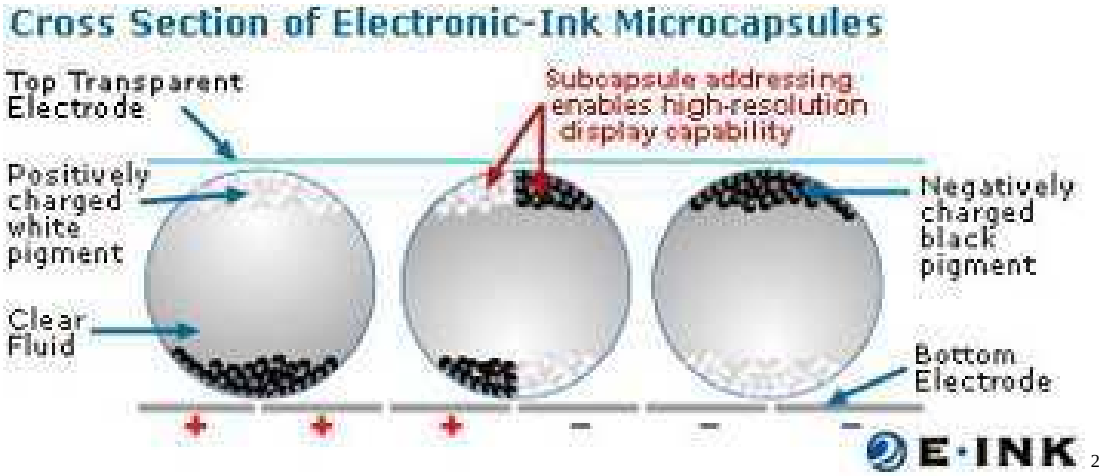
### *5.5.1 LCD*

Η τεχνολογία LCD καταναλώνει αρκετή ενέργεια και δεν είναι τόσο φιλική για μικρές συσκευές. Για τους ηλεκτρονικούς αναγνώστες η τεχνολογία δεν είναι κατάλληλη, για παράδειγμα είναι πολύ δύσκολο το διάβασμα κάτω από το φως του ήλιου, καταναλώνει πολύ μπαταρία και τα σχέδια δεν εμφανίζονται αρκετά σωστά.

Δύο ηλεκτρονικοί αναγνώστες εμφανίστηκα το 1998, ο Soft Book Reader και ο Rocket eBook. Η μπαταρία τους είχε αυτονομία 20 και 5 ώρες αντίστοιχα. Από τότε έχουν κυκλοφορήσει διάφοροι ηλεκτρονικοί αναγνώστες με οθόνη LCD αλλά αν και βελτιωμένη η τεχνολογία συνεχίζει να είναι κατώτερη του Electronic Paper.

### *5.5.2 E-paper*

Η τεχνολογία Electronic Paper βασίζεται στο Electronic Ink Vizplex ανεπτυγμένο από την εταιρία Eink. Η τεχνολογία βασίζεται σε εκατομμύρια μικρό κάψουλες, οι οποίες έχουν διάμετρο όσο μία ανθρώπινη τρίχα. Κάθε συστατικό περιέχει άσπρα και μαύρα σωματίδια που είναι ευαίσθητα σε ηλεκτρονική ενεργεία. Ηλεκτρικά πεδία επηρεάζουν αυτά τα σωματίδια να κινηθούν με τέτοιο τρόπο ώστε να δημιουργήσουν το κείμενο. Στην περίπτωση που δεν πρέπει να εμφανιστεί κάποιο κείμενο τα άσπρα σωματίδια κινούνται προς τα πάνω και τα μαύρα προς τα κάτω ώστε να μην φαίνονται. Οι οθόνες με τεχνολογία e-paper χρησιμοποιούν ενέργεια μόνο όταν κάποια σελίδα ανανεώνεται.




EIKONA 10: ELECTRONIC INK

[2] Η εικόνα είναι διαθέσιμη στο http://www.phosphorwatches.com/v/site_pages/einktechnology.asp

# ΚΕΦΑΛΑΙΟ 6

## Συσκευές ηλεκτρονικής ανάγνωσης

Οι ηλεκτρονικοί αναγνώστες αποτελούνται από ένα πλαστικό ή μεταλλικό περίβλημα, με κουμπιά για την πλοήγηση των κειμένων και για τις λειτουργίες του μενού. Η κατασκευή μπορεί να έχει θύρες USB και επιπλέον θύρες για κάρτες μνήμης. Μερικά από αυτά μπορεί να προσφέρουν Wi-Fi και GSM επικοινωνίες. Επίσης, μερικά μπορεί να αποτελούνται και από οθόνες αφής. Το μέγεθος τους συνήθως είναι A4 ή A5. Μπορεί να υποστηρίζουν ήχο και να έχουν τον δικό τους web browser.

Σε αυτό το κεφάλαιο θα αναλυθούν λεπτομερειακά όλα τα μοντέλα ηλεκτρονικών αναγνωστών που βρίσκονται στην αγορά.

## 6.1 Amazon Kindle


ΕΙΚΟΝΑ 115: AMAZON KIDLE

Ο Amazon Kindle είναι ένας φορητός ηλεκτρονικός αναγνώστης. Πιο ακριβή, είναι ένα λογισμικό, μία συσκευή και μία πλατφόρμα δικτύου ανεπτυγμένο από την Amazon η οποία χρησιμοποίει ασύρματη σύνδεση ώστε οι χρήστες της να μπορούν να αγοράσουν ηλεκτρονικά βιβλία και εφημερίδες. Το Kindle χρησιμοποιεί E Ink και electronic paper οθόνη η οποία απεικονίζει 16 σκιές του γκρίζου, ελαχιστοποιεί την χρήση ενέργειας και προσομοιώνει το διαβαστεί στην οθόνη ανάλογα την ενέργεια.

Αρκετές συσκευές υποστηρίζουν αυτή την πλατφόρμα. Τα πιο πρόσφατα Kindle είναι η τρίτη γενιά της πρώτης έκδοσης, επίσημα ονομάζονται "Kindle" αλλά αναφέρονται ως "Kindle 3". Το Kindle 3 παρουσιάστηκε στις 27 Αυγούστου, 2010. Οι χρήστες του ανέφεραν ότι η νέα οθόνη του Kindle 3, με E Ink pearl τεχνολογία, είναι αρκετά καλύτερη των προηγούμενων εκδόσεων.

Περιεχόμενο για το Kindle μπορεί να αγοραστεί online και να "κατεβαστεί"(downloaded) χρησιμοποιώντας Wi-Fi για να συνδεθούν ασύρματα με τους servers της Amazon.

### *6.1.1 Ιστορική αναδρομή και τα τελευταία μοντέλα*

#### Αρχική έκδοση

Η Amazon παρουσίασε την πρώτη της έκδοση στις 19 Νοεμβρίου, 2007, στην τιμή $399 και είχαν πουληθεί όλα τα κομμάτια του μέσα στις πεντέμισι ώρες. Δεν υπήρχαν αποθέματα προς πώληση για τους 5 επόμενους μήνες έως το τέλος του Απριλίου του 2008 . Είναι το μόνο Kindle που υπάρχει η επιλογή προέκτασης μνήμης μέσω SD κάρτας θύρα.

Η Amazon δεν πούλησε την πρώτη έκδοση του Kindle σε άλλες χώρες εκτός των Η.Π.Α.

**Kindle 2**

Τις 10 Φεβρουαρίου, 2009, η Amazon ανακοίνωσε το Kindle 2. Ήταν διαθέσιμο προς πώληση στις 23 Φεβρουαρίου. 2009. Τα επιπλέον χαρακτηριστικά του Kindle 2 ήταν η "κείμενο σε ομιλία"(text-to-speech) επιλογή όπου διαβαζόταν το κείμενο δυνατά και 2GB εσωτερική μνήμη από την οποία το 1.4 GB μπορούσε να χρησιμοποιήσει ο χρήστης. Η Amazon εκτιμούσε τότε ότι το Kindle 2 θα μπορούσε να χωράει περίπου 1500 μη-εικογραφημένα βιβλία. Το Kindle 2 σε σχέση με το πρώτο δεν είχε θύρα υποδοχής για κάρτες SD και επίσης ήταν και πιο λεπτό από το πρώτο.

**Η Διεθνής έκδοση του Kindle 2**

Στις 7 Οκτωβρίου, 2009, ανακοίνωσε την διεθνή έκδοση του Kindle 2 για 100 χώρες. Έγινε διαθέσιμη στις 19 Οκτωβρίου, 2009. Η διεθνής έκδοση του Kindle 2 ήταν εξωτερικά η ίδια με το αμερικάνικο μοντέλο. αν και χρησιμοποιούσε πρότυπα ασύρματης δικτύωσης. Η αμερικάνικη έκδοση χρησιμοποιούσε το πρότυπο CDMA2000. Η διεθνής έκδοση χρησιμοποιούσε το πρότυπο GSM και 3G GSM.

Η διεθνής έκδοση πιστεύετε ότι έχει μεγαλύτερη ανάλυσης οθόνη, αν και η Amazon δεν το διαφημίζει αυτό. Επίσης άλλα test που έγιναν έδειξαν ότι στο Kindle 2 με τις αλλαγές που έκαναν ήταν δυσκολότερη η ανάγνωση απ' ότι την προηγούμενη έκδοση.

**Kindle DX**

Η Amazon ανακοίνωσε το Kindle DX στις 6 Μαΐου, 2009. Αυτή η συσκευή έχει μεγαλύτερη οθόνη από ότι το Kindle 2 και υποστήριζε απλά PDF αρχεία. Επίσης ήταν το πιο λεπτό Kindle και προσφέρει αν επιταχυνσιόμετρο (accelerometer), το οποίο επιτρέπει στον χρήστη να περιστρέφει ομαλά τις σελίδες όταν το Kindle DX είναι γυρισμένο το πλάι. Διαφημίστηκε σαν μία ευκολία διαβάσματος εφημερίδας. Η συσκευή μπορεί να συνδεθεί μόνο με το ασύρματο δίκτυο της Amazon Whisper net στις Η.Π.Α.

Από τις 19 Ιανουάριου, 2010, η διεθνής έκδοση του Kindle DX έφτασε σε 100 χώρες

**Kindle DX Graphite**

Την πρώτη Ιουλίου, 2010 , η Amazon παρουσίασε μία νέα έκδοση του Kindle DX την οποία ονόμασε "Graphite"και κυκλοφορεί αποκλειστικά σε γραφίτη χρώμα. Το νέο Kindle DX έχει οθόνη E Ink με 50% καλύτερη αντίθεση. Πιθανολογείται, χρησιμοποιήθηκε το συγκεκριμένο χρώμα για να βελτιώσει την αντίθεση της οθόνης. Όπως και τα προηγούμενα Kindle το Graphite δεν υποστηρίζει Wi-Fi σύνδεση. Το Kindle DX Graphite(DXG) θεωρείται η τρίτη γενιά του Kindle DX αλλά παρόλα αυτά είναι ένας συνδυασμός τρίτης γενιάς hardware και δεύτερης γενιάς software. Ο επεξεργαστής είναι συγχρονισμένος στην ίδια ταχύτητα με το Kindle 3 αλλά είναι διαφορετικής έκδοσης. Αν και το DX Graphite είναι μεγαλύτερο έχει τη μισή μνήμη (128MB) απ' ότι το Kindle 3 (256MB). Λόγω αυτών των διαφορών το DXG τρέχει στο ίδιο Firmware όπως το Kindle . Συνεπώς το DXG δεν μπορεί να διαβάσει κυριλλικούς χαρακτήρες και ο web browser είναι περιορισμένος στα χαρακτηριστικά του Kindle 2.

**Kindle 3**

Η Amazon ανακοίνωσε την νέα γενιά Kindle στις 28 Ιουλίου, 2010. Το Kindle 3είναι διαθέσιμο σε δύο εκδόσεις. Μια από αυτές, το Kindle Wi-Fi, το οποίο συνδέεται στο ιντερνέτ αποκλειστικά μέσω Wi-Fi. Η άλλη έκδοση, αναφέρεται σαν τον αντικαταστάτη του Kindle 2 και υποστηρίζει και 3G και Wi-Fi συνδεσιμότητα. Το 3G χρησιμοποιεί τα ίδια σήματα με τα κινητά

τηλέφωνα το οποίο το επιτρέπει να κατεβάζει και να αγοράζει από όποια τοποθεσία υπάρχει σήμα για κινητό. Το νέο Kindle χρησιμοποιεί E ink οθόνη με υψηλότερη ανάλυση. από τα προηγούμενα μοντέλα και υψηλότερο ρυθμό ανανέωσης(refresh rate).

Το Kindle 3 είναι 0.5 inches κοντύτερο και στενότερο απ' ότι το Kindle 2. Υποστηρίζει επιπλέον γραμματοσειρές και Unicode χαρακτήρες. Ένας πειραματικός web browser βασισμένος στον WebKit, καθώς και text-to-speech μενού πλοήγησης. Η εσωτερική μνήμη επεκτείνεται στα 4GB με σχεδόν 3GB διαθέσιμα για τον χρήστη. Η μπαταρία φημολογείται ότι κρατάει μέχρι και ένα μήνα διαβάσματος με το ασύρματο δίκτυο κλειστό.

Στις 25 Αυγούστου, 2010, η Amazon ανακοίνωσε ήταν το πιο γρήγορο Kindle σε πωλήσεις.

### 6.1.2 Πρότυπα υποστηριζόμενα από το Kindle

Το πρώτο Kindle υποστήριζε μόνο MobiPocket βιβλία (Mobi, Prc) χωρίς DRM, plain text(txt), topaz(TPZ) και της Amazon το πρότυπο (AZW). Η έκδοση 2.3 για το Kindle 2 πρόσθεσε και την υποστήριξη PDF αρχείων. ePUB πρότυπα δεν υποστηρίζει ακόμα αλλά υπάρχουν προγράμματα, όπως το Calibre, που μπορεί να μετατρέψει τα ePUB αρχεία που δεν έχουν ασφάλεια DRM σε πρότυπο Mobi όπου οι ηλεκτρονικοί αναγνώστες μπορούν να διαβάσουν. Η Amazon επίσης προσφέρει μια υπηρεσία όπου κάποιος μπορεί να στείλει αρχεία Jpeg, gif, png και BMP μέσω e-mail και να τα μετατρέψει σε γραφικά τύπου AZW. Επίσης, μπορεί κάποιος κάτοχος Kindle συσκευής να στείλει κάποια αρχεία και η Amazon να τα μετατρέψει σε κάποιο αναγνωρίσιμο πρότυπο χωρίς επιπλέον χρέωση. Επίσης υποστηρίζει ήχο μορφής Mp3 ο οποίος πρέπει να μεταφερθεί στο Kindle μέσω USB ή κάρτας SD. Επίσης, τα μοντέλα Kindle 2, DX και 3 υποστηρίζουν το πρότυπο HTML όποτε μπορούν να επισκεφτούν ιστοσελίδες μέσω του ιντερνέτ.

## 6.2 Barnes & Noble Nook

EIKONA12: NOOK READER

Το Barnes & Noble Nook(ή απλά Nook) είναι ένας ηλεκτρονικός αναγνώστης ανεπτυγμένος από την εταιρία διανομής βιβλίων Barnes & Noble βασισμένο στην πλατφόρμα Android. Η αρχική συσκευή ανακοινώθηκε στις Η.Π.Α στις 20 Οκτωβρίου, 2009 με κόστος αγοράς $259. Το αρχικό Nook υποστήριζε Wi-Fi και AT&T 3G ασύρματη δικτύωση., οθόνη 6 ιντσών E Ink οθόνη και άλλη μία ξεχωριστή μικρότερη οθόνη αφής LCD η οποία χρησιμοποιείται για την πλοήγηση. Στις 21 Ιουνίου 2010, η Barnes & Noble ανακοινώσανε μείωση τιμής στα $199 και μια Wi-Fi συσκευή στα $149.

### *6.2.1 Χαρακτηριστικά*

Το αρχικό Nook είχε μία ασπρόμαυρη E Ink οθόνη για την προβολή των ψηφιακών δεδομένων με την πλοήγηση να γίνεται μέσω της οθόνης αφής. Το αρχικό Nook συνδέεται με το Barnes and Noble online κατάστημα μέσω μίας δωρεάν σύνδεσης στο δίκτυο AT&T 3G ή μέσω διαθέσιμων Wi-Fi δικτύων. Οι χρήστες μπορούν να διαβάσουν βιβλία χωρίς ασύρματη σύνδεση δικτύου, έτσι μπορούν να παρατείνουν την μπαταρία μέχρι και δέκα ημέρες.

Η συσκευή έχει θύρα για MicroSD κάρτες για επιπλέον χώρο αποθήκευσης και μία επαναφορτιζόμενη μπαταρία. η μπαταρία μπορεί να φορτιστεί μέσω κανονικής πρίζας; ρεύματος ή με

καλώδιο micro-USB 2.0. Οι συσκευή επίσης, περιέχει web browser , λεξικό , σκάκι και Sudoku και μπορεί να παίξει μουσική.

Πρότυπα όπου το Nook υποστηρίζει:

- eReader PDB με της Barnes & Noble DRM
- ePUB με της Barnes & Noble DRM
- ePUB με της Adobe ADEPT DRM
- PDF με της Adobe ADEPT DRM

Επίσης υποστηρίζει πρότυπα ήχου και audiobooks συμπεριλαμβανομένων των Mp3 και Ogg Vorbis. Όπως και τα πρότυπα για εικόνες jpg, gif, png και bmp, που χρησιμοποιούνται για εξώφυλλα, μικρογραφίες και wallpapers.

Το Nook υποστηρίζει την εφαρμογή "LendME" που επιτρέπει στους χρήστες να μοιραστούν κάποια βιβλία με άλλα άτομα, εξαρτάται από την άδεια που έχει δώσει ο εκδότης του βιβλίου. Ο αγοραστής κάποιου βιβλίου απαγορεύεται να μοιραστεί ένα βιβλίο με κάποιον άλλον για πάνω από δύο εβδομάδες.

### *6.2.2 Εκδόσεις λογισμικού*

Η Barnes and Noble διανέμει αναβαθμίσεις για το λογισμικό της αυτόματα ή χειροκίνητα. Η πιο καινούργια έκδοση για το Nook, είναι η έκδοση 1.5, όπου παρουσιάστηκε στις 22 Νοεμβρίου 2010 και πρόσθεσε στο λογισμικό μία επιπλέον επιλογή για προαιρετική προστασία με κωδικό για τις συσκευές, μία "My Shelves" υπηρεσία για να οργανώνουν καλύτερα τις βιβλιοθήκες τους οι χρήστες. Επίσης, βελτίωσαν το γύρισμα των σελίδων και τις επιλογές της αναζήτησης.

Η έκδοση 1.2, παρουσιάστηκε το Φεβρουάριο του 2010, βελτίωσε την ανταπόκριση της συσκευής, τη χρήση σελιδοδεικτών, τη συνδεσιμότητα με το online κατάστημα και βελτιστοποίησαν την μπαταρία. Η αναβάθμιση επίσης περιείχε αλλαγές στο γραφικό περιβάλλον και στη βελτίωση της πλοήγησης.

Η έκδοση 1.3 παρουσιάστηκε τον Απρίλιο του 2010 και πρόσθεσε web browser, τα παιχνίδια σκάκι και Sudoku και περισσότερες επιλογές για Wi-Fi συνδεσιμότητα.

Η έκδοση 1.4 παρουσιάστηκε το Ιούνιο του 2010, βελτιστοποίησε τις επιλογές στα ασύρματα δίκτυα, πρόσθεσε μία τεράστια γραμματοσειρά και την υπηρεσία "Go-to Page" .

## 6.3 Sony Readers

Οι Sony Readers είναι μία σειρά ηλεκτρονικών αναγνωστών κατασκευασμένοι από την Sony. και χρησιμοποιούν electronic paper E Ink οθόνες.

Οι αναγνώστες διαθέτουν ένα γραφικό περιβάλλον από όπου ο χρήστης μπορεί να αγοράσει βιβλία από το online κατάστημα της Sony eBook Library (διαθέσιμο μόνο για τις Η.Π.Α και Καναδά). Τα πρότυπα που μπορεί να προβάλει είναι:

- ePUB με της Adobe DRM
- PDF με της Adobe DRM
- RSS ιστολόγια.
- BBeB το πρότυπο ανεπτυγμένο από τη Sony.

Επίσης, υποστηρίζει το πρότυπο εικόνων Jpeg και πρότυπα ήχου Mp3 και αποκρυπτογραφημένα AAC.

Με την υποστήριξη του Digital rights management(DRM) να προστατεύει τα PDF και ePUB αρχεία επιτρέπει στους χρήστες να δανειστούν βιβλία από δανειστικές βιβλιοθήκες σε αρκετές χώρες. Οι κανόνες για τα ψηφιακά δικαιώματα στους Sony Readers επιτρέπουν ένα οπουδήποτε αγορασμένο βιβλίο να διαβαστεί μέχρι και σε έξι διαφορετικές συσκευές που είναι γραμμένοι (registered) στον ίδιο λογαριασμό χρήστη.

### *6.3.1 Τα μοντέλα*

Τα μοντέλα ηλεκτρονικών αναγνωστών της Sony που έχουν κυκλοφορήσει στην αγορά είναι αρκετά. Ξεκίνησαν με το PRS-500 όπου και αντικαταστήθηκε από το PRS-505. Ακολούθησε το PRS-700 με την μεγάλη οθόνη αφής το οποίο όμως σταμάτησε να αναβαθμίζεται από την Sony. Επίσης υπάρχει το PRS-300 και το PRS-600 με οθόνη αφής. Αυτά τα δύο τώρα πια είναι αντικατεστημένα από το PRS-350 και το PRS-650 με την νέα οθόνη τεχνολογίας E Ink Pearl. Επίσης, υπάρχει και η σειρά PRS-900 η οποία τώρα πια είναι αντικαταστημένη από το PRS-950 "Daily edition".

**Γενικά χαρακτηριστικά**

**Θετικά**

- Μπορεί να διαβαστούν 7500 σελίδες με μία φόρτιση της μπαταρίας, περίπου 20 ώρες ζωής.
- Μπορεί να διαβαστεί και σε εξωτερικούς χώρους όπου υπάρχει ήλιος.
- Ανάλυση 167dpi.
- Χρησιμοποιεί ανοιχτού κώδικα λειτουργικό σύστημα (Linux).
- Περισσότερα από 50000 η-βιβλία διαθέσιμα στο ηλεκτρονικό κατάστημα της Sony.

**Αρνητικά**

- Η αλλαγή των σελίδων είναι αργή.
- Η ανάλυση δεν είναι αρκετά υψηλή για να προβάλει μικρά γραμματοσειρές. Γραφήματα δεν παρουσιάζονται σωστά λόγω της ανάλυσης.

### *6.3.2 PRS-350 και PRS-950*

Στην παρακάτω υπό-ενότητα θα αναλυθούν λεπτομερειακά τα δύο βασικότερα μοντέλα των Sony ηλεκτρονικών αναγνωστών το PRS-350 και PRS-950.


ΕΙΚΟΝΑ13:SONY PRS-350

**PRS-350**

Ο **Sony PRS-350** είναι ο δεύτερης γενιάς ηλεκτρονικός αναγνώστης "Pocket Edition" της Sony. Έχει οθόνη 5 ιντσών και είναι ένας από τους μικρότερους και ελαφρύτερους ηλεκτρονικούς αναγνώστες που έχουν κατασκευαστεί ποτέ. Όπως και ο προκάτοχός του, ο PRS-300, παρουσιάζεται ως ο ηλεκτρονικός αναγνώστης "που χωράει στην τσέπη σου" και το νέο μοντέλο είναι ακόμα πιο μικρό από το προηγούμενο. Έχει διαστάσεις (ύψος/ πλάτος/ πάχος) 145 x 104 x 8,4 χιλιοστά (5.71 x 4.11 x 0.33 ίντσες) και βάρος 160 γραμμάρια (5.64 ουγγιές), που σημαίνει ότι είναι περίπου 125 χιλιοστά πιο μικρός και περίπου 55 γραμμάρια πιο ελαφρύς. Έχει καλή ποιότητα κατασκευής πλαίσιο από αλουμίνιο σε ροζ και ασημένιο χρώμα.

**Χαρακτηριστικά**

Η βασική διαφορά του Sony Reader PRS-350 από τον PRS-300 είναι ότι ο καινούργιος έχει οθόνη αφής. Το σημαντικό με τη νέα οθόνη αφής είναι ότι δεν απαιτεί μια επιπρόσθετη μεμβράνη για τη λειτουργία της αφής, που προκαλούσε γυαλάδα στην οθόνη (glare). Χρησιμοποιείται η τεχνολογία υπερύθρων zForce της NeoNode για τον χειρισμό της οθόνης αφής, με αποτέλεσμα να έχει πολύ καλή απόκριση και εύκολη στη χρήση με το δάχτυλο ή με τη γραφίδα που παρέχεται. Στα άκρα της οθόνης όμως η απόκριση στο χειρισμό με το δάχτυλο μειώνεται, χωρίς να υπάρχει κάποιος συγκεκριμένος λόγος. Οι νέες οθόνες είναι αναβαθμισμένες, τελευταίας γενιάς οθόνες Pearl της E Ink, οι ίδιες που χρησιμοποιούνται στα Kindle3 και Kindle DX του Amazon, και έχουν καλύτερο κοντράστ και πιο βαθύ μαύρο από τις παλιότερες οθόνες Vizplex. Καθώς η οθόνη είναι μικρή, τα μικρότερα μεγέθη των χαρακτήρων είναι πιο βολικά για την ανάγνωση, αλλιώς θα χρειάζεται να αλλάζουμε συχνά σελίδα.

Σε σύγκριση με το Kindle, όμως, η γραμματοσειρά που χρησιμοποιεί ο Sony PRS-350 είναι λεπτότερη, κι έτσι το αποτέλεσμα δεν είναι τόσο καλό. Η Sony δε δίνει τη δυνατότητα αλλαγής της γραμματοσειράς της συσκευής. Αν ρυθμίσουμε το κοντράστ της συσκευής, οι χαρακτήρες φαίνονται πιο έντονοι, αλλά και πιο θολοί στο τελείωμά τους ανάλογα με τις ρυθμίσεις.

Ο νέος Sony Reader Pocket Edition έχει μη-επεκτάσιμη εσωτερική μνήμη 2 GB, με τα 1,4GB να είναι διαθέσιμα για αποθήκευση eBooks και εγγράφων, που αντιστοιχεί σε 1200 αρχεία περίπου. Η μπαταρία διαρκεί για 10.000 γυρίσματα σελίδων.

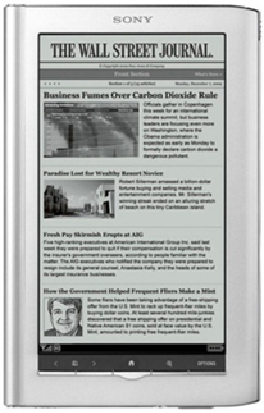
Υποστηρίζει αρχεία ePUB και PDF (με και χωρίς DRM), κάτι που δίνει μια μεγάλη επιλογή για κατέβασμα δωρεάν και αγορασμένων eBooks από τα πολλά ηλεκτρονικά βιβλιοπωλεία που υποστηρίζουν το DRM. Υποστηρίζει επίσης αρχεία κειμένου txt.rtf και Word και αρχεία εικόνων jpeg ,png, gif και bmp. Δεν υποστηρίζει αρχεία ήχου.

**Αδυναμίες και μειονεκτήματα**

Στις **αδυναμίες** του Sony PRS-350 συγκαταλέγονται ότι έχει μία μόνο γραμματοσειρά, και μάλιστα αρκετά λεπτή, ενώ η αποκοπή των περιθωρίων δε φαίνεται να δουλεύει για όλα τα βιβλία. Δε δίνει επίσης τη δυνατότητα να προσαρμόσουμε το ύψος και την απόσταση των γραμμών και τα περιθώρια και άλλες τέτοιες παραμέτρους της εμφάνισης του κειμένου. Στον οριζόντιο προσανατολισμό της οθόνης (landscape mode), ένα τμήμα του κειμένου της προηγούμενης σελίδας επαναλαμβάνεται στην επόμενη, δυσκολεύοντας να συνεχίσουμε το διάβασμα από εκεί που είχαμε μείνει. Κάποιες από τις ρυθμίσεις για την εμφάνιση της σελίδας κάθε φορά που ξανά ανοίγουμε το αρχείο. Τέλος, ο χωρισμός σε στήλες είναι μόνο κάθετος, που είναι χρήσιμο μόνο για τα αρχεία PDF με στήλες.

Τα δύο κυριότερα **μειονεκτήματα** του Sony PRS-350 είναι πάντως ότι είναι ακριβότερο από το Kindle 3 Wi-Fi και το Nook και ότι δεν έχει τη δυνατότητα σύνδεσης στο ιντερνέτ με Wi-Fi. Η τιμή είναι αναμενόμενο που είναι υψηλότερη, όπως κάνει η Sony και με τα άλλα της προϊόντα. Η σύνδεση με το ιντερνέτ από έναν ηλεκτρονικό αναγνώστη, που είναι βέβαια ένα σημαντικό bonus, είναι για άλλους είναι σημαντική και για άλλους όχι, είναι περισσότερο θέμα προσωπικών προτιμήσεων.

**PRS-950**




EIKONA14:SONY PRS-950

Ο ηλεκτρονικός αναγνώστης Sony PRS-950, είναι η έκδοση πολυτελείας της Sony. Υποστηρίζει Wi-Fi για πλοήγηση στο internet με νέο βασικό web browser και δωρεάν (μόνο για τις Η.Π.Α και τον Καναδά) 3G συνδεσιμότητα για να συνδέονται στο ηλεκτρονικό
κατάστημα της Sony και να κάνουν τις αγορές τους.

**Χαρακτηριστικά**

Το "δυνατότερο" χαρακτηριστικό που έχει το PRS-950 είναι η οθόνη αφής του. Όχι μόνο είναι μία αρκετά υψηλότερης ανάλυση οθόνη με αρκετά μεγαλύτερη αντίθεση, αλλά δεν υπάρχει καμία λάμψη να συσχετίζεται με την οθόνη αφού δεν υπάρχει πια κανένα πλαίσιο πάνω από την οθόνη. Αντί αυτού , η οθόνη χρησιμοποιεί υπέρυθρες ακτίνες για τον εντοπισμών των εντολών που δίνει ο χρήστης.

Με αυτό η Sony κατάφερε να λύσει το πρόβλημα που είχε με τις οθόνες αφής, τα προηγούμενα χρόνια, διατηρώντας παράλληλα όλα τα χαρακτηριστικά που έκαναν τους η-αναγνώστες της Sony μοναδικούς. Η οθόνη αφής λειτουργεί με τα δάχτυλα αλλά και με ένα ειδικό στυλό που περιλαμβάνεται στην συσκευασία. Η ανταπόκριση είναι πραγματικά πολύ καλή και μπορεί να ενεργοποιηθεί με το άγγιγμα ενός φτερού. Η PRS-950 έχει όλα τα χαρακτηριστικά και τις λειτουργίες των PRS-350 και PRS-650: μπορείτε να προσθέσετε σημειώσεις με το πληκτρολόγιο της οθόνης, να προσθέσετε σελιδοδείκτες, με διπλό κλικ σε μία λέξει θα εμφανιστεί το λεξικό, να δημιουργήσετε, να διαχειριστείτε και διαγράψετε ψηφιακές συλλογές, να εκτελέσετε αναζητήσεις να επισκεφτείτε hyperlinks και ούτω καθεξής.

Αυτό που κάνει το PRS-950 μοναδικό είναι ο μόνος ηλεκτρονικός αναγνώστης που έχει 7 ιντσών οθόνη. Οι περισσότεροι χρησιμοποιούν 6 ή 5 ιντσών οθόνη, Υπάρχουν κάποιοι άλλοι με 8 και 9.7 ιντσών οθόνη αλλά η Sony είναι η μόνοι που χρησιμοποιεί 7 ιντσών.

Λόγω της μεγάλης οθόνης , κάποιοι θα νομίζουν ότι το PRS-950 είναι αρκετά μεγάλο σε μέγεθος. Αλλά πραγματικά δεν δίνει αυτό το συναίσθημα. Καμία σχέση με το Kindle DX.
Βασικά είναι ακριβώς το ίδιο μέγεθος όσο το Kindle 3, απλά μισή ίντσα ψηλότερο και μερικά γραμμάρια βαρύτερο.

Η συσκευή έχει 2GB εσωτερική μνήμη από τα οποία μπορεί να χρησιμοποιήσει σχεδόν το 1.6GB. Υπάρχει και η δυνατότητα παρέκταση της μνήμης με SD κάρτα ή κάποιο memory usb stick.

**Εμφάνιση**

Γενικά, το PRS-950 μοιάζει αρκετά με το PRS-900, αλλά υπάρχουν μερικές μικρές διαφορές. Αρχικά, το PRS-950 κυκλοφορεί σε ασημένιο χρώμα ενώ το 900 σε μαύρο. Το 900 έχει κατασκευαστεί μέσα σε μία θήκη και το πίσω μέρος του ήταν το πίσω μέρος της θήκης. Το 950 όμως, δεν περιέχεται σε θήκη και το πίσω μέρος του είναι μεταλλικό όπως και το μπροστινό μέρος και δεν μπορεί να αφαιρεθεί τόσο εύκολα ώστε κάποιος να έχει πρόσβαση στην μπαταρία.

Το 950 σε σχέση με τον προκάτοχο του PRS-900 είναι λίγο πιο ελαφρύ. Είναι 25% ελαφρύτερο. Και επίσης, είναι λεπτότερο και κοντύτερο.

**Web Browser**

Το PRS-950 είναι ο πρώτος η-αναγνώστης της Sony που περιέχει web browser. Ο web browser δουλεύει πάνω σε Wi-Fi, αλλά όχι 3G, δίκτυα και είναι αρκετά καλός για ιστοσελίδες με κείμενα και ιστοσελίδες σχεδιασμένες για κινητές συσκευές.

Υπάρχει μενού για χρησιμοποιήσει σελιδοδεικτών και επιλογή. Τα κουμπιά που χρησιμοποιούνται για την αλλαγή των σελίδων κατά το διάβασμα δουλεύουν για την πλοήγηση επόμενων ή προηγούμενων ιστοσελίδων. Δεν υπάρχει επιλογή για μεγέθυνση.

## 6.4 Kobo eReaders

Οι Kobo eReaders είναι ηλεκτρονικοί αναγνώστες κατασκευασμένοι από την εταιρία Kobo Inc η οποία εδρεύει στο Toronto του Καναδά. Η πρώτη έκδοση παρουσιάστηκε τον Ιούλιου του 2010 και διαφημίστηκε ως κάτι εναλλακτικό σε σχέση υπάρχοντα που ήταν διαθέσιμα τότε.

**Ιστορική αναδρομή**

Η εταιρία Kobo Inc. ανακοίνωσε το πρώτο της ηλεκτρονικό αναγνώστη την 1 Μαρτίου του 2010. Είχε μία επεκτάσιμη μνήμη, μία επιπλέον 4GB SD κάρτα μνήμης και περιορισμένη συνδεσιμότητα μέσω Bluetooth για να συνδέεται με άλλες blackberry συσκευές. Ήταν διαθέσιμο σε μαύρο και άσπρο χρώμα και υπήρχαν προ-εγκατεστημένα εκατό βιβλία.

Όμως, οι παρουσιάσεις που κάνανε για αυτό τον η-αναγνώστη ήτανε αρκετά μέτριες, η έλλειψη Wi-Fi ή 3G το έκαναν να είναι αρκετά κατώτερο σε σχέση με το συναγωνισμό. Έτσι το αρχικό Kobo διακόπηκε.

Στις 15 Οκτωβρίου του 2010 άρχισε να πωλείται ένα νέο μοντέλο με δυνατότητα Wi-Fi. Στην παρακάτω υποενότητα θα αναλυθεί επαρκή το συγκεκριμένο μοντέλο.

### *6.4.1 Kobo Wireless e-Reader*


ΕΙΚΟΝΑ15: KOBO WI-FI EREADER

Το Kobo Wireless e-Reader είναι ένα τεράστιο βήμα προς τα εμπρός για την Kobo σε σχέση με το αρχικό Kobo e-Reader. Το νέο μοντέλο υποστηρίζει ασύρματη δικτύωση με την οποία

επιτρέπεται στον χρήστη να κάνει τις αγορές του μέσω του ηλεκτρονικού μαγαζιού της Kobo, και έρχεται με νέα χαρακτηριστικά όπως το ενσωματωμένο λεξικό της "Webster".

**Χαρακτηριστικά**

Το Kobo Wireless e-Reader έχει μία 6 ιντσών E Ink Vizplex οθόνη με 16 επίπεδα grayscale και με ανάλυση 600x800pixels. Το αρχικό kobo είχε μόνο 8 επίπεδα grayscale. Οπότε η αντίθεση και η ανάλυση είναι αρκετά καλύτερη για να προβληθούν εξώφυλλα και το διάβασμα θα είναι πιο ευχάριστο. Επίσης, ο κεντρικός επεξεργαστής έχει αναβαθμιστεί σε σχέση με του αρχικού kobo, οι αλλαγές στις σελίδες γίνονται δύο φορές γρηγορότερα. Το Kobo Wireless e-Reader έρχεται με 1GB εσωτερική μνήμη και μπορεί να επεκταθεί μέσω καρτών SD μέχρι και 4GB.

Ένα από τα νέα χαρακτηριστικά είναι ότι υποστηρίζει Wi-Fi 802.11 b/g συνδεσιμότητα . Αυτό επιτρέπει να γίνουν αγορές από το ηλεκτρονικό κατάστημα της Kobo και να διαβάσεις τις καθημερινές εφημερίδες ασύρματα. Το Wi-Fi υποστηρίζει και τοπικά ασύρματα δίκτυα τα οποία είναι ελεύθερα προς χρήση ή είναι αποκρυπτογραφημένα με αποκρυπτογράφηση WEP. Τέλος, η μπαταρία μπορεί να κρατήσει σχεδόν δύο εβδομάδες ή αλλιώς 10.000 αλλαγές σελίδων αν το Wi-Fi είναι απενεργοποιημένο.

**Ηλεκτρονικά Βιβλία και παράδοση**

Στο Kobo Wi-Fi e-Reader έχει βελτιωθεί αρκετά ο τρόπος στην αγορά ηλεκτρονικών βιβλίων από το ηλεκτρονικό κατάστημα της Kobo. Για να μπορεί κάποιος να αγοράσει η-βιβλία θα πρέπει αρχικά να δημιουργήσει ένα λογαριασμό(account) στην ιστοσελίδα της Kobo το οποίο όμως δεν μπορεί να γίνει μέσω του Kobo Wi-Fi e-Reader αλλά μόνο από κάποιον ηλεκτρονικό υπολογιστή ή laptop. Όταν ο λογαριασμός είναι πλέον δημιουργημένος, εισάγεται στον ηλεκτρονικό αναγνώστη και μπορεί ο χρήστης να έχει πρόσβαση στα η-βιβλία και στα περιοδικά.

Το καλύτερο πρότυπο η-βιβλίων που υποστηρίζει αυτή τη στιγμή ο η-αναγνώστης είναι το ePUB. Το Kobo Wi-Fi e-Reader έχει πέντε διαφορετικές γραμματοσειρές για τα η-βιβλία, ώστε ο χρήστης να μπορεί να αυξήσει ή να μειώσει το μέγεθος του κειμένου ανάλογα τις ανάγκες του.

Το γραφικό περιβάλλον για την αγορά των η-βιβλίων μέσω του ηλεκτρονικού καταστήματος της Kobo είναι πολύ απλό προς τη χρήση του. Τα η-βιβλία είναι ταξινομημένα κατά κατηγορίες και επίσης υπάρχει και μία λίστα με τα 50 πρώτα σε πωλήσεις.

Τέλος, ένα νέο αρκετά καλό χαρακτηριστικό είναι ότι μπορείς να γραφτείτε στην υπηρεσία διανομής ψηφιακών εφημερίδων της Kobo. Με αυτή την υπηρεσία ο χρήστης μπορεί να διαβάσει τις καθημερινές εφημερίδες της περιοχής του. Η πρώτη διανομή είναι δωρεάν για να τη δοκιμάσει ο χρήστης έπειτα η συνδρομή είναι $14.99 ανά μήνα . Η υπηρεσία αυτή είναι διαθέσιμη μόνο για τις Η.Π.Α και τον Καναδά.

**6.5 Bookeen e-Readers**

Bookeen είναι μία γαλλική εταιρία που κατασκευάζει ηλεκτρονικούς αναγνώστες. Το 2003 μετά την αποτυχία της εταιρίας Cytale, της πρώτης ευρωπαϊκής εταιρείας στην κατασκευή ηλεκτρονικών αναγνωστών κάποια πρώην μέλη της αγόρασαν τα πνευματικά δικαιώματα της ηλεκτρονικής συσκευής ανάγνωσης βιβλίων , το Cybook Gen 1. Έπειτα, ιδρύσαν, την εταιρία Bookeen, για να αναπτύξουν τους δικούς η-αναγνώστες. Το πρώτο τους προϊόν ήταν το Cybook Gen 1.

Το Cybook Gen 1ήταν εξολοκλήρου φτιαγμένο από την Bookeen. Όταν, οι οθόνες E Ink παρουσιαστήκαν και ισχυριζόταν ότι οι τεχνολογία τους έμοιαζε τόσο με το πραγματικό χαρτί που δεν κούραζε τα μάτια, η Bookeen υιοθέτησε την τεχνολογία της E Ink.Το 2007 άρχισε να πουλάει το Cybook Gen, τον πρώτο τους ηλεκτρονικό αναγνώστη με E-Ink οθόνη.

Το 2009 παρουσίασαν το Cybook Opus, μία μικρότερη έκδοση του Cybook Gen 3 αλλά με περισσότερες βελτιώσεις. Ενώ τον Οκτώβριο του 2010 παρουσίασαν το Cybook Orizon. Λεπτομερής ανάλυση θα γίνει στις δύο παρακάτω υποενότητες.

### *6.5.1 Cybook Opus*


ΕΙΚΟΝΑ16: CYBOOK OPUS

Το Cybook Opus είναι ένας αρκετά ποιοτικός ηλεκτρονικός αναγνώστης από την εταιρία Bookeen. Ο ηλεκτρονικός αναγνώστης είναι αρκετά γνωστός κυρίως στην ευρωπαϊκή αγορά. Στην Αμερική δεν λαμβάνει τόσο μεγάλη δημοσιότητα λόγο κυρίως των ανταγωνιστών του όπως το Amazon Kindle και τους νέους ηλεκτρονικούς αναγνώστες της Sony.

Λειτουργεί με της Adobe Digital Editions και υποστηρίζει προστατευμένα με DRM τα πρότυπα ePUB και PDF και την επιλογή για αναβάθμιση του firmware για την υποστήριξη και του πρότυπου MobiPocket αλλά αυτόματα χάνεται η υποστήριξη των άλλων δύο.

**Χαρακτηριστικά**

Το Cybook Opus διαφημίζεται σαν έναν ηλεκτρονικό αναγνώστη τσέπης. Έχει 5 ιντσών E Ink οθόνη και ζυγίζει 150 γραμμάρια. Είναι σχεδιασμένο για να εφαρμόζει και στα δύο χέρια άνετα και η μπαταρία του κρατάει για σχεδόν 8000 αλλαγές σελίδων.

Το πιο μοναδικό χαρακτηριστικό του είναι ο G-sensor αισθητήρας που διαθέτει ο οποίος ανιχνεύει αυτόματα και γυρίζει το κείμενο όταν η συσκευή είναι πλαγίως γυρισμένη, η αλλαγή γίνεται αρκετά γρήγορα και είναι ιδιαίτερα χρήσιμο για το διάβασμα PDF αρχείων.

Επίσης υπάρχει η δυνατότητα να μετατραπεί η συσκευή εντελώς ανάποδα για τους χρήστες που είναι αριστερόχειρες, όταν γίνεται αυτό τα κουμπιά αλλάζουν θέση και αυτά ώστε να βολεύουν και αυτά.

Υπάρχουν δώδεκα διαφορετικές γραμματοσειρές για να μειώσουν ή αν αυξήσουν το μέγεθος του κειμένου. Επίσης μπορεί κάποιος να αλλάξει την γραμματοσειρά σε txt και html αρχεία αλλά όχι και σε ePUB.

Για την οργάνωση υπάρχουν αρκετές επιλογές για την εμφάνιση του μενού. Μπορεί ο χρήστης να διαλέξει πόσα βιβλία να προβάλλονται, πως να προβάλλονται και πως να είναι ταξινομημένα.

**Ηλεκτρονικά Βιβλία και πρότυπα**

Ανάλογα με το firmware που θα διαλέξει ο χρήστης, μπορεί να αγοράσει προστατευμένα η-βιβλία σε PDF ή ePUB μορφή από διάφορα ηλεκτρονικά καταστήματα που υπάρχουν στο διαδίκτυο.

Αν πάλι διαλέξει η συσκευή να υποστηρίζει MobiPocket αρχεία μπορεί να πάει στην ιστοσελίδα MobiPocket και να διαλέξει από τους 120.000 τίτλους που υπάρχουν διαθέσιμοι.

Το Opus υποστηρίζει τα εξής πρότυπα:
Με το firmware για την υποστήριξη MobiPocket αρχείων:

- Mobi με προστασία DRM
- txt αρχεία
- Html
- PDF

ΜΕ το firmware για την υποστήριξη ePub:

- ePUB με προστασία DRM
- PDF
- txt
- Html

Επίσης, υποστηρίζει από τα πρότυπα εικόνων τα jpeg, gif και png.

### *6.5.2 Cybook Orizon*

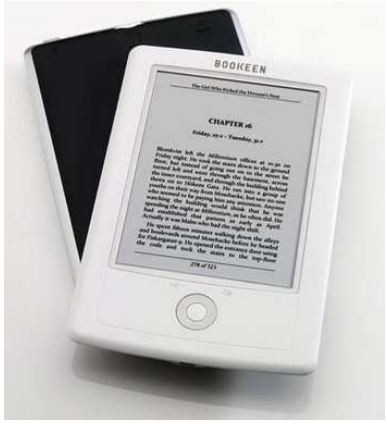
Το Cybook Orizon είναι μια ποιοτική συσκευή, σαφώς αναβαθμισμένη σε σχέση με τους προηγούμενους ηλεκτρονικούς αναγνώστες της Bookeen. Έχει ένα σπάνιο συνδυασμό: ηλεκτρονικά βιβλία σε ePUB, πρόσβαση στο internet με Wi-Fi, αλλά και οθόνη αφής.

**Γενικά**

Η οθόνη αφής είναι πραγματικά κάτι αρκετά άμεσο και βολικό. Δε χρειάζεται να ανοίγει κανείς μενού και υπομενού. Ιδιαίτερα βολική είναι για τα αρχεία PDF, γιατί κάνει το scrolling, τη περιήγηση στη σελίδα ενώ έχει ζουμαριστεί, εύκολο και άμεσο. Είναι από τις καλύτερες εμπειρίες για την ανάγνωση PDF σε οθόνη 6 ιντσών. Και η αφή λειτουργεί ικανοποιητικά, με καλή απόκριση και με έξυπνη εκμετάλλευσή της με shortcuts σε διάφορα σημεία της οθόνης για το μενού, τα bookmarks και τη μετάβαση σε άλλη σελίδα. Οι κινήσεις multi-touch που υποστηρίζονται είναι αρκετές και συμβάλλουν στον πιο άμεσο χειρισμό της συσκευής.

Η οθόνη είναι της SiPix, μια εταιρεία που τον τελευταίο καιρό μπαίνει στο ηλεκτρονικό χαρτί απέναντι στην κυρίαρχη στο χώρο E Ink. Η οθόνη δεν έχει το επίπεδο του contrast που έχουν οι οθόνες Pearl της E Ink, που είναι η τελευταία γενιά οθονών της, αλλά οι Pearl χρησιμοποιούνται μόνο στα Kindle και τους Sony Reader. Σε όλες τις άλλες συσκευές χρησιμοποιούνται οι παλιότερες οθόνες της E Ink, η Vizplex, που βρίσκονται στο ίδιο επίπεδο με τις οθόνες της SiPix. Πάντως, στην πράξη, διαβάζοντας με το Cybook Orizon δεν προβληματίζει η οθόνη ή το contrast. Με το επόμενο firmware update μάλιστα θα μπορούμε να κάνουμε πιο μαύρα τα γράμματα και έτσι να έχουμε και καλύτερο contrast. Τα bookmarks, η μετάβαση σε άλλες σελίδες, κεφάλαια και υποσημειώσεις γίνεται χωρίς πρόβλημα και με ικανοποιητική ταχύτητα.

Το Cybook Orizon δεν υποστηρίζει σημειώσεις και υπογραμμίσεις και αυτό δεν είναι απαραίτητα μεγάλο πρόβλημα για αρκετούς, αλλά το πρόβλημα είναι ότι η Bookeen είχε ανακοινώσει και διαφημίσει ότι θα τις υποστηρίζει από την αρχή. Το έχει βάλει στις προτεραιότητές της πάντως και στο επόμενο firmware update θα υποστηρίζονται οι υπογραμμίσεις. Σημαντικό έξτρα που θα ήθελα να δω είναι η ενσωμάτωση λεξικών, έστω για τα αγγλικά ή τα γαλλικά.




ΕΙΚΌΝΑ17: CYBOOK ORIZON

**Χαρακτηριστικά**

- Οθόνη ηλεκτρονικού χαρτιού πολλαπλής (multi-touch) αφής της SiPix, 6 ίντσες, 167 dpi, 600 x 800 pixels, 16 επίπεδα αποχρώσεων του γκρι
- Μπαταρία λιθίου-πολυμερών διάρκειας περίπου 2 με 3 εβδομάδων μία πλήρη φόρτιση με το Wi-Fi απενεργοποιημένο.
- Επεξεργαστής Samsung ARM στα 400MHz
- Δυνατότητα αλλαγής μεγέθους και είδους γραμματοσειράς για τα αρχεία ePUB, HTML, TXT και άλλα αρχεία κειμένου. Υπάρχει δυνατότητα ζουμ, αλλά όχι reflow για τα PDF. Μπορείτε να προσθέσετε τις δικές σας γραμματοσειρές.
- Σελιδοδείκτες στα eBookss, υποστήριξη πίνακα περιεχομένων, links μέσα στο βιβλίο προς τις υποσημειώσεις (σημειώσεις και υπογραμμίσεις με το επόμενο firmware update)
- Αισθητήρας κίνησης, προσαρμόζει αυτόματα την οθόνη σε κάθετο ή οριζόντιο προσανατολισμό (g-sensor/accelerometer)
- Διαστάσεις: Ύψος: 189,8 χιλιοστά, Πλάτος: 125,7 χιλιοστά, Πάχος: 7,6 χιλιοστά, Βάρος: 245γρ.
- Εσωτερική μνήμη 2 GB (1.500 έως 2.000 βιβλία), θύρα κάρτας microSDHC (8 GB max, για έως περίπου 8.000 τίτλους), θύρα micro-USB για σύνδεση με τον υπολογιστή (PC ή Mac)
- Υποστηρίζει τα ελληνικά. Διαθέτει εν μέρει ελληνικό μενού, το όνομα του αρχείου μπορεί να είναι στα ελληνικά και μπορείτε να διαβάσετε αρχεία Mobipocket, PDF και αρχεία κειμένου στα ελληνικά (από το Word, το ιντερνέτ και αλλού) χωρίς ενσωματωμένες γραμματοσειρές. Διαβάζονται επίσης τα αρχεία ePUB με ενσωματωμένες τις ελληνικές γραμματοσειρές. (Λόγω αδυναμιών του Adobe Mobile Reader, που έχουν οι περισσότερες συσκευές e-readers, δεν είναι δυνατό να διαβαστούν [εμφανίζεται ένα ? στη θέση κάθε τονισμένου γράμματος] αρχεία ePUB στα οποία δεν είναι ενσωματωμένες οι γραμματοσειρές - αυτό όμως είναι ένα θέμα που αφορά γενικότερα τους ηλεκτρονικούς αναγνώστες, όχι μόνο το Cybook Orizon).
- Ενσωματωμένος browser, σύνδεση στο internet μέσω Wi-Fi (802. 11 b/g/n)
- Υποστηρίζει αρχεία κειμένου: ePUB / PDF (με ή χωρίς Adobe DRM), TXT και αρχεία HTML. Αρχεία εικόνων (ασπρόμαυρες): JPEG, GIF και PNG.
- Γρήγορη εκκίνηση με από τη συσκευή σε αναμονή.

### 6.6 Ηλεκτρονικοί αναγνώστες PocketBook

Η PocketBook είναι μία από τις μεγαλύτερες εταιρίας κατασκευής και πώλησής ηλεκτρονικών αναγνωστών στον πλανήτη. Ιδρύθηκε στο Κίεβο της Ουκρανίας το 2007 και αρχικά επικεντρώθηκε στην ευρωπαϊκή αγορά. Στα μέσα του 2010 έγινε πολυεθνική εταιρία με αντιπροσωπίες στο Χονγκ Κονγκ, στις Η.Π.Α., στη Γερμανία και στη Ρωσία.

Η PocketBook International έχει ενεργή επιχειρηματική παρουσία σε χώρες της Κοινοπολιτείας Ανεξάρτητων Κρατών, στην Ευρωπαϊκή Ένωση, στις Η.Π.Α., στη Μέση Ανατολή και στην Ασία. Τον Ιανουάριο του 2011, η PocketBook International απασχολεί περισσότερα από 150 άτομα. Οι μηνιαίες πωλήσεις ηλεκτρονικών συσκευών PocketBook της εταιρείας ξεπερνούν τα 50.000 τεμάχια. Το μερίδιο αγοράς της PocketBook στις χώρες της Κοινοπολιτείας Ανεξάρτητων Κρατών είναι 43% και το μερίδιό της στη διεθνή αγορά ανέρχεται σε 5%.

#### *6.6.1 Βασικά χαρακτηριστικά Μοντέλων.*

Η PocketBook έχει δημιουργήσει αρκετά μοντέλα για την ανάγνωση των ψηφιακών βιβλίων, απ' τα οποία τα περισσότερα χρησιμοποιούν E-Ink τεχνολογίας οθόνες. Η μεταφορά των βιβλίων γίνεται πολύ εύκολα. Απλά συνδέοντας την συσκευή στον ηλεκτρονικό υπολογιστή μέσω της θύρας USB, ο υπολογιστής αναγνωρίζει την συσκευή σαν χώρο αποθήκευσης. το οποίο επιτρέπει την μεταφορά ηλεκτρονικών βιβλίων στον ηλεκτρονικό αναγνώστη.

Ένα δυνατό χαρακτηριστικό των ηλεκτρονικών αναγνωστών PocketBook, είναι ότι υποστηρίζουν πάρα πολλά πρότυπα ψηφιακών μέσων.

Τα πρότυπα για τα η-βιβλία που υποστηρίζουν είναι: CHM, DJVU, DOCX, EPUB,FB2, PDF, MOBI, RTF, TRC, TXT. Επίσης, υποστηρίζει τα πρότυπα ePUB και PDF με προστασία DRM. Για τον ήχο μπορεί να "τρέχει" αρχεία τύπου Mp3 και σε μερικά μοντέλα και τα AAC και WMA. Τα PocketBook μπορούν να τρέξουν και βίντεο της μορφής 3GP, AVI και MP4. Τέλος, μπορεί να προβάλει εικόνες πρότυπου jpeg, png, tiff και bmp.

### *6.6.2 Παρουσίαση Μοντέλων*

Η σειρά των ηλεκτρονικών αναγνωστών από την PocketBook είναι μεγάλη. Για το λόγο αυτό θα αναφέρουμε ονομαστικά όλα τα μοντέλα της και έπειτα θα ακολουθήσει αναλυτική παρουσίαση του τελευταίου μοντέλου που έχουν κυκλοφορήσει το PocketBook IQ 701.

Όλα τα μοντέλα της είναι:

- PocketBook 301
- PocketBook 302
- PocketBook 360
- PocketBook Pro 602
- PocketBook Pro 603
- PocketBook Pro 902
- PocketBook Pro 903
- PocketBook IQ 701

### *6.6.3 PocketBook IQ 701*

ΕΙΚΟΝΑ18: POCKETBOOK IQ 701

Με την 7 ιντσών οθόνη του το PocketBook IQ είναι τόσο ένας ηλεκτρονικός αναγνώστης όσο και έναν προσωπικός υπολογιστής tablet. Περιέχει το λειτουργικό σύστημα της Google το Android τροποποιημένο από την PocketBook για διάβασμα και κατέβασμα ηλεκτρονικών βιβλίων από το δικό τους ηλεκτρονικό μαγαζί, το Bookland.net, επίσης υπάρχει και η ιδιότητα εγκατάστασης προγραμμάτων τρίτων κατασκευαστών (3rd party programs), συμπεριλαμβανομένου των Kindle, Kobo, Aldiko, Borders και μια τεράστια πληθώρα που προσφέρει το Android.

**Χαρακτηριστικά και λειτουργίες.**

Μιας και στο PocketBook IQ μπορούν να εγκατασταθούν προγράμματα, δεν είναι περιορισμένο μόνο για το διάβασμα ψηφιακών μέσων. Υπάρχουν προγράμματα για σχεδόν τα πάντα. Μπορεί κάποιος να στείλει και να λάβει e-mails, να το χρησιμοποιήσει σαν ημερολόγιο, να πλοηγηθεί στο internet, να κατεβάσει και να στείλει αρχεία, να χρησιμοποιήσει την εφαρμογή Google Maps, να κατεβάσει αναβαθμίσεις του λειτουργικού, να παίξει μουσική ή βίντεο αλλά και πάρα πολλά άλλα.

Έρχεται με 2GB μνήμη αποθήκευσης, 256MB RAM και έχει και θύρα για SD κάρτες μέχρι 32GB. Επίσης, υπάρχει mini USB θύρες, 2 ηχεία και μικρόφωνο. Η μπαταριά κρατάει γύρω στις 5-8 ώρες, ανάλογα με την χρήση.

Το PocketBook IQ έχει μία 7 ιντσών οθόνη TFT LCD με ανάλυση 800x480. Η οθόνη είναι αρκετά ακριβείς και ευέλικτη. Ακόμα και πατήματα σε μικρές περιοχές όπως σε συνδέσμους δεν υπάρχει κανένα πρόβλημα.

**Το PocketBook IQ σαν ένας ηλεκτρονικός αναγνώστης,**

Αν κάποιος δεν έχει πρόβλημα να διαβάσει σε μία LCD οθόνη, τότε το PocketBook IQ είναι ένας φοβερός ηλεκτρονικός αναγνώστης. Αυτό γιατί του επιτρέπεται να εγκαταστήσει προγράμματα που βοηθούν και καλυτερεύουν την ανάγνωση ψηφιακών μέσων.

Η εφαρμογή της PocketBook για το διάβασμα ηλεκτρονικών βιβλίων περιέχει αρκετά χαρακτηριστικά αλλά χρειάζεται ακόμα δουλεία. Δεν υποστηρίζει DRM αρχεία μέχρι να αναβαθμίσουν το firmware και δεν υπάρχουν και πολλές επιλογές για να διαμορφώσει ο χρήστης το γραφικό περιβάλλον.

Η συσκευή περιλαμβάνει: λεξικό, σημειωματάριο, πίνακα περιεχομένων, μετάβαση στην σελίδα, αναζήτηση και κατάσταση για νυχτερινό διάβασμα. Η γραμματοσειρά μπορεί να αλλάξει από το 12 μέχρι το 36.

**Συμπέρασμα**

Το PocketBook IQ είναι ένας ηλεκτρονικός αναγνώστης αλλά και ένα tablet pc. Με την ιδιότητα να κατεβάζει και να προβάλει η-βιβλία από τα μεγαλύτερα ηλεκτρονικά μαγαζιά. Είναι πιο ευπροσάρμοστο απ' ότι ένας κανονικός η-αναγνώστης, συν όλα τα δωρεάν προγράμματα που είναι διαθέσιμα για αυτόν. Αλλά ένα χαρακτηριστικό που ίσως να προβληματίσει κάποιους είναι η οθόνη και η αυτονομία της μπαταρίας. Θα υπάρχουν προβλήματα αντανάκλασης για όσους προσπαθήσουν να διαβάσουν σε εξωτερικούς χώρους.

### 6.7 BeBook eBook Readers

Οι ηλεκτρονικοί αναγνώστες BeBook μία "μετατρεπομένη" έκδοση των κινέζικων η-αναγνωστών HanLin και Onyx. Χρησιμοποιούν ακριβώς τα ίδια υλικά κατασκευής με τους HanLin και Onyx, αλλά έχουν διαφορετικές εκδόσεις firmware εγκατεστημένες. Η εταιρία που τα εισάγει ονομάζεται Endless Ideas, εδρεύει στην Ολλανδία και πουλάει τις συσκευές τις σε ολόκληρο τον κόσμο.

Το χαρακτηριστικό που κάνει αυτές τις συσκευές να ξεχωρίζουν είναι η προσβασιμότητα τους. Υποστηρίζουν πάνω από 20 διαφορετικές γλώσσες και πρότυπα αρχείων. Είναι πολύ δύσκολο κάποιος χρήστης να βρει κάποιο διάσημο βιβλίο σε μορφή που να μην υποστηρίζει. Mp3 και audiobooks υποστηρίζονται επίσης, όπως και διάφορα αρχεία κειμένου και αρχεία εικόνων.

#### *6.7.1 BeBook Neo Wi-Fi*

ΕΙΚΟΝΑ19: BEBOOK NEO

Το BeBook Neo είναι ο πιο ολοκληρωμένος ηλεκτρονικός αναγνώστης της σειράς BeBook της ολλανδικής εταιρείας Endless Ideas. Έχει οθόνη αφής από ηλεκτρονικό χαρτί και λειτουργεί με γραφίδα ή από τις επιλογές του κεντρικού κουμπιού 5 κατευθύνσεων. Υποστηρίζει σημειώσεις τόσο με εικονικό πληκτρολόγιο όσο και με ελεύθερο χέρι. Συνδέεται στο internet μέσω Wi-Fi, με δυνατότητα περιήγησης σε πλήρεις σελίδες του web, όχι μόνο στη mobile εκδοχή τους. Η μπαταρία διαρκεί εβδομάδες, ενώ το βάρος περιορίζεται στα 298 γραμμάρια

Αυτό που ξεχωρίζει στη συσκευή, όπως και γενικότερα στα BeBook, είναι η υποστήριξη μεγάλου αριθμού αρχείων. Έτσι, στο BeBook Neo πέρα από τα αναμενόμενα κλειδωμένα και ξεκλείδωτα ePUB και PDF διαβάζονται επίσης αρχεία DJVU, αρχεία παραπλήσια με τα PDF, αλλά ελαφρύτερα.

Η οθόνη αφής συμβάλει στη μετάβαση ευκολότερα σε διαφορετικά σημεία της ίδιας σελίδας (scrolling)σε ένα PDF ή στο internet. Για τα PDF ειδικά διαθέτει και reflow, έτσι ώστε τα PDF κειμένου να μπορούν όχι μόνο να ζουμαριστούν, αλλά να αυξομειωθεί και το μέγεθος της γραμματοσειράς τους (λειτουργία αντίστοιχη με την αλλαγή μεγέθους γραμματοσειράς στα ePUB, αλλά με επιπτώσεις στη μορφοποίηση της σελίδας). Η οθόνη του είναι η Vizplex της Eink,

**Τεχνικά Χαρακτηριστικά**

- Οθόνη αφής τεχνολογίας Wacom, η οθόνη είναι ηλεκτρονικό χαρτί Vizplex της E Ink, 6 ίντσες, ανάλυση 600 x 800 pixels, 16 επίπεδα αποχρώσεων του γκρι, κατακόρυφος και οριζόντιος προσανατολισμός
- Επεξεργαστής 532 MHz Freescale, 128 MB RAM
- Διαστάσεις: 196 χιλιοστά (ύψος) x 121 χιλιοστά (πλάτος) x 10,6 χιλιοστά (πάχος).
- Εσωτερικός αποθηκευτικός χώρος: 512MB μνήμη flash, 310 MB για αποθήκευση βιβλίων.
- Τροφοδοσία: μπαταρία Li-Ion 1600mAh, 7.000 γυρίσματα σελίδας,
- Θύρα micro USB για σύνδεση με τον υπολογιστή για φόρτιση και μεταφορά αρχείων
- Υποστηριζόμενα αρχεία: ePUB και PDF με και χωρίς κλείδωμα Adobe DRM, DJVU, TXT, HTML, RTF, MOBI (χωρίς κλείδωμα), FB2, CHM, PDB. Ανάγνωση ePUB στα ελληνικά και χωρίς ενσωματωμένες γραμματοσειρές. Αρχεία κόμιξ: CBR, CBZ. Αρχεία εικόνας: JPG, PNG, GIF, BMP, TIFF. Αρχεία ήχου: MP3
- Text-to-speech (ανάγνωση του κειμένου από τη συσκευή, δεν υποστηρίζεται για τα ελληνικά).
- Δυνατότητα αλλαγής μεγέθους και είδους γραμματοσειράς για τα αρχεία ePUB, HTML, TXT και άλλα αρχεία κειμένου. Υπάρχει δυνατότητα ζουμ και reflow για τα PDF.
- Ενσωματωμένος browser, σύνδεση στο internet μέσω Wi-Fi. Πρόσβαση σε online βιβλιοπωλεία για e-books.

**6.8 Πως να διαλέξεις τον καλύτερο έναν Ηλεκτρονικό Αναγνώστη.**

Οι ηλεκτρονικοί αναγνώστες είναι μία τεχνολογία που αναπτύσσεται αλματωδώς. Η επιλογή ενός είναι αρκετά δύσκολη. Καθημερινά εμφανίζεται και ένα νέο διαφορετικό μοντέλο στην αγορά.

Όλοι υπόσχονται να κάνουν σωστή προβολή κειμένου ειδικά των η-βιβλίων. Αλλά υπάρχουν και μερικές άλλες βασικές απαιτήσεις . Πρέπει να προσφέρουν μεγάλη διάρκεια ζωής. να έχουν οθόνη που να μην κουράζει τα μάτια και να μπορεί εύκολα να διαβαστεί από οποιοδήποτε μέρος, συμπεριλαμβανομένου. Ευτυχώς, οι περισσότεροι ηλεκτρονικοί αναγνώστες σήμερα διαθέτουν αυτά τα χαρακτηριστικά.

Σε αυτή την ενότητα αναλυθεί, ποιά χαρακτηριστικά πρέπει να προσέξει κάποιος από την αγορά πριν κάποιου ηλεκτρονικού αναγνώστη ώστε να κάνει την καλύτερη επιλογή.

**Τιμή**

Η τιμή είναι ένα βασικό χαρακτηριστικό που πρέπει να γνωρίζει κάποιος πριν να αγοράσει ένα eBook reader. Ως προς την τιμή το Amazon Kindle και το Kobo eReader είναι αυτά με την χαμηλότερη τιμή  τα οποία προσφέρουν και σύνδεση Wi-Fi.

**Μέγεθος και Βάρος**

Το βάρος και το μέγεθος, ίσως να μην είναι ένα από τα κριτήρια για  αγοράς για όλους τους χρήστες. Αλλά αν κάποιον τον ενδιαφέρει, μπορεί να το συγκρίνει διάφορες συσκευές μεταξύ τους. Μερικοί χρήστες προτιμούν μικρότερες συσκευές και άλλοι μεγαλύτερες.  Οι περισσότεροι ηλεκτρονικοί αναγνώστες είναι αρκετά ελαφριοί, γύρω στα 150-600 γραμμάρια. Ένα κανονικό χάρτινο βιβλίο ζυγίζει γύρω στα 300 γραμμάρια, μπορεί να χρησιμοποιήσει κάποιος αυτό σαν οδηγό για την αγορά του.

**Μέγεθος και Τύπος οθόνης**

Η ποιότητα προβολής του ηλεκτρονικού αναγνώστη είναι αρκετά σημαντική. Σήμερα τα πιο πολλά eReaders έχουν 6 ή 7 ιντσών και υπάρχουν ελάχιστα με 9 ιντσών οθόνη.

Συσκευές όπως οι  Kindle, Kobo, Sony Reader, Nook, and BeBook έχουν E-Ink οθόνες. Αυτές οι οθόνες προσφέρουν άνετα διάβασμα σε οποιοδήποτε μέρος βρίσκεται ο χρήστης, ακόμα και κάτω από το φως του ήλιου και καταναλώνουν ελάχιστη ενέργεια.

Συσκευές όπως οι Pandigital Novel και the Nook Color έχουν LCD οθόνες. Αυτές είναι σαν τις οθόνες που έχουν οι σημερινοί υπολογιστές laptop. Οι οθόνες αυτές είναι αρκετά κουραστικές όταν κάποιος διαβάζει με αυτές κάτω από το φως του ήλιου, αφού αντανακλούν την ακτινοβολία. Επίσης, καταναλώνουν αρκετή μπαταρία.

**Αρχεία που υποστηρίζονται**

Αυτό είναι αρκετά σημαντικό, προσδιορίζει το τύπο των ηλεκτρονικών βιβλίων όπου ηλεκτρονική συσκευή θα μπορεί να διαβάσει. Υπάρχουν συσκευές που υποστηρίζουν αρκετά πρότυπα ώστε κάποιος να μπορεί να διαβάσει όποιο βιβλίο θέλει σε οποιοδήποτε πρότυπο το βρει. Αλλά, υπάρχουν και συσκευές όπου υποστηρίζουν συγκεκριμένα πρότυπα και τα η-βιβλία μπορούν να αγοραστούν από συγκεκριμένες ιστοσελίδες.  Τέτοιες συσκευές είναι οι Kindle και το Nook.

Μερικοί ηλεκτρονικοί αναγνώστες επίσης παίζουν μουσική MP3. Το οποίο ίσως να είναι σημαντικό για κάποιους αγοραστές.

**Μνήμη**

Η μνήμη της συσκευής είναι και αυτό ένας αρκετά σημαντικός παράγοντας. Όλα τα ηλεκτρονικά βιβλία που είναι εγκατεστημένα στη συσκευή αποθηκεύονται στη μνήμη οπότε η μνήμη πρέπει να είναι αρκετά μεγάλη για να μπορούν αν αποθηκευτούν αρκετά eBooks. Συνήθως η μνήμη ενός ηλεκτρονικού αναγνώστη είναι στα 2- 4GB περίπου από τα 600-700MB χρησιμοποιούνται από το λειτουργικό σύστημα. Βέβαια, υπάρχει και η επιλογή, αν ο eBook reader διαθέτει θύρες SD, να επεκταθεί η μνήμη με κάρτες SD μέχρι και 32GB.

**Wi-Fi ή 3G**

Wi-Fi και 3G ονομάζεται ο τρόπος ασύρματης συνδεσιμότητας. Το Wi-Fi μπορεί να χρησιμοποιηθεί στο σπίτι ή σε σημεία όπου παρέχουν ασύρματο δίκτυο. Το 3G χρησιμοποιεί το ίδιο δίκτυο με τα κινητά τηλέφωνα, οπότε όπου υπάρχει διαθέσιμο δίκτυο κινητής τηλεφωνίας μπορεί και ο χρήστης να συνδεθεί με τον eBook reader του. Και τα δύο πρότυπα προσφέρουν ασύρματη σύνδεση στο internet ώστε ο χρήστης να μπορεί να αγοράσει και να "κατεβάσει" στην συσκευή του όποιο ηλεκτρονικό βιβλίο θέλει. Βέβαια στην Ελλάδα το 3G είναι αρκετά ακριβό, συνεπώς πολύ χρήστες κοιτάζουν συνήθως ο ηλεκτρονικός αναγνώστης να υποστηρίζει Wi-Fi συνδεσιμότητα.

**Σχέδιο (Design)**

Το τι σχέδιο θα διαλέξει κάποιος είναι καθαρά στην κρίση του αγοραστή. Αλλά καλό θα ήταν πριν γίνει η αγορά να γίνει ένας έλεγχος, ώστε να δοκιμάσει ο χρήστης αν η συσκευή βολεύει για την χρήση ενός ηλεκτρονικού αναγνώστη . Πχ να ελέγχει αν τα κουμπιά εξυπηρετούν στο σημείο που είναι τοποθετημένα, την υφή και γενικά την αίσθηση που δίνει κατά το διάβασμα. Η ποιότητα κατασκευής της συσκευής είναι σημαντικός παράγοντας.

Αυτά ήτανε τα χαρακτηριστικά που ο χρήστης θα πρέπει να προσέξει και να μελετήσει πριν από την αγορά κάποιου ηλεκτρονικού αναγνώστη αν και την τελευταία λέξη την έχει αγοραστής ανάλογα με την επιλογή που θα κάνει.

**6.9 Πίνακας σύγκρισης ηλεκτρονικών συσκευών.**

Στον παρακάτω πίνακα εμφανίζονται τα χαρακτηριστικά των μοντέλων που έγινε παρουσίαση πιο πάνω και επίσης υπάρχουν τα θετικά και αρνητικά για την κάθε συσκευή.

| Μοντέλο | Amazon Kindle 3 | Amazon Kindle Dx | B&N Nook | Sony PRS-950 | Kobo eReader Wi-Fi | Cybook Opus | PocketBook IQ 701 | BeBook Neo |
|---|---|---|---|---|---|---|---|---|
| Κατ/στης | Hon Hai Precision Industries | Hon Hai Precision Industries | Barnes &Noble | Sony | Netronix | Bookeen | PocketBook | Endless Ideas |
| Φωτο/φίες |  |  |  |  |  |  |  |  |
| Μέγεθος οθόνης | 6" | 9.7" | 6" | 7" | 6" | 5" | 7" | 6" |
| Ασύρματο δίκτυο | 3G, Wi-Fi | 3G | 3G, Wi-Fi | 3G, Wi-Fi | Wi-Fi | Όχι | Wi-Fi | Wi-Fi |
| Οθόνη Αφής | Όχι | Όχι | Ναι | Ναι | Όχι | Όχι | Ναι, LCD οθόνη | Ναι |
| Μνήμη | 4GB | 4GB | 2GB, θύρα για κάρτα Micro SD | 2GB, θύρα για κάρτα SD και Pro Duo | 1GB, θύρα για κάρτα Micro SD | 1GB, θύρα για κάρτα Micro SD | 2GB, θύρα για κάρτα Micro SD | 512MB, θύρα για κάρτα SD |
| Πρότυπα | AZW,PDF, TXT,MOBI, PRC,AAX, AA,MP3 | AZW, PDF, TXT, MOBI, PRC, AAX, AA, MP3 | EPUB, PDF, PDB, JPG, GIF, PNG, BMP, MP3 | EPUB, PDF, TXT, RTF, LRF, DOC, JPG, GIF, PNG, BMP, AAC, MP3 | EPUB, PDF, TXT | ePUB ή MOBI, PRC, PDF,HTML, TXT,JPG, GIF,PNG | EPUB, PDF, HTML, DJVU, RTF, TXT, PRC, DOC, TCR, FB2, ZIP, περισσότερα μέσω εφαρμογών για Androids | EPUB, PDF, TXT, HTML, RTF, MOBI, CHM, PDB, JPG, PNG, GIF, BMP, TIFF |
| Ήχος | Ηχεία, Ακουστικά, TTS | Ηχεία, Ακουστικά, TTS | Ηχεία, Ακουστικά | Ακουστικά | Όχι | Όχι | Ηχεία, Ακουστικά | Ακουστικά |
| Μπαταρία | 4εβδομαδες με το wi-fi κλειστό, 10 μέρες αν είναι ανοιχτο | 7-14 μέρες/ 7500 Σελίδες | 4-10 Μέρες | 10-22 Μέρες | 10000 Σελίδες | 8000 Σελίδες | 6-8 Ώρες | 7000 Σελίδες |
| Λεξικό | Ναι | Ναι | Ναι | Ναι | Ναι | Όχι | Ναι | Ναι |
| Θετικά | Μεγάλη αντίθεση οθόνης, WebKit browser, φτηνά η-βιβλία, TSS, Wi-Fi | 9.7" οθόνη, φτηνά η-βιβλία, TSS, Wi-Fi. αυτόματη γύρισμα της οθόνης πλάγια | Οθόνη, Λειτουργικό Android, LCD οθόνη, αλλαγή γρα/σειρών στάλσιμο η-βιβλίων, web browser, Wi-Fi | 7.1" Pearl οθόνη, Αναβαθμισμένη αντίθεση, μεγέθυνση PDF, web browser, οθόνη αφής, πολύ γρήγορο. | Χαμηλή τιμή, Υποστηρίζει της Adobe το DRM, 100 δωρεάν βιβλία προεγκατεστη-μένα, ημερήσιες εφημερίδες | Αυτόματη περιστροφή της οθόνης, αλλαγή γραμματοσειράς -12 μεγέθη διαθέσιμα, υποστηρίζει DRM MOBI | 7" οθόνη, λειτουργικό Android, αρκετές εφαρμογές μέσω Android, 2 χρόνια εγγύηση | Υποστηρίζει αρκετά eBook ηλεκτρονικά μαγαζιά. web browser, σημειώσεις. οθόνη αφής.Wi-Fi |
| Αρνητικά | Δεν υποστηρίζει ePUB, όχι δωρεάν βιβλία | Δεν υποστηρίζει ePUB, όχι δωρεάν βιβλία, το πληκτρολόγιο δεν λειτουργεί αρκετά καλά | Μπαταρία, προβολή PDF, Αρκετά βαρύ | Χρειάζεται στυλό για την οθόνη, το βίντεο είναι αργό και κολάει, φτηνά υλικά κατασκευής | Πολύ βασικός η-αναγνώστης Δεν υποστηρίζει Σελιδοδείκτες σημειώσεις, δεν προβάλει EPUB όταν είναι πλάγια. | Μερικές φορές η συσκευή κολάει και χρειάζεται επανεκκίνηση, δεν υποστηρίζει την χρήση σελιδοδεικτών. | Αργό Βίντεο, ζωή μπαταρίας | Δεν υπάρχει θήκη, αργή πλοήγηση στο internet, χρειάζεται στυλό για την οθόνη, Τεχνική υποστήριξη |

Πίνακας 3: Σύγκριση ηλεκτρικών αναγνωστών και τα θετικά - αρνητικά του καθενός.

# ΚΕΦΑΛΑΙΟ 7

## Ψηφιακή Διαχείριση Δικαιωμάτων

### 7.1 Ορισμός του DRM

Από άποψη λειτουργικότητας, το DRM σύστημα σημαίνει πολλά διαφορετικά πράγματα. Για κάποιους είναι απλά μια τεχνική διαδικασία προστασίας ψηφιακού περιεχομένου. Για άλλους πρόκειται για μια ολοκληρωμένη διαδικασία υποστήριξης ασφαλών συναλλαγών δικαιωμάτων και περιεχομένου στο Διαδίκτυο. Γι' αυτό συχνά το DRM χωρίζεται σε δύο λειτουργικούς τομείς.

- Την αναγνώριση και περιγραφή της πνευματικής ιδιοκτησίας και διαχείριση των δικαιωμάτων που συνδέονται με έργα και τους δημιουργούς τους (διαχείριση ψηφιακών δικαιωμάτων). Οι κάτοχοι των δικαιωμάτων πρέπει να προσδώσουν αναγνωριστικά στο περιεχόμενο, να παρέχουν μετά-δεδομένα για την περιγραφή του, να καθορίσουν τα δικαιώματα των χρηστών και τους περιορισμούς χρήσης και να διανείμουν το περιεχόμενο.
- Την τεχνική υποστήριξη των περιορισμών χρήσης (ψηφιακή διαχείριση δικαιωμάτων). Διασφαλίζεται ότι το περιεχόμενο χρησιμοποιείται σύμφωνα με τους όρους και περιορισμούς χρήσης που έχουν καθοριστεί από τον κάτοχο δικαιωμάτων.

Επομένως το DRM αναφέρεται στην τεχνολογία και στις διαδικασίες που εφαρμόζονται στο ψηφιακό περιεχόμενο για την περιγραφή και την αναγνώρισή του καθώς και τον καθορισμό, την εφαρμογή και την υποστήριξη των κανόνων χρήσης του με ασφαλή τρόπο.

Όταν δημιουργείται το περιεχόμενο, ένα σύνολο δικαιωμάτων κληρονομείται στον κάτοχο, που του επιτρέπουν να το δει, να το τροποποιήσει, να το εκτυπώσει, να το εκτελέσει, να το αντιγράψει κ.α. Υπάρχουν τρία διαφορετικά είδη δικαιωμάτων:

- Νομικά: Δικαιώματα τα οποία αποκτήθηκαν είτε αυτόματα από τον νόμο, είτε μετά από κάποια νομική διαδικασία (π.χ. υποβάλλοντας μια πατέντα)
- Συναλλακτικά: Δικαιώματα που αποκτά ή δίνει κάποιος μέσω μιας συναλλαγής, π.χ. αγοράζοντας ένα βιβλίο ή πουλώντας ένα χειρόγραφο σε έναν εκδότη.
- Έμμεσα: Δικαιώματα που ορίζονται από το μέσο που φέρει το περιεχόμενο.

Είναι πολύ σημαντικό για τα DRM συστήματα ότι τα πρώτα δύο είδη δικαιωμάτων δεν έχουν αλλάξει πολύ με την ανάπτυξη των τεχνολογιών του Διαδικτύου, της κινητής τηλεφωνίας και των MP3 αρχείων. Οι συναλλαγές παρέμειναν ίδιες παρόλο που πλέον γίνονται μέσω του Διαδικτύου. Η διαφορά βρίσκεται στη φύση των έμμεσων δικαιωμάτων. Το Διαδίκτυο έχει μετατρέψει αυτά τα δικαιώματα από έμμεσα σε άμεσα. Αυτό μπορεί να προκαλέσει τόσο προβλήματα όσο και ευκαιρίες για τους παρόχους περιεχομένου και τους καταναλωτές.

Η έννοια των DRM συστημάτων αναφέρεται στον ψηφιακό έλεγχο και τη διαχείριση των δικαιωμάτων του περιεχομένου τους. Η ανάγκη για έλεγχο και διαχείριση αυξάνεται συνέχεια καθώς οι ψηφιακές τεχνολογίες δικτύων έχουν μετατρέψει σε πολύ δύσκολο τον έλεγχο των τρόπων χρήσης, της εφαρμογής των πνευματικών δικαιωμάτων και της διακίνησης του περιεχομένου.

### 7.2 Επιστημονικά πεδία που συμμετέχουν σε ένα DRM σύστημα

Στα DRM συστήματα εμπλέκονται συνεργάζονται διάφορα επιστημονικά πεδία εκτός του τεχνολογικού. Σε αυτό το πλαίσιο προστασίας περιεχομένου συμμετέχουν το νομικό, το κοινωνικό και το οικονομικό πεδίο. Δεδομένου ότι εστιάζουμε στις τεχνολογικές πτυχές του DRM, θα καλύψουμε τις άλλες πτυχές του εν συντομία.

**Νομικές.** Η τεχνολογία των DRM συστημάτων δεν μπορεί να βοηθήσει χωρίς την επιβολή από την νομοθεσία των δικαιωμάτων των ιδιοκτητών του περιεχομένου. Το DRM πρέπει να είναι σε θέση να εφαρμόσει αποτελεσματικά τους τοπικούς και διεθνείς νόμους για να προστατεύσει αυτά τα

δικαιώματα ιδιαίτερα στην περίπτωση που οι διαφορετικές χώρες έχουν πολύ διαφορετική νομοθεσία πνευματικών δικαιωμάτων. Επιπλέον, κάποιες τεχνολογίες ασφάλειας δεν μπορούν να χρησιμοποιηθούν σε ορισμένες χώρες. Παραδείγματος χάριν, η αμερικανική κυβέρνηση απαγορεύει την εξαγωγή των αμερικάνικων 128-bit κρυπτογραφικών τεχνολογιών σε ορισμένες χώρες.

**Κοινωνικές.** Τα DRM συστήματα απευθύνονται σε έναν πλήθος κοινωνικών ζητημάτων όπως η μυστικότητα (privacy) και η δίκαιη χρήση (Fair-use). Μερικοί χρήστες προτιμούν την ανωνυμία όταν καταναλώνουν ένα ψηφιακό περιεχόμενο ενώ άλλοι δεν θα ήθελαν οποιαδήποτε σκιαγράφηση τους. Υπήρξαν πολλές συζητήσεις σχετικά με την έννοια της δίκαιης χρήσης (παραδείγματος χάριν, αν είναι δίκαιη η δημιουργία ενός εφεδρικού αντιγράφου). Η ασυγκράτητη πειρατεία ειδικά στην ψηφιακή μουσική, έχει δημιουργήσει μια νοοτροπία ότι το ψηφιακό περιεχόμενο πρέπει να γίνεται ελεύθερα διαθέσιμο και κοινόχρηστο. Μαζί με τη δημόσια εκπαίδευση, σημαντικός ρόλος των DRM συστημάτων είναι να παρουσιάσει στους χρήστες την αξία της χρήσης τους και την σημασία του σεβασμού των πνευματικών δικαιώματα του ψηφιακού περιεχομένου.

**Οικονομικές.** Τα DRM δημιουργούν ορισμένες οικονομικές ερωτήσεις όπως ποιος θα πληρώσει για τη δομή του DRM, οι χρήστες ή οι ιδιοκτήτες του περιεχομένου; Νέα επιχειρησιακά πρότυπα δημιουργούνται και εξελίσσονται. Παραδείγματος χάριν, τα online οικονομικά γραφεία συμψηφισμού θα πρέπει να χειριστούν τις άδειες του περιεχομένου και να εξετάσουν τις μικροπληρωμές.

## 7.3 Παράγοντες ανάπτυξης και επέκτασης των DRM

Οι παράγοντες που χρειάζεται να ληφθούν υπόψη κατά την ανάπτυξη και την επέκταση των DRM συστημάτων είναι οι ακόλουθοι:

- Εμπιστοσύνη
- Ασφάλεια
- Ευχρηστία
- Εξελιξιμότητα
- Διαλειτουργικότητα

### *7.3.1 Εμπιστοσύνη*

Είναι μια από τις βασικότερες έννοιες του DRM. Η έννοια της εμπιστοσύνης γίνεται καλύτερα κατανοητή ως η ικανότητα ενός συστήματος να παράγει ένα προβλέψιμο αποτέλεσμα. Μια μηχανή ή ένα σύστημα έχει ένα ιδιαίτερο στόχο: Ο βαθμός στον οποίο ο χειριστής της μηχανής είναι σε θέση να βασιστεί στη λειτουργία της μηχανή για την παράδοση του επιθυμητού αποτελέσματος είναι ανάλογος με το επίπεδο εμπιστοσύνης του συστήματος.
Πολλοί παράγοντες μπορούν να παρεμποδίσουν το αναμενόμενο αποτέλεσμα:

- Μια μηχανική ρωγμή στη λειτουργία του συστήματος,
- Ένα προγραμματιστικό κενό,
- Μια παραβίαση της ασφάλεια του συστήματος.

Όσο πιο σύνθετο είναι το περιβάλλον του συστήματος τόσο πιο δύσκολη γίνεται η διαδικασία εμπιστοσύνης του. Ακριβώς όπως τα ανθρώπινα όντα έχουν μηχανισμούς για τις εμπιστευμένες σχέσεις μεταξύ τους, έτσι και οι συσκευές και τα τμήματα σε ένα σύνθετο περιβάλλον συστημάτων πρέπει να δημιουργήσουν μια εμπιστευμένη σχέση το ένα με το άλλο και με τους χρήστες του συστήματος.

Για να γίνει κατανοητή αυτή η έννοια καλύτερα, θεωρήστε τη χρήση των αυτοματοποιημένων μηχανών ανάληψης (ATM) που δίνει τη δυνατότητα πολλοί άνθρωποι να λαμβάνουν μετρητά από τους τραπεζικούς λογαριασμούς τους από διαφορετικές θέσεις. Τα μετρητά διανέμονται σε έναν χρήστη σύμφωνα με μια οδηγία που στέλνεται σε αυτόν - αυτή η οδηγία εγκρίνεται από την τράπεζα από την οποία ο χρήστης επιθυμεί να κάνει ανάληψη. Για την οδηγία που εφαρμόζεται, πρέπει να υπάρξει μια εμπιστευμένη σχέση μεταξύ του χρήστη και της εξωτερικής διεπαφής του συστήματος

του ATM (πραγματοποιείται χρησιμοποιώντας έναν προσωπικό αριθμό αναγνώρισης), μεταξύ των διαφορετικών μερών του δικτυωμένου συστήματος που παραδίδει τις πληροφορίες για τις οδηγίες του χρήστη στην τράπεζα έγκρισης και μεταξύ της τράπεζας και του συστήματος. Οποιαδήποτε αποτυχία σε αυτές τις σχέσεις - ένα σπάσιμο στην αλυσίδα εμπιστοσύνης θα οδηγήσει σε αποτυχία του επιθυμητού ή προβλεφθέντος αποτελέσματος. Τα DRM συστήματα πρέπει να λειτουργήσουν με τον ίδιο τρόπο εάν πρόκειται να χρησιμοποιηθούν για τη διαχείριση δικαιωμάτων περιεχομένου.

### *7.3.2 Ασφάλεια*

Οι ειδικοί ασφάλειας γνωρίζουν ότι η ασφάλεια ενός συγκεκριμένου περιβάλλοντος δεν είναι μια απόλυτα καθορισμένη ενέργεια. Πρέπει να εφαρμοστεί αναλογικά με τον κίνδυνο που προβλέπεται μέσα στο συγκεκριμένο περιβάλλον και καθώς αυτό δεν είναι κάτι στατικό, πρέπει η λύση ασφάλειας να έχει δυνατότητα αναθεώρησης.
Η ανανεωσιμότητα (Renewability) της λύσης ασφάλειας είναι επομένως ουσιαστική για την αποτελεσματικότητά της, αλλά προκαλεί περιπλοκές και προβλήματα. Αφ' ενός, το κλείσιμο του περιεχομένου σε μια μηχανή ή ένα κομμάτι πλαστικού παρέχει κάποιου βαθμού ασφάλεια. Από την άλλη, η ανανεωσιμότητα της ασφάλειας κάνει το σύστημα ανοικτό σε διαφορετικές μορφές επίθεσης. Επίσης το ετερογενές περιβάλλον του Διαδικτύου αυξάνει τις προκλήσεις ασφάλειας επιπλέον.

Στόχος είναι η εύρεση ισορροπίας μεταξύ του επιπέδου ασφάλειας και της δυνατότητας χρησιμοποίησης του συστήματος. Ο ειδικός στις διαδικασίες ασφάλειας Bruce Schneider προτείνει μια δοκιμή πέντε βημάτων για την αξιολόγηση των αναγκών ασφάλειας:

**Βήμα 1:**Ποια χαρακτηριστικά προσπαθείτε να προστατεύσετε;
**Βήμα 2:**Ποιοι είναι οι κίνδυνοι για αυτά τα χαρακτηριστικά;
**Βήμα 3:**Πόσο καλά μετριάζει αυτούς τους κινδύνους η λύση ασφάλειας;
**Βήμα 4:**Ποιους άλλους κινδύνους προκαλεί η λύση ασφάλειας;
**Βήμα 5:**Ποιες δαπάνες και ανταλλαγές επιβάλλει η λύση ασφάλειας;

Η ασφάλεια μέσα σε ένα DRM επιτρέπει στο σύστημα να είναι σε θέση να προστατεύσει όχι μόνο το περιεχόμενο και τα δικαιώματα αλλά και τις αντίστοιχες διαχειριστικές διαδικασίες και τα αποτελέσματα αυτών των διαδικασιών, όπως για παράδειγμα η συλλογή και η επεξεργασία των στοιχείων χρήσης, η τιμολόγηση και η συλλογή της πληρωμής για τη χρήση, κτλ.

### 7.3.3 Ευχρηστία

Το πρώτο θύμα ενός υπερβολικά ασφαλούς συστήματος είναι η ευχρηστία. Η λειτουργική πολυπλοκότητα καθιστά πολύ δύσκολη ή πολύ ακριβή τη χρήση του συστήματος. Το περιεχόμενο και τα δικαιώματα είμαι ασφαλή αλλά αφού δεν υπάρχει ευκολία πρόσβασης ή χαμηλό κόστος το συγκεκριμένο σύστημα είναι σπάνια χρησιμοποιημένο.

Υπάρχουν πολλοί παράγοντες που πρέπει να ληφθούν υπόψη τους για να είναι ένα σύστημα λειτουργικά ασφαλές και, αναπόφευκτα, ένας από αυτούς είναι οι χρήστες του συστήματος, είτε χρησιμοποιώντας το σύστημα για να κάνουν διαθέσιμο το περιεχόμενό τους είτε για να αποκτήσουν πρόσβαση και να χρησιμοποιήσουν το περιεχόμενο του συστήματος.

Επομένως ένα κρίσιμο στοιχείο στο σχεδιασμό και τη λειτουργία ενός DRM συστήματος, είναι να βρεθεί η σωστή μέση λύση μεταξύ της ασφάλειας και της ευχρηστίας του συστήματος. Ο στόχος είναι να παρέχεται στο τελικό χρήστη το επιθυμητό αποτέλεσμα, στο οποίο οι διαδικασίες διαχείρισης δικαιωμάτων είναι ουσιαστικά αόρατες.

### *7.3.4 Εξελιξιμότητα*

Ένα άλλο ζήτημα είναι αν το συστήματος είναι σε θέση να εξελίσσεται ανάλογα με το δίκτυο, τις συσκευές και τους χρήστες. Σίγουρα ο σχεδιασμός ενός συστήματος που λειτουργεί αποτελεσματικά μέσα σε μια περιορισμένη περιοχή έχει μεγάλη διαφορά από το να επεκταθεί σε ένα σύστημα με χρήστες σε όλη τον κόσμο, που συνδέονται μέσω του Διαδικτύου.

Οι πρόωρες εφαρμογές δυναμικού DRM επέτρεψαν στα συστήματα που απέτυχαν λόγω της πολυπλοκότητάς και του υψηλού κόστους τους, να επεκταθούν από άποψη λειτουργικής διαχείρισης και υποστήριξης. Τα πιο πρόσφατα συστήματα στοχεύουν σε υψηλότερο βαθμό αυτοματοποίησης και ελάχιστη απαίτηση ξένης υποστήριξης.

### *7.3.5 Διαλειτουργικότητα*

Το τελευταίο ζήτημα που πρέπει να εξεταστεί σε γενικό επίπεδο στη συζήτηση για τα DRM συστήματα είναι το σύνθετο ζήτημα της διαλειτουργικότητας. Αν και υπάρχει κάποια τυποποίηση μερικών τμημάτων των συστημάτων DRM, τα εμπορικά διαθέσιμα συστήματα είναι ως επί το πλείστον ιδιωτικά. Επομένως τα διαφορετικά συστήματα είναι σπάνια ικανά να επικοινωνήσουν το ένα με το άλλο επειδή χρησιμοποιούν διαφορετικά συστήματα κωδικοποίησης και κρυπτογράφησης, διαφορετικούς μηχανισμούς επικύρωσης των χρήσεων, διαφορετικά σχήματα αρχείων, διαφορετικές δομές μετά-δεδομένων και διαφορετικές γλώσσες έκφρασης δικαιωμάτων.

Αυτό δημιουργεί προβλήματα στους προμηθευτές του περιεχομένου και στους χρήστες. Ο προμηθευτής περιεχομένου μπορεί να αναγκαστεί να κάνει διαθέσιμο το περιεχόμενο και να αναπτύξει τα αντίστοιχα δικαιώματα του για τα διαφορετικά συστήματα διαχείρισης περιεχομένου. Αντιθέτως, ο τελικός χρήστης μπορεί να πρέπει να χρησιμοποιήσει μια σειρά διαφορετικών συστημάτων για να λάβει όλο το επιδιωκόμενο περιεχόμενο.

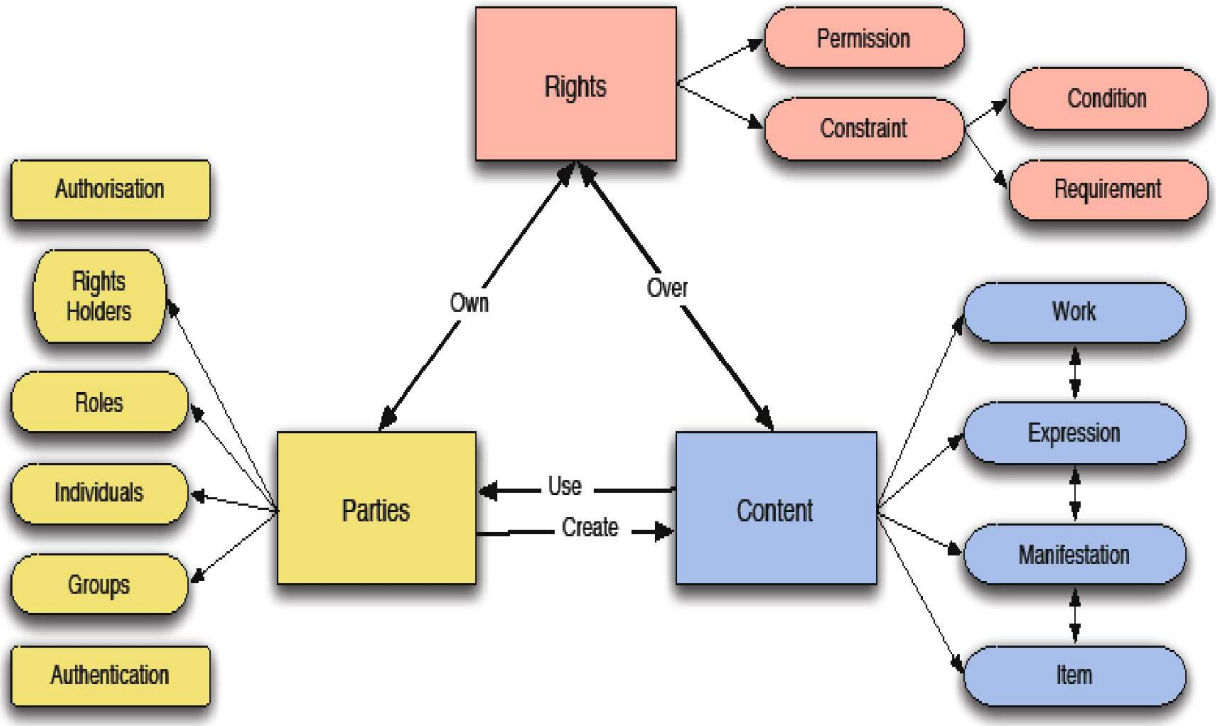
Εντούτοις, ενώ το πρόβλημα είναι προφανές, η λύση δεν είναι. Υπάρχουν σύνθετα εμπορικά, νομικά και τεχνικά ζητήματα που περιλαμβάνονται στην καθιέρωση της διαλειτουργικότητας μεταξύ των διαφορετικών συστημάτων. Τα ανοικτά πρότυπα των βασικών τμημάτων του DRM και η χρήση ανοικτών τεχνολογιών είναι η λύση.

## 7.4 Οντότητες του DRM

Είναι σημαντικό να υιοθετηθεί ένα σαφές και επεκτάσιμο πρότυπο για τις οντότητες των DRM συστημάτων και τις σχέσεις τους με τις άλλες οντότητες. Η βασική αρχή στο πρότυπο <indecs> είναι να διαχωριστούν σαφώς και να προσδιοριστούν οι τρεις βασικές οντότητες:

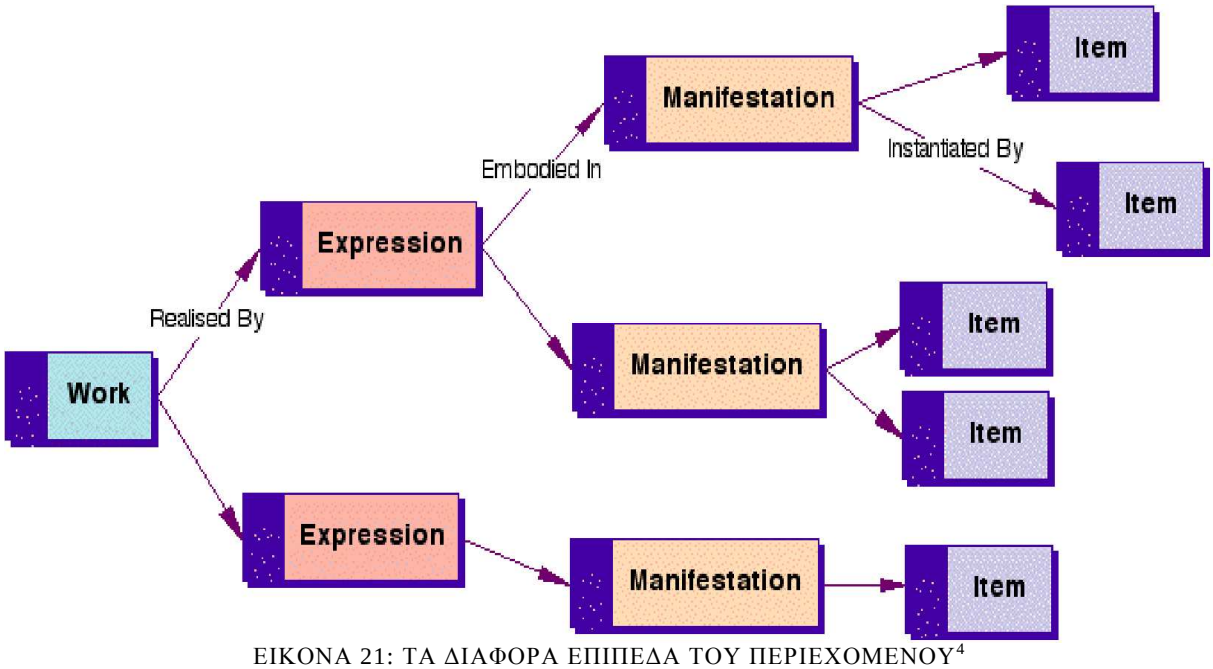
- Οι χρήστες,
- το περιεχόμενο και
- τα δικαιώματα (όπως φαίνεται στην εικόνα 20).

Οι χρήστες μπορούν να είναι από έναν κάτοχο δικαιωμάτων ως και ένας τελικός καταναλωτής. Το περιεχόμενο είναι οποιοσδήποτε τύπος περιεχομένου σε οποιοδήποτε επίπεδο συνάθροισης. Η οντότητα δικαιωμάτων είναι μια έκφραση των αδειών, των περιορισμών και των υποχρεώσεων μεταξύ των χρηστών και του περιεχομένου. Ο αρχικός λόγος για αυτό το πρότυπο είναι ότι παρέχει τη μέγιστη ευελιξία κατά την ανάθεση των δικαιωμάτων σε οποιαδήποτε συνδυασμό ή διάταξη στα στρώματα των χρηστών και του περιεχομένου.




ΕΙΚΟΝΑ 206: ΟΙ ΟΝΤΟΤΗΤΕΣ ΤΟΥ DRM ΚΑΙ ΟΙ ΣΧΕΣΕΙΣ ΜΕΤΑΞΥ ΤΟΥΣ[3]

Το ίδιο το περιεχόμενο πρέπει επίσης να διαμορφωθεί. Η βασική αρχή στη διαμόρφωση του περιεχομένου είναι ότι το περιεχόμενο περιέχει πολλά επίπεδα ανάλογα με τα διάφορα επίπεδα διανοητικής εξέλιξης και ανάπτυξής του.




ΕΙΚΟΝΑ 21: ΤΑ ΔΙΑΦΟΡΑ ΕΠΙΠΕΔΑ ΤΟΥ ΠΕΡΙΕΧΟΜΕΝΟΥ[4]

[3] Η εικόνα είναι διαθέσιμη στο http://www.dlib.org/dlib/june01/iannella/06iannella.html
[4] Η εικόνα είναι διαθέσιμη στο http://www.dlib.org/dlib/june01/iannella/06iannella.html

### *7.4.1 Προσδιορισμός και περιγραφή των οντοτήτων*

Όλες οι οντότητες πρέπει να προσδιοριστούν και να περιγράφουν. Ο προσδιορισμός πρέπει να ολοκληρωθεί μέσω των ανοικτών και τυποποιημένων μηχανισμών για κάθε οντότητα στο πρότυπο. Οι οντότητες και τα αρχεία μεταδεδομένων για τις οντότητες πρέπει να είναι ευπροσδιόριστες. Τα ανοικτά πρότυπα όπως τα ομοιόμορφα προσδιοριστικά των πόρων, τα ψηφιακά προσδιοριστικά αντικειμένου και ο διεθνής τυποποιημένος κώδικας κειμένου εργασίας του ISO είναι χαρακτηριστικά σχέδια χρήσιμα για τον προσδιορισμό δικαιωμάτων.

Το περιεχόμενο πρέπει να περιγραφεί χρησιμοποιώντας τα πιο κατάλληλα πρότυπα μεταδεδομένων ανάλογα με το ύφος της πληροφορίας (παραδείγματος χάριν, τα πρότυπα ONIX για τα βιβλία και το πρότυπο πληροφοριών μεταδεδομένων των πόρων εκμάθησης IMS για τα εκπαιδευτικά αντικείμενα εκμάθησης). Είναι επίσης κρίσιμο ότι τέτοια πρότυπα μεταδεδομένων δεν συμπεριλαμβάνουν τα στοιχεία μεταδεδομένων που εξετάσουν τις διοικητικές πληροφορίες των δικαιωμάτων, δεδομένου ότι αυτό θα προκαλέσει σύγχυση σχετικά με πού να περιγραφούν τέτοιες εκφράσεις δικαιωμάτων. Παραδείγματος χάριν, τα πρότυπα ONIX έχουν τα στοιχεία για διάφορους κατόχους δικαιωμάτων (π.χ., συντάκτες και εκδότες), τα πεδία των δικαιωμάτων τους και τις ενιαίες πληροφορίες για τις τιμές.

Για την περιγραφή των χρηστών, τα vCard είναι τα πιο γνωστά πρότυπα μεταδεδομένων για την περιγραφή των ανθρώπων και οργανώσεων. Ένα πρόσθετο και σημαντικό μέρος του προτύπου δικαιωμάτων είναι να αρθρωθεί ο ρόλος που ο χρήστης έχει αναλάβει όσον αφορά το περιεχόμενο. Ένας περιεκτικός κατάλογος ρόλων μπορεί να βρεθεί στον κατάλογο MARC Relators.

### *7.4.2 Έκφραση των δηλώσεων δικαιωμάτων*

Η οντότητα δικαιωμάτων επιτρέπει να δημιουργούνται εκφράσεις για τις επιτρεπόμενες άδειες, τους περιορισμούς, τις υποχρεώσεις και οποιαδήποτε άλλα δικαιώματα σχετικά με τους χρήστες και το περιεχόμενο. Ως εκ τούτου, η οντότητα δικαιωμάτων είναι κρίσιμη επειδή αντιπροσωπεύει την εκφραστικότητα της γλώσσας που θα χρησιμοποιηθεί για να ενημερώσει τα μεταδεδομένα των δικαιωμάτων.

Οι εκφράσεις δικαιωμάτων μπορούν να γίνουν σύνθετες αρκετά γρήγορα. Λόγω αυτού, διαμορφώνονται για να κατανοήσουμε τις σχέσεις μέσα στις εκφράσεις δικαιωμάτων. Οι εκφράσεις δικαιωμάτων πρέπει να αποτελούνται από:

- τις άδειες χρήσεις - τι έχετε την άδεια να κάνετε
- τους περιορισμούς - περιορισμοί στις άδειες
- τις υποχρεώσεις - τι πρέπει να κάνω/παρέχω/δέχομαι
- τον κάτοχος δικαιωμάτων - ποιος έχει δικαίωμα σε τι.

## 7.5 Στόχοι του DRM

Οι κύριοι στόχοι του DRM είναι οι εξής:

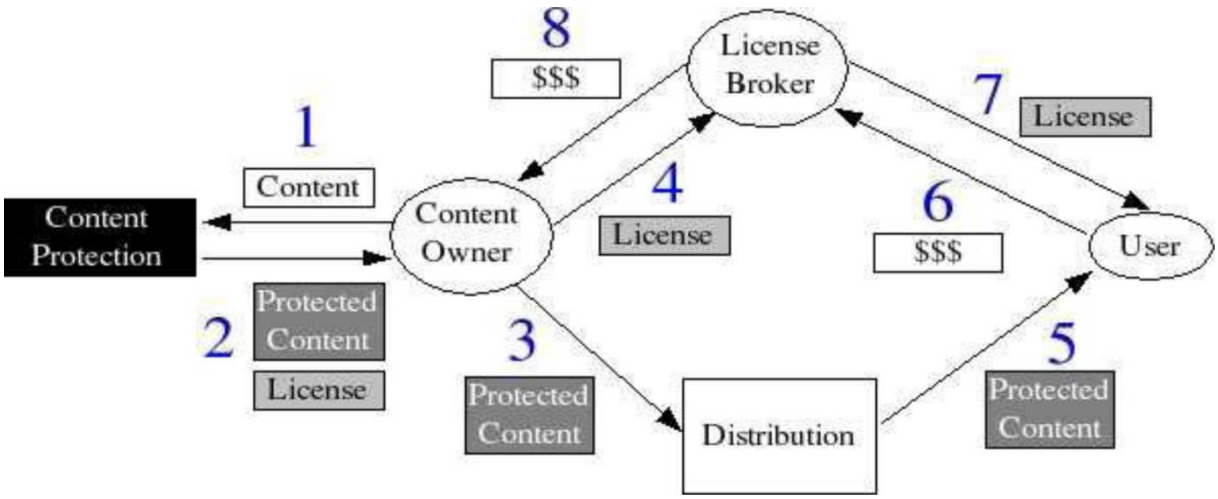
- Να παρέχει μια απαραίτητη υποδομή πληροφορίας για το ψηφιακό περιεχόμενο και τα ιδιαίτερα χαρακτηριστικά του. Οι υπηρεσίες που προσφέρονται ποικίλουν από τυπικές e-commerce εφαρμογές (ηλεκτρονικοί κατάλογοι και καλάθι αγορών) μέχρι προηγμένες υπηρεσίες, όπως αναζήτηση π.χ. εικόνων με βάση το κυρίαρχο χρώμα και εντοπισμό μη εξουσιοδοτημένων μορφών χρήσης.
- Να προστατεύσει το copyright του ψηφιακού περιεχομένου μέσω, παραδειγμάτων χάριν ανθεκτικών τεχνικών υδατοσήμανσης.
- Να υποστηρίξει την διαδικασία διαχείρισης ψηφιακών δικαιωμάτων και τις συναλλαγές που υφίστανται.

- Να παρέχει αποτελεσματικούς μηχανισμούς ανίχνευσης μη εξουσιοδοτημένης και καταχρηστικής χρήσης του περιεχομένου.

### 7.6 Ένα απλό παράδειγμα λειτουργίας DRM

Παρακάτω περιγράφεται ένα απλό χαρακτηριστικό DRM σύστημα. Υπάρχουν τρία βασικά συμβαλλόμενα μέρη στην οργάνωση που διευκρινίζεται στην εικόνα 22, ο ιδιοκτήτης περιεχομένου, ο μεσίτης αδειών και ο χρήστης.

Ο ιδιοκτήτης περιεχομένου κατέχει συνήθως όλων των δικαιωμάτων στο περιεχόμενο. Μπορεί να αναφέρεται σε μια εταιρία μουσικής αναπαραγωγής ή σε ένα καλλιτέχνη. Ο μεσίτης αδειών χειρίζεται όλες τις συναλλαγές, εξ ονόματος του ιδιοκτήτη περιεχομένου, σχετικά με την έκδοση μιας άδειας που διευκρινίζει ακριβώς τις δυνατότητες που χορηγούνται σε έναν χρήστη για την χρήση του περιεχομένου, υπό ορισμένους όρους και διατάξεις. Ο χρήστης αναφέρεται εδώ σε ένα έμπιστο τρίτο (υλικό/ λογισμικό) που είναι ένα πληρεξούσιο στο χρήστη (καταναλωτή). Πιστοποιεί δηλαδή ότι δεν εκτελείται παράνομη πρόσβαση στο περιεχόμενο από το χρήστη. Επίσης επιβάλλει τους όρους και τις διατάξεις της χρήσης του περιεχομένου.




ΕΙΚΟΝΑ 22: ΈΝΑ ΑΠΛΟ ΠΑΡΑΔΕΙΓΜΑ ΛΕΙΤΟΥΡΓΙΑΣ ΤΟΥ DRM

# ΚΕΦΑΛΑΙΟ 8

## Σύστημα Ψηφιακής Διαχείρισης Δικαιωμάτων -Τεχνολογίες

### 8.1 Διαχείριση Πνευματικών Δικαιωμάτων

Η διαχείριση πνευματικών δικαιωμάτων (Digital Rights Management) αναφέρεται στις τεχνολογίες ελέγχου πρόσβασης που χρησιμοποιούνται από κατασκευαστές υλικού και λογισμικού, εκδότες και κατόχους ψηφιακής πνευματικής ιδιοκτησίας με σκοπό να περιορίσουν ή και να δημιουργήσουν μηχανισμούς ελέγχου στην διακίνηση και αναπαραγωγή των ψηφιακών έργων. Πολλές φορές ο χαρακτηρισμός DRM συνέχεται με την έννοια της «προστασίας αντιγραφής». Η αλήθεια είναι ότι οι DRM τεχνολογίες χρησιμοποιούνται κυρίως σε πολυμέσα ενώ η προστασία αντιγραφής παρέχει μηχανισμούς προστασίας σε επίπεδο λογισμικού υπολογιστών. Οι τεχνολογίες DRM χρησιμοποιήθηκαν και χρησιμοποιούνται κατά κόρον από εταιρείες όπως η Sony, η Apple (στο ηλεκτρονικό της κατάστημα iTunes Store), η Microsoft κ.α.

Η χρήση τέτοιων τεχνολογιών δημιούργησε αντιπαραθέσεις στους καταναλωτές πολυμεσικών υπηρεσιών. Οι υποστηρικτές της εφαρμογής DRM στα ψηφιακά έργα επισημαίνουν την αναγκαιότητα τέτοιων υπηρεσιών ούτως ώστε να διαφυλάσσονται τα έσοδα για τους πνευματικούς δημιουργούς. Αντίθετα οι πολέμιοι τέτοιων εφαρμογών, (όπως είναι το Free Software Foundation) αναφέρουν ότι η λέξη «Δικαίωμα» στη φράση Διαχείριση Πνευματικών Δικαιωμάτων είναι παραπλανητική και στην ουσία θα έπρεπε να αντικατασταθεί από την λέξη «Περιορισμός» - Διαχείριση Ψηφιακών Περιορισμών. Υποστηρίζουν δηλαδή ότι οι κάτοχοι ψηφιακής πνευματικής ιδιοκτησίας προσπαθούν να περιορίσουν τη χρήση των έργων τους με τρόπους όμως που είναι ενάντια στην σύγχρονη νομοθεσία και νομολογία. Το Electronic Frontier Foundation [10] επίσης θεωρεί τα συστήματα DRM ως πρακτικές που εμποδίζουν ή και μειώνουν τον υγιή ανταγωνισμό στην οικονομία της αγοράς. Με τη χρήση των DRM δεν είναι δυνατή η πώληση μεταχειρισμένου υλικού ή λογισμικού, κάτι που θεωρείται αντισυνταγματικό βάση της απόφασης του Ανώτατου Δικαστηρίου των Ηνωμένων Πολιτειών του 1908.

Σε πρακτικό επίπεδο, όλα τα ευρέως διαδεδομένα DRM συστήματα δεν εκπληρώνουν πλήρως τον σκοπό τους αφού οι περιορισμοί οι οποίοι θα τεθούν σε λειτουργία αφορούν αποκλειστικά και μόνο την ψηφιακή αντιγραφή και δεν μπορούν να αντιμετωπίσουν την αναλογική οδό. Το γεγονός αυτός έχει εγείρει συζητήσεις πάνω στο ζήτημα της απόλυτης προστασίας με τις τεχνολογίες DRM, κάτι, που για την ώρα τουλάχιστον, δείχνει ανέφικτο.

### 8.2 Τα συστήματα Διαχείρισης και προστασίας Ψηφιακών Πνευματικών Δικαιωμάτων

#### Γενικά Στοιχεία

Ιδιαίτερη είναι η σημασία της νομικής θωράκισης των τεχνολογικών μέσων προστασίας πνευματικών δικαιωμάτων, μια διαδικασία που σχετικά πρόσφατα και με πυξίδα την Ευρωπαϊκή Οδηγία άρχισε να γίνεται πραγματικότητα στις επιμέρους εθνικές νομοθεσίες των κρατών μελών. Ακολουθεί μια συνοπτική αναφορά στις τεχνολογίες που χρησιμοποιούνται για το συγκεκριμένο σκοπό, στα σημαντικότερα συστήματα που αξιοποιούν αντίστοιχες τεχνολογικές λύσεις καθώς και στα κυριότερα προϊόντα που διατίθενται στην αγορά προσφέροντας ολοκληρωμένες λύσεις για την προστασία και τη διαχείριση του δικαιώματος αναπαραγωγής και των συγγενικών δικαιωμάτων.

Τα τεχνολογικά μέσα προστασίας όπως προκύπτουν από τις ενδεδειγμένες πρακτικές και τα προγράμματα συνοψίζονται παρακάτω:

- Ασφάλεια και ακεραιότητα των λειτουργικών συστημάτων των ηλεκτρονικών υπολογιστών. Περιλαμβάνονται και παραδοσιακές μέθοδοι ελέγχου της πρόσβασης σε αρχεία, πιστοποίησης χρηστών, παροχής δικαιωμάτων κ.α.
- Κρυπτογραφία: Επιτρέπει την κρυπτογράφηση του ψηφιακού περιεχομένου, ώστε η αποκρυπτογράφηση του να είναι δυνατή μόνο από τους νόμιμους χρήστες.

- Υδατογραφία ή απόκρυψη δεδομένων (data hiding): Ενσωματώνει πληροφορία (π.χ. σχετικά με τον κάτοχο του. δικαιώματος αναπαραγωγής) σε ένα ψηφιακό αρχείο. Ένα ψηφιακό υδατογράφημα βοηθά τους ιδιοκτήτες πνευματικών δικαιωμάτων να ανιχνεύουν τη μη-εξουσιοδοτημένη χρήση, αντιγραφή και διανομή των ψηφιακών δεδομένων.
- Έμπιστα (trusted) συστήματα: Σε μία εκδοχή της μελλοντικής εξέλιξης της επιστήμης της πληροφορικής, η ασφάλεια θα έχει σημαντική θέση στο σχεδιασμό των υπολογιστικών συστημάτων, οδηγώντας στην εκτεταμένη υιοθέτηση συστημάτων προστασίας και ελέγχου της Πνευματικής Ιδιοκτησίας με την αξιοποίηση εξειδικευμένου υλικού και λογισμικού. Τα «έμπιστα» αυτά συστήματα συνθέτουν ένα ανοικτό πεδίο έρευνας.
- Σήμανση (Marking): Για τη μετάδοση πληροφοριών πάνω στο περιεχόμενο, δηλ. εάν υπάρχει προστασία αντιγραφής, ποιος είναι ο ιδιοκτήτης των δικαιωμάτων και ποια είδη χρήσης επιτρέπονται, γίνεται σχετική σήμανση των δεδομένων από τον ιδιοκτήτη των δικαιωμάτων πριν την πώληση.
- Επιλεκτική ασυμβατότητα (Selective Incompatibility): Όταν ένας παραγωγός για παράδειγμα κωδικοποιεί λάθη στο περιεχόμενο ενός CD, προσπαθεί να καθορίσει εάν μπορεί το CD να παιχτεί σε υπολογιστή, ραδιόφωνο αυτοκινήτου, φορητή συσκευή, κινητό τηλέφωνο κλπ.

Κατά πόσο ένα τεχνολογικό μέσο προστασίας είναι αποδοτικό εξαρτάται από την τεχνολογική του πληρότητα, το περιεχόμενο που προστατεύει και την επιχείρηση (ή τομέα) στην οποία είναι εγκατεστημένο. Τα κυριότερα χαρακτηριστικά του είναι:

- Ευχρηστία: Ένα δύσχρηστο μέσο προστασίας αυτόματα αποθαρρύνει την ευρεία χρήση του.
- Καταλληλότητα ως προς το περιεχόμενο: Το κόστος του σχεδιασμού, της ανάπτυξης και εγκατάστασης του συστήματος πρέπει να είναι σε αρμονία με τον τύπο του περιεχομένου. Για χαμηλού κόστους περιεχόμενο το οποίο ήδη διατίθεται σε λογική τιμή με αναλογικά μέσα (όχι μέσω του Διαδικτύου), δεν υπάρχει λόγος υλοποίησης ενός υψηλού κόστους συστήματος προστασίας το οποίο θα αυξήσει την τιμή της διάθεσης του περιεχόμενου μέσω του Διαδικτύου.
- Καταλληλότητα ως προς την απειλή: Η αποτροπή των έντιμων καταναλωτών (παραβατών χωρίς πρόθεση) από το να διαμοιράζουν μικρού αριθμού αντίγραφα ενός προϊόντος, μπορεί να απαιτεί μόνο ένα λογικά τιμολογημένο ψηφιακό προϊόν, ένα καλό σύστημα διάθεσης και ένα σαφώς καθορισμένο σύνολο οδηγιών. Η αποτροπή της ηλεκτρονικής σύλησης εξαιρετικά πολύτιμου υλικού, το οποίο πρέπει να υπάρχει σε δίκτυο ηλεκτρονικών υπολογιστών, απαιτεί ένα πολύπλοκο μηχανισμό προστασίας και ακόμα και η καλύτερη διαθέσιμη τεχνολογία ίσως να μην αρκεί για την προστασία του.
- Ανάλυση κόστους – οφέλους: Μία πολύπλοκη αλλά απαραίτητη μελέτη που θα πρέπει πάντα να προηγείται των όποιων αποφάσεων.

### 8.3 Συστήματα κρυπτογράφησης

Η κρυπτογράφηση είναι η διαδικασία κατά την οποία ένα κείμενο δεν μπορεί να γίνει κατανοητό από κανένα άλλο εκτός από αυτόν που κατέχει το κλειδί αποκρυπτογράφησης. Οι σύγχρονες τεχνολογίες DRM χρησιμοποιούν το σύστημα κρυπτογραφίας για να εξασφαλίσουν ότι δεν παραβιάζονται οι άδειες που παρέχονται από τον ιδιοκτήτη περιεχομένου. Ένα αρχείο κρυπτογραφείται χρησιμοποιώντας ένα συγκεκριμένο κλειδί για κάθε χρήστη. Ένα κλειδί για την εξέταση ή το άκουσμα του περιεχόμενου παρέχεται στο χρήστη κατά την αγορά. Αλλά, το δικαίωμα χρήσης μπορεί να απαγορεύσει την αντιγραφή, την εκτύπωση, και την ανακατανομή του περιεχομένου. Όταν ο χρήστης ανοίγει ένα αρχείο περιεχομένου, το λογισμικό DRM ελέγχει την ταυτότητα του χρήστη και έρχεται σε επαφή με τον ιστοχώρο του ιδιοκτήτη. Εάν η άδεια χορηγείται, το αρχείο αποκρυπτογραφείται και η πρόσβαση επιτρέπεται. Αυτοί τα συστήματα εμφανίζουν μεγάλη ποικιλία. Στην απλούστερη μορφή, το περιεχόμενο κρυπτογραφείται χρησιμοποιώντας ένα ενιαίο κύριο κλειδί. Αλλά, μια τέτοια προσέγγιση είναι αρκετά εύθραυστη. Το σύστημα μπορεί να παρέχει

"πολλαπλά κλειδιά για πολλαπλές κρυπτογραφήσεις" πλησιάζοντας το δημόσιο βασικό σύστημα υποδομής (PKI).

Στα πιο σύνθετα συστήματα, τα κλειδιά είναι μοναδικά όχι μόνο για το περιεχόμενο αλλά και για τη λειτουργία, τη διάρκεια ζωής και τη συσκευή. Τα διαφορετικά κλειδιά δείχνουν διαφορετικά προνόμια και χρησιμοποιούνται για να καθορίσουν και να επιβάλουν αυτόματα τα όρια ενέργειας των χρηστών. Ο κάτοχος των δικαιωμάτων του περιεχομένου μπορεί να περιορίσει την πρόσβαση με διάφορους τρόπους. Παραδείγματος χάριν, ένα έγγραφο να επιτρέπει την ανάγνωσή του αλλά όχι την εκτύπωση. Ο κάτοχος των δικαιωμάτων μπορεί να διευκρινίσει ότι το περιεχόμενο του χρησιμοποιείται μόνο σε μια ενιαία συσκευή, για περιορισμένες λειτουργίες και για ένα συγκεκριμένο χρονικό διάστημα. Συμφώνα με αυτούς τους περιορισμούς, ο χρήστης οφείλει να υποβάλει τους αύξοντες αριθμούς των συσκευών στις οποίες θα χρησιμοποιηθεί το περιεχόμενο. Τα κλειδιά κρυπτογράφησης μπορούν να παραχθούν χρησιμοποιώντας τους υποβληθέντες αριθμούς των συσκευών σαν παράγοντα τους. Αυτό το παράδειγμα είναι μια πιο περίπλοκη και επίμονη προσέγγιση και απαιτεί την περιοδική επικοινωνία του χρήστη και του διανομέα του περιεχομένου.

Ενώ οι πιο σύγχρονες τεχνολογίες DRM χρησιμοποιούν ένα σύστημα κρυπτογράφησης παρόμοιο με αυτό του PKI, για τον έλεγχο της πρόσβασης των χρηστών στο ψηφιακό περιεχόμενο, μερικά συστήματα διανομής επιλέγουν την ενσωμάτωση του ψηφιακού περιεχομένου με ένα DRM λογισμικό. Έτσι η προστασία πνευματικών δικαιωμάτων δεν στηρίζεται μόνο στην καλή πίστη ενός χρήστη. Με την μεταφόρτωση του περιεχομένου στον υπολογιστή του χρήστη, δεν υπάρχει καμία περαιτέρω επαφή με το σύστημα διανομής. Οι χρήστες έχουν πρόσβαση στο ψηφιακό περιεχόμενο κάτω από συγκεκριμένους περιορισμούς. Εάν κάποιος χρήστης προσπαθήσει να εκτελέσει μια λειτουργία που δεν εγκρίνεται από το EULA, το ενσωματωμένο λογισμικό DRM που μεταφορτώνεται και εγκαθίσταται μαζί με το περιεχόμενο, θα τερματίσει την ενέργεια που πρόκειται να εκτελεστεί. Αυτή η προσέγγιση δεν έχει καταπατά την ιδιωτικότητα των χρηστών με την συλλογή προσωπικών πληροφοριών. Επίσης η χρήση του ψηφιακού περιεχομένου μπορεί να πραγματοποιηθεί με καθολική μυστικότητα, ακόμα και off-line. Εντούτοις, εκτός από τους προφανείς κινδύνους ασφάλειας, μια τέτοια προσέγγιση αποτελεί σοβαρή εισβολή στη μυστικότητα με την εγκατάσταση του λογισμικού στον υπολογιστή του χρήστη χωρίς πλήρη γνώση τους.

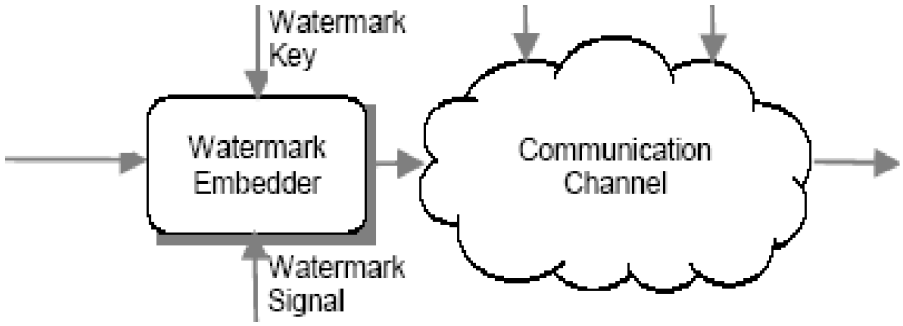
### 8.4 Ψηφιακό υδατογράφημα

Το υδατογράφημα δεν είναι μια νέα τεχνική. Είναι η συνέχεια μιας τεχνικής γνωστής ως στενογραφίας που έχει υπάρξει για τουλάχιστον μερικές εκατοντάδες χρόνια. Η στενογραφία είναι μια τεχνική για την κρυμμένη επικοινωνία. Σε αντίθεση με το σύστημα κρυπτογραφίας όπου το περιεχόμενο ενός μηνύματος επικοινωνίας είναι μυστικό, στη στενογραφία η ίδια η ύπαρξη του μηνύματος επικοινωνίας είναι ένα μυστικό και η παρουσία της είναι γνωστή μόνο από τα μέρη που συμμετέχουν στην επικοινωνία. Η στενογραφία είναι τεχνική απόκρυψης ενός μυστικού μηνύματος μέσα σε ένα άλλο ανεξάρτητο μήνυμα και η εμφάνισή του στο άλλο συμβαλλόμενο μέρος. Μερικές από τις τεχνικές στενογραφίας όπως η χρήση του αόρατου μελανιού, οι χωριζόμενες κατά διαστήματα λέξεις στα τυπωμένα έγγραφα, τα μηνύματα κωδικοποίησης στις συνθέσεις μουσικής, κ.λπ., έχουν χρησιμοποιηθεί από στρατιωτικές επιχειρήσεις από την εποχή του αρχαίου ελληνικού πολιτισμού.

Το υδατογράφημα μπορεί να θεωρηθεί ως ειδική τεχνική στενογραφίας όπου ένα μήνυμα ενσωματώνεται μέσα σε ένα άλλο και τα δύο μηνύματα συσχετίζονται το ένα με το άλλο με κάποιο τρόπο. Τα πιο κοινά παραδείγματα της υδατοσήμανσης είναι η παρουσία συγκεκριμένων σχεδίων στα χαρτονομίσματα που είναι ορατές μόνο όταν το φως πέφτει με συγκεκριμένη γωνία στο χαρτονόμισμα και τα λογότυπα των τυπωμένων εγγράφων κειμένου. Οι τεχνικές υδατοσήμανσης αποτρέπουν την παραποίηση των φυσικών αντικειμένων.

Το ψηφιακή υδατογράφημα είναι παρόμοια με το υ υδατογράφημα στα φυσικά αντικείμενα εκτός από το ότι η τεχνική της υδατοσήμανσης χρησιμοποιείται για το ψηφιακό περιεχόμενο αντί των φυσικών αντικειμένων. Στο ψηφιακό υδατογράφημα χαμηλής ενέργειας ένα σήμα ενσωματώνεται ανεπαίσθητα σε ένα άλλο σήμα. Το χαμηλής ενέργειας σήμα καλείται υδατόσημο και απεικονίζει μερικά μεταδεδομένα, όπως την ασφάλεια ή τις πληροφορίες δικαιωμάτων για το κύριο σήμα. Το κύριο σήμα στο οποίο το υδατογράφημα ενσωματώνεται ονομάζεται σήμα κάλυψης γιατί καλύπτει το

υδατογράφημα. Το σήμα κάλυψης είναι γενικά μια ακίνητη εικόνα, ένας ακουστικός συνδετήρας, μια τηλεοπτική ακολουθία ή ένα έγγραφο κειμένων σε ψηφιακή μορφή.




ΕΙΚΟΝΑ 23: ΈΝΑ ΑΠΛΟ ΣΥΣΤΗΜΑ ΨΗΦΙΑΚΟΥ ΥΔΑΤΟΓΡΑΦΗΜΑΤΟΣ

Το σύστημα ψηφιακού υδατογραφήματος αποτελείται ουσιαστικά από έλα σύστημα ενσωμάτωσης του υδατογραφήματος και έναν ανιχνευτή υδατογραφημάτων. Το σύστημα ενσωμάτωσης του υδατογραφήματος παρεμβάλλει ένα υδατογράφημα επάνω στο σήμα κάλυψης και ο ανιχνευτής υδατογραφημάτων ανιχνεύει την παρουσία σήματος υδατογραφημάτων. Μια οντότητα αποκαλούμενη κλειδί υδατογραφημάτων χρησιμοποιείται κατά τη διάρκεια της διαδικασίας. Το κλειδί υδατογραφημάτων έχει μια ένα προς ένα αντιστοιχία με το σήμα υδατογραφημάτων (δηλ., ένα μοναδικό κλειδί υδατογραφημάτων υπάρχει για κάθε σήμα υδατογραφημάτων). Το κλειδί υδατογραφημάτων είναι ιδιωτικό και γνωστό μόνο στα εξουσιοδοτημένα συμβαλλόμενα μέρη. Έτσι εξασφαλίζει ότι μόνο τα εξουσιοδοτημένα συμβαλλόμενα μέρη μπορούν να ανιχνεύσουν το υδατογράφημα. Αξίζει να σημειώσουμε ότι το κανάλι επικοινωνίας μπορεί να είναι θορυβώδες και εχθρικό επιρρεπές σε επιθέσεις ασφάλειας και ως εκ τούτου οι ψηφιακές τεχνικές υδατοσήμανσης πρέπει να είναι ελαστικές στις επιθέσεις θορύβου και ασφάλειας.

### *8.4.1 Εφαρμογές του ψηφιακού υδατογραφήματος*

Οι ψηφιακές τεχνικές υδατοσήμανσης έχουν τις εφαρμογές wide.ranging. Μερικές από τις εφαρμογές αναφέρονται παρακάτω.

- **Προστασία πνευματικών δικαιωμάτων**: Τα ψηφιακά υδατογραφήματα μπορούν να χρησιμοποιηθούν για να προσδιορίσουν και να προστατεύσουν την ιδιοκτησία πνευματικών δικαιωμάτων. Το ψηφιακό περιεχόμενο μπορεί να ενσωματωθεί με τα υδατογραφήματα απεικονίζοντας τα μεταδεδομένα που προσδιορίζουν τους ιδιοκτήτες πνευματικών δικαιωμάτων.
- **Προστασία αντιγράφων**: Το ψηφιακό περιεχόμενο μπορεί να υδατογραφηθεί για να δείξει ότι το περιεχόμενο δεν μπορεί να αναδιανεμηθεί παράνομα. Οι συσκευές ανίχνευσης αναδιανομής μπορούν έπειτα να ανιχνεύσουν τέτοια υδατογραφήματα και να αποτρέψουν την μη εξουσιοδοτημένη αναδιανομή του περιεχομένου.
- **Tracking:** Τα ψηφιακά υδατογραφήματα μπορούν να χρησιμοποιήσουν για να ακολουθήσουν τη χρήση του ψηφιακού περιεχομένου. Κάθε αντίγραφο του ψηφιακού περιεχομένου μπορεί να είναι μεμονωμένα watermarked με τα μεταδεδομένα που διευκρινίζουν τους εξουσιοδοτημένους χρήστες του περιεχομένου. Τέτοια υδατογραφήματα μπορούν να χρησιμοποιηθούν για να ανιχνεύσουν την παράνομη αναδιανομή του περιεχομένου με τον προσδιορισμό των χρηστών που διέδωσαν το περιεχόμενο παράνομα. Η τεχνική υδατοσήμανσης που χρησιμοποιείται για την καταδίωξη καλείται fingerprint.

## 8.5 Ηλεκτρονικές υπογραφές

Μια παρόμοια με αυτή της κρυπτογράφησης μέθοδος χρησιμοποιείται για τη δημιουργία «ψηφιακών υπογραφών» που μπορούν να χρησιμοποιούνται για την πιστοποίηση της ταυτότητας ενός προσώπου για να μπορεί να διαπιστωθεί αν δικαιούται να έχει πρόσβαση σε ένα ψηφιακό έργο. Μια

απλή ψηφιακή υπογραφή αποτελείται από τον κώδικα του κρυπτογραφημένου μηνύματος. Όταν ένα άτομο υπογράψει το μήνυμά του και το στείλει σε ένα άλλο μαζί με ψηφιακή υπογραφή, το άλλο άτομο μπορεί να αποκρυπτογραφήσει την υπογραφή χρησιμοποιώντας το κλειδί αποκρυπτογράφησης και να συγκρίνει το αποτέλεσμα με το κείμενο που έλαβε. Εάν είναι ταυτόσημα, μπορεί να υποθέσει ότι το μήνυμα έφτασε πράγματι από τον αποστολέα του και όχι από κάποιον άλλο.

### 8.6 Ψηφιακά πιστοποιητικά

Μια τρίτη μέθοδος πιστοποίησης που είναι όμοια με τις ψηφιακές υπογραφές είναι τα «ψηφιακά πιστοποιητικά». Τα πιστοποιητικά αυτά ταυτοποιούν τους χρήστες στον ψηφιακό κόσμο και διανέμονται έναντι τρίτου από εταιρίες γνωστές ως «Αρχές Πιστοποίησης». Ένα ψηφιακό πιστοποιητικό περιέχει τον αριθμό έκδοσής του, τον σειριακό αριθμό χρήστη, τον αλγόριθμο κρυπτογράφησης που χρησιμοποιήθηκε για τη δημιουργία της υπογραφής του, το όνομα της Αρχής Πιστοποίησης που το εκδίδει, την ημερομηνία λήξης του πιστοποιητικού, το όνομα χρήστη, το δημόσιο κλειδί κρυπτογράφησης και την ψηφιακή υπογραφή του χρήστη. Τα πιστοποιητικά αυτά είναι αρκετά σημαντικά και βοηθούν στην ασφάλεια, αφού οι administrators διάφορων συστημάτων μπορούν να ελέγχουν με διάφορους τρόπους από ποιες Αρχές πιστοποίησης τα πιστοποιητικά θα δέχονται από τους servers και ποια όχι. Μια αρκετά γνωστή εταιρία που δρα ως «Αρχή πιστοποίησης» είναι η VeriSign.(www.VeriSign.com ).

Για να αυξηθεί περισσότερο η ασφάλεια στο Διαδίκτυο και να αξιοποιηθούν οι προαναφερθείσες μέθοδοι, έχουν αναπτυχθεί ειδικά πρωτόκολλα ασφαλούς επικοινωνίας που μπορούν να χειρίζονται μόνο την κρυπτογράφηση και την αποκρυπτογράφηση της πληροφορίας. Ένα παράδειγμα είναι το πρωτόκολλο στρώματος ασφαλούς σωλήνωσης (Secure Socket Layer Protocol – SSL), για το οποίο μπορείτε να βρείτε περαιτέρω πληροφορίες στο παράρτημα σχετικά με την κρυπτογραφία . Το πρωτόκολλο αυτό λειτουργεί ως εργαλείο πιστοποίησης και για άλλα πρωτόκολλα Διαδικτυακών εφαρμογών όπως το HTTP, SMTP, TELNET, FTP κλπ.

### 8.7 Σύστημα κωδικοποιημένου περιεχομένου (Content Scramble System)

Το Content Scramble System (CSS) είναι μια τεχνολογία DRM που χρησιμοποιείται σε όλα σχεδόν τα εμπορικά DVD. Χρησιμοποιεί αλγόριθμο κρυπτογράφησης 40-bit.
Στους κατασκευαστές DVD συσκευών ή δίσκων δόθηκαν σετ κλειδιών CSS από την εταιρεία DVD Copy Control Association, για να ενσωματώσουν τα κλειδιά αυτά στις συσκευές (σε CSS Decryption Modules) ή στους δίσκους που κατασκευάζουν. Ένα κλειδί CSS αποτελείται από επιμέρους κλειδιά:

- Authentication Key (Κλειδιά ταυτοποίησης) Χρησιμοποιείται από το DVD drive και το CSS Decryption module της συσκευής κατά την πρώτη ανάγνωση του δίσκου και πριν την ανάγνωση των δεδομένων, για να είναι δυνατή η συμβατότητα και συνεργασία μεταξύ τους.
- Title keys (Κλειδιά τίτλου) χρησιμοποιούνται για τον τεμαχισμό και την ενοποίηση των δεδομένων στα DVD. Ένα τίτλος μπορεί να είναι μια ολόκληρη ταινία ή ένα τμήμα της.
- Disc keys (Κλειδιά δίσκου) Χρησιμοποιούνται για την αποκρυπτογράφηση των κλειδιών τίτλου.
- Player keys (Κλειδιά αναπαραγωγής) Χρησιμοποιούνται για την αποκρυπτογράφηση των κλειδιών δίσκου στα DVD. Σε κάθε κατασκευαστή DVD συσκευών αντιστοιχεί ένα από τα περίπου 400 κλειδιά για να το ενσωματώσει στις συσκευές που παράγει.

Τα κλειδιά σε επίπεδο DVD Disc, αποθηκεύονται στις αρχικές περιοχές του δίσκου (lead-in area). Ο σκοπός του CSS είναι διττός. Κυρίως δεν επιτρέπει την αντιγραφή byte προς byte μιας ροής βίντεο MPEG, αφού κατά την αντιγραφή δεν θα συμπεριληφθούν τα απαραίτητα κλειδιά που όπως αναφέρθηκε παραπάνω βρίσκονται κρυμμένα στην lead-in περιοχή του DVD Disc. Επίσης επιβάλλει την συμβατότητα των συσκευών διαφορετικών κατασκευαστών και διέπεται από τα ακόλουθα χαρακτηριστικά:

- Τα περιεχόμενα των DVD είναι κρυπτογραφημένα

- Τα κλειδιά που επιτρέπουν την αναπαραγωγή των DVD είναι επίσης κρυπτογραφημένα
- Μόνο οι συσκευές που είναι κατασκευασμένες με άδεια από το CSS μπορούν να αναπαράγουν τις ταινίες στα DVD.
- Οι συσκευές απαγορεύουν την αντιγραφή περιεχομένου από τα DVD εκτός εξαιρετικών περιπτώσεων.

Από τη στιγμή που μια συσκευή αναπαραγωγής υλικού εξασφαλίσει άδεια από το CSS, εξυπονοείται ότι «αποδέχεται» και λειτουργεί σύμφωνα με τους ακόλουθους κανόνες:.

- Το περιεχόμενο που αποκρυπτογραφείται από τη συσκευή πρέπει να προστατεύεται από μη εξουσιοδοτημένη χρήση από «μέσα» από τη συσκευή. Με λίγα λόγια από αποσυναρμολόγηση και μετατροπή της συσκευής.
- Τα περιεχόμενα των DVD μπορούν να αναπαράγονται σε συγκεκριμένες συσκευές εξόδου όπως αναλογικές εξόδους με τεχνολογία που εμποδίζει την αντιγραφή (με τρόπους που θα δούμε αργότερα) όπως αναλογικά VCR, και ασφαλείς ψηφιακές εξόδους όπως είναι το DTCP που θα δούμε επίσης αργότερα.
- Συσκευές που πωλούνται σε διαφορετικές γεωγραφικές ζώνες μπορούν να αναπαράγουν DVDs που φτιάχτηκαν ειδικά για αναπαραγωγή στις ίδιες ζώνες.
- Όταν οι κατασκευαστές των συσκευών που έχουν άδεια από το CSS παραβιάζουν τους κανόνες διώκονται δικαστικά.
- Τα στούντιο παραγωγής ταινιών δικαιούνται να κωδικοποιούν τα ίδια τις ταινίες τους και να απαγορεύουν την αντιγραφή των DVDs τους

### 8.8 Ασύμμετρος Κατακερματισμός Εφαρμογών

Asymmetric Application Segmentation (AAS) ονομάζεται η τεχνική αφαίρεσης ενός κομματιού από τον εκτελέσιμο κώδικα ενός προγράμματος το οποίο κομμάτι έπειτα αποθηκεύεται σε έναν απομακρυσμένο server και στην θέση του αντί να μείνει κενό δημιουργείται ένα ειδικό κομμάτι κώδικα συγκεκριμένο για τέτοιες περιπτώσεις, τον «γάντζο» (hook). Όταν ο χρήστης εκτελεί το πρόγραμμα, σε κάποια στιγμή απαιτείται να εκτελεστεί το κομμάτι του κώδικα που λείπει. Τότε διαβάζεται από τη μνήμη ο κώδικας του «γάντζου». Μέσω του κώδικα γάντζου, το πρόγραμμα επικοινωνεί με τον απομακρυσμένο σερβερ όπου είναι αποθηκευμένο το κομμάτι που λείπει. Ο server κάνει πιστοποίηση και εκτελεί το κώδικα που είναι αποθηκευμένος σε αυτόν και γυρίζει το αποτέλεσμα στον χρήστη.

### 8.9 Προστασία Περιεχομένου από ψηφιακή μετάδοση

Η τεχνολογία Digital Transmission Content Protection (DTCP)έχει ως σκοπό αυτής να αποτρέπει τη μη εξουσιοδοτημένη διανομή και αντιγραφή οπτικοακουστικού υλικού που υπάρχει στα σπίτια σε ψηφιακή αποκρυπτογραφημένη μορφή. Αυτή η τεχνολογία ελέγχει την μετάδοση χρησιμοποιώντας μια συσκευή «πηγή» με DTCP (καλωδιακή ή δορυφορική τηλεόραση, DVD Player, PlayStation) η οποία αναπαράγει το οπτικοακουστικό υλικό και μια πηγή «νεροχύτη» η οποία το προβάλλει (Απλή οικιακή τηλεόραση, ηλεκτρονικός υπολογιστής, VCR). Η συσκευή "sink device" προγραμματίζεται έτσι ώστε το περιεχόμενο που προβάλλεται να μην μπορεί να διανεμηθεί στο internet. Η τεχνολογία DTCP εκδίδει ειδικές άδειες όπως η CSS όπως αναφέρθηκε πιο πάνω.

### 8.10 Σύστημα διαχείρισης σειριακής αντιγραφής

Το Serial Copy Management System (SCMS) σύστημα αποτρέπει την παράνομη παραγωγή πολλών γενεών ψηφιακών αντιγράφων (αντίγραφα των αντιγράφων) από ένα αυθεντικό έργο προστατευμένο από νόμους πνευματικής ιδιοκτησίας. Αυτό γίνεται με την βοήθεια υδρογραφημάτων (watermarks). Υδατογράφημα ονομάζεται η πληροφορία που είναι ψηφιακά κωδικοποιημένη και έχει ενσωματωθεί ψηφιακά μέσα σε ένα ψηφιακό αρχείο με τρόπου ώστε να είναι φανερή ή κρυφή. Η πληροφορία από ένα υδατογράφημα χρησιμοποιείται για να ταχτοποιηθεί το έργο ή ο δημιουργός του

και να εντοπιστούν τα αντίγραφά του. Στην περίπτωση του φανερού υδρογραφήματος το ψηφιακό αρχείο ορίζεται ακατάλληλο για αναπαραγωγή ή προς έκθεση. Τα υδρογραφήματα επίσης χρησιμοποιούνται σε έργα που χρησιμοποιούνται μόνο για λόγους διαφήμισης και προώθησης, ή ως δείγματα.

ΕΙΚΟΝΑ 24 : ΟΡΑΤΟ ΥΔΑΤΟΓΡΑΦΗΜΑ ΣΕ ΕΙΚΟΝΑ

Τα υδρογραφήματα ενσωματώνονται στο έργο (είτε εικόνας, είτε κειμένου, είτε βίντεο, είτε ήχου) με τη χρήση ειδικού λογισμικού. Το λογισμικό αυτό μπορεί να ελέγξει την ύπαρξη αόρατου υδρογραφήματος σε ένα αρχείο και να διαβάσει όλες τις πληροφορίες που έχουν προστεθεί μέσω της υδατογράφησης. Οι πληροφορίες αυτές μπορούν να αφαιρεθούν μόνο αν είναι ακριβώς οι ίδιες με αυτές που προστέθηκαν . Ένα αόρατο υδατογράφημα πρέπει να μην αλλοιώνει την αρχική εικόνα του έργου αλλά να είναι ανιχνεύσιμο, ενώ ένα ορατό υδατογράφημα πρέπει να μην μπορεί να αφαιρεθεί εύκολα από μη εξουσιοδοτημένους χρήστες.

Στο ίδιο κλίμα, οι καλές τεχνικές ψηφιοποίησης περιεχομένου της Ευρωπαϊκής Ένωσης προτείνουν όλες οι εικόνες αλλά και τα βίντεο ή ηχητικά αποσπάσματα να είναι διαθέσιμα στο διαδίκτυο σε πολύ χαμηλή ανάλυση ή ευκρίνεια, είτε να προστίθεται σε αυτά θόρυβος, ή να υπόκεινται σε γεωμετρικούς μετασχηματισμούς, φιλτράρισμα, οριζόντια και κάθετη μετατόπιση frames κλπ, ούτως ώστε όποιος θέλει να μπορεί να τα βλέπει, αλλά να μην του είναι χρήσιμα για αντιγραφή και άλλη χρήση.

### 8.11 Προστασία Περιεχομένου από ψηφιακή μετάδοση

Digital Transmission Content Protection (DTCP). Ο σκοπός αυτής της τεχνολογίας είναι να αποτρέπει μη εξουσιοδοτημένη διανομή οπτικοακουστικού υλικού που υπάρχει στο σπίτι σε ψηφιακή μορφή σε αποκρυπτογραφημένη μορφή. Αυτή η τεχνολογία ελέγχει την μετάδοση χρησιμοποιώντας μια συσκευή «πηγή» με DTCP (καλωδιακή ή δορυφορική τηλεόραση, DVD Player, PlayStation) η οποία αναπαράγει το οπτικοακουστικό υλικό και μια πηγή «νεροχύτη» η οποία το προβάλλει (Απλή οικιακή τηλεόραση, ηλεκτρονικός υπολογιστής, VCR). Η συσκευή «νεροχύτης» (sink device) προγραμματίζεται με τρόπο που να μην μπορεί να διανέμει το περιεχόμενο που προβάλλει στο διαδίκτυο. Η τεχνολογία εκδίδει και αυτή με τη σειρά της ειδικές άδειες, όπως κάνει και η CSS που είδαμε πιο πριν.

### 8.12 Secure Digital Music Initiative

Secure Digital Music Initiative (SDMI). Από τη στιγμή που η κρυπτογράφηση δεν εφαρμόστηκε στα απλά CD μουσικής, η μουσική μπορεί εύκολα να αντιγραφεί και μάλιστα να συμπιεστεί με το πρότυπο mp3 και να αναπαραχθεί ή να διανεμηθεί πανεύκολα στο διαδίκτυο, σε φορητές συσκευές, σκληρούς δίσκους, κάρτες μνήμης, κινητά τηλέφωνα κλπ. Για να αντιμετωπιστούν τα προβλήματα στην προστασία των ψηφιακών πνευματικών δικαιωμάτων που προέκυψαν από αυτό, ανέλαβε πρωτοβουλία μια τεράστια ομάδα από 200 εταιρίες και οργανισμούς που εκπροσώπευαν τον

χώρο της πληροφορικής, των ηλεκτρονικών συσκευών, τις τεχνολογίες της ασφάλειας, την παγκόσμια δισκογραφία και τους παροχείς υπηρεσιών διαδικτύου, να καταγράψει οδηγίες και προδιαγραφές που σκόπευαν στην υλοποίηση τεχνολογιών προστασίας των εμπορικών μουσικών κομματιών. Οι οδηγίες αυτές διακήρυτταν ένα «άτρωτο» και αδιάβλητο σύστημα κρυπτογράφησης και υδατογραφημάτων το οποίο θα προστάτευε τα μουσικά κομμάτια από μη εξουσιοδοτημένη αναπαραγωγή και χρήση (αντιγραφή και διαμοιρασμό). Τα αποτελέσματα αυτού του κολοσσιαίου και πολλά υποσχόμενου εγχειρήματος εξετάζονται στο επόμενο κεφάλαιο, μαζί με τα αποτελέσματα όλων των άλλων, καθώς το επόμενο κεφάλαιο εξετάζει τους παράγοντες αποτυχίας όλων αυτών των μέτρων.

### 8.13 Windows Media DRM

Η Microsoft για να εξασφαλίσει ελεγχόμενη ροή πολυμέσων δημιούργησε το σύστημα διαχείρισης πνευματικών δικαιωμάτων με τον τίτλο Windows Media DRM. Η υπηρεσία αυτή υποστηρίζεται στην πλατφόρμα Windows. Είναι σχεδιασμένη έτσι ώστε να προσφέρει ασφαλή μετάδοση ήχου και βίντεο σε PC μέσα σε ένα IP δίκτυο. Επίσης είναι δυνατή η χρήση του συστήματος για την μετάδοση των πολυμέσων και σε άλλες συσκευές αναπαραγωγής (που είναι συμβατές με το Windows Media DRM). Το σύστημα περιλαμβάνει τα ακόλουθα μέρη:

- Windows Media Rights Manager (WMRM) SDK για την δημιουργία της ροής δεδομένων σύμφωνα με το WMDRM και για θέματα αδειών χρήσης των δεδομένων.
- Windows Media Format SDK (WMF SDK) για την δημιουργία εφαρμογών συμβατών με το WMDRM και σχετικά με το WMA πρότυπο της Microsoft.
- Windows Media DRM for Portable Devices (WMDRM-PD). Αυτό αφορά χρήση του συστήματος διαχείρισης της Microsoft σε φορητές συσκευές και για αναπαραγωγή που γίνεται όχι σε πραγματικό χρόνο (offline playback).
- Windows Media DRM for Network Devices (WMDRM-ND) για την μετάδοση προστατευμένου περιεχομένου σε συσκευές οικιακού δικτύου.

Το σύστημα διαχείρισης σχεδιάστηκε ούτως ώστε να είναι εύκολη η αναβάθμισή του, αφού εξ αρχής η εταιρεία θεώρησε ότι θα «σπαστεί» ο αλγόριθμος και ότι θα είναι απαραίτητη η συχνή αναβάθμισή του. Πράγματι, αρκετές εκδόσεις του Windows Media DRM έχουν παραβιαστεί αρκετές φορές αλλά λόγω των συνεχών αναβαθμίσεων καμία δεν αποτέλεσε πανάκεια για να προσπεράσει κάποιος χρήστης τους περιορισμούς του συγκεκριμένου συστήματος διαχείρισης. Η πρώτη έκδοση κυκλοφόρησε τον Απρίλιο του 1999 και έδινε την δυνατότητα στους παρόχους προστατευμένου περιεχομένου να ελέγχουν βασικές λειτουργίες όπως πχ τις ημερομηνίες λήξης του περιεχομένου. Η δεύτερη έκδοση κυκλοφόρησε τον Ιανουάριο του 2003 και ήταν συμβατή με τις εκδόσεις του προγράμματος αναπαραγωγής των Windows, του Windows Media Player 7 και 9. Η τρίτη έκδοση, γνωστή και ως DRM v10 κυκλοφόρησε το 2004 και χρησιμοποιείται μέχρι και σήμερα.

### 8.14 Apple's Fair Play

Εάν ένα αρχείο προσφέρεται σε μορφή AAC, τότε κατά πάσα πιθανότητα έχει κωδικοποιηθεί με το σύστημα DRM της Apple που καλείται «Fair Play». Τα προστατευμένα αρχεία με την τεχνολογία Fair Play είναι αρχεία τύπου mp4 στα οποία ενθυλακώνεται μια κωδικοποιημένη μορφή ήχου AAC. Η ροή του ήχου κρυπτογραφείται χρησιμοποιώντας τον αλγόριθμο AES. Το βασικό κλειδί αποκρυπτογράφησης της κωδικοποιημένης μορφής ήχου επίσης ενθυλακώνεται στο αρχείο. Το κλειδί που απαιτείται για την αποκρυπτογράφηση του βασικού κλειδιού λέγεται «user key». Κάθε φορά που κάποιος πελάτης χρησιμοποιεί το πρόγραμμα iTunes για την αγορά ενός τραγουδιού δημιουργείται ένα καινούριο τυχαίο user key και χρησιμοποιείται για την κρυπτογράφηση του βασικού κλειδιού. Το user key αποθηκεύεται μαζί με τα στοιχεία λογαριασμού του χρήστη στους Servers της Apple και αποστέλλεται στο iTunes. Το iTunes καταχωρεί τα κλειδιά σε μια βάση δεδομένων. Από τη βάση αυτή, αντλεί κάθε φορά το κατάλληλο κλειδί που απαιτείται για την αποκρυπτογράφηση του βασικού κλειδιού. Χρησιμοποιώντας το βασικό κλειδί το πρόγραμμα μπορεί να αποκρυπτογραφήσει την μορφή AAC και να αναπαράγει το αρχείο. Τα δικαιώματα που δίνονται στους χρήστες είναι :

- Αναπαραγωγή σε οποιοδήποτε αριθμό iPod ή iPhone (Οι συσκευές διαθέτουν επίσης βάσεις δεδομένων με τα κλειδιά. Έτσι κατά την αντιγραφή του αρχείου από τον υπολογιστή στο iPod ή στο iPhone, αντιγράφονται επίσης όλα τα απαραίτητα στοιχεία για την αναπαραγωγή του αγορασμένου αρχείου. Αυτό εύλογα καθιστά αδύνατη την αναπαραγωγή των εν λόγω αρχείων σε συσκευές άλλου τύπου)
- Αναπαραγωγή μέχρι και σε 5 διαφορετικούς υπολογιστές
- Οποιαδήποτε Playlist που περιλαμβάνει τραγούδια προστατευμένα με FairPlay μπορεί να εγγραφεί μέχρι 7 φορές σε Audio CD
- Οποιοδήποτε τραγούδι μπορεί να εγγραφεί σε Audio CD άπειρες φορές

Βλέπουμε από τα παραπάνω ότι μέσω της τεχνολογίας Fair Play δεν επηρεάζεται η δυνατότητα αντιγραφής (αφού είναι εφικτή σε CD), αλλά η δυνατότητα αναπαραγωγής του σε συγκεκριμένα μέσα.

### 8.15 Adobe Content Server

Ο Adobe Content Server επιτρέπει την διανομή ηλεκτρονικών βιβλίων και εγγράφων από οποιοδήποτε διαδικτυακό τόπο, με ασφαλή και αξιόπιστο τρόπο. Τα αρχεία διανέμονται σε μορφή PDF (Portable Document Format) ή ePUB παρέχοντας ταυτόχρονα ένα ολοκληρωμένο σύστημα διαχείρισης δικαιωμάτων (DRM). Ο Adobe Content Server είναι το εργαλείο που προσφέρει τις υπηρεσίες διαχείρισης δικαιωμάτων και διασυνδέει αρκετές από τις ανεξάρτητες λειτουργικές μονάδες της βιομηχανικής αλυσίδας εκμετάλλευσης ψηφιακού περιεχομένου. Υπάρχει η δυνατότητα ενσωμάτωσης του Server στην ήδη υπάρχουσα διαδικτυακή υποδομή ενός οργανισμού, ή ακόμα και η λειτουργία του ως ανεξάρτητη υπηρεσία σε έναν Application Service Provider (ASP).

Η δημιουργία ενός ασφαλούς και σταθερού περιβάλλοντος για τη διανομή και την πώληση ψηφιακού περιεχομένου, παρέχει νέους τρόπους διάθεσης και νέα επιχειρηματικά μοντέλα για τη βιομηχανία διανομής περιεχομένου.

Ο Adobe Content Server βασίζεται στα πιο σύγχρονα σχήματα διαχείρισης δικαιωμάτων ψηφιακού περιεχομένου και ενσωματώνει τη μέγιστη δυνατή ασφάλεια που στηρίζεται στην τεχνολογία της κρυπτογραφίας που αναπτύσσεται στα εργαστήρια της RSA.

### 8.16 DRM και eBooks

Οι πλατφόρμες έκδοσης e-books, οι παραδοσιακοί εκδότες και οι κατασκευαστές e-readers φρόντισαν να πάρουν από νωρίς τα μέτρα τους. Έτσι, το κλείδωμα των ηλεκτρονικών βιβλίων είναι πολύ πιο αποτελεσματικό από τη μουσική όχι μόνο την εποχή της κασέτας, αλλά και την εποχή του CD για τη μουσική και του DVD για τις ταινίες. Αν οι αυξημένες δυνατότητες της ψηφιακής εποχής επέτρεπαν τη χωρίς κόστος και γρήγορη αντιγραφή της μουσικής από τα CD και τα DVD στον υπολογιστή, οι ακόμα μεγαλύτερες δυνατότητες της τεχνολογίας σήμερα χρησιμοποιούνται για να γίνεται το κλείδωμα των e-books όλο και πιο πολύπλοκο και όλο και πιο αποτελεσματικό.

Το κλείδωμα των e-books σήμερα, η "διαχείριση των πνευματικών τους δικαιωμάτων" (Digital Rights Management - DRM), διακρίνεται σε τρεις κατηγορίες, ανάλογα με το πόσοι περιορισμοί υπάρχουν για την ανάγνωση των βιβλίων.

Στην πρώτη κατηγορία είναι ο πρωταθλητής του κλειδώματος, το Amazon, με τις συσκευές Kindle και τα Kindle e-books. Τα e-books του Amazon δεν είναι απλά κλειδωμένα με την έννοια ότι κανείς δεν μπορεί να τα αντιγράψει ή να τα διαβάσει χωρίς να τα έχει αγοράσει. Πρόκειται για κάτι πολύ περισσότερο, κανένας άλλος ηλεκτρονικός αναγνώστης δεν μπορεί να διαβάσει τα e-books του Amazon και κανένα αρχείο από κανένα άλλο βιβλιοπωλείο δεν μπορεί να διαβαστεί στις συσκευές Kindle. Άρα τα e-books που αγοράζει κανείς από το Amazon μπορούν να διαβαστούν μόνο από το δικό του ηλεκτρονικό αναγνώστη και από τη στιγμή που αγοράζει τη συσκευή δεν μπορεί να αγοράσει κανένα e-book από άλλο βιβλιοπωλείο. Και για να είναι σίγουρο το Amazon για όλα αυτά έχει αποκλείσει εντελώς τα αρχεία ePUB, που είναι τα πιο διαδεδομένα σήμερα στα online βιβλιοπωλεία e-books, ενώ μπορεί να καταργήσει από τη συσκευή σας ένα αγορασμένο e-book για

τον οποιοδήποτε λόγο, όπως είχε κάνει -ειρωνικά- τον Ιούλιο του 2009 με το "1984" και τη "Φάρμα των Ζώων" του Τζωρτζ Όργουελ γιατί αποφάσισε να σταματήσει να τα πουλάει (επέστρεψε τα χρήματα σε όσους τα είχαν αγοράσει, αλλά δεν είναι αυτό το θέμα). Ακόμα χειρότερα, αν αποφασίσετε να αγοράσετε κάποια στιγμή έναν άλλο ηλεκτρονικό αναγνώστη, που δεν είναι Kindle, τότε απλά δε θα έχετε πρόσβαση στη βιβλιοθήκη σας. Πρόκειται λοιπόν για κάτι πολύ παραπάνω από την προστασία από την "πειρατεία", είναι μια προσπάθεια του Amazon να μονοπωλήσει την αγορά των e-books και των ηλεκτρονικών αναγνωστών, βασιζόμενο και στις καλές του συσκευές και στο πλούσιο σε περιεχόμενο βιβλιοπωλείο του. Χωρίς ένα μεγάλο κατάλογο e-books και χωρίς μια συσκευή υψηλού επιπέδου όλο αυτό το κλείδωμα δε θα είχε νόημα και θα απομόνωνε στην αγορά το Amazon. Τέλος, το κλείδωμα των e-books επιτρέπει και μια ακόμα στρατηγική κίνηση: οι συσκευές είναι σχετικά φτηνές και η τιμή τους δεν είναι μόνο το προϊόν μιας έγκαιρης εισόδου στην αγορά των e-books και μιας σειράς σωστών αποφάσεων για την καλύτερη σχέση τιμής και δυνατοτήτων της συσκευής με βάση τη διαθέσιμη τεχνολογία σήμερα, είναι επίσης το αποτέλεσμα της επιδότησης της τιμής της συσκευής με το στόχο την πώληση περισσότερων e-books από το Amazon, κάτι αρκετά σίγουρο με δεδομένο ότι δεν μπορεί να αγοράσει ο κάτοχος Kindle από πουθενά αλλού.

Στη δεύτερη κατηγορία εντάσσονται το Barnes & Noble, με τη συσκευή Nook και τα δικά του e-books, και η Apple με την εφαρμογή της iBooks στο iPad, το iPhone και το iPod Touch και το iBookstore. Τα πράγματα εδώ και η στρατηγική είναι παρόμοια. Λόγω της πιο αδύναμης θέσης του Barnes & Noble, κυρίως γιατί άργησε να μπει σε αυτήν την αγορά, τα δικά του e-books είναι κλειδωμένα με ένα ειδικό, αποκλειστικό κλείδωμα με το Adobe Content Server, οπότε δε διαβάζονται σε κανέναν άλλο ηλεκτρονικό αναγνώστη, αλλά επιτρέπει την ανάγνωση κλειδωμένων e-books και από άλλα βιβλιοπωλεία που χρησιμοποιούν το στάνταρτ κλείδωμα με το Adobe Content Server, που όμως δεν μπορούν να κατέβουν απευθείας μέσω ιντερνέτ στη συσκευή, αλλά πρέπει να περάσουν πρώτα από τον υπολογιστή. Εύκολες και γρήγορες αγορές λοιπόν μόνο από το site του Barnes & Noble. Και πάλι εδώ βλέπουμε ότι οι σκοποί του κλειδώματος είναι πολύ πέρα από την προστασία από την αντιγραφή. Η Apple ακολουθεί μια αντίστοιχη τακτική με το Barnes & Noble, εξάλλου είναι γνωστή για τα κλειστά της συστήματα. Με το πλεονέκτημα που της δίνει το iPad, δεν επιτρέπει την ανάγνωση των δικών της e-books έξω από το δικό της σύστημα συσκευών, αλλά οι συσκευές της διαβάζουν κλειδωμένα e-books από άλλα online βιβλιοπωλεία με την εγκατάσταση της αντίστοιχης δωρεάν εφαρμογής.

Amazon και Barnes & Noble είναι αλήθεια ότι προφέρουν εφαρμογές για την ανάγνωση στους υπολογιστές, στα κινητά και στο iPad. "Buy once, read everywhere", είναι το σλόγκαν του Amazon. Οι εφαρμογές αυτές δε χαλαρώνουν ιδιαίτερα το κλείδωμα, γιατί καμιά τους δε δίνει τη δυνατότητα ανάγνωσης σε έναν ανταγωνιστικό ηλεκτρονικό αναγνώστη, σε μια συσκευή που να έχει και αυτή οθόνη ηλεκτρονικοί χαρτιού. Η Apple, που δεν έχει δική της συσκευή e-reader, διαθέτει εφαρμογές για το iPad, το iPhone και το iPod Touch, όχι όμως για Mac OS και Windows, κάτι όμως πιθανόν να αλλάξει στο μέλλον τουλάχιστον για τους Mac.

Στην τρίτη κατηγορία ανήκουν, με τις διαφορές τους, όλα τα υπόλοιπα βιβλιοπωλεία και όλοι οι υπόλοιποι κατασκευαστές e-books που κλειδώνουν τα e-books τους. Πρόκειται για κλείδωμα με το Adobe Content Server, που χρησιμοποιεί το ADEPT (Adobe Digital Experience Protection Technology). Εδώ, τα αρχεία μπορούν να διαβαστούν από όλους τους ηλεκτρονικούς αναγνώστες που συνεργάζονται με το Adobe Digital Editions, χοντρικά με όλους τους ηλεκτρονικούς αναγνώστες που δεν είναι Kindle. Σε αυτήν την κατηγορία ανήκει και η Kobo, που κατασκευάζει τους ομώνυμους ηλεκτρονικούς αναγνώστες και συνεργάζεται με το βιβλιοπωλείο Borders, με το έξτρα πλεονέκτημα ότι διαθέτει εφαρμογές για κινητά και tablet PC. Στην περίπτωση της χρήσης του ADEPT της Adobe φτάνουμε στην ουσία του τι σημαίνει κλείδωμα ενός e-book. Ένα τυπωμένο βιβλίο δανείζεται και χαρίζεται ή μπορεί και να μεταπωληθεί, αλλά, πέρα από αυτά, δεν μπαίνουν όροι μετά την πώλησή του στο πώς θα το χρησιμοποιήσει κανείς, πού θα μπορεί να το διαβάζει κανείς και πού όχι. Με τα κλειδωμένα e-books με το Adobe Content Server μπορεί να υπάρχουν δυνατότητες στην επιλογή συσκευής, αλλά το αρχείο σας δεν μπορεί να μετατραπεί (που αρκετές φορές χρειάζεται) και δεν μπορεί να διαβαστεί από το πρόγραμμα της επιλογής σας, μόνο με το Adobe Mobile Reader που συνεργάζεται με το Adobe Digital Editions. Δεν μπορεί να διαβαστεί απαραίτητα σε όσες συσκευές έχετε (e-readers, υπολογιστές κλπ). Δυνητικά η Adobe επιτρέπει μέχρι 6 συσκευές (και παραπάνω αν της το ζητήσετε), αλλά στην πράξη οι εκδότες περιορίζουν το νούμερο. Επίσης, αρκετές πλατφόρμες έχουν περιορισμούς στο πόσες φορές μπορείς να κατεβάσεις το ίδιο βιβλίο. Έτσι, αν καταστραφεί ο

σκληρός σας δίσκος, δεν είναι απίθανο να χάσετε και τα e-books που έχετε αγοράσει. Το Adobe Digital Editions κάνει την αγορά πιο περίπλοκη απ' όσο χρειάζεται, καθώς απαιτεί την εγκατάσταση ενός ειδικού software, που ναι μεν είναι δωρεάν και υπάρχει τόσο για Windows όσο και για Mac OS (αλλά όχι για Linux), αλλά θα ήταν περιττό αν δεν υπήρχε το κλείδωμα. Το ίδιο το κλείδωμα μάλιστα έχει κόστος, το οποίο, παρόλο που όσο περισσότερα e-books έχει ένας εκδότης ή μια ψηφιακή πλατφόρμα έκδοσης η επιβάρυνση είναι μικρότερη ανά βιβλίο, μετακυλύετε στον αγοραστή του e-book.

### 8.17 DRM και ταινίες

Ένα από τα πρώτα παράδειγμα ενός DRM συστήματος είναι το Σύστημα Ανακατεμένου Περιεχόμενου (Content Scrambling System (CSS)), που χρησιμοποιήθηκε από το DVD- forum για ταινίες τύπου DVD περίπου από το 1996. Το Content Scrambling System (CSS) χρησιμοποίει έναν απλό αλγόριθμο κρυπτογράφησης και απαιτεί από τους κατασκευαστές συσκευών να υπογράψουν συμφωνίες αδειών. Το Advanced Access Content System (AACS) είναι ένα σύστημα DRM για HD-DVD και δίσκους Blue-Ray που αναπτύσσονται από τον AACS εξουσιοδοτημένο διαχειριστή, LLC (AACS LA), μια κοινοπραξία που περιλαμβάνει τη Disney, την Intel, τη Microsoft, τη Matsushita (Panasonic), τους Warner Brothers, την IBM, τη Toshiba και τη Sony. Τον Δεκέμβριο του 2006 ένα κλειδί δημοσιεύθηκε στο διαδίκτυο από τους crackers, επιτρέποντας την απεριόριστη πρόσβαση στο AACS -περιορισμένο περιεχόμενο των HD-DVD. Αφότου ανακλήθηκαν τα σπασμένα κλειδιά, τα περαιτέρω σπασμένα κλειδιά απελευθερώθηκαν.

Η έννοια broadcast flag concept αναπτύχθηκε με τη Fox Broadcasting το 2001 και υποστηρίχθηκε από το MPAA και τη FCC. Μια απόφαση τον Μάιο του 2005 από ένα αμερικανικό Εφετείο υποστήριξε ότι η FCC στερήθηκε την αρχή για να την επιβάλει στη τηλεοπτική βιομηχανία στις ΗΠΑ. Απαίτησε ότι όλα HDTVs υπακούνε μια καθοριστική προδιαγραφή stream, εάν το stream μπορεί ή όχι να καταγραφεί. Αυτό θα μπορούσε να εμποδίσει τις περιπτώσεις δίκαιης χρήσης, όπως η χρόνο-μετατόπιση. Αυτό έτυχε περισσότερης επιτυχίας αλλού, όταν υιοθετήθηκε από το ψηφιακό τηλεοπτικό πρόγραμμα ραδιοφωνικής αναμετάδοσης (DVB), μια κοινοπραξία περίπου 250 εκφωνητών, κατασκευαστών, χειριστών δικτύων, υπεύθυνων για την ανάπτυξη λογισμικού, και ρυθμιστικών οργανισμών περίπου 35 χώρες που συμμετέχουν στην προσπάθεια να αναπτυχθούν τα νέα ψηφιακά πρότυπα TV.

Μια ενημερωμένη παραλλαγή του broadcast flag έχει αναπτυχθεί στην προστασίας περιεχομένου και διαχείριση αντιγράφων (DVB-CPCM). Αναπτύχθηκε ιδιωτικά, και η τεχνική προδιαγραφή υποβλήθηκε ευρωπαϊκά τον Μάρτιο του 2007. Όπως με πολλά DRM, το σύστημα CPCM προορίζεται να ελέγξει το είδος χρήση του υλικού από τον τελικό χρήστη, για το συμφέρον του κατόχου πνευματικών δικαιωμάτων. Το DVB υποστηρίζει ότι τα συστήματα δεδομένων θα εναρμονίσουν τους ελέγχους των κατόχων των πνευματικών δικαιωμάτων στις διαφορετικές τεχνολογίες και θα καταστήσουν έτσι τα πράγματα ευκολότερα για τους τελικούς χρήστες. Το σύστημα CPCM αναμένεται για να υποβληθεί στο ευρωπαϊκό ίδρυμα broadcast flag το 2008.

### 8.18 DRM και μουσική

#### 8.18.1 Ακουστικά CDs

Το 2002, η Bertelsmann, που περιλαμβάνει τις BMG, Arista και RCA, ήταν η πρώτη εταιρία που χρησιμοποίησε DRM σε ακουστικό CDs. Αυτό έγινε αρχικά σε προωθητικά CDs, αλλά όλα τα CDs από αυτές τις επιχειρήσεις θα χρησιμοποιούσαν τελικά κάποιο DRM σύστημα. Πρέπει να σημειωθεί ότι οι δίσκοι με εγκατεστημένο DRM σύστημα δεν είναι νόμιμα πρότυπα Compact Disc (CDs) αλλά κάποια μέσα CD-ROM, επομένως στερούνται το λογότυπο CD που βρίσκεται σε δίσκους που ακολουθούν τα πρότυπα. Εντούτοις, αυτά τα CDs δεν θα μπορούσαν να παιχτούν σε όλα τα

μηχανήματα αναπαραγωγής CD. Επίσης πολλοί καταναλωτές δεν θα μπορούσαν να παίξουν τα αγορασμένα CDs στους υπολογιστές τους.

Το 2005, η Sony BMG εισήγαγε μια νέα τεχνολογία DRM που εγκατέστησε το λογισμικό DRM στους υπολογιστές του χρήστη, χωρίς να ειδοποιήσει σαφώς τον χρήστη ή να απαιτήσει την επιβεβαίωσή του. Μεταξύ άλλων, το εγκατεστημένο λογισμικό περιελάμβανε ένα rootkit, το οποίο δημιούργησε μια αυστηρή ευπάθεια ασφάλειας που κάποιοι θα μπορούσαν να εκμεταλλευτούν. Όταν έγινε γνωστό αυτό το θέμα, η Sony ελαχιστοποίησε αρχικά τη σημασία των ευπαθειών του λογισμικού που είχε δημιουργήσει, αλλά αναγκάστηκε τελικά να αποσύρει τα εκατομμύρια CDs και πραγματοποίησε διάφορες προσπάθειες να επιδιορθωθεί το κρυφά εγκατεστημένο λογισμικό ώστε να αφαιρέσει τουλάχιστον το rootkit.

Το λογισμικό του DRM της Sony είχε πραγματικά μόνο περιορισμένη δυνατότητα να αποτρέψει την αντιγραφή, δεδομένου ότι είχε επιπτώσεις μόνο στην αναπαραγωγή ήχου στους υπολογιστές που χρησιμοποιούσαν λογισμικό Windows και όχι σε άλλο εξοπλισμό. Ακόμη και στα Windows, οι χρήστες παράκαμπταν τακτικά τους περιορισμούς. Έτσι ενώ η τεχνολογία της Sony DRM δημιούργησε τις θεμελιώδεις ευπάθειες στους υπολογιστές των πελατών, αυτά τα μέρη μπορούσαν να παρακαμφτούν εύκολα με τη συγκράτηση του κλειδιού «μετατόπισης» που παρεμβάλλονταν στο CD, ή με το να θέσουν εκτός λειτουργίας το χαρακτηριστικό γνώρισμα «auto run». Επιπλέον, τα audio tracks θα μπορούσαν απλά να παιχτούν και να επανακαταγραφούν, ώστε να παρακάμπτεται εντελώς όλο το DRM (γνωστό ως αναλογική τρύπα (analog hole)).

Τον Ιανουάριο του 2007, η EMI σταμάτησε την έκδοση ακουστικών CDs με DRM, δηλώνοντας ότι «οι δαπάνες για το DRM δεν έδιναν τα επιθυμητά αποτελέσματα». Η EMI ήταν ο τελευταίος εκδότης και πλέον δεν εκδίδονται ακουστικά CDs που περιέχουν DRM λογισμικό.

### 8.18.2 Μουσική Διαδικτύου

Πολλά on-line καταστήματα μουσικής υιοθετούν DRM συστήματα για να περιορίσουν τη χρήση της μουσικής που αγοράζεται και μεταφορτώνεται on-line. Υπάρχουν πολλές επιλογές για τους καταναλωτές που αγοράζουν την ψηφιακή μουσική μέσω Διαδικτύου και από άποψη καταστημάτων και επιλογών αγοράς.

Το iTunes κατάστημα, της Apple Inc., επιτρέπει στους χρήστες να αγοράσουν ένα κομμάτι on-line. Οι αγορές κομματιών χρησιμοποίησαν το σύστημα DRM FairPlay της Apple. Από τις 17 Οκτωβρίου 2007,μετά από μεγάλη αναστάτωση επί του θέματος οι χρήστες μπορούσαν να μεταφορτώσουν μουσική χωρίς ή με χρήση DRM για την ίδια τιμή.

Το κατάστημα μουσικής Napster προσφέρει μια συνδρομή-βασισμένη σε DRM παράλληλα με τις μόνιμες αγορές. Οι συνδρομητές χρήστες της υπηρεσίας μπορούν να μεταφορτώσουν ένα απεριόριστο όγκο μουσικής που κωδικοποιείται σε ήχο MEDIA Windows (WMA). Όταν όμως ο χρήστης σταματάει τη συνδρομή, η υπηρεσία καθιστά όλη την μεταφορτωμένη μουσική ακατάλληλη προς χρήση. Το Napster χρεώνει πρόσθετα τους χρήστες που επιθυμούν να χρησιμοποιήσουν τη μουσική στη φορητή συσκευή τους. Τα τραγούδια που αγοράζονται μέσω Napster μπορούν να παιχτούν στους φορείς που φέρνουν το λογότυπο της Microsoft PlaysForSure.

Η Wal-Mart Music Downloads, ένα άλλο κατάστημα on-line μεταφόρτωσης μουσικής, χρησιμοποιεί επίσης DRM. Όλα τα προϊόντα του είναι σε θέση να παιχτούν σε οποιοδήποτε Windows PlaysForSure προϊόν. Η μουσική παίζει στο φορέα SanDisk's Sansa mp3, παραδείγματος χάριν, αλλά με την προϋπόθεση ότι θα αντιγραφεί στην εσωτερική μνήμη του φορέα.

Η Sony λειτουργεί μια on-line υπηρεσία μεταφόρτωσης μουσικής αποκαλούμενη «Connect» που χρησιμοποιεί την ιδιόκτητη τεχνολογία OpenMG DRM της Sony. Η μουσική που μεταφορτώνεται από αυτό το κατάστημα (συνήθως μέσω του λογισμικού SonicStage της Sony) αναπαράγεται μόνο στους υπολογιστές που τρέχουν τα Windows και υλικό της Sony (συμπεριλαμβανομένου του PSP).

Οι διάφορες παρεχόμενες υπηρεσίες δεν είναι αυτήν την περίοδο διαλειτουργικές, αν και εκείνοι που χρησιμοποιούν το ίδιο σύστημα DRM (παραδείγματος χάριν τα διάφορα καταστήματα του σχήματος MEDIA DRM Windows, συμπεριλαμβανομένου του Napster) παρέχουν τραγούδια που μπορούν να παιχτούν μέσω του ίδιου φορέως προγράμματος.

### 8.19 DRM και έγγραφα

Η Enterprise digital rights management (E-DRM ή ERM), ή Μηχανισμός Συναλλαγματικών Ισοτιμιών, είναι η εφαρμογή της τεχνολογίας DRM για τον έλεγχο της πρόσβασης σε εταιρικά έγγραφα όπως Microsoft Word, αρχεία PDF, AutoCAD, ηλεκτρονικό ταχυδρομείο και ιστοσελίδας διαδικτύου παρά στον έλεγχο των καταναλωτικών μέσων. Το E-DRM, γνωστό ως IRM (διαχείριση δικαιωμάτων πληροφοριών), προορίζεται γενικά να αποτρέψει την αναρμόδια χρήση των ιδιωτικών εγγράφων. Το IRM ενσωματώνει κάποια τυπικά χαρακτηριστικά με το λογισμικό των συστημάτων διαχείρισης περιεχομένου. Ένα παράδειγμα ενός IRM συστήματος είναι οι διοικητικές υπηρεσίες των δικαιωμάτων της Microsoft. Οι πρόσθετοι προμηθευτές E- DRM περιλαμβάνουν τα Adobe Systems, την GigaTrust, την Oracle και την εταιρία EMC.

Ένα DRM σύστημα έχει χρησιμοποιηθεί από τις οργανώσεις όπως η βρετανική βιβλιοθήκη για την υπηρεσία ασφαλής ηλεκτρονικής παράδοσης, ώστε να επιτρέψει την παγκόσμια πρόσβαση σε έναν κάποια σπάνια και σε πολλές περιπτώσεις μοναδικά έγγραφα που, για νομικούς λόγους, ήταν διαθέσιμα προηγουμένως μόνο στα εξουσιοδοτημένα άτομα που επισκέπτονταν το κέντρο εγγράφων της βιβλιοθήκης στην Αγγλία.

### 8.20 Μεταδεδομένα διαχείρισης δικαιωμάτων

Ο ορισμός που μπορεί να δοθεί στο όρο «μεταδεδομένα» είναι δεδομένα για τα δεδομένα. Τα μεταδεδομένα είναι πληροφορίες που αντιπροσωπεύουν ένα αντικείμενο ή πόρο ανεξάρτητα την μορφή του, φυσική ή ηλεκτρονική. Παρά το γεγονός πως ο όρος «μεταδεδομένα» είναι σχετικά νέος, η σπουδαιότητα που κρύβεται πίσω από τη χρήση τους αναγνωρίστηκε από τη στιγμή που άρχισε η συστηματική οργάνωση και δόμηση της πληροφορίας. Οι καρτέλες αρχειοθέτησης που χρησιμοποιούνται για πολλές δεκαετίες από τις βιβλιοθήκες, είναι στην ουσία ένα εξαιρετικά επιτυχημένο σύνολο μεταδεδομένων που στοχεύει στη θεματική κατηγοριοποίηση των βιβλίων, τη σύνθεση συλλογών και την εύκολη αναζήτηση τίτλων. Τα μεταδεδομένα μπορούν να πληθυσμώνονται χειρονακτικά ή να ανακτώνται αυτόματα με τη χρήση προγραμμάτων λογισμικού.

Το Dublin Core Metadata Initiative είναι ένα διεθνές πρότυπο που χρησιμοποιείται για να βοηθήσει στην αυτοματοποίηση της αναζήτησης και της δεικτοδότησης των ψηφιακών πόρων του διαδικτύου, ανεξάρτητα με το αν ο πόρος είναι ένα ηλεκτρονικό έγγραφο ή ένα «πραγματικό» φυσικό αντικείμενο. Το Dublin Core πρότυπο μεταδεδομένων προτείνει ένα αντίστοιχο δελτίο αρχειοθέτησης, ταξινόμησης και χαρακτηρισμού των ψηφιακών πόρων, όπου αποτυπώνονται αρκετά τεχνολογικά και σημασιολογικά στοιχεία που μπορούν να λειτουργήσουν επικουρικά προς τα συστήματα αναζήτησης και ανάκτησης πληροφορίας στο Διαδίκτυο.

Η πλήρης καταγραφή όλων των επιπλέον στοιχείων που χαρακτηρίζουν το περιεχόμενο, επιτρέπει στα πολιτιστικά ιδρύματα να ορίσουν και να εφαρμόσουν τη στρατηγική τους σχετικά με τη διαδικασία εκκαθάρισης πνευματικών δικαιωμάτων. Επιπλέον, όλη αυτή η πληροφορία που συλλέγεται, συσσωρεύεται ως επιπρόσθετος πλούτος στο ίδρυμα, καθώς μπορεί με βάση αυτή την πληροφορία να αναπτύξει, να παρέχει, ακόμα και να εκμεταλλευτεί εμπορικά μία πλειάδα υπηρεσιών προς το χρήστη. Σημαντική επίσης είναι και η υπεραξία που αποκτά το περιεχόμενο λόγω των ενεργειών που πραγματοποιούνται πάνω του σε καθημερινή βάση (όπως είναι μία νέα φωτογράφηση ενός έργου, ακαδημαϊκές εργασίες που συγγράφονται από το εργατικό δυναμικό του μουσείου, νέο περιεχόμενο που παράγεται για τον διαδικτυακό τόπο κ. α). Τα παραπάνω καταδεικνύουν, πως πέρα από τα δικαιώματα που είναι αναγκαία για την αναπαραγωγή του περιεχομένου (“rights in”), υπάρχει σημαντικό όφελος και από την καταγραφή των δικαιωμάτων που ένα πολιτιστικό ίδρυμα μπορεί να μεταβιβάσει σε ξένους (“rights out”). Καθώς τα δικαιώματα μεταβιβάζονται μέσα από γραπτές συμφωνίες που ονομάζονται συμβόλαια, κάθε σύστημα διαχείρισης δικαιωμάτων θα πρέπει να είναι

σε θέση να καθορίσει με σαφήνεια και να καταγράψει με ομοιογενή και δυσλειτουργικό τρόπο τους όρους, τις συνθήκες και τους περιορισμούς που διέπουν μια συμφωνία.

Η παρακάτω εικόνα που ακολουθεί παρουσιάζει συνοπτικά ένα ενδεικτικό ελάχιστο σχήμα μεταδεδομένων, ικανό να υποστηρίξει τις ανάγκες, σε σημασιολογικό επίπεδο, ενός συστήματος διαχείρισης δικαιωμάτων.

| "Rights in" Μεταδεδομένα | "Rights out" Μεταδεδομένα |
|---|---|
| Ημερομηνία Τελευταίας τροποποίησης του έργου | Ημερομηνία Τελευταίας τροποποίησης του έργου |
| Κατάσταση Πνευματικής Ιδιοκτησίας του περιεχομένου | Κατάσταση Πνευματικής Ιδιοκτησίας του περιεχομένου |
| Στοιχεία Επικοινωνίας του Κάτοχου των Πνευματικών δικαιωμάτων | Στοιχεία επικοινωνίας του αιτούντος για τη μεταβίβαση των δικαιωμάτων |
| Στοιχεία επικοινωνίας για οποιοδήποτε δευτερεύοντα κάτοχο δικαιωμάτων, ή επιπλέον στοιχεία επικοινωνίας για τον κύριο κάτοχο των πνευματικών δικαιωμάτων | Στοιχεία επικοινωνίας για όλους του δευτερεύοντες κατόχους δικαιωμάτων |
| Συνοπτική περιγραφή των "Rights in" δικαιωμάτων | Συνοπτική περιγραφή των "Rights out" δικαιωμάτων |
| Λεπτομέρειες για την ικανότητα εκ νέου αδειοδότησης προς τρίτα μέρη | Λεπτομέρειες για την ικανότητα εκ νέου αδειοδότησης προς τρίτα μέρη |
| Σημειώσεις και σχόλια που καταγράφουν την ιστορική εξέλιξη της πνευματικής ιδιοκτησίας "ημερομηνίες προγενέστερων μεταβιβάσεων δικαιωμάτων κ.α" | Σημειώσεις και σχόλια που καταγράφουν την ιστορική εξέλιξη της πνευματικής ιδιοκτησίας "ημερομηνίες προγενέστερων μεταβιβάσεων δικαιωμάτων κ.α" |
| Διάρκεια της άδειας | Διάρκεια της άδειας |
| Εναρκτήρια ημερομηνία της άδειας | Εναρκτήρια ημερομηνία της άδειας |
| Καταληκτική ημερομηνία της άδειας | Καταληκτική ημερομηνία της άδειας |

ΕΙΚΟΝΑ 257: ΜΕΤΑΔΕΔΟΜΕΝΑ ΣΥΣΤΗΜΑΤΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΑΙΩΜΑΤΩΝ[5]

[5] Η εικόνα είναι διαθέσιμη στο
http://nemertes.lis.upatras.gr/dspace/bitstream/123456789/520/1/Nimertis_Meidanis(m).pdf

Το θέμα της διαχείρισης δικαιωμάτων, είναι ένα ανοικτό πρόβλημα και αποτελεί αντικείμενο μελέτης και έρευνας πολλών προγραμμάτων από τον ακαδημαϊκό και βιομηχανικό χώρο. Υπάρχουν αρκετά προγράμματα και πρωτοβουλίες που προτείνουν ενδεικτικές λύσεις σε συγκεκριμένα προβλήματα. Ωστόσο, καμία από τις προτεινόμενες λύσεις δεν μπορεί να αντιμετωπίσει συνολικά το πρόβλημα και να καλύψει την ποικιλία των επιχειρηματικών μοντέλων που απαντώνται στο χώρο της ψηφιοποίησης, προβολής και αξιοποίησης πολιτιστικού υλικού.

# ΚΕΦΑΛΑΙΟ 9

## Τα creative commons ως η βέλτιστη λύση

Όπως έχει γίνει φανερό, οι οργανισμοί, οι εταιρίες, τα κινήματα και οι τάσεις που επικρατούν, τείνουν να διαχωρίζονται σε δύο στρατόπεδα: στο στρατόπεδο των υποστηρικτών της ύπαρξης των copyrights και της εφαρμογής του DRM, με «στρατιώτες» τις μεγάλες εταιρίες, τις κυβερνήσεις, τους παραγωγούς, τους μεσάζοντες και κάποιους από τους δημιουργούς, και στο στρατόπεδο των «φιλελευθέρων», θιασωτών της ελεύθερης και δωρεάν δημιουργίας, χρήσης, διακίνησης και αντιγραφής ψηφιακού πνευματικού έργου, με «στρατιώτες» κάποιου δημιουργούς και τους τελικούς χρήστες-καταναλωτές, απλού κόσμου.

Σε αυτό το κεφάλαιο θα προταθεί μια ενδιάμεση τάση που υπόσχεται να «σμίξει» τους ανθρώπους των δύο στρατοπέδων, και να τους ενώσει κάτω από την ίδια στέγη. Αν καταργηθεί ο διαχωρισμός αυτός, αν τα συμφέροντα δεν είναι αλληλοσυγκρουόμενα αλλά αλληλοσυμπληρούμενα, αν πάψει το κυνηγητό μεταξύ κέρδους - δωρεάν, θύτη μεγαλοεπιχειρηματία και θύματος καταναλωτή ή του θύτη «πειρατή» και του θύματος δημιουργού, τότε αυτό που θα μείνει θα είναι μια κατάσταση όπου ο κάθε δημιουργός θα αμείβεται για το έργο του, οι παραγωγοί, οι μεσάζοντες και οι επιχειρηματίες θα βγάζουν κέρδη, και οι απλοί καταναλωτές θα απολαμβάνουν εύκολη, φτηνή, και άμεση πρόσβαση στα ψηφιακά πνευματικά έργα, και άρα στη ψυχαγωγία, στη μόρφωση, στη γνώση, στην πνευματική καλλιέργεια. Όλα αυτά είναι τα ιδανικά του οργανισμού «Creative Commons».

### 9.1 Γνωριμία

Από τη σκοπιά της οργανωτικής δομής το Creative Commons είναι φιλανθρωπική εταιρία, αναγνωρισμένη από το κράτος, με έδρα τη Μασαχουσέτη των ΗΠΑ. Για την προώθηση των στόχων του Creative Commons εργάζονται επίσης εθελοντές επικεφαλείς κατά τόπους ομάδων σε κάθε μία από τις εθνικές δικαιοδοσίες για τις οποίες έχουν ήδη προσαρμοστεί οι άδειες Creative Commons. Το Creative Commons International και οι εθελοντές επικεφαλείς των τοπικών ομάδων είναι ανεξάρτητες και ξεχωριστές οντότητες, ωστόσο συνεργάζονται και συνεισφέρουν εξίσου για να προωθήσουν την υιοθέτηση των αδειών και των εργαλείων που προσφέρει το Creative Commons.

Η ιδέα πίσω από το Creative Commons είναι ότι κάποιοι άνθρωποι μπορεί να μη θέλουν να εξασκήσουν όλα τα δικαιώματα πνευματικής ιδιοκτησίας που τους επιφυλάσσει ο νόμος. Πιστεύουμε πως υπάρχει μεγάλη ζήτηση για έναν εύκολο αλλά και αξιόπιστο τρόπο να εκφραστεί η διακήρυξη «Με επιφύλαξη κάποιων δικαιωμάτων» (Some rights reserved) ή ακόμα και η διακήρυξη «Χωρίς επιφύλαξη κανενός δικαιώματος» (No rights reserved). Πολλοί άνθρωποι έχουν καταλήξει από καιρό στο συμπέρασμα ότι η επιδίωξη ολοκληρωτικής προστασίας για τα δικαιώματα πνευματικής ιδιοκτησίας εμποδίζει τη διάδοση του έργου τους στο ευρύτερο δυνατό κοινό και δεν τους βοηθά να αποκτήσουν την αναγνώριση που επιθυμούν. Πολλοί επιχειρηματίες και καλλιτέχνες έχουν καταλήξει ότι προτιμούν να βασίζονται σε καινοτόμα επιχειρηματικά μοντέλα αντί της ολοκληρωμένης προστασίας των δικαιωμάτων πνευματικής ιδιοκτησίας προκειμένου να εξασφαλίσουν καρπούς από την «επένδυση» τους σε δημιουργικότητα. Άλλοι πάλι αισθάνονται ικανοποίηση συνεισφέροντας και συμμετέχοντας σε μια δημιουργική κοινότητα διανόησης (intellectual commons). Ανεξάρτητα από το λόγο, είναι φανερό ότι πολλοί πολίτες του Διαδικτύου θέλουν να μοιράζονται γενναιόδωρα με άλλους το έργο τους, καθώς και τη δυνατότητα άλλοι να επαναχρησιμοποιούν, να τροποποιούν και να διακινούν το ίδιο αυτό έργο. Το Creative Commons στοχεύει να βοηθήσει τους ανθρώπους να εκφράσουν αυτή ακριβώς την προτίμηση τους να μοιράζονται, προσφέροντας στον κόσμο δωρεάν μέσω του ιστοχώρου μας ένα σύνολο από άδειες χρήσης.

Το Creative Commons ιδρύθηκε το 2001 από τους ειδικούς σε νομικά θέματα των τεχνολογιών πληροφορικής, επικοινωνιών και διαδικτύου και σε θέματα διανοητικής ιδιοκτησίας James Boyle, Michael Carroll και Lawrence Lessig, τον καθηγητή επιστήμης υπολογιστών του MIT Hal Abelson, το δικηγόρο που εξελίχθηκε σε κινηματογραφιστή ντοκιμαντέρ και στη συνέχεια σε ειδικό σε νομικά θέματα του διαδικτύου Eric Saltzman και στο διαδικτυακό εκδότη δημοσίων κειμένων Eric Eldred. Επιστημονικοί συνεργάτες και φοιτητές στο Berkman Center for Internet &

Society του Harvard Law School βοήθησαν στο ξεκίνημα της προσπάθειας και για τα δύο πρώτα χρόνια της ύπαρξης του το Creative Commons στεγαζόταν και απολάμβανε τη γενναιόδωρη υποστήριξη του Center for Internet & Society στο Stanford Law School.

Πολύ συχνά η διαμάχη για τον έλεγχο των ψηφιακών έργων και των δικαιωμάτων πάνω σε αυτά, (όπως προαναφέραμε) καταλήγει σε δύο άκρα. Στον ένα πόλο έχουμε την οπτική του πλήρους ελέγχου – έναν κόσμο στον οποίο η κάθε χρήση ενός έργου ρυθμίζεται νομικά και όλα τα πνευματικά δικαιώματά που φέρει επιφυλάσσονται από τον δημιουργό της. Στον άλλο πόλο υπάρχει η οπτική της αναρχίας – ένας κόσμος όπου οι δημιουργοί απολαμβάνουν ποικιλία ελευθεριών αλλά μένουν εκτεθειμένοι στην εκμετάλλευση. Η ισορροπία, ο συμβιβασμός και η μετριοπάθεια που κάποτε διέκριναν τα συστήματα ccopyrights και που λάμβαναν υπόψη την καινοτομία και την προστασία ισάξια, τώρα έγιναν είδη προς εξαφάνιση.

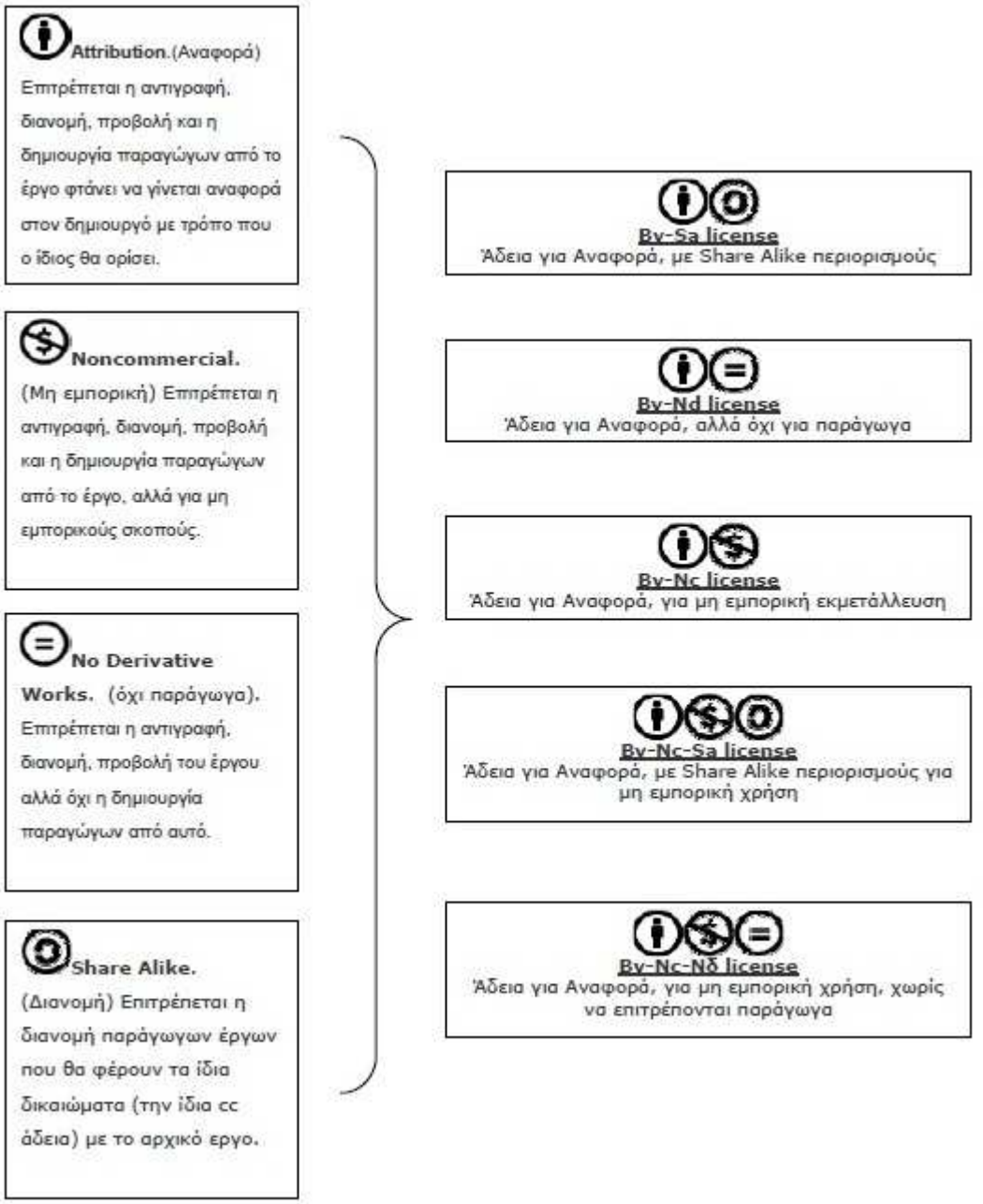
«Ο οργανισμός Creative Commons δουλεύει να ξαναφέρει στη ζωή αυτά τα χαρακτηριστικά. (Στον οργανισμό) χρησιμοποιούμε το ιδιωτικά δικαιώματα για να δημιουργούμε κοινά αγαθά: δημιουργικές δουλειές απελευθερωμένες για καθορισμένες χρήσεις. Όπως και τα κινήματα του δωρεάν και το ανοικτού κώδικα λογισμικού, τα κίνητρα μας είναι αυτά της συνεργασίας και της κοινωνικότητας, αλλά τα μέσα μας είναι εθελοντικά και φιλελεύθερα. Δουλεύουμε για να προσφέρουμε στους δημιουργούς τον καλύτερο τρόπο να προστατεύουν τα έργα τους με τρόπο που να εξυπηρετούνται και οι δύο «κόσμοι», ενώ ταυτόχρονα ενθαρρύνουμε συγκεκριμένες χρήσεις τους – διακηρύσσουμε το «some rights reserved»!

ΕΙΚΟΝΑ 268: ΤΑ CREATIVE COMMONS ΚΑΘΟΡΙΖΟΥΝ ΤΟ ΦΑΣΜΑ ΔΥΝΑΤΟΤΗΤΩΝ ΜΕΤΑΞΥ ΤΟΥ FULL COPYRIGHT (ΕΠΙΦΥΛΑΞΗ ΟΛΩΝ ΤΩΝ ΔΙΚΑΙΩΜΑΤΩΝ) ΚΑΙ ΤΟΥ PUBLIC DOMAIN (ΚΑΝΕΝΑ ΔΙΚΑΙΩΜΑ ΔΕΝ ΕΠΙΦΥΛΑΣΣΕΤΑΙ). Ο ΚΥΚΛΟΣ ΜΕ ΤΟ «CC» ΠΟΥ ΒΡΙΣΚΕΤΑΙ ΣΤΟ ΚΕΝΤΡΟ ΕΙΝΑΙ ΤΟ ΛΟΓΟΤΥΠΟ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ[6]

### 9.2 Άδειες και Αδειοδότηση

Οι δημιουργοί έργου που συμβάλλουν με τα creative commons έχουν την δυνατότητα εύκολα, μέσα από το site και μέσα σε ένα λεπτό, να εφοδιάσουν τα έργα τους με τις ακόλουθες άδειες (και τους συνδυασμούς τους):

[6] Η εικόνα είναι διαθέσιμη στο http://www.marinos.com.gr/bbpdf/pdfs/msg57.pdf




ΕΙΚΟΝΑ 27: ΆΔΕΙΕΣ CREATIVE COMMONS, ΚΑΙ ΣΥΝΔΥΑΣΜΟΙ ΑΔΕΙΩΝ.

Όταν το προς αδειοδότηση έργο είναι λογισμικό, οι δημιουργοί του μπορούν να το εφοδιάσουν με τις εξής άδειες:

- CC-GNU GPL : Προσθέτει τα απαραίτητα μεταδεδομένα και **to** "Commons Deed" (εξηγείται πιο κάτω) στην άδεια GNU GPL του FSF που παρουσιάστηκε στο προηγούμενο κεφάλαιο.
- CC-GNU LGPL : Προσθέτει τα απαραίτητα μεταδεδομένα και το commons Deed στην άδεια GNU Lesser General Public License του FSF.
- BSD : Δίνει δικαιώματα διαμοιρασμού και δημιουργίας παραγώγων χωρίς όμως να γίνεται χρήση του ονόματος του συγγραφέα για επικύρωση παράγωγων έργων χωρίς τουλάχιστον την προηγούμενη συναίνεσή του.

Όλες οι άδειες που εκδίδει ο Creative Commons εκφράζονται σε τρία επίπεδα:

- Commons Deed: Μια απλή περιγραφή σε απλή γλώσσα της άδειας που περιλαμβάνει και όλα τα σχετικά εικονίδια και σύμβολα.
- Legal Code: Η νομική ορολογία και περιγραφή που χρειάζεται για να είναι οι άδειες έγκυρες στο δικαστήριο.
- Digital Code: μετάφραση της άδειας σε γλώσσα μηχανής. Μεταδεδομένα και κώδικας που μπορούν να διαβαστούν από μηχανές αναζήτησης και άλλες συσκευές και εφαρμογές για να αναγνωρίζουν ένα έργο από τους όρους χρήσης του.

### 9.3 Αναζήτηση και εύρεση έργων με άδειες creative commons

Για να έχει νόημα να αδειοδοτεί κανείς το έργο του με Creative Commons, πρέπει να υπάρχει εύκολος τρόπος οι χρήστες να έχουν πρόσβαση σε αυτό, να βλέπουν τί δικαιώματα έχουν πάνω του, και να μπορούν να το χρησιμοποιήσουν. Σε αυτό το σκοπό συμβάλλει η «Digital Code» έκφραση των αδειών. Με τη βοήθειά της, σε κάθε έργο προστίθενται μεταδεδομένα που περιγράφουν τις άδειες που φέρει. Έτσι, με τη βοήθεια του σημασιολογικού ιστού, μπορεί κανείς χρησιμοποιώντας κάποια μηχανή αναζήτησης όπως το Google ή το Yahoo! Να ανατρέξει σε αυτά τα μεταδεδομένα και να βρει τα έργα που φέρουν συγκεκριμένες Creative commons άδειες.

Στο site του Creative Commons υλοποιήθηκε και λειτουργεί μηχανή μετά-αναζήτησης έργων με αυτές τις άδειες με τη βοήθεια άλλων μηχανών. Στο www.flickr.com υπάρχει η δυνατότητα αναζήτησης μόνο φωτογραφιών που φέρουν συγκεκριμένες άδειες Creative Commons. Ο νέος περιηγητής ιστού της Mozilla, ο Firefox έχει υλοποιεί προεγκατεστημένες λειτουργίες αναζήτησης έργων με άδειες Creative Commons.

### 9.4 Διεθνοποίηση αδειών Creative Commons

Με την διάδοση του διαδικτύου, οι στόχοι του Creative Commons μπορούν να επιτευχθούν μόνο αν οι άδειες του διαδοθούν και εφαρμοστούν παγκόσμια. Γι' αυτό το σκοπό ο «Creative Commons international» (CCi), προσπαθεί να πείσει της διάφορες νομοθεσίες σχετικές για τα copyrights σε όλο τον πλανήτη να υιοθετήσουν τα βασικά χαρακτηριστικά των αδειών Creative Commons. Πριν ξεκινήσει αυτή η διαδικασία πρέπει να μεταφράσουν τις άδειες στις γλώσσες των χωρών που πρόκειται να τις προωθήσουν, αλλά και να τις τροποποιήσουν ανάλογα με τις νομικές ανάγκες τις περιοχής . Αυτή η δουλεία γίνεται εθελοντικά από διάφορα άτομα εθελοντικά σε κάθε περιοχή οι οποίοι αναλαμβάνουν να τις παρουσιάσουν στις χώρες τους και έρχονται σε επαφή συνεχώς με επενδυτές σε μια προσπάθεια να τους πείσουν να υιοθετήσουν τις άδειες στην περιοχή δικαιοδοσίας τους.

Η διαδικασία εισαγωγής περιλαμβάνει τα εξής βήματα:

1. Τη σύσταση θυγατρικών τοπικών οργανισμών και την επιλογή τοπικών επί κεφαλής του έργου εισαγωγής και επί κεφαλής νομικών θεμάτων
2. Την υπογραφή συμφώνων συνεργασίας και κατανόησης (Memorandum Of understanding - MOU) από τους επί κεφαλής και τον Creative Commons
3. Εσωτερική διοίκηση και καθορισμό χρονοδιαγραμμάτων
4. Επιθεώρηση πρώτου προσχεδίου αδειών από τον Chi
5. Δημόσιες διαβουλεύσεις
6. Ο επί κεφαλής για νομικά θέματα εκδίδει δεύτερο προσχέδιο
7. Επιθεώρηση δεύτερου προσχεδίου από τον CCi
8. Ο επί κεφαλής έργου οριστικοποιεί τις άδειες και ρυθμίζει τις τεχνικές λεπτομέρειες
9. Η εθνική έκδοση των αδειών ξεκινά

### 9.5 Το Creative Commons συμμετέχει στην ψηφιακή διαχείριση δικαιωμάτων (DRM);

Όχι. Εργάζονται πάνω στην έκφραση ψηφιακών δικαιωμάτων, όχι τη διαχείριση τους. Τα εργαλεία μας καθιστούν εύκολο για ένα δημιουργό να εκφράσει ποια δικαιώματα επιφυλάσσει. Αλλά δεν παρέχουμε εργαλεία για την επιβολή των δικαιωμάτων που ο δημιουργός επιφυλάσσει. Αυτό επιτελεί η Ψηφιακή Διαχείριση Δικαιωμάτων (ή «DRM»). Επιπλέον της ψηφιακής έκφρασης δικαιωμάτων, ένα σύστημα DRM παρέχει τεχνολογικά μέσα για την επιβολή των δικαιωμάτων αυτών.

Γιατί δε χρησιμοποιούνται τεχνολογικά μέσα για την επιβολή δικαιωμάτων; Υπάρχουν περισσότεροι λόγοι από όσους μπορούν να αναλύσουν εδώ. Ίσως ο πιο γνώριμος λόγος είναι η διαπίστωση ότι η τεχνολογία δεν μπορεί να περιφρουρήσει ελευθερίες όπως η «δίκαιη χρήση» («fair use»), δηλαδή τους νόμιμους περιορισμούς του περιουσιακού δικαιώματος του δημιουργού και το ηθικό δικαίωμα του δημιουργού βάσει του νόμου. Για να το θέσουμε και διαφορετικά, η «δίκαιη χρήση» δεν μπορεί να περιγραφεί ή να οριοθετηθεί τεχνικά, με κώδικα σε κάποια γλώσσα προγραμματισμού. Αλλά ακόμη πιο σημαντικός λόγος είναι, κατά την πεποίθηση μας, ότι η επιβολή με τεχνολογικά μέσα δυσχεραίνει τη δημιουργική επαναχρησιμοποίηση έργων λόγου. Εμείς, αντίθετα, θέλουμε να ενθαρρύνουμε τέτοια χρήση. Και μας διακατέχει, μαζί με πολλούς άλλους, η ανησυχία ότι το οικοσύστημα της δημιουργικότητας θα διαταραχθεί βάναυσα αν κυριαρχήσει η χρήση τεχνολογικών μέσων για τη «διαχείριση» των δικαιωμάτων.

Τα δικαιώματα πνευματικής ιδιοκτησίας πρέπει, χωρίς αμφιβολία, να γίνονται σεβαστά. Όμως εμείς προτιμάμε ο σεβασμός να επιδεικνύεται με τον παραδοσιακό τρόπο: οι άνθρωποι να σέβονται έμπρακτα τις ελευθερίες και τους περιορισμούς που τίθενται όπως επιλέγει ο δημιουργός και επιβάλλει ο νόμος.

# ΚΕΦΑΛΑΙΟ 10

## Παρουσίαση Adobe's InDesign και οδηγός δημιουργίας ενός ηλεκτρονικού βιβλίο.

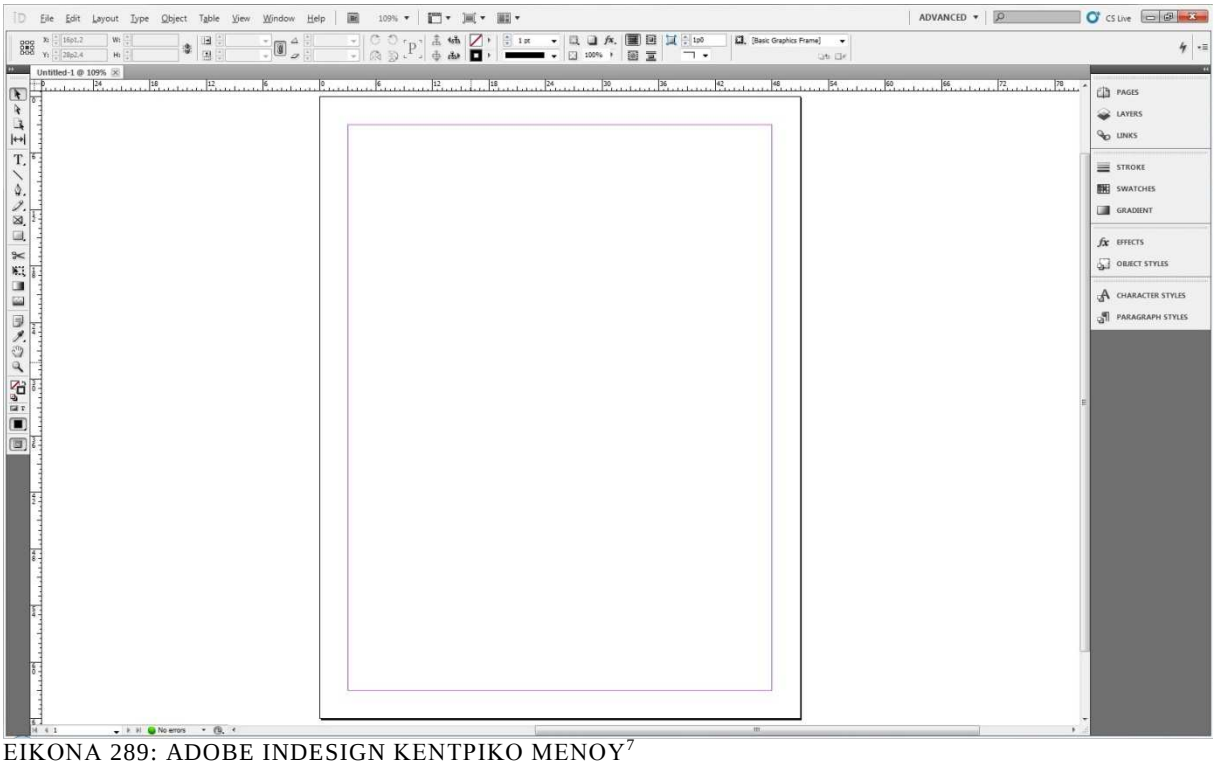
### 10.1 Τι είναι το Adobe InDesign

Το πρόγραμμα της Adobe, InDesign, είναι ένα επαγγελματικό εργαλείο το οποίο επιτρέπει σε κάποιον να σχεδιάσει και να εκδώσει ένα κείμενο ή βιβλίο με διάφορους τρόπους όπως εκτυπώνοντας ή "ανεβάζοντας" το στο Internet αλλά και αποθηκεύοντας το σε φορητές ηλεκτρονικές συσκευές ανάγνωσης , όπως τους eBook readers αλλά και τα κινητά.

Το InDesign προορίζεται κυρίως για επαγγελματίες σχεδιαστές που ασχολούνται με την έκδοση περιοδικών, το σχεδιασμό διαφημίσεων, εφημερίδων, βιβλίων, ηλεκτρονικών βιβλίων και στην κατασκευή καταλόγων εταιριών.

### 10.2 Περιήγηση στο γραφικό περιβάλλον του InDesign

Όπως και στα περισσότερα προγράμματα της Adobe το γραφικό περιβάλλον του InDesign αποτελείται από το κεντρικό μενού στο πάνω μέρος του παραθύρου, στα αριστερά υπάρχει η εργαλειοθήκη όπου υπάρχουν όλα τα σχεδιαστικά εργαλεία χρειάζονται για το σχεδιασμό του ψηφιακού κειμένου. Στο κέντρο βρίσκεται ο καμβάς όπου μπορούμε να σχεδιάσουμε και να γράψουμε το έργο μας και στα δεξιά υπάρχει το μενού που είναι υπεύθυνο για την προσθήκη και τροποποίηση διάφορων στοιχείων μέσα στο κείμενο μας.




ΕΙΚΟΝΑ 289: ADOBE INDESIGN ΚΕΝΤΡΙΚΟ ΜΕΝΟΥ[7]

[7] Όλες οι εικόνες του κεφαλαίου 10 είναι δημιουργία από τον συγγραφέα της πτυχιακής εργασίας

### *10.2.1 Η εργαλειοθήκη του InDesign*

Η εργαλειοθήκη του InDesign αποτελείται από είκοσι δύο κουμπιά και χωρίζονται πέντε κατηγορίες όπως φαίνονται στην εικόνα 29. Τα πρώτα τέσσερα είναι σχετικά για την επιλογή στοιχείων μέσα στην σελίδα και για την αυξομείωση των κενών που υπάρχουν μέσα στις σελίδες ων κειμένων.

ΕΙΚΟΝΑ29: ΠΡΩΤΑ 4 ΚΟΥΜΠΙΑ ΤΗΣ ΕΡΓΑΛΕΙΟΘΗΚΗΣ

Στην δεύτερη κατηγορία βρίσκονται τα βασικά κουμπιά για την σχεδίαση του κείμενου. Αυτά είναι :

- **Type Tool:** Με το οποίο επιλέγοντάς το μπορούμε να σχεδιάσουμε ένα ορθογώνιο μέσα στον καμβά μας όπου μέσα σε αυτό το ορθογώνιο μας επιτρέπεται να γράψουμε ότι θέλουμε. Με αυτό τον τρόπο έχουμε την επιλογή να γράψουμε σε όποιο κομμάτι τις σελίδας θέλουμε και μπορούμε να επιλέξουμε και ακριβώς το μέγεθος που θέλουμε το κείμενο μας να πιάσει.
- **Line Tool:** Το Line Tool μας επιτρέπει να σχεδιάσουμε διάφορες γραμμές μέσα στο κείμενο μας, όπου θεωρούμε ότι είναι απαραίτητο, ώστε να έχουμε ένα πιο καλό σχεδιαστικά αποτέλεσμα.
- **Pen Tool:** Το pen tool απαιτεί αρχικά κάποια εξάσκηση ώστε κάποιος να εξοικειωθεί μαζί του. Με το pen tool μπορούμε να σχεδιάσουμε απλές καμπύλες μέχρι και αρκετά σύνθετες.
- **Pencil Tool:** Το Pencil Tool, είναι ακριβώς αυτό που λέει το όνομα του. Επιλέγοντας το, μπορούμε να σχεδιάσουμε πάνω στην σελίδα σαν να κρατάμε ένα μολύβι στο χέρι μας. Το σχέδιο που θα δημιουργήσουμε μπορούμε να το χρησιμοποιήσουμε σαν ένα απλό σχέδιο ή και ακόμα να γράψουμε κείμενο μέσα σε αυτό.
- **Rectangle Frame Tool :** Με το Rectangle Frame Tool μπορούμε να σχεδιάσουμε ένα τετράγωνο μέσα στην σελίδα σχεδιασμού μας όπου μέσα σε αυτό πρόκειται τοποθετήσουμε κάποιο ψηφιακό στοιχείο όπως εικόνες ή video ή και διάφορα άλλα flash αρχεία.
- **Rectangle Tool: Το** Rectangle Tool κάνει σχεδόν ότι και το Rectangle Frame Tool. Απλά στο Rectangle Frame Tool μέσα στο τετράγωνο που δημιουργεί τοποθετείται και ένα X το οποίο μας υπενθυμίζει ότι πρόκειται να τοποθετήσουμε κάποιο εικονικό αρχείο εκεί μέσα.

ΕΙΚΟΝΑ 30: ΤΑ ΕΠΟΜΕΝΑ 5 ΚΟΥΜΠΙΑ ΤΗΣ ΕΓΑΛΙΟΘΗΚΗΣ[8]

[8] Όλες οι εικόνες του κεφαλαίου 10 είναι δημιουργία από τον συγγραφέα της πτυχιακής εργασίας

Οι επόμενες τρεις κατηγορίες κουμπιών δεν θα μας απασχολήσουν σχεδόν καθόλου . Το μόνο κουμπί που αξίζει να αναφερθεί είναι το κουμπί για την μεγέθυνση.

Επιλέγοντας το **Zoom Tool,** μπορούμε πατώντας πάνω στον καμβά σχεδιασμό να μεγεθύνουμε την εικόνα ώστε να μπορέσουμε να διακρίνουμε καλύτερα μικρές λεπτομέρειες που ίσως χρειάζονται διάφορες τροποποιήσεις.. Πατώντας περισσότερες από μία φορές η εικόνα μεγεθύνεται περισσότερο και πατώντας πάλι στο Zoom Tool στην εργαλειοθήκη η εικόνα επιστρέφει στο κανονικό της μέγεθος.

### *10.2.3 Οδηγός δημιουργίας eBook μέσω της εφαρμογής InDesign*

Ο ακόλουθος οδηγός, παρουσιάζει τον τρόπο δημιουργίας ενός ηλεκτρονικού βιβλίου και συγκεκριμένα πρότυπου ePUB με πολύ απλά βήματα ώστε να είναι κατανοητός στον κάθε ενδιαφερόμενο.

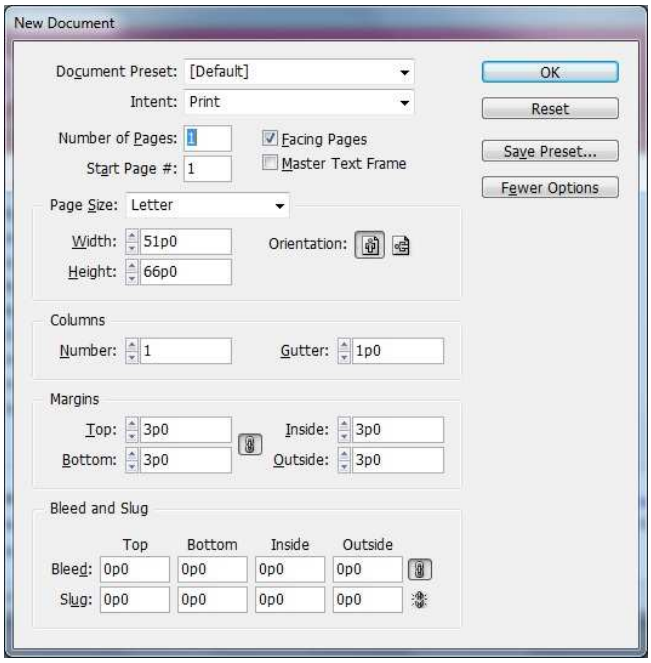
**ΒΗΜΑ Α'**

Αφού έχουμε εγκαταστήσει την εφαρμογή InDesign της Adobe(μπορείτε να αγοράσετε την εφαρμογή από το επίσημο site της Adobe) την τρέχουμε. Θα μας εμφανιστεί το ακόλουθο παράθυρο:


ΕΙΚΟΝΑ 3110: ΔΗΜΙΟΥΡΓΙΑ Η-ΒΙΒΛΙΟΥ ΜΕΣΩ ΤΗΣ ΕΦΑΡΜΟΓΗ INDESIGN[9]

Επιλέγουμε από την κατηγορία "Create New" την επιλογή "Document" θα μας εμφανιστεί το ακόλουθο παράθυρο το οποίο μας ζητάει να δώσουμε διάφορες τιμές για το μέγεθος που θέλουμε να έχουν οι σελίδες του βιβλίου μας .Εικόνα 32

[9] Όλες οι εικόνες του κεφαλαίου 10 είναι δημιουργία από τον συγγραφέα της πτυχιακής εργασίας



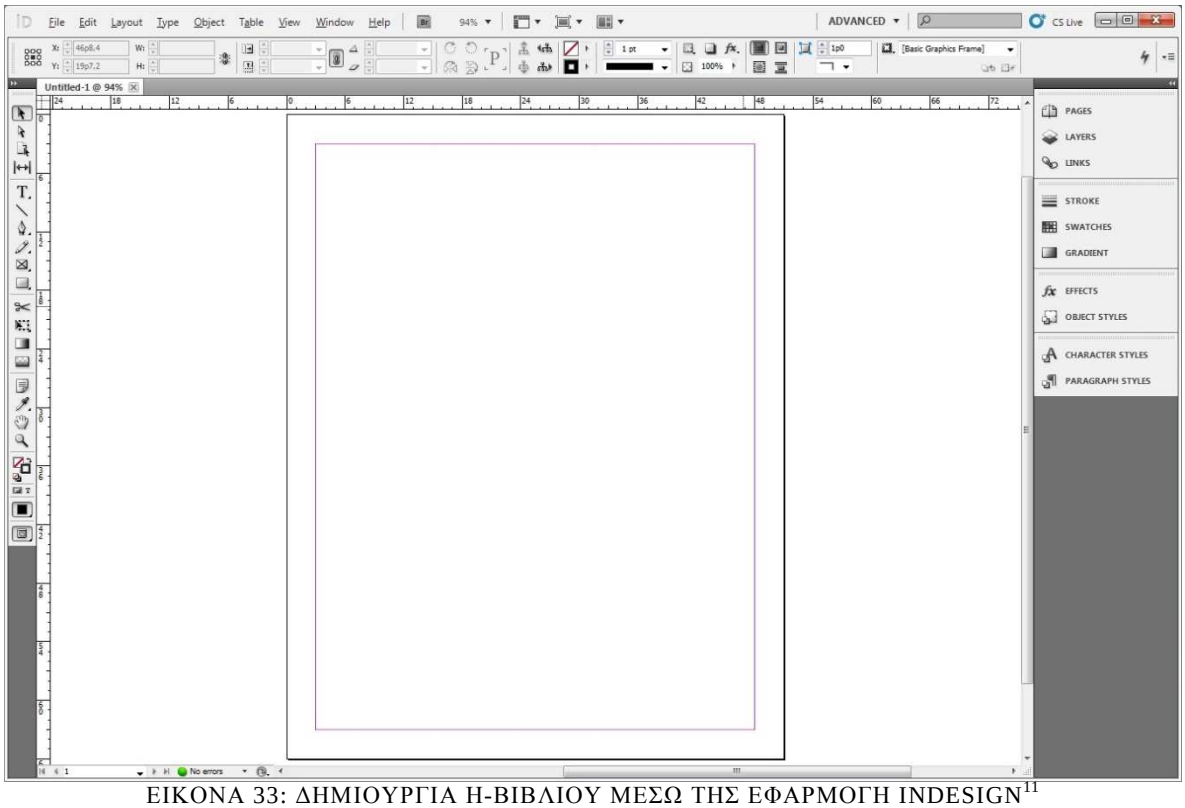

ΕΙΚΟΝΑ 3211:ΔΗΜΙΟΥΡΓΙΑ Η-ΒΙΒΛΙΟΥ ΜΕΣΩ ΤΗΣ ΕΦΑΡΜΟΓΗ INDESIGN[10]

Αν θέλετε το βιβλίο σας να έχει το μέγεθος των σελίδων που συνήθως χρησιμοποιείται για τα βιβλία συμπληρώστε τις τιμές όπως φαίνονται στην εικόνα 32, αλλιώς μπορείτε να δώσετε οπουδήποτε τιμή πιστεύεται ότι θα είναι η καλύτερη για εσάς.

**ΒΗΜΑ Β'**

Ακολουθώντας τα προηγούμενα βήματα θα πρέπει να έχουμε ένα τέτοιο αποτέλεσμα στην οθόνη μας.

[10] Όλες οι εικόνες του κεφαλαίου 10 είναι δημιουργία από τον συγγραφέα της πτυχιακής εργασίας



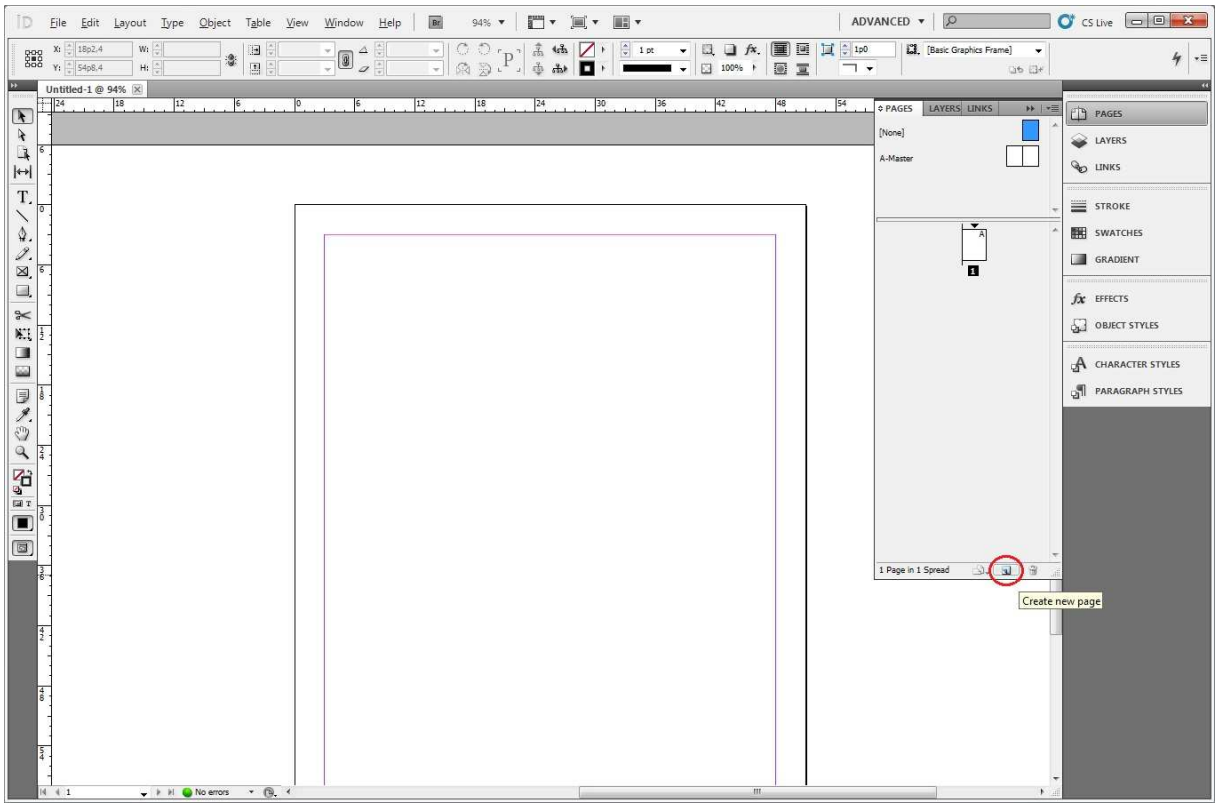

ΕΙΚΟΝΑ 33: ΔΗΜΙΟΥΡΓΙΑ Η-ΒΙΒΛΙΟΥ ΜΕΣΩ ΤΗΣ ΕΦΑΡΜΟΓΗ INDESIGN[11]

Έπειτα, χρησιμοποιώντας κάποια εφαρμογή σχεδίασης όπως το photoshop της adobe δημιουργούμαι ένα εξώφυλλο για το η-βιβλίο μας. Για να το εισάγουμε στο InDesign επιλέγουμε το Type Tool δημιουργούμε ένα ορθογώνιο όσο η σελίδα μας και στη συνέχεια επιλέγουμε από το μενού πάνω αριστερά, "File" > "Place..." Ένα παράθυρο θα εμφανιστεί, βρίσκουμε που έχουμε αποθηκεύσει το εξώφυλλο μας το επιλέγουμε και πατάμε "Open". Αν όλα έχουν γίνει σωστά το εξώφυλλο θα εμφανιστεί και θα έχει πιάσει το χώρο που σχεδιάσαμε με το Type Tool.

**ΒΗΜΑ Γ**

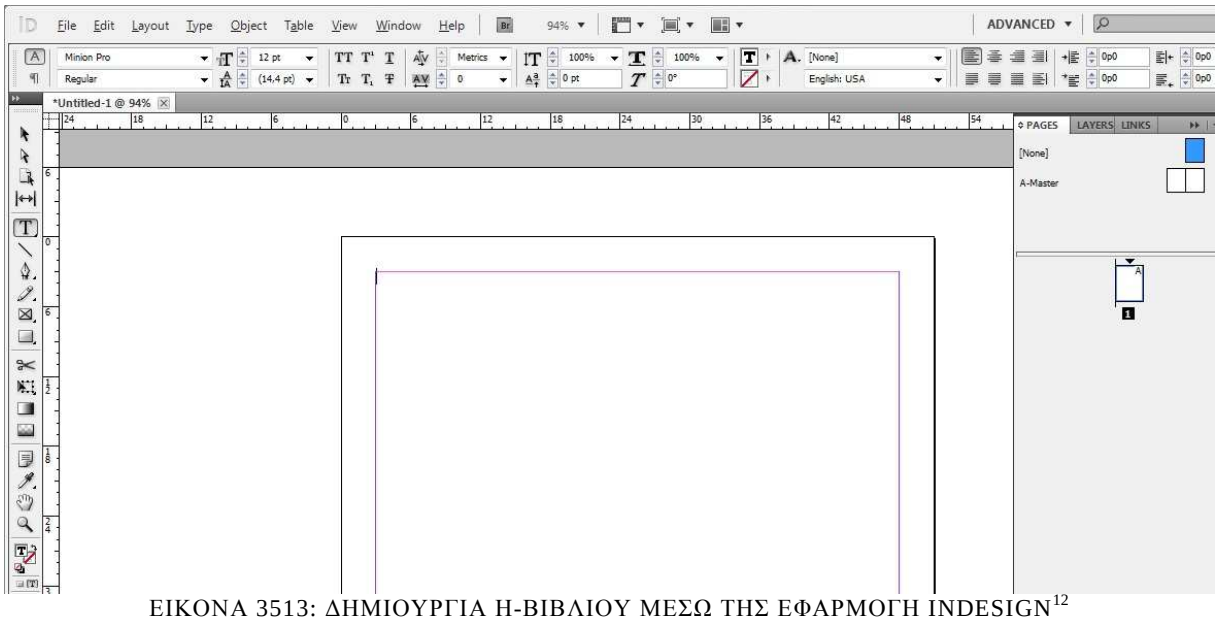
Για να αρχίσουμε να γράφουμε το κείμενου του βιβλίου μας θα χρειαστούμε να προσθέσουμε σελίδες στο κείμενο μας. Για να προσθέσουμε σελίδες, αρκεί να πάμε από το μενού που βρίσκεται δεξιά και επιλέξουμε την επιλογή "Pages" και από το παράθυρο που ανοιχτεί επιλέγουμε την επιλογή "Create new page", όπως φαίνεται στην εικόνα.

[11] Όλες οι εικόνες του κεφαλαίου 10 είναι δημιουργία από τον συγγραφέα της πτυχιακής εργασίας




ΕΙΚΟΝΑ 3412: ΔΗΜΙΟΥΡΓΙΑ Η-ΒΙΒΛΙΟΥ ΜΕΣΩ ΤΗΣ ΕΦΑΡΜΟΓΗ INDESIGN

Αφού δημιουργήσουμε την νέα σελίδα επιλέγουμε πάλι το Type Tool και δημιουργούμε μέσα στην σελίδα του βιβλίου ένα text box όπου εκεί μπορούμε να γράψουμε το κείμενο που μας ενδιαφέρει. Όταν γράφουμε κάποιο κείμενο το μενού αλλάζει και εμφανίζεται το μενού για το κείμενο όπως φαίνεται και στην εικόνα 35.




ΕΙΚΟΝΑ 3513: ΔΗΜΙΟΥΡΓΙΑ Η-ΒΙΒΛΙΟΥ ΜΕΣΩ ΤΗΣ ΕΦΑΡΜΟΓΗ INDESIGN[12]

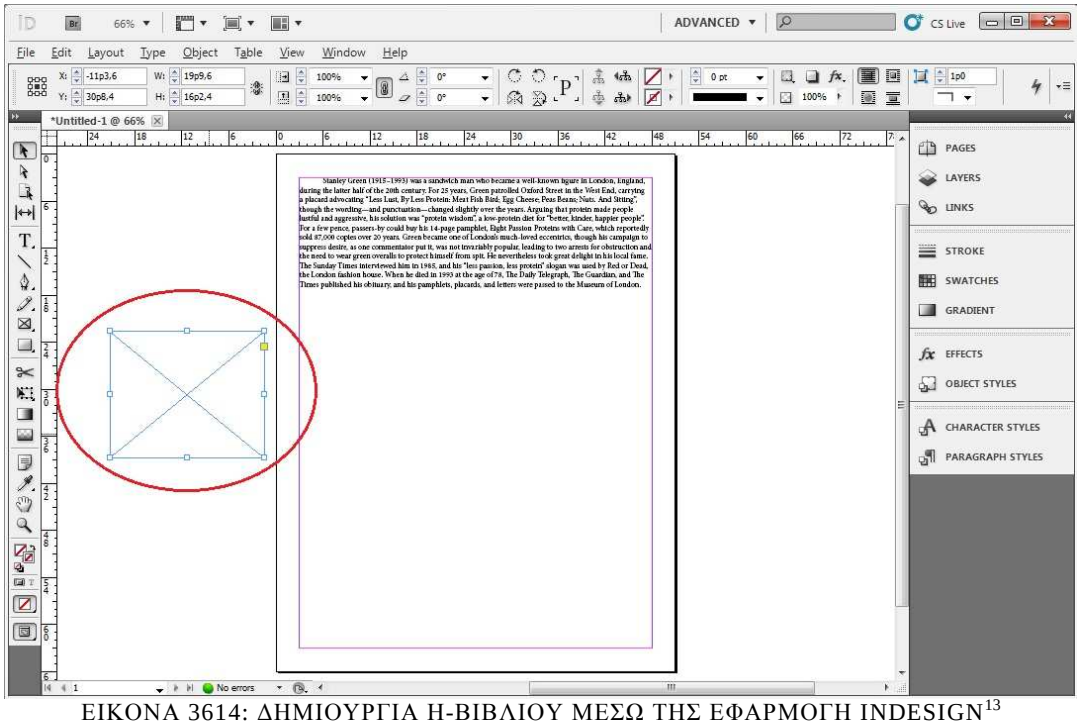
[12] Όλες οι εικόνες του κεφαλαίου 10 είναι δημιουργία από τον συγγραφέα της πτυχιακής εργασίας

**ΒΗΜΑ Δ'**

Αν θέλουμε στο βιβλίο μας να προσθέσουμε εικόνες πρέπει να κάνουμε μία διεργασία κάπως χρονοβόρα αλλά είναι ο μόνος τρόπος για να εμφανίζονται σωστά οι εικόνες σε ένα ePUB αρχείο.

Έχοντας δημιουργήσει ένα text box που για ολόκληρη την σελίδα μας θα μπορούσαμε να πάρουμε το Rectangle Frame Tool να δημιουργήσουμε ένα κουτί μέσα στην σελίδα μας και να προσθέσουμε την εικόνα που θέλουμε. Αλλά αν κάνουμε αυτό η εικόνα μας δεν θα εμφανιστεί σωστά κατά την ανάγνωση του ePUB αρχείου, η εικόνα θα εμφανιστεί μόνο όταν έχει τελειώσει ολόκληρο το κείμενο μας.

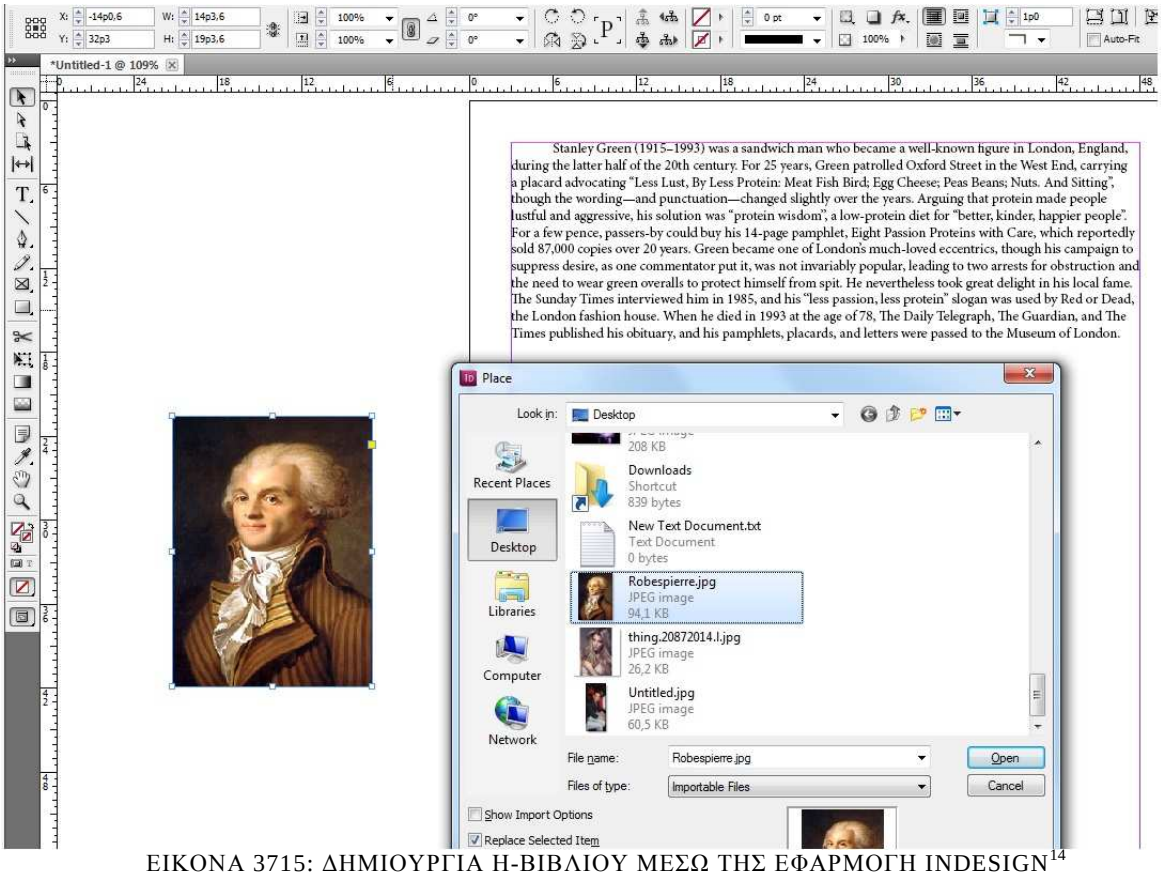
Για να εμφανιστεί με την σωστή σειρά η εικόνα θα πρέπει με το Rectangle Frame Tool να δημιουργήσουμε ένα κουτί έξω από την σελίδα για την εικόνα που θέλουμε όπως φαίνεται και στην εικόνα 36.




ΕΙΚΟΝΑ 3614: ΔΗΜΙΟΥΡΓΙΑ Η-ΒΙΒΛΙΟΥ ΜΕΣΩ ΤΗΣ ΕΦΑΡΜΟΓΗ INDESIGN[13]

Έπειτα, έχοντας επιλεγμένο το κουτί που έχουμε φτιάξει για την εικόνα, πατάμε CTRL+D και εμφανίζεται το παράθυρο για να βρούμε και να τοποθετήσουμε την εικόνα μας μέσα στο frame που έχουμε φτιάξει. Εικόνα 37. Επιλέγουμε, την εικόνα που μας ενδιαφέρει και πατάμε "Open".

[13] Όλες οι εικόνες του κεφαλαίου 10 είναι δημιουργία από τον συγγραφέα της πτυχιακής εργασίας



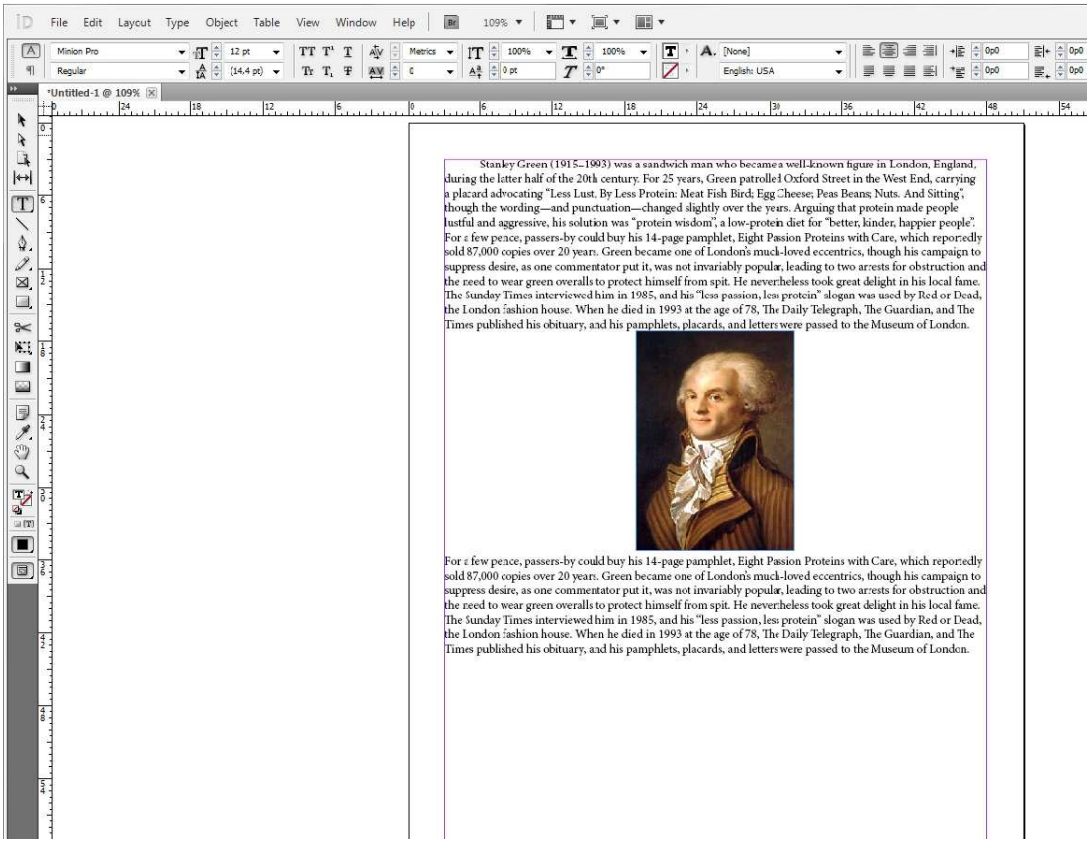

ΕΙΚΟΝΑ 3715: ΔΗΜΙΟΥΡΓΙΑ Η-ΒΙΒΛΙΟΥ ΜΕΣΩ ΤΗΣ ΕΦΑΡΜΟΓΗ INDESIGN[14]

Αφού έχουμε κάνει τα παραπάνω, επιλέγουμε πάλι την εικόνα μας με το Selection Tool και πατάμε CTRL+X. Στην συνέχεια κάνουμε διπλό κλικ μέσα στο text box όπου υπάρχει το κείμενο μας ώστε να εμφανιστεί ο κέρσορας του text και πηγαίνουμε τον κέρσορα στο σημείο που θέλουμε να τοποθετηθεί η και πατάμε το CTRL+C. Με τον τρόπο αυτό η εικόνα ενσωματώνεται μέσα στο κείμενο. Εικόνα 38.

Έτσι κάνοντας το βήμα Γ' και Δ' , προσθέτοντας σελίδες, το κείμενο και τις εικόνες που μας ενδιαφέρουν, μπορούμε να γράψουμε το δικό μας ηλεκτρονικό βιβλίο.

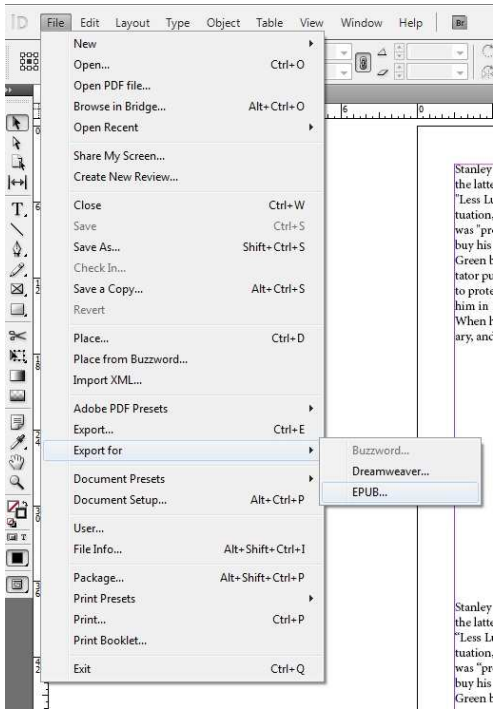
Υπάρχουν βέβαια και διάφορα άλλα χαρακτηριστικά που θα μπορούσαν να χρησιμοποιηθούν. Αλλά απαιτούν αρκετή εργασία και γνώση της εφαρμογής InDesign. Η καλύτερη λύση για να μάθει κάποιος την εφαρμογή είναι η συνεχής εξάσκηση.

[14] Όλες οι εικόνες του κεφαλαίου 10 είναι δημιουργία από τον συγγραφέα της πτυχιακής εργασίας




ΕΙΚΟΝΑ 3816: ΔΗΜΙΟΥΡΓΙΑ Η-ΒΙΒΛΙΟΥ ΜΕΣΩ ΤΗΣ ΕΦΑΡΜΟΓΗ INDESIGN

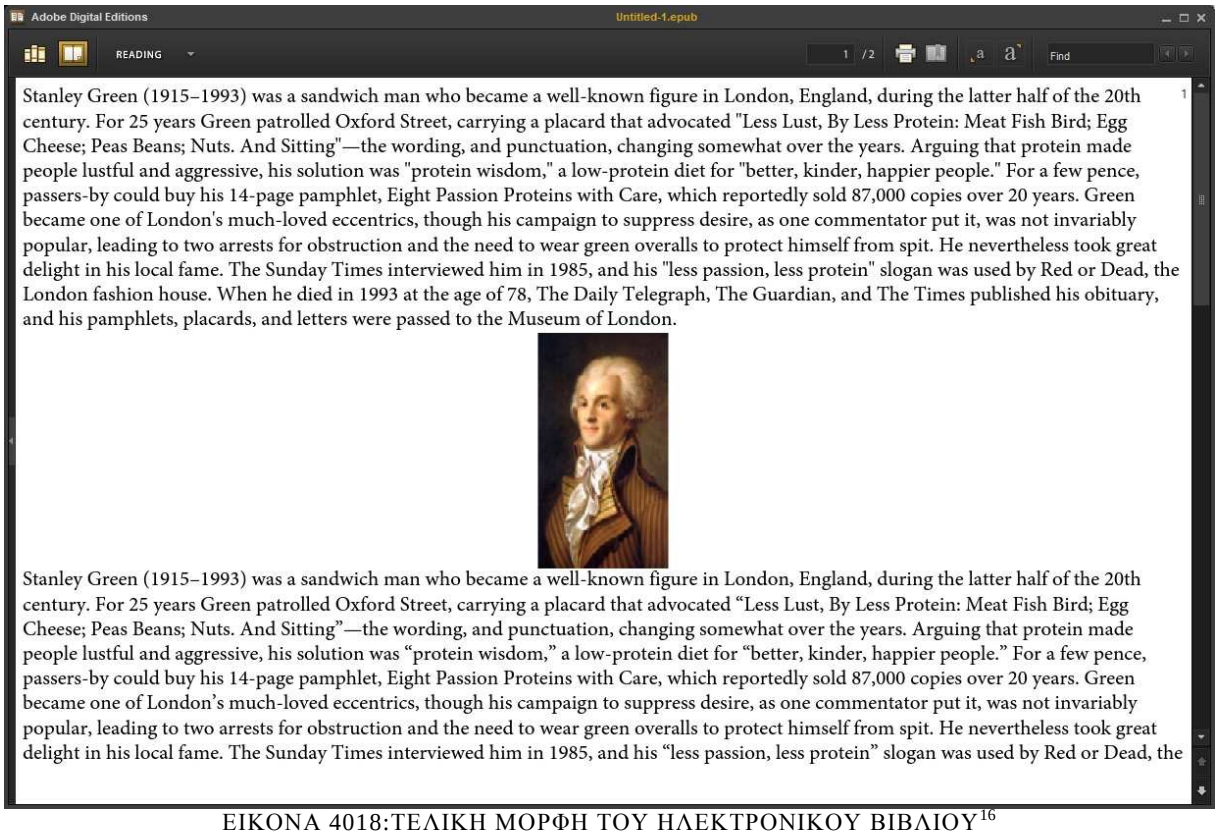
Τώρα για να εξάγουμε το βιβλίο σαν ePUB αρχείο αρκεί να πάμε από το μενού "File" > "Export For" > "Epub..."




ΕΙΚΟΝΑ 3917:ΔΗΜΙΟΥΡΓΙΑ Η-ΒΙΒΛΙΟΥ ΜΕΣΩ ΤΗΣ ΕΦΑΡΜΟΓΗ INDESIGN[15]

[15] Όλες οι εικόνες του κεφαλαίου 10 είναι δημιουργία από τον συγγραφέα της πτυχιακής εργασίας

Πατώντας στη επιλογή "Epub..." θα μας ζητηθεί να ορίσουμε που θέλουμε να αποθηκευτεί το ePub αρχείο. Επιλέγουμε την περιοχή και έπειτα ένα νέο παράθυρο θα εμφανιστεί όπου θα μας ζητηθεί να ορίσουμε κάποιες ρυθμίσεις σχετικά με ePub. Πατήστε αμέσως "Export" (μιας και αυτές οι ρυθμίσεις δεν μας αφορούν άμεσα) και θα έχετε δημιουργήσει το δικό σας ePUB ηλεκτρονικό βιβλίο. Εικόνα 40




ΕΙΚΟΝΑ 4018:ΤΕΛΙΚΗ ΜΟΡΦΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΒΙΒΛΙΟΥ[16]

[16] Όλες οι εικόνες του κεφαλαίου 10 είναι δημιουργία από τον συγγραφέα της πτυχιακής εργασίας

# ΠΑΡΑΡΤΗΜΑ Α

# ΚΡΥΠΤΟΓΡΑΦΙΑ

Κρυπτογραφία είναι η επιστήμη και η ικανότητα να γράφεις με μυστικότητα - κρατώντας τις πληροφορίες μυστικές. Όταν αναφερόμαστε σε υπολογιστές, η κρυπτογραφία προστατεύει δεδομένα έναντι της αποκάλυψης αυτών χωρίς άδεια. Μπορεί να αναγνωρίσει την ταυτότητα του χρήστη και φανερώνει την πλαστογραφία χωρίς άδεια. Σε αυτό το κεφάλαιο θα μελετήσουμε αυτές τις χρήσεις και θα παρουσιάσουμε μερικές μεθόδους κρυπτογράφησης που χρησιμοποιούνται σήμερα .

## 1.1 Αναγκαιότητα της Κρυπτογραφίας

Τα συστήματα υπολογιστών εκτίθενται σε διάφορους κινδύνους, όπως είδαμε στις θεματικές υποενότητες «Προστασία Δεδομένων» και «Ασφάλεια Δικτύων». Στη συνέχεια θα δούμε συνοπτικά τις επιπτώσεις που μπορεί να έχει η πραγματοποίηση των κινδύνων αυτών, τους βασικούς στόχους προστασίας και ασφάλειας που θέτουμε, όπως επίσης και τα μέτρα με τα οποία επιτυγχάνονται αυτοί οι στόχοι.

## 1.2 Βασικοί στόχοι ασφάλειας

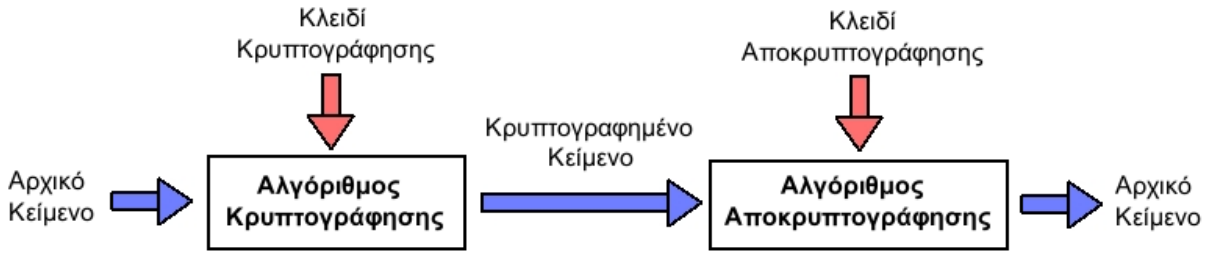
Στο πλαίσιο της ασφάλειας υπολογιστικών και επικοινωνιακών συστημάτων τίθενται ως βασικοί στόχοι η διατήρηση (διασφάλιση) τριών ιδιοτήτων ή χαρακτηριστικών (δηλαδή η αντιμετώπιση των αντίστοιχων κινδύνων): της «εμπιστευτικότητας», της «ακεραιότητας» και της «διαθεσιμότητας». Στη συνέχεια θα δούμε συνοπτικά τις τρεις αυτές ιδιότητες.

- Εμπιστευτικότητα (Confidentiality) Εμπιστευτικότητα είναι η ιδιότητα των δεδομένων ή πληροφοριών να είναι προσπελάσιμα μόνο από τις εξουσιοδοτημένες προς τούτο οντότητες. Η εμπιστευτικότητα αναφέρεται στο περιεχόμενο ηλεκτρονικών εγγράφων ή, γενικά, αρχείων και μηνυμάτων, στην ύπαρξή τους και στην ταυτότητα αυτών που εκτελούν ενέργειες και ανταλλάσσουν μηνύματα. Επίσης, αναφέρεται στο χρόνο και την ποσότητα μηνυμάτων που ανταλλάσσονται. Η εμπιστευτικότητα, μερικές φορές, καλείται και «ιδιωτικότητα» ή «μυστικότητα» ή «προστασία του απορρήτου».
- Ακεραιότητα (Integrity). Η ακεραιότητα είναι η ιδιότητα των δεδομένων και πληροφοριών και των υπολογιστικών και επικοινωνιακών πόρων να τροποποιούνται μόνο από εξουσιοδοτημένες οντότητες κατά εξουσιοδοτημένο τρόπο. Η ακεραιότητα έχει να κάνει με την ακρίβεια και τη συνέπεια στη λειτουργία συστημάτων και διεργασιών. Τα δεδομένα σε κάθε σύστημα πρέπει να παραμένουν πλήρη και ορθά. Η ακεραιότητα διατηρείται όταν διατηρούνται και οι ιδιότητες: η ακρίβεια, η μη τροποποίηση ή τροποποίηση από εξουσιοδοτημένους χρήστες ή διεργασίες, με συνέπεια, κατά αποδεκτό τρόπο. Έχουν αναγνωριστεί τρεις καθοριστικές συνιστώσες του όρου *ακεραιότητα:* οι «εξουσιοδοτημένες ενέργειες», ο «διαχωρισμός και η προστασία αγαθών» και, τέλος, «η ανίχνευση και διόρθωση σφαλμάτων».
- Διαθεσιμότητα (variability). Η διαθεσιμότητα είναι η ιδιότητα των δεδομένων ή πληροφοριών και των υπολογιστικών και επικοινωνιακών πόρων να είναι διαθέσιμα στους εξουσιοδοτημένους προς τούτο χρήστες σύμφωνα με τα δικαιώματά τους. Η διαθεσιμότητα -όπως και η ακεραιότητα- είναι μια σύνθετη έννοια. Αναφέρεται στα δεδομένα και στις υπηρεσίες ή, αλλιώς, στους υπολογιστικούς πόρους (computing resources), στην παρουσία αντικειμένων ή υπηρεσιών σε χρησιμοποιήσιμη μορφή, στην ύπαρξη αρκετά μεγάλης χωρητικότητας για την κάλυψη των όποιων απαιτήσεων, καθώς και στην ποιότητα της παρεχόμενης υπηρεσίας

- Φυσικά μέτρα: Αναφέρονται στον έλεγχο φυσικής πρόσβασης στους υπολογιστικούς και επικοινωνιακούς πόρους, όπως επίσης και στην προστασία από φυσικά φαινόμενα ή ατυχήματα, όπως διαρροή νερού ή πλημμύρες, φωτιά, σεισμό κ.ά.
- Οργανωτικά - διοικητικά: Αναφέρονται στη διαχείριση ασφάλειας, στην εκπόνηση ανάλυσης επικινδυνότητας, στην κατάρτιση σχεδίου ασφάλειας, πολιτικής ασφάλειας και σχεδίου έκτακτης ανάγκης. Τα μέτρα αυτά εξετάζονται και αναθεωρούνται σε τακτά χρονικά διαστήματα.
- Λειτουργικά μέτρα: Αναφέρονται σε όλους εκείνους τους μηχανισμούς που πρέπει να ενεργοποιούνται κατά τη λειτουργία συστημάτων υπολογιστών. Στα μέτρα αυτά συγκαταλέγονται οι ακόλουθες κατηγορίες: της γνησιότητας (authentication) προέλευσης δεδομένων ή ταυτότητας χρηστών, της ακεραιότητας ή γνησιότητας περιεχομένου (integrity), της εμπιστευτικότητας (confidentiality), του ελέγχου πρόσβασης (access control) και της μη αμφισβήτησης (non - repudiation).

### 1.3 Ορολογία

- Κρυπτογράφηση (encryption) ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με την χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη.
- Η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα ονομάζεται αποκρυπτογράφηση (decryption).
- Κρυπτογραφικός αλγόριθμος (cipher) είναι η μέθοδος μετασχηματισμού δεδομένων σε μία μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος είναι μία πολύπλοκη μαθηματική συνάρτηση.
- Αρχικό κείμενο (plaintext) είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.
- Κλειδί (key) είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στην συνάρτηση κρυπτογράφησης.
- Κρυπτογραφημένο κείμενο (cipher text) είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.
- Κρυπτανάλυση (cryptanalysis) είναι μία επιστήμη που ασχολείται με το "σπάσιμο" κάποιας κρυπτογραφικής τεχνικής ούτως ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί.
- Η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης φαίνεται στο παρακάτω σχήμα.




ΕΙΚΟΝΑ 4119: ΈΝΑ ΤΥΠΙΚΟ ΣΥΣΤΗΜΑ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ - ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗΣ[17]

### 1.4 Βασικές αρχές σχεδιασμού κρυπτογραφημάτων ομάδας (block ciphers)

[17] Η εικόνα είναι διαθέσιμη στο http://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1

### *1.4.1 Τα μέτρα του Shannon*

Ο Shannon ο θεμελιωτής της θεωρίας της πληροφορίας διατύπωσε το 1949 ένα σύνολο από μέτρα τα οποία χαρακτηρίζουν έναν ορθά σχεδιασμένο αλγόριθμο κρυπτογράφησης

- Βαθμός απαιτούμενης κρυπτογραφικής ασφάλειας. Το μέτρο αυτό αφορά το κέρδος του αντιπάλου σε πληροφορία, όταν παρατηρεί το κρυπτοκείμενο.
- Μήκος του κλειδιού. Η ευκολία χειρισμού του κλειδιού εξαρτάται από το μήκος του.
- Πρακτική εκτέλεση της κρυπτογράφησης και της αποκρυπτογράφησης. Η προσπάθεια που απαιτείται για την κρυπτογράφηση και την αποκρυπτογράφηση, σε χρόνο ή λειτουργίες.
- Διόγκωση του κρυπτοκειμένου. Είναι επιθυμητό το κρυπτοκείμενο να έχει το ίδιο μήκος (ή συγκρίσιμου μεγέθους) με το απλό κείμενο.
- Διάδοση των σφαλμάτων κρυπτογράφησης. Είναι επιθυμητό ένα σφάλμα κατά την κρυπτογράφηση να επηρεάζει σε όσο το δυνατό λιγότερο βαθμό την αποκρυπτογράφηση.
-

Η ύπαρξη των μέτρων σε ένα κρυπτοσύστημα είναι υποχρεωτική, αλλά συγχρόνως και αντιφατική, με αποτέλεσμα να μην υπάρχει στην πραγματικότητα κρυπτοσύστημα το οποίο να ικανοποιεί όλα τα μέτρα στο μέγιστο τους. Για παράδειγμα, πλήρης έλλειψη του πρώτου μέτρου σημαίνει ότι ο αντίπαλος μπορεί να ανακτήσει πλήρως το απλό κείμενο. Η πλήρης έλλειψη του τρίτου και τέταρτου μέτρου επιτρέπει κρυπτό-συστήματα που μπορούν να μεγιστοποιούν όλα τα άλλα μέτρα. Η πλήρης έλλειψη του πέμπτου μέτρου δέχεται ύπαρξη κρυπτοσυστήματος που μεγιστοποιεί όλα τα άλλα μέτρα, αλλά σε περίπτωση σφάλματος κατά την κρυπτογράφηση, η ανάκτηση του απλού κειμένου θα ήταν αδύνατη, ακόμη και για κάποιο τμήμα αυτού.

### *1.4.2 Σύγχυση (confusion) και Διάχυση (diffusion)*

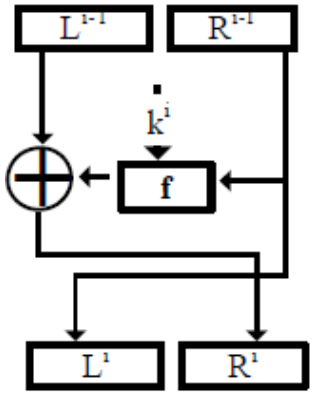
Για την σωστή σχεδίαση ενός κρυπταλγορίθμου χρησιμοποιούνται δύο βασικά χαρακτηριστικά η σύγχυση (confusion)και η διάχυση (diffusion).
Έστω ένα απλό κείμενο το οποίο αντιστοιχεί σε ένα κρυπτοκείμενο μέσω ενός κρυπταλγορίθμου. Εάν αντικαταστήσουμε ένα σύμβολο του απλού κειμένου και κρυπτογραφήσουμε το νέο απλό κείμενο, τότε για ένα κρυπταλγόριθμο με υψηλή διάχυση, ο αντίπαλος δεν θα μπορεί να προβλέψει ποια σύμβολα του κρυπτοκειμένου θα μεταβληθούν η γενικότερα θα επηρεαστούν.

Σύγχυση είναι η ικανότητα του αλγορίθμου κρυπτογράφησης όπου ο "αντίπαλος" δεν είναι σε θέση να προβλέψει ποιες μεταβολές θα συμβούν στο κρυπτοκείμενο, δεδομένης μιας μεταβολής το απλό κείμενο. Δηλαδή, ένας αλγόριθμος έχει υψηλή σύγχυση όταν η σχέση μεταξύ του απλού κειμένου και του κρυπτοκειμένου είναι αρκετά πολύπλοκες, ώστε να χρειάζεται ο αντίπαλος να ξοδέψει σημαντικό χρόνο προκειμένου να τις προσδιορίσει.

Η διάχυση είναι η ικανότητα του αλγορίθμου κρυπτογράφησης όπου ένα τμήμα του απλού κειμένου να έχει την ευκαιρία να επηρεάζει όσο το δυνατόν περισσότερα τμήματά του κρυπτοκειμένου. Ένας αλγόριθμος έχει υψηλή διάχυση όταν ένα στοιχειώδες τμήμα του απλού κειμένου έχει την δυνατότητα να επηρεάσει όλα τα τμήματα του κρυπτοκειμένου ανεξαρτήτως της τοποθεσίας του τμήματος αυτού στο απλό κείμενο.

### *1.4.3 Δίκτυα Feistel*

Η κρυπτογραφική πράξη τύπου Feistel είναι της μορφής του σχήματος που ακολουθεί, η οποία αποτελείται από ένα γινόμενο κρυπτοσυστήματος το οποίο δημιουργεί ένα γύρο. Το κυρίως χαρακτηριστικό ενός δικτύου Feistel είναι η πλήρης ελευθερία στην επιλογή της συνάρτησης γύρου f. Η δομή του δικτύου Feistel είναι τέτοια ώστε η αντίστροφη σχέση ορίζεται πάντοτε, ακόμα και αν η συνάρτηση δεν είναι ενριπτική. Επιπλέον, σε ορισμένες περιπτώσεις ένα δίκτυο Feistel μπορεί να είναι αρκετά ασφαλές.




ΕΙΚΟΝΑ 4220: ΈΝΑΣ ΓΥΡΟΣ FEISTEL

Σε κάθε γύρο η είσοδος χωρίζεται στο αριστερό και στο δεξιό τμήμα. Τα δύο τμήματα της εισόδου του i-στου γύρου συμβολίζονται με $L^{i-1}$ και $R^{i-1}$, ενώ οι έξοδοι συμβολίζονται με $L^t$ και R\ Στον πρώτο γύρο τα τμήματα $L^0$και $R^0$ αντιστοιχούν στο απλό κείμενο, ενώ στον τελικό γύρο τα τμήματα $L^r$ και $R^r$ αντιστοιχούν στο κρυπτοκείμενο.

Κατά το γύρο του i, η συνάρτηση γύρου f δέχεται ως είσοδο το δεξιό τμήμα της εισόδου και το κλειδί $k^i$ το οποίο προέρχεται από το πρόγραμμα κλειδιού. Η έξοδος της συνάρτησης συνδυάζεται με το αριστερό τμήμα της εισόδου με αποκλειστική διάζευξη και το αποτέλεσμα της πράξης αντιστοιχίζεται στο δεξιό τμήμα της εξόδου, ενώ το δεξιό τμήμα της εισόδου αντιστοιχίζεται στο αριστερό τμήμα της εξόδου. Η ανταλλαγή του αριστερού τμήματος με το δεξί έχει ως αποτέλεσμα ο επόμενος γύρος να εφαρμόσει το αποτέλεσμα της συνάρτησης σε εκείνο το τμήμα της εισόδου το οποίο μεταφέρθηκε ατόφιο από την είσοδο στην έξοδο. Είναι φανερό ότι σε κρυπτοσύστημα με έναν και μόνο γύρο, το δεξιό τμήμα του κρυπτοκειμένου θα είναι ίσο με το αριστερό τμήμα του απλού κειμένου. Αυτό είναι ένα χαρακτηριστικό της κρυπτογραφικής πράξης τύπου Feistel και θεωρητικά ένα δίκτυο όπου τα δύο τμήματα εισόδου έχουν το ίδιο μέγεθος, θα πρέπει να περιλαμβάνει τουλάχιστον τρεις γύρους προκειμένου το κρυπτοσύστημα να έχει τη δυνατότητα να αποκρύψει πλήρως το απλό κείμενο. Στην πράξη όμως απαιτούνται πολύ περισσότεροι γύροι για να είναι ένα κρυπτοσύστημα τύπου Feistel ασφαλές. Ο αριθμός των γύρων καθώς και η κρυπτογραφική δύναμη του κρυπτοσυστήματος εξαρτάται από τη συνάρτηση f.

Έστω $n_L$ και $n_R$ το μέγεθος του αριστερού και δεξιού τμήματος αντίστοιχα, με συνολικό μήκος εισόδου $n= n_L+ n_R$. Η συνάρτηση γύρου θα ορίζει την αντιστοιχία $f:\{0,1\}^{n}{}_{R}$^-$\{0,1\}^{n}{}_{L}$. Αν $n_L=n_R=n/2$ το δίκτυο Feistel ονομάζεται ισορροπημένο. Η πράξη κρυπτογράφησης ορίζεται από την επανάληψη της κρυπτογραφικής πράξης:

$$e_{i,i}(L^i, R^i) = L^{i-1} \,||\, (f(R^{i-1},k^i) + L^{i''1}, \text{για } 0< i < r,$$

Για το απλό κείμενο θα είναι $p=L^0||R^0$, ενώ για το κρυπτοκείμενο θα είναι $c=L^r||R^r$. Το κλειδί επιλέγεται σε κάθε γύρο από το πρόγραμμα κλειδιού {k ,k ,....,k }. Κατά την αποκρυπτογράφηση εφαρμόζεται η ίδια πράξη με τη διαφορά ότι το πρόγραμμα του κλειδιού ακολουθεί την αντίστροφη σειρά.

Το τμήμα της εισόδου το οποίο τροφοδοτείται στη συνάρτηση γύρου ονομάζεται προέλευση, ενώ το τμήμα της εισόδου στο οποίο εφαρμόζεται το αποτέλεσμα της συνάρτησης με αποκλειστική διάζευξη ονομάζεται στόχος. Αν το μέγεθος της πηγής είναι μεγαλύτερο από το μέγεθος του στόχου, τότε το δίκτυο ονομάζεται δίκτυο Feistel σημαίνουσας προέλευσης, ενώ στην περίπτωση που το μέγεθός του στόχου είναι μεγαλύτερο, το δίκτυο ονομάζεται δίκτυο Feistel σημαίνοντος στόχου. Αν το άθροισμα του μεγέθους της πηγής και του στόχου είναι ίσο με το μέγεθος της εισόδου, τότε το δίκτυο ονομάζεται τέλειο ενώ στην περίπτωση που το άθροισμα της πηγής και του στόχου είναι μικρότερο, το δίκτυο ονομάζεται ατελές. Σε ένα ατελές δίκτυο υπάρχει τμήμα της εισόδου το οποίο εμφανίζεται ατόφιο στην έξοδο και επιπλέον δεν συμπεριλαμβάνεται στην πράξη της συνάρτησης γύρου. Το τμήμα αυτό ονομάζεται μηδενικό.

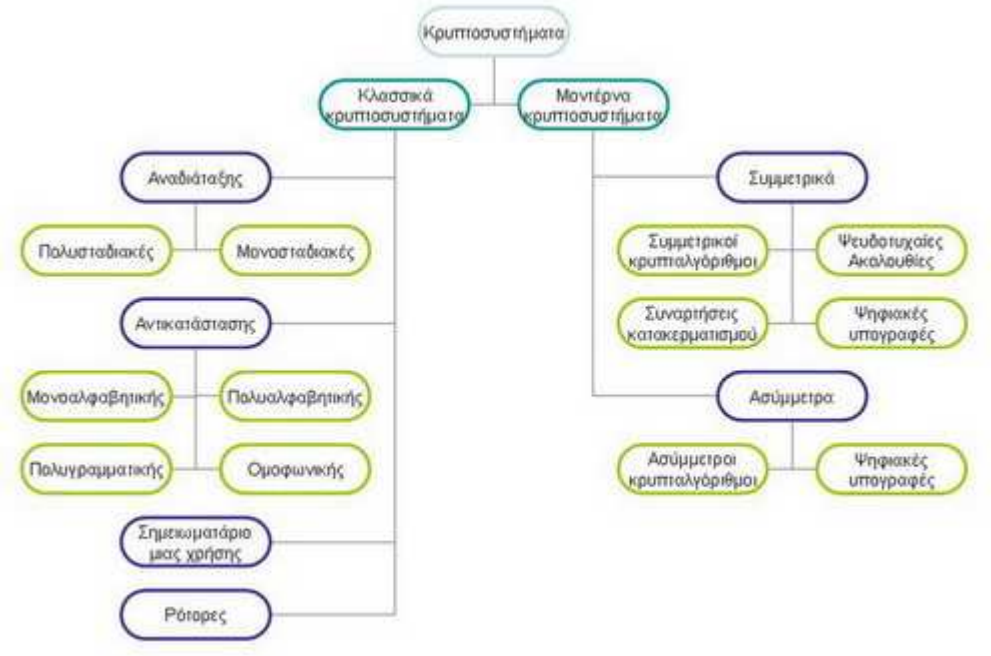
Στη βιβλιογραφία το συντριπτικό ποσοστό στην έρευνα των δικτύων Feistel αποδίδεται σε ισορροπημένα δίκτυα Feistel, δηλαδή το αριστερό τμήμα της εισόδου είναι ο στόχος και είναι ίσο με το δεξιό τμήμα της εισόδου που είναι η προέλευσή. Ο βασικός λόγος εκτενούς μελέτης των ισορροπημένων δικτύων Feistel είναι επειδή τα πιο διαδεδομένα κρυπτοσυστήματα τα οποία βασίζονται σε δίκτυα Feistel είναι ισορροπημένα, όπως το κρυπτοσύστημα DES που θα υλοποιήσουμε στην συνέχεια. Ωστόσο, η ασύμμετρη κατανομή των τμημάτων της εισόδου σε δίκτυα Feistel σημαίνουσας προέλευσης και σημαίνοντος στόχου δημιουργεί υποψίες ότι ένα μη ισορροπημένο δίκτυο Feistel μπορεί να είναι κρυπτογραφικά αδύναμο. Στην περίπτωση το δικτύου Feistel σημαίνοντος στόχου θα υπάρχουν σε κάθε γύρο γραμμικές σχέσεις μεταξύ ορισμένων bits εισόδου με ορισμένα bits εξόδου. Στην περίπτωση δικτύου Feistel σημαίνουσας προέλευσης απαιτούνται περισσότεροι γύροι για να εμφανιστεί κάθε bit στο τμήμα του στόχου.

### 1.5. Είδη Κρυπτοσυστημάτων

Τα κρυπτοσυστήματα χωρίζονται σε 2 μεγάλες κατηγορίες τα Κλασσικά Κρυπτοσυστήματα και τα Μοντέρνα κρυπτοσυστήματα.
Επιπροσθέτως, οι κρυπτογραφικοί αλγόριθμοι μπορούν να χωριστούν σε δύο διαφορετικές κατηγορίες με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων:

- Δέσμης (Block Ciphers), οι οποίοι χωρίζουν το μήνυμα σε κομμάτια και κρυπτογραφούν κάθε ένα από τα κομμάτια αυτά χωριστά.
- Ροής (Stream Ciphers), οι οποίοι κρυπτογραφούν μία ροή μηνύματος (stream) χωρίς να την διαχωρίζουν σε τμήματα.

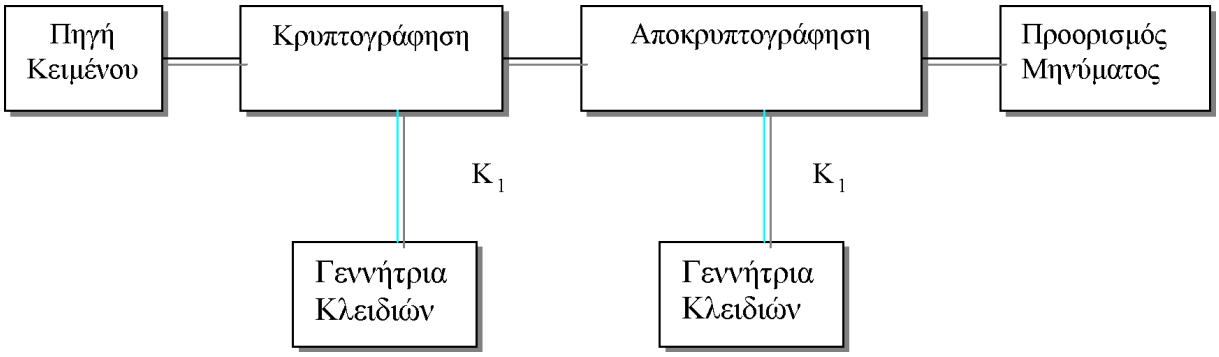
Κλασσικά Κρυπτοσυστήματα
Μοντέρνα Κρυπτοσυστήματα
Συμμετρικά Κρυπτοσυστήματα




ΕΙΚΟΝΑ 43: ΜΠΛΟΚ ΑΝΑΛΥΣΗΣ ΕΙΔΩΝ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΟΣ.[18]

[18] Η εικόνα είναι διαθέσιμη στο http://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1

**Συμμετρικό κρυπτοσύστημα** είναι το σύστημα εκείνο το οποίο χρησιμοποιεί κατά την διαδικασία της κρυπτογράφησης αποκρυπτογράφησης ένα κοινό κλειδί. Η ασφάλεια αυτών των αλγορίθμων βασίζεται στην μυστικότητα του κλειδιού. Τα συμμετρικά κρυπτοσυστήματα προϋποθέτουν την ανταλλαγή του κλειδιού μέσα από ένα ασφαλές κανάλι επικοινωνίας ή μέσα από την φυσική παρουσία των προσώπων. Αυτό το χαρακτηριστικό καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων.




ΕΙΚΟΝΑ 4421: ΜΟΝΤΕΛΟ ΣΥΜΜΕΤΡΙΚΟΥ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΟΣ[19]

Τα στάδια της επικοινωνίας του σχήματος 32 είναι τα ακόλουθα:

1. Ο Κώστας ή η Βασιλική αποφασίζει για ένα κλειδί το οποίο το επιλέγει τυχαία μέσα από τον κλειδοχώρο.
2. Η Βασιλική αποστέλλει το κλειδί στον Κώστα μέσα από ένα ασφαλές κανάλι.
3. Ο Κώστας δημιουργεί ένα μήνυμα όπου τα σύμβολα m ανήκουν στον χώρο των μηνυμάτων.
4. Κρυπτογραφεί το μήνυμα με το κλειδί που έλαβε από την Βασιλική και η παραγόμενη κρυπτοσυμβολοσειρά αποστέλλεται.
5. Η Βασιλική λαμβάνει την κρυπτοσυμβολοσειρά και στην συνέχεια με το ίδιο κλειδί την αποκρυπτογραφεί και η έξοδος που παράγεται είναι το μήνυμα.

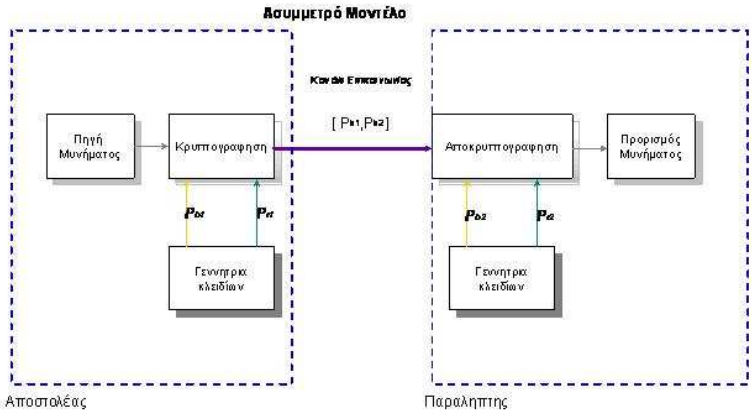
Έχουμε το αρχικό μήνυμα, (ένα σύνολο δυαδικών ψηφίων (bits) (μί, όπου i = 1, 2, ..., n}), και το κλειδί γνωστό σε αποστολέα και παραλήπτη, (ένα άλλο σύνολο δυαδικών ψηφίων (κ i, όπου i = 1, 2, ..., n}). Αν δημιουργήσουμε τον γρίφο που θα αποσταλεί, (ένα σύνολο δυαδικών ψηφίων γί, που να ικανοποιούν την σχέση {γί = μί Φκί, όπου ί = 1, 2, ..., η}), τότε θα ισχύει επίσης ότι {μί = γί Φκί, όπου i = 1, 2, ..., n} και ο παραλήπτης του γρίφου με χρήση του κλειδιού θα αναδημιουργήσει το μήνυμα.
Μηνύματα μεγάλου μήκους μπορούν να κρυπτογραφούνται σε ομάδες των n δυαδικών ψηφίων. Το σύμβολο Φ συμβολίζει την πράξη αποκλειστικό Ή (XOR) που περιγράφεται στο άρθρο Λογικές συναρτήσεις.

Το **ασύμμετρο κρυπτοσύστημα** ή κρυπτοσύστημα δημοσίου κλειδιού δημιουργήθηκε για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα. Χαρακτηριστικό του είναι ότι έχει δυο είδη κλειδιών ένα ιδιωτικό και ένα δημόσιο. Το δημόσιο είναι διαθέσιμο σε όλους ενώ το ιδιωτικό είναι μυστικό. Η βασική σχέση μεταξύ τους είναι : ότι κρυπτογραφεί το ένα, μπορεί να το αποκρυπτογραφήσει μόνο το άλλο.
Τα στάδια της επικοινωνίας του σχήματος 33 είναι τα ακόλουθα:

1. Η γεννήτρια κλειδιών του Μένιου παράγει 2 ζεύγη κλειδιών,
2. Η γεννήτρια κλειδιών της Ελένης παράγει 2 ζεύγη κλειδιών
3. Η Ελένη και ο Μένιος ανταλλάσσουν τα δημόσια ζεύγη
4. Ο Μένιος δημιουργεί ένα μήνυμα όπου τα σύμβολα m ανήκουν στον χώρο των μηνυμάτων.
5. Κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί της Ελένης και η παραγόμενη κρυπτοσυμβολοσειρά αποστέλλεται

[19] Η εικόνα είναι διαθέσιμη στο http://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1

6. Η Ελένη λαμβάνει την κρυπτοσυμβολοσειρά και στην συνέχεια με το ιδιωτικό της κλειδί την αποκρυπτογραφεί και η έξοδος που παράγεται είναι το μήνυμα.




ΕΙΚΟΝΑ 4522: ΜΟΝΤΕΛΟ ΑΣΥΜΜΕΤΡΟΥ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΟΣ[20]

### 1.5.1. Εφαρμογές Κρυπτογραφίας.

Η εξέλιξη της χρησιμοποίησης της κρυπτογραφίας ολοένα αυξάνεται καθιστώντας πλέον αξιόπιστη την μεταφορά της πληροφορίας για διάφορους λειτουργικούς σκοπούς:

1. Ασφάλεια συναλλαγών σε τράπεζες δίκτυα - ATM
2. Κινητή τηλεφωνία (ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM)
3. Σταθερή τηλεφωνία (crypto phones)
4. Διασφάλιση Εταιρικών πληροφοριών
5. Στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)
6. Διπλωματικά δίκτυα (Τηλεγραφήματα)
7. Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές)
8. Ηλεκτρονική ψηφοφορία
9. Ηλεκτρονική δημοπρασία
10. Ηλεκτρονικό γραμματοκιβώτιο
11. Συστήματα συναγερμών
12. Συστήματα βιομετρικής αναγνώρισης
13. Έξυπνες κάρτες
14. Ιδιωτικά δίκτυα (VPN)
15. World Wide Web
16. Δορυφορικές εφαρμογές (δορυφορική τηλεόραση)
17. Ασύρματα δίκτυα (Hipperlan, Bluetooth, 802.11x)
18. Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων
19. Τηλεδιάσκεψη - Τηλεφωνία μέσω διαδικτύου (VOIP)

[20] Η εικόνα είναι διαθέσιμη στο http://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1

### 1.6. Τρόποι και Μέθοδοι Κρυπτογράφησης

Οι τρόποι κρυπτογράφησης μυστικού κλειδιού τυπικά χωρίζονται σε 2 κατηγορίες. Η πρώτη περιλαμβάνει διαδικασίες κρυπτογράφησης που εφαρμόζονται πάνω σε ένα μοναδικό bit (ή byte ή word) και υλοποιούν κάποιο μηχανισμό ανατροφοδότησης έτσι ώστε το κλειδί να αλλάζει συνεχώς. Για αυτό και ονομάζονται κρυπτογράφοι ροής (stream ciphers). Η δεύτερη κατηγορία (κρυπτογράφοι μπλοκ - block ciphers) αποτελείται από αλγορίθμους κρυπτογράφησης που λειτουργούν πάνω σε ομάδες δεδομένων κάθε χρονική στιγμή χρησιμοποιώντας το ίδιο κλειδί για κάθε ομάδα. Έτσι στην γενική περίπτωση, όταν το ίδιο μυστικό κλειδί χρησιμοποιείται, η ίδια ομάδα δεδομένων ενός plaintext θα κρυπτογραφηθεί στο ίδιο cipher text όταν η κρυπτογράφηση γίνεται με έναν αλγόριθμο κρυπτογράφησης μπλοκ αλλά σε διαφορετικό cipher text όταν χρησιμοποιηθεί ένας κρυπτογράφος ροής. Για τους κρυπτογράφους μπλοκ, έχουν επινοηθεί αρκετοί τρόποι λειτουργίας (modes) ώστε να βελτιωθούν κάποια χαρακτηριστικά τους όπως η ασφάλεια που προσφέρουν ή να γίνουν πιο κατάλληλοι για διάφορες εφαρμογές. Τέσσερις είναι οι κυριότεροι τρόποι λειτουργίας :

**Electronic Codebook (ECB)**

Αυτός ο τρόπος λειτουργίας είναι ο απλούστερος και ο πλέον προφανής. Το μυστικό κλειδί χρησιμοποιείται για την κρυπτογράφηση κάθε μπλοκ δεδομένων του plaintext. Κατά συνέπεια με την χρήση του ίδιου κλειδιού, το ίδιο plaintext μπλοκ θα μετατρέπεται πάντα στο ίδιο cipher text μπλοκ. Είναι ο πλέον κοινός τρόπος λειτουργίας των κρυπτογράφων μπλοκ γιατί είναι ο απλούστερος και άρα ο πιο εύκολα υλοποιήσιμος και συνάμα ο πιο γρήγορος καθώς δεν χρησιμοποιείται κάποιου είδους ανατροφοδότηση. Μειονέκτημα του είναι ότι είναι ο πιο ευάλωτος τρόπος κρυπτογράφησης σε επιθέσεις τύπου brute-force (ως επίθεση brute-force θεωρείται η προσπάθεια εύρεσης του μυστικού κλειδιού με την εξαντλητική δοκιμή πιθανών κλειδιών).

**Cipher Block Chaining (CBC)**

Χρησιμοποιώντας την CBC λειτουργία, προστίθεται σε έναν κρυπτογράφο μπλοκ ένας μηχανισμός ανατροφοδότησης. Ο τρόπος αυτός λειτουργίας ορίζει ότι προτού να γίνει η κρυπτογράφηση ενός νέου μπλοκ plaintext, γίνεται XOR (αποκλειστικό-Ή) του μπλοκ αυτού και του cipher text μπλοκ που μόλις πριν έχει παραχθεί. Με τον τρόπο αυτό, 2 ταυτόσημα μπλοκ plaintext δεν κρυπτογραφούνται ποτέ στο ίδιο cipher text. Σε σχέση με τον ECB προσφέρεται μεγαλύτερη ασφάλεια, με κόστος όμως κυρίως στην ταχύτητα κρυπτογράφησης καθώς για να ξεκινήσει η επεξεργασία ενός μπλοκ plaintext είναι απαραίτητο να έχει ολοκληρωθεί πλήρως η κρυπτογράφηση του προηγούμενου μπλοκ. Αποτρέπεται έτσι η χρήση τεχνικών pipelining (software ή hardware) που μπορούν να επιταχύνουν την διαδικασία.

**Cipher Feedback (CFB)**

Ο τρόπος αυτός λειτουργίας επιτρέπει σε έναν κρυπτογράφο μπλοκ να συμπεριφερθεί σαν ένας κρυπτογράφος ροής. Αυτό είναι θεμιτό όταν πρέπει να κρυπτογραφούνται δεδομένα που μπορεί να έχουν μέγεθος μικρότερο από ένα μπλοκ. Παράδειγμα τέτοιας εφαρμογής μπορεί να είναι η διαδικασία κρυπτογράφησης ενός terminal session. Περιληπτικά, κατά την CFB λειτουργία χρησιμοποιείται ένας shift καταχωρητής στο μέγεθος του block μέσα στον οποίο τοποθετούνται τα δεδομένα προς κρυπτογράφηση. Όλος ο καταχωρητής κρυπτογραφείται και αυτό που προκύπτει είναι το cipher text. Η ποσότητα των δεδομένων που μπαίνουν μέσα στον shift καταχωρητή καθορίζεται από την εφαρμογή.

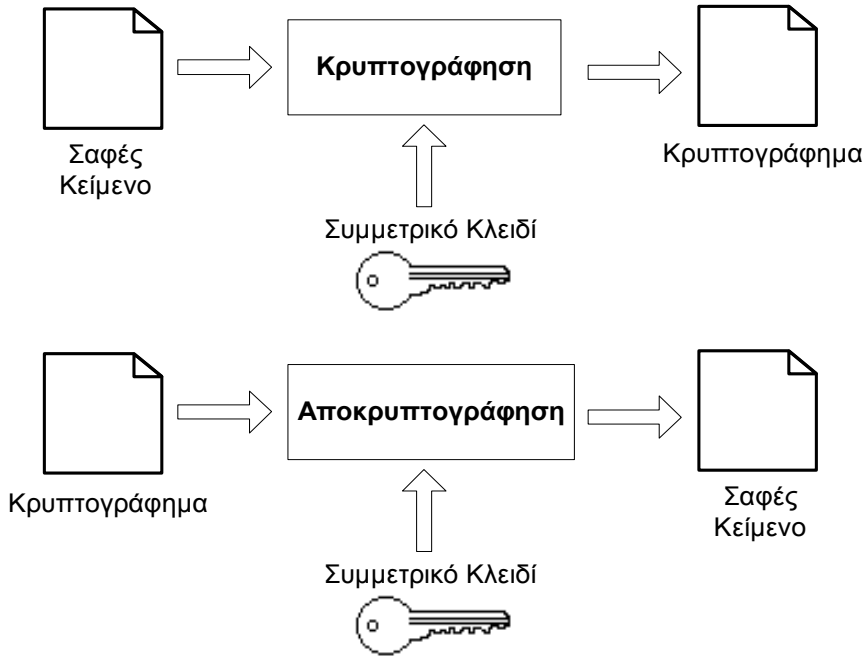
**Output Feedback (OFB)**

Στόχος και αυτού του τρόπου λειτουργίας των μπλοκ κρυπτογράφων είναι να εξασφαλίσει ότι το ίδιο plaintext μπλοκ δεν μπορεί να παράγει το ίδιο cipher text μπλοκ. Σε σχέση με το CBC, χρησιμοποιείται και εδώ ένας μηχανισμός ανατροφοδότησης παρόλα αυτά είναι εσωτερικός και ανεξάρτητος από τα plaintext και cipher text δεδομένα.

Σημαντικοί αλγόριθμοι αυτής της κατηγορίας είναι οι DES (Data Encryption Standard), 3DES, DESX, ο AES (Advanced Encryption Standard), οι RC2, RC4, RC5 και IDEA (International Data Encryption Algorithm). Οι αλγόριθμοι της σειράς DES είναι οι πλέον χρησιμοποιούμενοι σήμερα αλγόριθμοι, αν και πλέον αντικαθιστούνται από τον AES. Επινοήθηκαν από την IBM την δεκαετία του '70 και υιοθετήθηκαν από το National Bureau of Standards (νυν NIST) των ΗΠΑ. Οι DES αλγόριθμοι χρησιμοποιούν κλειδιά μήκους 56 bits (ο 3DES και ο DESX επεκτείνουν κατάλληλα αυτόν τον αριθμό χρησιμοποιώντας περισσότερα κλειδιά) και επεξεργάζονται μπλοκ των 64 bits. Ο AES αλγόριθμος είναι το πρότυπο που καθιερώθηκε από το NIST ως διάδοχος του DES και πλέον αποτελεί τον προτεινόμενο αλγόριθμο κρυπτογράφησης για εφαρμογές υψηλής ασφάλειας. Οι αλγόριθμοι RC είναι αλγόριθμοι μεταβλητού κλειδιού από την RSA Security ενώ ο IDEA χρησιμοποιείται στο πρότυπο PGP (Pretty Good Privacy).

## 1.7 Συμμετρική Κρυπτογράφηση

Η συμμετρική κρυπτογραφία βασίζεται στην ύπαρξη ενός μοναδικού κλειδιού, γνωστό ως *μυστικό ή συμμετρικό κλειδί (secret key)*, με το οποίο γίνεται η κρυπτογράφηση και η αποκρυπτογράφηση της πληροφορίας. Ο αποστολέας και ο παραλήπτης είναι οι μοναδικές οντότητες που γνωρίζουν και χρησιμοποιούν το μυστικό κλειδί. Στην εικόνα 46 περιγράφει την διαδικασία της συμμετρικής κρυπτογραφίας. Τα μηνύματα προς κρυπτογράφηση, γνωστά ως το *σαφές κείμενο (plaintext)*, κρυπτογραφούνται με χρήση του συμμετρικού (ή μυστικού) κλειδιού. Η διαδικασία της κρυπτογράφησης έχει ως έξοδο ένα κείμενο σε ακατανόητη μορφή, γνωστό ως *κρυπτογράφημα (ciphertext)*. Η ασφάλεια της μεταδιδόμενης πληροφορίας επιτυγχάνεται ακριβώς επειδή το κρυπτογράφημα μεταδίδεται σε ακατανόητη μορφή. Η διαδικασία της ανάκτησης της αρχικής πληροφορίας με τη χρήση του ίδιου συμμετρικού κλειδιού ονομάζεται αποκρυπτογράφηση.




[21]

ΕΙΚΟΝΑ 4623: ΔΙΑΔΙΚΑΣΙΑ ΣΥΜΜΕΤΡΙΚΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

[21] Η εικόνα είναι διαθέσιμη εδώ

Η συμμετρική κρυπτογραφία χρησιμοποιείται εδώ και χιλιάδες χρόνια. Ένας από τους παλιότερους γνωστούς κώδικες κρυπτογραφίας είναι ο αλγόριθμος του Καίσαρα, που αποτελεί έναν απλό κώδικα αντικατάστασης. Άλλοι γνωστοί και πιο σύγχρονοι αλγόριθμοι είναι οι αλγόριθμοι DES,IDEA, RC5, και AES.

Στα πλεονεκτήματα της συμμετρικής κρυπτογραφίας συγκαταλέγονται οι υψηλές ταχύτητες κρυπτογράφησης και αποκρυπτογράφησης που μπορούν να υπερβούν τα 100Mbps καθώς επίσης και οι μικρές απαιτήσεις της σε μνήμη και υπολογιστική ισχύ. Έτσι καθίσταται δυνατή η εφαρμογή της σε περιβάλλοντα όπως αυτά ενός κινητού τηλεφώνου ή μιας έξυπνης κάρτας. Επίσης το μέγεθος του κρυπτογραφήματος είναι αρκετά μικρότερο από αυτό του αρχικού κειμένου.

Η ανάγκη της ανταλλαγής του συμμετρικού κλειδιού μεταξύ αποστολέα και παραλήπτη είναι ένας από τους σημαντικότερους περιορισμούς της συμμετρικής κρυπτογραφίας. Η ασφάλεια της συμμετρικής κρυπτογραφίας βασίζεται αποκλειστικά στο γεγονός ότι ο αποστολέας και ο παραλήπτης μοιράζονται το συμμετρικό κλειδί πριν από την αποστολή του μηνύματος. Έτσι κρίνεται απαραίτητη η επίτευξη μιας ασφαλούς ζεύξης για την μεταφορά του συμμετρικού κλειδιού. Κάτι τέτοιο όμως δεν είναι πάντα εφικτό εξαιτίας πρακτικών αλλά και λειτουργικών δυσκολιών. Η διαδικασία της ασφαλούς ανταλλαγής του συμμετρικού κλειδιού γίνεται ακόμα μεγαλύτερη όταν οι δύο οντότητες, ο παραλήπτης και ο αποστολέας , είναι άγνωστες μεταξύ τους. Σε αυτή την περίπτωση προκύπτει η ανάγκη πιστοποίησης της ταυτότητας κάθε οντότητας έτσι ώστε να αποφευχθεί η διαβίβαση του κλειδιού σε κάποια τρίτη, μη εξουσιοδοτημένη οντότητα. Συνήθως στη συμμετρική κρυπτογραφία η μεταφορά του κλειδιού γίνεται είτε μέσω μιας φυσικής ζεύξης (ανταλλαγή κλειδιού πρόσωπο με πρόσωπο) είτε μέσω μίας έμπιστης τρίτης οντότητας, την οποία οι χρήστες εμπιστεύονται για την ασφαλή μεταφορά του κλειδιού

Ένας ακόμη σημαντικός περιορισμός αφορά στη δυσκολία κλιμάκωσης της μεθόδου. Καθώς το πλήθος των χρηστών που θέλουν να επικοινωνήσουν μεταξύ τους μεγαλώνει, γίνεται αυτονόητο ότι μεγαλώνει και το πλήθος των κλειδιών που θα χρησιμοποιηθούν για κάθε επιμέρους επικοινωνία. Για την επίτευξη επικοινωνίας μεταξύ n χρηστών απαιτούνται $n^2/2$ μοναδικά συμμετρικά κλειδιά, συμπεριλαμβανομένου και του κλειδιού που έχει κάθε χρήστης για τον εαυτό του. Τα προβλήματα της διαχείρισης των κλειδιών (key management) γίνονται ακόμα μεγαλύτερα γιατί κάθε κλειδί θα πρέπει περιοδικά να αντικαθίσταται από κάποιο καινούριο με σκοπό τη μείωση των δεδομένων που κρυπτογραφούνται με το ίδιο κλειδί.

### *1.7.1 Αλγόριθμος κρυπτογράφησης Data Encryption Standard (DES)*

Ο κρυπταλγόριθμος DES (Data Encryption Standard) είναι ένας κρυπταλγόριθμος τμήματος με $F = G = \{0, 1\}^{64}$ και $\boldsymbol{K} = \{0, 1\}^{56}$. Στην πραγματικότητα το αρχικό κλειδί έχει μέγεθος 64 bits, αλλά μόνον τα 56 από αυτά συμμετέχουν στην κρυπτογράφηση. Τα υπόλοιπα 8 bits του κλειδιού χρησιμοποιούνται για αρτιότητα (parity bits). Αποτελείται από 18 κρυπτογραφικές πράξεις, οι οποίες είναι μια αρχική μετάθεση του απλού κειμένου, ένα ισορροπημένο δίκτυο Feistel με 16 γύρους, και τέλος από μια μετάθεση του κειμένου του τελευταίου γύρου. Σε κάθε γύρο του κρυπτογραφικού γινομένου του δικτύου Feistel, συμμετέχουν 48 bits του κλειδιού, όπως καθορίζονται από το πρόγραμμα του κλειδιού.

Ο DES δημοσιεύθηκε το 1977 και είναι ο κρυπταλγόριθμος στον οποίο έχει γίνει η περισσότερη έρευνα σχετικά με την κρυπτογραφική του δύναμη. Οι απόπειρες κρυπτανάλυσης του DES είχαν σαν αποτέλεσμα την ανακάλυψη και καθιέρωση ποικίλλων αρχών σχεδίασης των κρυπταλγόριθμων τμήματος. Ο DES είναι βασισμένος στον κρυπταλγόριθμο Lucifer της IBM, του οποίου το τμήμα του απλού κειμένου, του κρυπτοκειμένου, καθώς και το μέγεθος του κλειδιού είναι 128 bits.

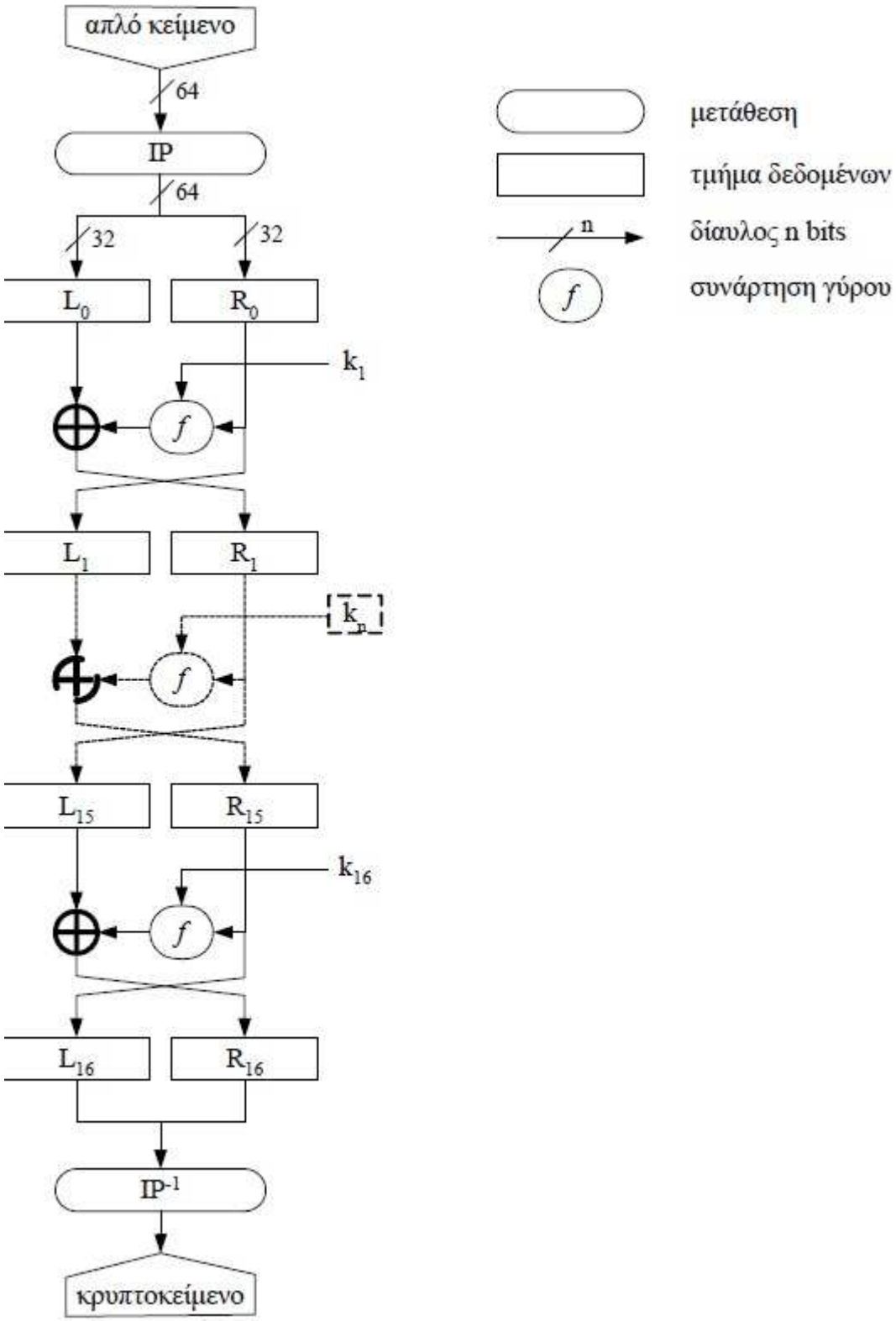
DES σχεδιάσθηκε με βάση τα κριτήρια σχεδιασμού τα οποία διατυπώθηκαν το 1972 από το Υπουργείο Εμπορίου των ΗΠΑ, που επιζητούσε να βελτιωθεί η εθνική ασφάλεια με κρυπτογραφικές μεθόδους για την αποθήκευση, επεξεργασία, και διανομή της πληροφορίας. Τα κριτήρια ήταν τα ακόλουθα:

- υψηλό επίπεδο ασφάλειας,
- πλήρεις και διαφανείς προδιαγραφές,

- η ασφάλεια δε θα πρέπει να εξαρτάται από τη μυστικότητα του κρυπταλγορίθμου,
- διαθέσιμο σε, και προσβάσιμο από, όλους τους χρήστες,
- κατάλληλο για ποικιλία εφαρμογών,
- χαμηλό κόστος υλοποίησης,
- να είναι επιτρεπτή η εξαγωγή του,
- να είναι δυνατή η αξιολόγησή του.

Ωστόσο, στην πράξη συνέβησαν ορισμένα γεγονότα τα οποία ήρθαν σε αντίφαση με τα παραπάνω κριτήρια. Αρχικά, όσον αφορά το πρώτο κριτήριο της απαίτησης της υψηλής ασφάλειας, ο DES είχε πολύ μικρότερο κλειδί από αυτό του προκατόχου του, τον Lucifer. Στην περίπτωση του DES, ο κλειδοχώρος ορίζεται από $2_{56} \approx 72 \cdot 10_{15}$ κλειδιά, έναντι του κλειδοχώρου του Lucifer, ο οποίος περιέχει $2_{128} \approx 34 \cdot 10_{37}$ κλειδιά. Σε αυτό ευθύνεται η Υπηρεσία Εθνικής Ασφάλειας (National Security Agency, NSA) των ΗΠΑ, η οποία άσκησε πιέσεις για μικρό μήκος κλειδιού.

Όσον αφορά το κριτήριο της διαφάνειας των προδιαγραφών, τα κριτήρια σχεδιασμού των κουτιών αντικατάστασης που περιέχονται στη συνάρτηση γύρου του DES αποκαλύφθηκαν στα μέσα περίπου της δεκαετίας του ’90. Τα κριτήρια σχεδιασμού των κουτιών περιείχαν ενδείξεις ότι η τεχνική διαφορικής κρυπτανάλυσης που ανακαλύφθηκε επίσημα στις αρχές της δεκαετίας του ’90, ήταν γνωστή 15 χρόνια πριν. Επίσης η συγκεκριμένη επιλογή του αριθμού των γύρων του δικτύου Feistel του DES, έγινε ώστε ο DES να είναι ανθεκτικός σε διαφορική κρυπτανάλυση.




ΕΙΚΟΝΑ 4724: Ο ΚΡΥΠΤΑΛΓΟΡΙΘΜΟΣ ΤΜΗΜΑΤΟΣ DES[22]

.

[22] Η εικόνα είναι διαθέσιμη στο http://utopia.duth.gr/~vkatos/documents/the_book/ch5.pdf

### *1.7.1.1 Τεχνικά χαρακτηριστικά του DES*

Ο κρυπταλγόριθμος DES παρουσιάζεται στην εικόνα 47, όπου διακρίνονται η είσοδος του απλού κειμένου, η αρχική μετάθεση IP, η ακολουθία των 16 γύρων τύπου Feistel, η τελική μετάθεση IP-1 και τέλος η έξοδος του κρυπτοκειμένου. Ο κρυπταλγόριθμος DES έχει το χαρακτηριστικό ότι η κρυπτογράφηση και η αποκρυπτογράφηση μπορούν να υλοποιηθούν με την ίδια διαδικασία, με τη μόνη διαφορά ότι το πρόγραμμα κλειδιού της αποκρυπτογράφησης παράγει την αντίστροφη ακολουθία που παράγει το πρόγραμμα κλειδιού της κρυπτογράφησης. Αν δηλαδή κατά την κρυπτογράφηση το πρόγραμμα κλειδιού είναι {$k1$,$k2$,…,$k15$}, το πρόγραμμα κλειδιού κατά την αποκρυπτογράφηση θα είναι {$k15$,$k14$,…,$k1$}.

**Αρχική και τελική μετάθεση**

Η αρχική μετάθεση είναι η αντιστροφή της τελικής μετάθεσης και αντίστροφα. Ο λόγος που επιλέχθηκε αυτή η εξάρτηση των δύο μεταθέσεων είναι για να μπορεί να χρησιμοποιηθεί η ίδια διαδικασία και στην κρυπτογράφηση και στην αποκρυπτογράφηση, με τη μόνη διαφορά του προγράμματος των κλειδιών, όπως αναφέρθηκε παραπάνω. Στις δύο αυτές μεταθέσεις δε συμμετέχει το κλειδί, και επομένως δεν προσθέτουν ουσιαστικά περαιτέρω ασφάλεια στην κατασκευή. Η ύπαρξη της αρχικής και τελικής μετάθεσης έγινε για λόγους πρακτικούς, για να υπάρχει κάποιος χώρος αποθήκευσης (μνήμη) του απλού κειμένου και του κρυπτοκειμένου, πριν και μετά την εφαρμογή του δικτύου Feistel. Η ύπαρξη αποθηκευτικών χώρων στην είσοδο και στα ηλεκτρονικά κυκλώματα είναι κοινή τακτική, και χρησιμοποιείται για να προσφέρει απομόνωση μεταξύ ενός ολοκληρωμένου κυκλώματος (microchip) και του υπολοίπου ηλεκτρονικού κυκλώματος. Ένας δεύτερος λόγος της επιλογής της συγκεκριμένης μετάθεσης είναι ότι δημιουργούνται ομαδοποιήσεις. Τα bits που βρίσκονται σε θέση πολλαπλάσια του αριθμού 8 δημιουργούν δυαδικές λέξεις. Έτσι στην περίπτωση που το απλό κείμενο αποτελείται από χαρακτήρες ASCII, διαχωρίζεται η πληροφορία του χαρακτήρα από το όγδοο bit αρτιότητας. Ωστόσο, δεν υπάρχουν ενδείξεις αν ο διαχωρισμός αυτός μειώνει ή αυξάνει την κρυπτογραφική δύναμη του DES. Γενικότερα κατά την ανάλυση του DES δεν εξετάζονται η αρχική και η τελική μετάθεση, αλλά στην πράξη η συμμετοχή αυτών είναι υποχρεωτική λόγω της τυποποιημένης προδιαγραφής του κρυπταλγορίθμου.

Η αρχική μετάθεση παρουσιάζεται στην εικόνα 48. Στην εικόνα ο πίνακας αριθμείται από αριστερά προς δεξιά και από επάνω προς τα κάτω. Η αρίθμηση καθορίζει το bit εξόδου, ενώ το περιεχόμενο του πίνακα καθορίζει το bit εισόδου. Έτσι, στο πρώτο bit της εξόδου της μετάθεσης θα εμφανισθεί το πεντηκοστό όγδοο (58) bit του απλού κειμένου, στο δεύτερο bit της εξόδου, το πεντηκοστό (50) bit, κ.ο.κ

IP=

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

ΕΙΚΟΝΑ 4825: Η ΑΡΧΙΚΗ ΑΛΛΗΛΟΜΕΤΑΘΕΣΗ IP

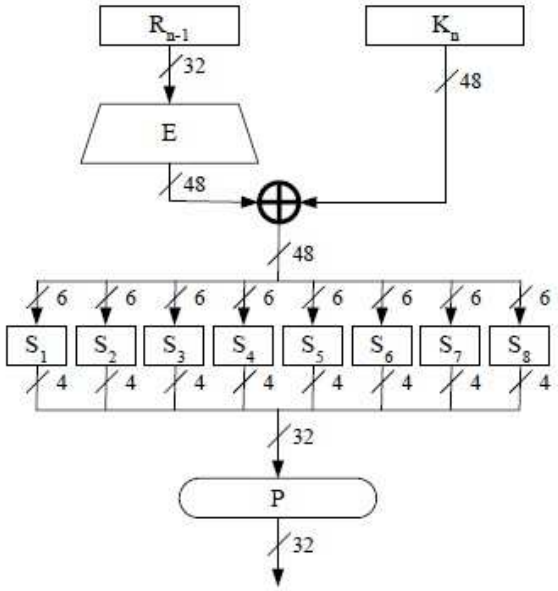
.

Η τελική μετάθεση προκύπτει από την αντιστροφή της IP. Για παράδειγμα, παρατηρούμε ότι το πρώτο bit της εισόδου στην IP εμφανίζεται στην 40-στη θέση, το δεύτερο bit στην όγδοη θέση, κ.ο.κ. Έτσι η τελική μετάθεση θα είναι:

IP-1=| 40 8 48 … |

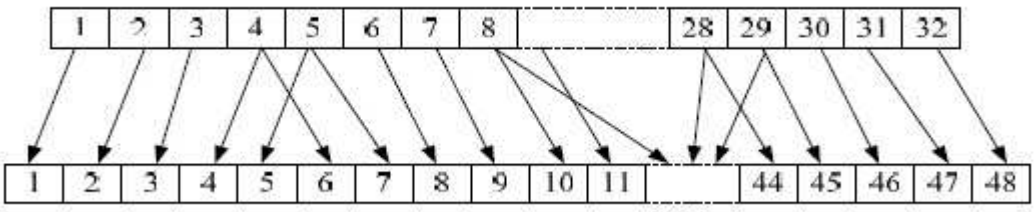
**Η συνάρτηση γύρου, f**

Η συνάρτηση γύρου αποτελείται από μια συνάρτηση επέκτασης $E$:{0,1}32→ {0,1}48, οκτώ κουτιά αντικατάστασης $Si$:{0,1}6→{0,1}4, και μια τελική συνάρτηση μετάθεσης $P$ των 32 bits. Η συνάρτηση γύρου παριστάνεται στην εικόνα 49.




ΕΙΚΟΝΑ 4926: Η ΣΥΝΑΡΤΗΣΗ ΓΥΡΟΥ ΤΟΥ DES[23]

Η συνάρτηση επέκτασης είναι μια μετάθεση στην οποία ορισμένα bits της εισόδου εμφανίζονται σε περισσότερες από μια θέσεις στην έξοδο. Πιο συγκεκριμένα, τα bits εισόδου στις θέσεις 4, 5, 8, 9, 12, 13, …, 28, 29 εμφανίζονται διπλά, όπως φαίνεται στην εικόνα 50. Είναι προφανές ότι υπάρχει γραμμική σχέση μεταξύ των bits της εισόδου και των bits της εξόδου της συνάρτησης επέκτασης.




ΕΙΚΟΝΑ 27: Η ΣΥΝΑΡΤΗΣΗ ΕΠΕΚΤΑΣΗΣ Ε.[24]

Η «καρδιά» του DES βρίσκεται στα οκτώ κουτιά αντικατάστασης. Τα κουτιά αυτά εισάγουν μη γραμμικότητα στην κατασκευή και η κρυπτογραφική δύναμη του κρυπταλγορίθμου εξαρτάται άμεσα από αυτά. Τα κριτήρια σχεδιασμού των κουτιών έγιναν γνωστά το 1994 σε δημοσίευση του Coppersmith και είναι τα εξής:

- Κάθε κουτί έχει είσοδο των 6 bits και έξοδο των 4 bits.
- Κανένα από τα bits της εξόδου δεν θα πρέπει να βρίσκεται σε γραμμική σχέση με οποιοδήποτε από το bits της εισόδου.
- Αν τα δύο πρώτα bits και τα δύο τελευταία bits της εισόδου είναι σταθερά ενώ τα ενδιάμεσα bits αλλάζουν, οι έξοδοι που προκύπτουν θα πρέπει να είναι μοναδικές.

[23] Η εικόνα είναι διαθέσιμη στο http://utopia.duth.gr/~vkatos/documents/the_book/ch5.pdf
[24] Η εικόνα είναι διαθέσιμη στο http://utopia.duth.gr/~vkatos/documents/the_book/ch5.pdf

- Αν η απόσταση Hamming δύο εισόδων είναι ίση με 1, τότε η απόσταση Hamming των αντίστοιχων εξόδων θα πρέπει να είναι το λιγότερο ίση με 2.
- Αν δύο είσοδοι διαφέρουν στα δύο μεσαία bits, τότε οι αντίστοιχες έξοδοι θα πρέπει να διαφέρουν το λιγότερο σε 2 bits.
- Αν δύο είσοδοι έχουν τα δύο πρώτα bits διαφορετικά ενώ τα δύο τελευταία bits είναι ίδια, τότε οι αντίστοιχες έξοδοι θα πρέπει να είναι διαφορετικές.
- Για οποιαδήποτε μη μηδενική διαφορά των 6 bits της εισόδου, θα πρέπει το πολύ 8 από τα 32 ζευγάρια να προκαλούν την ίδια διαφορά εξόδου.
- Όμοια με το παραπάνω κριτήριο, αλλά θα πρέπει να εφαρμόζεται συγχρόνως σε οποιαδήποτε 3 από τα 8 κουτιά αντικατάστασης.

Με βάση τα κριτήρια αυτά σχεδιάσθηκαν τα κουτιά *S*1 έως *S*8, όπως φαίνονται στην εικόνα 51

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 15 | 1 | 8 | 14 | 6 | 11 | 3 | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 |
| 1 | 3 | 13 | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 |
| 2 | 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | 5 | 8 | 12 | 6 | 9 | 3 | 2 | 15 |
| 3 | 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | 0 | 5 | 14 | 9 |

Το κουτί αντικατάστασης *S2*

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 10 | 0 | 9 | 14 | 6 | 3 | 15 | 5 | 1 | 13 | 12 | 7 | 11 | 4 | 2 | 8 |
| 1 | 13 | 7 | 0 | 9 | 3 | 4 | 6 | 10 | 2 | 8 | 5 | 14 | 12 | 11 | 15 | 1 |
| 2 | 13 | 6 | 4 | 9 | 8 | 15 | 3 | 0 | 11 | 1 | 2 | 12 | 5 | 10 | 14 | 7 |
| 3 | 1 | 10 | 13 | 0 | 6 | 9 | 8 | 7 | 4 | 15 | 14 | 3 | 11 | 5 | 2 | 12 |

Το κουτί αντικατάστασης *S3*

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 7 | 13 | 14 | 3 | 0 | 6 | 9 | 10 | 1 | 2 | 8 | 5 | 11 | 12 | 4 | 15 |
| 1 | 13 | 8 | 11 | 5 | 6 | 15 | 0 | 3 | 4 | 7 | 2 | 12 | 1 | 10 | 14 | 9 |
| 2 | 10 | 6 | 9 | 0 | 12 | 11 | 7 | 13 | 15 | 1 | 3 | 14 | 5 | 2 | 8 | 4 |
| 3 | 3 | 15 | 0 | 6 | 10 | 1 | 13 | 8 | 9 | 4 | 5 | 11 | 12 | 7 | 2 | 14 |

Το κουτί αντικατάστασης *S4*

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 2 | 12 | 4 | 1 | 7 | 10 | 11 | 6 | 8 | 5 | 3 | 15 | 13 | 0 | 14 | 9 |
| 1 | 14 | 11 | 2 | 12 | 4 | 7 | 13 | 1 | 5 | 0 | 15 | 10 | 3 | 9 | 8 | 6 |
| 4 | 4 | 2 | 1 | 11 | 10 | 13 | 7 | 8 | 15 | 9 | 12 | 5 | 6 | 3 | 0 | 14 |
| 3 | 11 | 8 | 12 | 7 | 1 | 14 | 2 | 13 | 6 | 15 | 0 | 9 | 10 | 4 | 5 | 3 |

Το κουτί αντικατάστασης *S5*

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 12 | 1 | 10 | 15 | 9 | 2 | 6 | 8 | 0 | 13 | 3 | 4 | 14 | 7 | 5 | 11 |
| 1 | 10 | 15 | 4 | 2 | 7 | 12 | 9 | 5 | 6 | 1 | 13 | 14 | 0 | 11 | 3 | 8 |
| 2 | 9 | 14 | 15 | 5 | 2 | 8 | 12 | 3 | 7 | 0 | 4 | 10 | 1 | 13 | 11 | 6 |
| 3 | 4 | 3 | 2 | 12 | 9 | 5 | 15 | 10 | 11 | 14 | 1 | 7 | 6 | 0 | 8 | 13 |

Το κουτί αντικατάστασης *S6*

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 4 | 11 | 2 | 14 | 15 | 0 | 8 | 13 | 3 | 12 | 9 | 7 | 5 | 10 | 6 | 1 |
| 1 | 13 | 0 | 11 | 7 | 4 | 9 | 1 | 10 | 14 | 3 | 5 | 12 | 2 | 15 | 8 | 6 |
| 2 | 1 | 4 | 11 | 13 | 12 | 3 | 7 | 14 | 10 | 15 | 6 | 8 | 0 | 5 | 9 | 2 |
| 3 | 6 | 11 | 13 | 8 | 1 | 4 | 10 | 7 | 9 | 5 | 0 | 15 | 14 | 2 | 3 | 12 |

Το κουτί αντικατάστασης S7

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 13 | 2 | 8 | 4 | 6 | 15 | 11 | 1 | 10 | 9 | 3 | 14 | 5 | 0 | 12 | 7 |
| 1 | 1 | 15 | 13 | 8 | 10 | 3 | 7 | 4 | 12 | 5 | 6 | 11 | 0 | 14 | 9 | 2 |
| 2 | 7 | 11 | 4 | 1 | 9 | 12 | 14 | 2 | 0 | 6 | 10 | 13 | 15 | 3 | 5 | 8 |
| 3 | 2 | 1 | 14 | 7 | 4 | 10 | 8 | 13 | 15 | 12 | 9 | 0 | 3 | 5 | 6 | 11 |

Το κουτί αντικατάστασης S8

ΕΙΚΟΝΑ 5128: ΚΟΥΤΙΑ ΑΝΤΙΚΑΤΑΣΤΑΣΗΣ ΣΤΟΝ DES

Τέλος, οι έξοδοι των οκτώ κουτιών εισέρχονται σε μια τελική μετάθεση P των 32 bits, που παρουσιάζεται στην εικόνα 52.

P=

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 16 | 7 | 20 | 21 | 29 | 12 | 28 | 17 |
| 1 | 15 | 23 | 26 | 5 | 18 | 31 | 10 |
| 2 | 8 | 24 | 14 | 32 | 27 | 3 | 9 |
| 19 | 13 | 30 | 6 | 22 | 11 | 4 | 25 |

ΕΙΚΟΝΑ 5229: Η ΜΕΤΑΘΕΣΗ P ΠΡΙΝ ΑΠΟ ΤΗΝ ΕΞΟΔΟ ΤΗΣ ΣΥΝΑΡΤΗΣΗΣ ΓΥΡΟΥ.

### *1.7.2 Ο κρυπταλγόριθμος ΑΕΣ*

Το πρότυπο AES περιγράφει μια συμμετρική μπλοκ διαδικασία κρυπτογράφησης μυστικού κλειδιού. Το πρότυπο υποστηρίζει την χρήση κλειδιών μήκους 128, 192 και 256 bits. Ανάλογα με το ποιο μήκος κλειδιού χρησιμοποιείται, συνήθως χρησιμοποιείται η συντόμευση AES-128, AES-192 και AES-256 αντίστοιχα. Ανεξάρτητα από το μήκος κλειδιού, ο αλγόριθμος επενεργεί πάνω σε μπλοκ δεδομένων μήκους 128 bits. Η διαδικασία κρυπτογράφησης είναι επαναληπτική. Αυτό σημαίνει ότι σε κάθε μπλοκ δεδομένων γίνεται μια επεξεργασία η οποία επαναλαμβάνεται έναν αριθμό από φορές ανάλογα με το μήκος κλειδιού. Κάθε επανάληψη ονομάζεται γύρος (round). Στον πρώτο γύρο επεξεργασίας ως είσοδος είναι ένα plaintext μπλοκ και το αρχικό κλειδί, ενώ στους γύρους που ακολουθούν ως είσοδος είναι το μπλοκ που έχει προκύψει από τον προηγούμενο γύρο καθώς και ένα κλειδί που έχει παραχθεί από το αρχικό με βάση κάποια διαδικασία που ορίζει ο αλγόριθμος. Το τελικό προϊόν της επεξεργασίας είναι το κρυπτογραφημένο μπλοκ (cipher text). Το μπλοκ αυτό πρέπει να σημειωθεί ότι έχει ακριβώς το ίδιο μέγεθος (128 bits) με το plaintext μπλοκ.

#### *1.7.2.1 Είσοδοι, Έξοδοι και Εσωτερική Κατάσταση.*

Όπως ήδη αναφέρθηκε, ο AES χρησιμοποιεί ακολουθίες των128 bits (μπλοκ) καθώς και κλειδιά, που μπορεί να έχουν μέγεθος 128, 192 ή 256 bits αντίστοιχα. Τα κλειδιά αυτά ονομάζονται κλειδιά κρυπτογράφησης (cipher keys) ώστε να ξεχωρίζουν από τα κλειδιά που παράγονται κατά την λειτουργία του αλγορίθμου.
Η βασική μονάδα επεξεργασίας στον AES είναι το byte. Έτσι τα bits ενός μπλοκ ή ενός κλειδιού χωρίζονται σε ομάδες των 8 για να σχηματιστούν τα bytes. Κάθε byte στον AES αντιστοιχεί σε ένα πολυώνυμο (αριθμητική πεπερασμένων πεδίων - finite field arithmetic). Αν υποθέσουμε ότι τα bits που αποτελούν ένα byte είναι τα {b7, b6, b5, b4, b3, b2, b1, b0}, τότε το byte αυτό αναπαριστά το πολυώνυμο :

$$b_7 x^7 + b_6 x^6 + b_5 x^5 + b_4 x^4 + b_3 x^3 + b_2 x^2 + b_1 x^1 + b_0 = \Sigma\, b_i x^1$$

Έτσι για παράδειγμα το byte {11001101} αντιστοιχεί στο πολυώνυμο $x^7 + x^6 + x^3 + x^2 + 1$. Κλείνοντας την αναφορά στις μονάδες των δεδομένων που διαχειρίζεται ο AES, πρέπει να αναφερθεί το πώς γίνεται η δεικτοδότηση των bits και των bytes στα μπλοκ και στα κλειδιά.

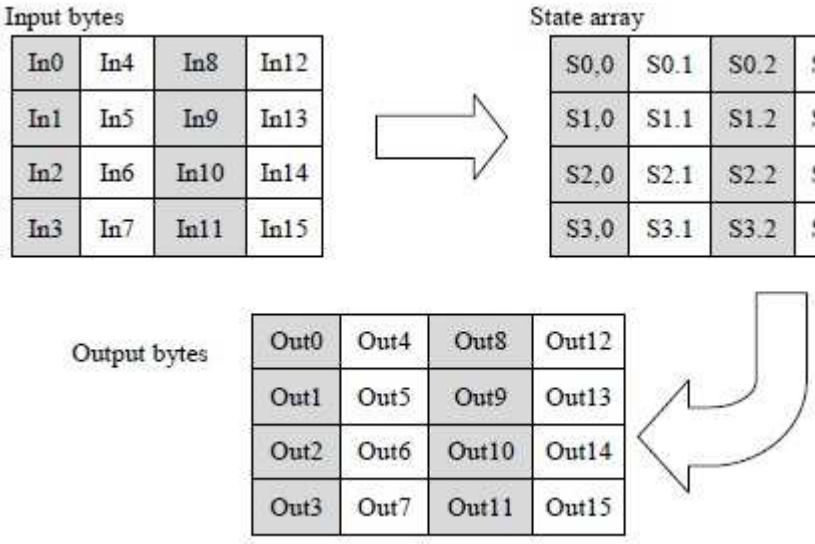
| Input bit sequence | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | ..... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Byte number | 0 | | | | | | | | 1 | | | | | | | | ..... |
| Bit numbers in byte | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | ..... |

Εικόνα 5330: Δεικτοδότηση των bits και bytes.

Όλες οι λειτουργίες που επιτελεί ο αλγόριθμος γίνονται πάνω σε ένα δισδιάστατο πίνακα που αποκαλείται Κατάσταση (State). Ο πίνακας αυτός περιλαμβάνει τέσσερις γραμμές από bytes, με κάθε

μία γραμμή να αποτελείται από Nb bytes. Ο αριθμός που αντιστοιχεί στην ποσότητα Nb υπολογίζεται αν διαιρεθεί το μήκος του μπλοκ με το 32. Εφόσον στον AES υποστηρίζονται μπλοκ μεγέθους μόνο 128 bits, το Nb θα έχει τιμή 4.

Το μπλοκ εισόδου περιλαμβάνει 16 bytes, τα οποία δεικτοδοτούνται in0 έως in15. Το κρυπτογραφημένο μπλοκ εξόδου περιλαμβάνει επίσης 16 bytes που δεικτοδοτούνται ως out0 έως out15. Η State χρησιμοποιεί την μεταβλητή s με δύο δείκτες που δηλώνουν την θέση κάθε byte στον πίνακα. Η πρώτη λοιπόν και τελευταία λειτουργία που μπορεί να υποτεθεί ότι γίνεται στον AES είναι να αντιστοιχηθούν τα bytes εισόδου σε κάποια θέση του πίνακα της State και το αντίστροφο στην έξοδο.




ΕΙΚΟΝΑ 5431: ΑΝΤΙΣΤΟΙΧΗΣΗ ΤΩΝ BYTES ΕΙΣΟΔΟΥ ΣΕ ΚΑΠΟΙΑ ΘΕΣΗ ΤΟΥ ΠΙΝΑΚΑ ΤΗΣ STATE ΚΑΙ ΤΟ ΑΝΤΙΣΤΡΟΦΟ ΣΤΗΝ ΕΞΟΔΟ[25]

Η αντιστοίχηση που περιγράφηκε παραπάνω μπορεί να περιγραφεί μαθηματικά. Η αντιστοίχηση εισόδου στην State περιγράφεται από την σχέση :

$$s[r,c] = in[r+4c] \text{ για } 0 < r < 4 \text{ και } 0 < c < Nb$$

ενώ η αντιγραφή της State στην έξοδο από την σχέση :

$$out[r+4c] = s[r,c] \text{ για } 0 < r < 4 \text{ και } 0 < c < Nb$$

Ένας άλλος τρόπος να δει κάποιος τα περιεχόμενα της State είναι σαν 32-bit λέξεις (words) αντί για byte. Μια 32-bit word περιλαμβάνει τα 4 bytes μιας στήλης, οπότε τα 4 words που αποτελούν την State είναι τα ακόλουθα :

w(0) = s(0,0) s(1,0) s(2,0) s(3,0) w(1) = s(0,1) s(1,1) s(2,1) s(3,1) w(2) = s(0,2) s(1,2) s(2,2) s(3,2)

w(3) = s(0,3) s(1,3) s(2,3) s(3,3)

Περιγραφή Αλγορίθμου: Όπως αναφέρθηκε στην προηγούμενη ενότητα, το πρότυπο AES ορίζει ότι τα μπλοκ που επεξεργάζεται ο αλγόριθμος έχουν μέγεθος 128 bits και αυτό ορίζεται από την ποσότητα Nb = 4, που συμβολίζει τον αριθμό των 32-bit λέξεων στο μπλοκ. Από την άλλη, τα κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση, μπορούν να έχουν μήκος 128, 192 ή 256 bits. Η μεταβλητή Nk συμβολίζει τον αριθμό των 32-bit λέξεων που μπορεί να περιλαμβάνει ένα κλειδί και κατά συνέπεια μπορεί να πάρει τις τιμές 4, 6 και 8. Ανάλογα με το μήκος κλειδιού που θα επιλεχθεί

[25] Η εικόνα είναι διαθέσιμη στο *http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf*

για την κρυπτογράφηση, ο αλγόριθμος ορίζει έναν αριθμό από γύρους επεξεργασίας που απαιτούνται για την ολοκλήρωση της. Η μεταβλητή Nr χρησιμοποιείται για να δηλώσει το πλήθος των γύρων. Αν χρησιμοποιηθεί μήκος κλειδιού 128 bits τότε απαιτούνται 10 γύροι επεξεργασίας. Για μήκη κλειδιού ίσα με 192 και 256 bits απαιτούνται αντίστοιχα 12 και 14 γύροι.

| | Key Length (Nk words) | Block Size (Nb words) | Number Of Rounds (Nr) |
|---|---|---|---|
| AES-128 | 4 | 4 | 10 |
| AES-192 | 6 | 4 | 12 |
| AES-256 | 8 | 4 | 14 |

ΕΙΚΟΝΑ 55: ΜΕΓΕΘΟΣ ΤΩΝ ΜΕΤΑΒΛΗΤΩΝ ΤΟΥ ΑΛΓΟΡΙΘΜΟΥ

- Nr = Αριθμός των γύρων
- Nb = Αριθμός των byte
- Nk = Μέγεθος κλειδιού

Να σημειωθεί ότι οι παραπάνω συνδυασμοί μήκους μπλοκ, μήκους κλειδιού και γύρων επεξεργασίας είναι αυτοί που ορίζονται αυστηρά στο πρότυπο AES. Ο αλγόριθμος κρυπτογράφησης Rijndael στον οποίο βασίζεται ο AES δίνει την δυνατότητα πραγματοποίησης περισσότερων συνδυασμών. Έτσι, καταλαβαίνει κανείς ότι ο AES ουσιαστικά ορίζει ένα υποσύνολο του αλγορίθμου Rijndael. Τόσο κατά την διάρκεια της διαδικασίας κρυπτογράφησης όσο και αποκρυπτογράφησης, κάθε γύρος επεξεργασίας αποτελείται από μια σειρά μετασχηματισμών σε επίπεδο byte. Για την ακρίβεια, χρησιμοποιούνται 4 τύποι μετασχηματισμών :

- ένας μετασχηματισμός αντικατάστασης bytes χρησιμοποιώντας κάποιον σχετικό πίνακα αντικατάστασης
- ένας μηχανισμός ολίσθησης των bytes της State κατά διαφορετικά offsets
- μια διαδικασία ανάμειξης των bytes της State
- μια πρόσθεση ενός κλειδιού στην State

### *1.7.2.2 Ο Αλγόριθμος Κρυπτογράφησης AES*

Στην αρχή της διαδικασίας κρυπτογράφησης ένα μπλοκ εισόδου (plaintext) αντιγράφεται στην State. Μετά από έναν αρχικό γύρο πρόσθεσης κλειδιού, ακολουθούν 10, 12 ή 14 γύροι επεξεργασίας, με τον τελευταίο γύρο να διαφέρει από τους υπόλοιπους. Η τελική State αντιγράφεται στην έξοδο και η επεξεργασία για το συγκεκριμένο block ολοκληρώνεται (παραγωγή του cipher text μπλοκ). Το μυστικό κλειδί κρυπτογράφησης που χρησιμοποιείται σαν είσοδος στον αλγόριθμο είναι το κλειδί που προστίθεται στο μπλοκ εισόδου πριν αρχίσει η επεξεργασία. Σε καθέναν από τους γύρους επεξεργασίας, όπως αναφέρθηκε παραπάνω, υπάρχει μια φάση κατά την οποία προστίθεται στο μπλοκ και ένα κλειδί. Το κλειδί που προστίθεται στις περιπτώσεις αυτές, δεν είναι το αρχικό μυστικό κλειδί αλλά κάποιο που έχει προκύψει με μια συγκεκριμένη διαδικασία από το μυστικό κλειδί και είναι διαφορετικό για κάθε γύρο. Για τον λόγο αυτό, τα κλειδιά αυτά ονομάζονται round keys. Η διαδικασία με την οποία προκύπτουν τα round κλειδιά ονομάζεται Επέκταση Κλειδιού και θα αναλυθεί σε επόμενη ενότητα.

Αυτό που πρέπει να διευκρινιστεί είναι η έννοια της πρόσθεσης στον AES αλγόριθμο. Σε προηγούμενη ενότητα έχει αναφερθεί ότι τα bytes της πληροφορίας κατά την επεξεργασία τους λαμβάνονται ως πολυώνυμα. Έτσι, η πράξη της πρόσθεσης είναι ουσιαστικά μια διαδικασία πρόσθεσης πολυωνύμων. Η πρόσθεση μεταξύ πολυωνύμων πραγματοποιείται με την πρόσθεση των συντελεστών των αντίστοιχων όρων (δυνάμεων) των πολυωνύμων. Η πρόσθεση γίνεται modulo-2, δηλαδή μέσω μιας XOR πράξης.

Αν κάθε βασικός μετασχηματισμός του AES αναπαρασταθεί από μια συνάρτηση που επενεργεί στην State, τότε ο αλγόριθμος κρυπτογράφησης μπορεί να περιγραφεί από τον ψευδοκώδικα που παρουσιάζεται παρακάτω:

```
Cipher (byte in [4*Nb], byte out [4*Nb], byte key [4*Nb]
word w [Nb*(Nr+1)])
Begin
Byte state [4, Nb]
State=in
KeyExpansion(key,w);
AddRoundKey (state, w [0, Nb-1])
For round=1 step 1 to Nr-1
SubBytes (state)
ShiftRows (state)
MixColumns (state)
AddRoundKey (state, w [round*Nb, (round+1)*Nb-1])
End for
SubBytes (state)
ShiftRows (state)
AddRoundKey (state, w [Nr*Nb, (Nr+1)*Nb-1]
Out=state
End
```

Οι συναρτήσεις αυτές αναφέρονται ως SubBytes(), ShiftRows(), MixColumns() και AddRoundKey() και αντιστοιχούν (με αυτήν την σειρά) στους μετασχηματισμούς 1 έως 4 όπως αναφέρθηκαν παραπάνω. Να σημειωθεί ότι το array w χρησιμοποιείται για να δηλώσει την συλλογή των round keys που παράγονται από την διαδικασία επέκτασης κλειδιού. Εξήγηση του ψευδοκώδικα για την διαδικασία κρυπτογράφησης. Όπως βλέπουμε παίρνει σαν είσοδο (In) το plaintextt βγάζει σαν έξοδο (out) το cipher text και παίρνουμε και τον πινάκα W ο οποίος έχει δημιουργηθεί κατά την λειτουργία της συνάρτησης key expansion όπου εκεί έχει ανακατευτεί το κλειδί που έχουμε δώσει. Λοιπόν στον γύρο 0 στο state όρισμα αντιγράφουμε το plaintextt και στη συνέχεια καλούμε τη συνάρτηση AddRoundKeyy. Μετά από το γύρο 1 έως τον Nr-1 (ανάλογα το bits αλγορίθμου που έχουμε επιλέξει για να δουλέψουμε 128,196,256) καλούμε με τη σειρά τις συναρτήσεις SubBytes, ShiftRows, MixColumns και AddRoundKeyy όπου εκεί θα ανακατευτεί διαδοχικά το state. Στον τελευταίο γύρο το state θα ανακατευτεί με τις συναρτήσεις SubBytes, ShiftRows και AddRoundKey όπου το τελικό αποτέλεσμα θα είναι το cipher text.

### 1.8 Ασύμμετρη Κρυπτογραφία ή Κρυπτογραφία Δημοσίου Κλειδιού

Στα μέσα της δεκαετίας του ‘70 οι Whitfield Diffie και Martin Hellman πρότειναν μια νέα τεχνική για τον περιορισμό των προβλημάτων της συμμετρικής κρυπτογραφίας. Η τεχνική αυτή, γνωστή ως κρυπτογραφία δημοσίου κλειδιού ή ασύμμετρη κρυπτογραφία, βασίζεται στην ύπαρξη ενός ζεύγους κλειδιών (key pair). Αυτό το ζεύγος κλειδιών αν και συσχετίζεται μεταξύ του με μία μαθηματική πράξη, η τιμή του είναι τελείως διαφορετική ώστε να μην είναι δυνατό να αποκαλυφτούν. Με αυτό το τρόπο επιτρέπεται το ένα κλειδί να είναι γνωστό. Το κλειδί αυτό ονομάζεται δημόσιο κλειδί (public key) και χρησιμοποιείται για την κρυπτογράφηση των δεδομένων. Το δεύτερο κλειδί Το δεύτερο κλειδί παραμένει ιδιωτικό για αυτό το λόγο ονομάζεται και "ιδιωτικό κλειδί" και χρησιμοποιείται κατά την αποκρυπτογράφηση

Τα βασικά χαρακτηριστικά του δημόσιου και του ιδιωτικού κλειδιού είναι:

- Κάθε κλειδί είναι ένα δυαδικό αλφαριθμητικό
- Τα κλειδιά, δημόσια και ιδιωτικά, παράγονται ταυτόχρονα από ειδικό πρόγραμμα λογισμικού.

- Τα κλειδιά δεν είναι ταυτόσημα, αλλά σχετίζονται μοναδικά έτσι ώστε να είναι δυνατή η χρήση τους για κρυπτογράφηση και αποκρυπτογράφηση δεδομένων. Η διαδικασία μέσω της οποίας παράγεται το ζεύγος των κλειδιών εξασφαλίζει ότι κάθε κλειδί σχετίζεται μοναδικά με το ταίρι του και κανένα κλειδί δεν μπορεί να παραχθεί από το άλλο.
- Τα κλειδιά, δημόσια και ιδιωτικά, που ανήκουν σε ένα ζεύγος είναι συμπληρωματικά, δηλαδή οι πληροφορίες που κρυπτογραφούνται με το ένα κλειδί μπορούν να αποκρυπτογραφηθούν μόνο με το άλλο και αντίστροφα. Με άλλα λόγια, ένα μήνυμα που έχει κρυπτογραφηθεί χρησιμοποιώντας ένα δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο χρησιμοποιώντας το αντίστοιχο ιδιωτικό κλειδί.
- Κάθε οντότητα που συμμετέχει σε ένα σύστημα επικοινωνίας δημοσίου κλειδιού έχει το δικό της ζεύγος δημόσιου και ιδιωτικού κλειδιού.

Το ιδιωτικό κλειδί:

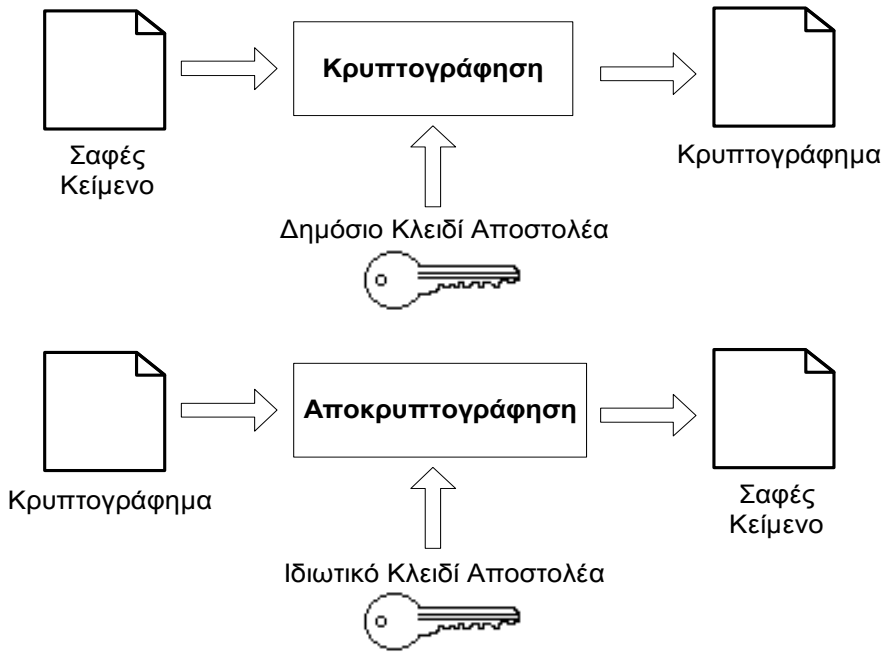
- Προστατεύεται από τον ιδιοκτήτη του
- Χρησιμοποιείται για την ψηφιακή υπογραφή μηνυμάτων

Το δημόσιο κλειδί:

- Διανέμεται ελεύθερα και είναι προσβάσιμο σε οποιονδήποτε
- Χρησιμοποιείται για την πιστοποίηση ψηφιακών υπογραφών
- Χρησιμοποιείται για την κρυπτογράφηση μηνυμάτων
- Αποθηκεύεται μέσα σε «ψηφιακά πιστοποιητικά» που παρέχουν την ακεραιότητα και την αυθεντικότητα του ιδιοκτήτη του κλειδιού

- Παρόλο που τα δημόσια κλειδιά μπορούν να διανέμονται ελεύθερα, τα ιδιωτικά κλειδιά δε θα πρέπει ποτέ να γίνονται γνωστά σε μη εξουσιοδοτημένες οντότητες.

Η εικόνα 56 περιγράφει τη διαδικασία κρυπτογράφησης δημοσίου κλειδιού. Ο αποστολέας κρυπτογραφεί με το δημόσιο κλειδί του παραλήπτη, το οποίο είναι ελεύθερα διαθέσιμο, το μήνυμα που θέλει να του στείλει. Το κρυπτογραφημένο μήνυμα φτάνει στον παραλήπτη ο οποίος το αποκρυπτογραφεί με το ιδιωτικό κλειδί του.




ΕΙΚΟΝΑ 56: ΔΙΑΔΙΚΑΣΙΑ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ[26]

[26] Η εικόνα είναι διαθέσιμη εδώ

Η κρυπτογραφία δημοσίου κλειδιού χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων καθώς και για την ψηφιακή υπογραφή τους. Η ασφάλεια της κρυπτογραφίας δημοσίου κλειδιού βασίζεται ακριβώς στο γεγονός ότι είναι υπολογιστικά αδύνατη η παραγωγή του ιδιωτικού από το δημόσιο κλειδί. Θεωρητικά, βέβαια, το ιδιωτικό κλειδί μπορεί πάντα να υπολογιστεί αλλά το κόστος σε χρόνο, μνήμη και υπολογιστική ισχύ για κάτι τέτοιο είναι τόσο μεγάλο που καθίσταται πρακτικά αδύνατο.

Το σημαντικότερο πλεονέκτημα της ασύμμετρης κρυπτογραφίας είναι ότι δεν απαιτείται ανταλλαγή μυστικού κλειδιού. Το δημόσιο κλειδί είναι ελεύθερα διαθέσιμο, πράγμα που κάνει τη διαχείριση των κλειδιών (key management) πολύ ευκολότερη, ενώ το ιδιωτικό κλειδί είναι γνωστό μόνο στον ιδιοκτήτη του, καθιστώντας έτσι δυσκολότερη την παραποίησή του. Επίσης με την κρυπτογραφία δημοσίου κλειδιού καθίσταται δυνατή η υλοποίηση μιας πολύ σημαντικής κρυπτογραφικής λειτουργίας, αυτή της ψηφιακής υπογραφής δεδομένων.

Η κρυπτογραφία δημοσίου κλειδιού έχει μεγάλες απαιτήσεις σε υπολογιστική ισχύ, σχεδόν 100 φορές παραπάνω από αυτή που απαιτείται στην συμμετρική κρυπτογραφία. Επίσης, είναι αρκετά αργή ειδικά όταν πρόκειται για μεγάλα μηνύματα. Γι' αυτό το λόγο συνήθως δεν κρυπτογραφούνται δεδομένα αλλά συμμετρικά κλειδιά.

### *1.8.1 Κρυπτογράφηση RSA*

Το RSA παίρνει την ασφάλειά του από τη δυσκολία δημιουργίας μεγάλων αριθμών. Τα δημόσια και ιδιωτικά κλειδιά (The public and private keys) είναι λειτουργίες ζευγαριών μεγάλων (100 έως 200 ψηφία ή ακόμα και μεγαλύτερα) βασικών αριθμών. Η ανάκτηση του plaintext από ένα δημόσιο κλειδί και το κρυπτογράφημα υποτίθεται πως θα ισοδυναμεί με την δημιουργία του προϊόντος (ζητούμενο κλειδί) από δυο άλλα βασικά.

Για να παραγάγετε τα δύο κλειδιά, επιλέξτε δύο τυχαίους μεγάλους πρωταρχικούς αριθμούς, τους p και q έτσι ώστε$p \neq q$, και για μέγιστη ασφάλεια επιλέξτε να έχουν το ίδιο μήκος. Υπολογίστε το αποτέλεσμα :

$$n = pq$$

Κατόπιν, υπολογίζουμε την συνάρτηση του Όιλερ: $\varphi(n) = (p-1)(q-1)$, έπειτα, επιλέγουμε ένα τυχαίο αριθμό $e > 1$ για κλειδί κρυπτογράφησης, έτσι ώστε $e \wedge \varphi(n) = 1$. Τέλος υπολογίζουμε το κλειδί αποκρυπτογράφησης αριθμό d έτσι ώστε $d.e = 1 \, mod \, \varphi(n)$.

Σημειώστε επίσης ότι οι αριθμοί d και n είναι επίσης συσχετιζόμενα πρωταρχικά (κλειδιά). Οι αριθμοί e και n είναι το δημόσιο κλειδί ο αριθμός d είναι το ιδιωτικό κλειδί. Τα δύο πρωταρχικά κλειδιά, το p και το q, δεν χρειάζονται πλέον. Δεν πρέπει να απορριφθούν, αλλά ούτε και να αποκαλυφθούν. Για να κρυπτογραφήσετε ένα μήνυμα m, πρώτα διαιρέστε αυτό στους αριθμητικά block μικρότερα από το n (με τα δυαδικά στοιχεία, επιλέξτε το μεγαλύτερο δυνατό από τα 2 και μικρότερο από το n).
Άρα τα κλειδιά θα είναι τα εξής:

- Δημόσιο: $(n, e)$
- ιδιωτικό:$(n, d)$

Δηλαδή εάν και το p και το q είναι βασικά 100-ψηφία , τότε το n θα έχει κάτω από 200 ψηφία και κάθε block μηνυμάτων, m, θα πρέπει να έχει πάνω από 200 ψηφία .
(Εάν πρέπει να κρυπτογραφήσετε έναν σταθερό αριθμό block, μπορείτε να τους γεμίσετε με μερικά μηδενικά από τα αριστερά για να εξασφαλίσετε ότι θα είναι πάντα λιγότερα από n.).

**Κρυπτογράφηση**

Το κρυπτογραφημένο μήνυμα, c, αποτελείται από τα ομοίως μεγέθους blocks μηνυμάτων, C, περίπου του ίδιου μήκους. Ο τύπος κρυπτογράφησης είναι απλά :

$$c = m^e \, mod n$$

**Αποκρυπτογράφηση**

Αφού ληφθεί ένα κρυπτογραφημένο μήνυμα $c$, για να διαβάσουμε το αρχικό μήνυμα προβαίνουμε στον ακόλουθο υπολογισμό:

$$m = c^d mod n \equiv (m^e)^d \, mod n \equiv m^{ed} \, mod n$$

Ξέρουμε πως $e.d \equiv 1 \pmod{p-1}$ και $e.d \equiv 1 \pmod{q-1}$, όποτε με το μικρό θεώρημα του Φερμάτ, έχουμε:

$$m^{ed} \equiv m^1 \equiv m \, mod p - 1$$

και

$$m^{ed} \equiv m^1 \equiv m \, mod q - 1$$

Οι αριθμοί $p$ και $q$ είναι πρώτοι μεταξύ τους, χρησιμοποιώντας λοιπόν το Κινέζικο Θεώρημα Υπολοίπων, έχουμε:

$$m^{ed} \equiv m \, mod n$$

### *1.8.1.1 Η ασφάλεια του RSA*

Η ασφάλεια του RSA εξαρτάται πλήρως από το πρόβλημα της δημιουργίας μεγάλων αριθμών. Τεχνικά, αυτό είναι ένα ψέμα. Υποτίθεται ότι η ασφάλεια του RSA εξαρτάται από το πρόβλημα δημιουργίας μεγάλων αριθμών. Δεν έχει αποδειχθεί ποτέ από μαθηματική άποψη ότι χρειάζεστε τον παράγοντα n για να υπολογίσετε το m από το c και το e. Είναι κατανοητό ότι ένας εξ ολοκλήρου διαφορετικός τρόπος για την κρυπτανάλυση του RSA μπορεί να ανακαλυφθεί . Εντούτοις, εάν αυτός ο νέος τρόπος επιτρέπει στην κρυπτανάλυση να μεγαλώνει το d, θα μπορούσε επίσης να χρησιμοποιηθεί ως νέος τρόπος παραγωγής μεγάλων αριθμών. Είναι επίσης δυνατό να επιτεθούμε στο RSA μαντεύοντας τα (p - 1) (q - 1). Αυτή η επίθεση δεν είναι όχι ευκολότερη από την παραγωγή του n.

Για τον ultra skeptical, μερικές παραλλαγές του RSA έχουν αποδειχθεί τόσο δύσκολες όσο η παραγωγή (factoring). Η ανάκτηση ακόμη και ορισμένων bits των πληροφοριών από ένα RSA-κρυπτογραφημένο κρυπτογράφημα είναι τόσο δύσκολη σαν να αποκρυπτογραφείς ολόκληρο μήνυμα. Η παραγωγή του n είναι ο προφανέστερος τρόπος της επίθεσης. Οποιοσδήποτε αντίπαλος θα μπορούσε να έχει το δημόσιο κλειδί, το e, και το συντελεστή, n. Για να βρει το κλειδί αποκρυπτογράφησης, d, πρέπει παράγει το n. Έτσι , ένας συντελεστής δεκαδικός- 129 ψηφίων - είναι η αιχμή της τεχνολογίας παραγωγής (factoring). Έτσι το n πρέπει να είναι μεγαλύτερο από αυτήν (key length).

Είναι βεβαίως πιθανό για ένα κρυπταναλυτή να δοκιμαστεί κάθε πιθανό d έως ότου να βρει το σωστό. Αυτή η επίθεση brute-force είναι λιγότερο αποδοτική από το να προσπαθήσουμε να παράγουμε (factor) το n. Από καιρό σε καιρό, οι άνθρωποι υποστηρίζουν ότι έχουν βρει τους εύκολους τρόπους να σπάσουν το RSA, αλλά καμία τέτοια αξίωση δεν έχει επαληθευτεί . Υπάρχει μια άλλη ανησυχία. Οι περισσότεροι κοινοί αλγόριθμοι για υπολογίζουν το p και το q με βάση πιθανοτήτων. Τι θα συμβεί όμως εάν το p ή το q είναι σύνθετα; Οι πιθανότητες τότε είναι παρά πολύ μικρές.

Αλλά ακόμα και αν συμβεί, οι πιθανότητες είναι ότι η κρυπτογράφηση και η αποκρυπτογράφηση δεν θα λειτουργήσουν καλά και θα παρατηρηθεί αμέσως. Υπάρχουν μερικοί αριθμοί, αποκαλούμενοι αριθμοί Carmichael, για τους οποίους ορισμένοι πιθανολογικοί αλγόριθμοι primality θα αποτύχουν να ανιχνεύσουν. Αυτοί είναι υπερβολικά σπάνιοι, αλλά είναι επισφαλείς.

### *1.8.2 Αλγόριθμος Digital Signature Algorithm (DSA)*

Ο αλγόριθμος DSA (Digital Signature Algorithm) προτάθηκε τον Αύγουστο του 1991 από το NIST (National Institute of Standards and Technology) της Αμερικής. Έχει προτυποποιηθεί ως FIPS 186 (Federal Information Processing Standard). Το πρότυπο αυτό έχει ονομαστεί DSS (Digital Signature Standard) και είναι ο πρώτος αλγόριθμος ψηφιακής υπογραφής που αναγνωρίστηκε παγκόσμια. Ο DSA αποτελεί μια παραλλαγή του αλγορίθμου ElGamal για ψηφιακές υπογραφές και σχεδιάστηκε αποκλειστικά για τη δημιουργία και επαλήθευση ψηφιακών υπογραφών και κατά συνέπεια και για τον έλεγχο της ακεραιότητας των δεδομένων. Η λογική του αλγορίθμου βασίζεται σε αυτήν της ασύμμετρης κρυπτογραφίας, αφού και σε αυτήν την περίπτωση κάθε οντότητα δημιουργεί ένα ζεύγος δημοσίου και ιδιωτικού κλειδιού. Τα βήματα που ακολουθούνται για την υλοποίηση του αλγορίθμου είναι τα παρακάτω:

1. Επιλέγεται ένας πρώτος αριθμός $q$ τέτοιος ώστε $2^{159} < q < 2^{160}$
2. Επιλέγεται ένας αριθμός $t$ τέτοιος ώστε $0 \le t \le 8$ και ένας πρώτος αριθμός $p$ τέτοιος ώστε $2^{511+64t} < p < 2^{512+64t}$ με την ιδιότητα ο $q$ να διαιρεί τον $(p-1)$
3. $g = h^{(p-1)/q} \bmod p$, όπου $h$ είναι ένας ακέραιος $1 < h < p-1$ έτσι ώστε $h^{(p-1)/q} \bmod p > 1$.
4. Έστω $x$ ένας τυχαίος ακέραιος έτσι ώστε $1 \le x \le q-1$
5. Υπολογίζεται το $y = g^x \bmod p$
6. Το δημόσιο κλειδί είναι το $(p,q,g,y)$. Το ιδιωτικό κλειδί είναι το $x$.

Έχοντας υπολογίσει τις παραπάνω παραμέτρους μπορούμε να δημιουργήσουμε μία ψηφιακή υπογραφή. Τα παρακάτω βήματα περιγράφουν τον τρόπο με τον οποίο μπορεί να υπογραφεί ψηφιακά, σύμφωνα με τον αλγόριθμο DSA, ένα μήνυμα $m$ τυχαίου μήκους:

1. Επιλέγεται ένας τυχαίος ακέραιος $k$, $0 < k < q$. Ο ακέραιος $k$ θα πρέπει να μείνει μυστικός.
2. Υπολογίζεται το $r = (g^k \bmod p) \bmod q$.
3. Υπολογίζεται το $k^{-1} \bmod q$.
4. Υπολογίζεται το $s = k^{-1}\{h(m) + xr\} \bmod q$. Η $h(m)$ είναι μια συνάρτηση κατακερματισμού (hash function). Πρόκειται για ένα αλφαριθμητικό μήκους 160 bits που προκύπτει ως έξοδος του αλγορίθμου SHA-1 ο οποίος περιγράφεται παρακάτω.
5. Η ψηφιακή υπογραφή για το μήνυμα $m$ είναι το ζεύγος $(r,s)$

Από τη στιγμή που ένας χρήστης Α ενός επικοινωνιακού συστήματος έχει υπογράψει ψηφιακά ένα μήνυμα θα πρέπει οι υπόλοιποι χρήστες του συστήματος να είναι σε θέση να επαληθεύσουν την υπογραφή του. Αυτό γίνεται με τη χρήση του δημοσίου κλειδιού του Α. Τα παρακάτω βήματα περιγράφουν τη διαδικασία της επαλήθευσης μιας ψηφιακής υπογραφής:

1. Το δημόσιο κλειδί $(p,q,g,y)$ του χρήστη Α είναι διαθέσιμο.
2. Επαληθεύεται ότι $0 < r < q$ και $0 < s < q$. Αν δεν ισχύουν τα παραπάνω η υπογραφή απορρίπτεται.
3. Υπολογίζεται $w = s^{-1} \bmod q$ και την $h(m)$.
4. Υπολογίζεται το $u_1 = w \cdot h(m) \bmod q$ και το $u_2 = rw \bmod q$.
5. Υπολογίζεται το $\upsilon = (g^{u_1} y^{u_2} \bmod p) \bmod q$.

6. Η υπογραφή είναι αποδεκτή μόνο όταν $\upsilon = r$ .

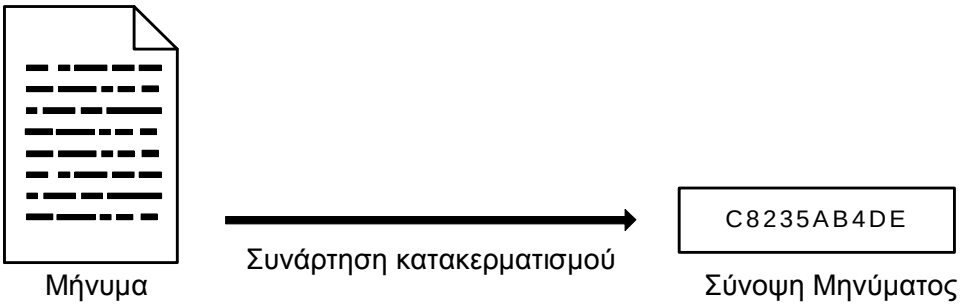
### *1.8.2.1 Ασφάλεια του DSA*

Η ασφάλεια του DSA βασίζεται στη δυσκολία του υπολογισμού διακριτών λογαρίθμων μέσα σε ένα πεπερασμένο σώμα. Έρευνες πάνω στον αλγόριθμο έχουν δείξει την ύπαρξη πρώτων αριθμών οι οποίοι θα μπορούσαν να οδηγήσουν στη δημιουργία κλειδιών ευάλωτων σε επιθέσεις. Όμως, αυτοί οι αριθμοί είναι ελάχιστοι και μπορούν εύκολα να αποφευχθούν σε μία σωστή διαδικασία δημιουργίας ζεύγους κλειδιών. Όπως φαίνεται και από τα βήματα του αλγορίθμου το μέγεθος του *q* πρέπει να είναι 160 bits ενώ το μέγεθος του *p* μπορεί να είναι οποιοδήποτε πολλαπλάσιο του 64 ανάμεσα στο 512 και το 1024. Ένας πρώτος αριθμός *p* μεγέθους 512 bit προστατεύει το σύστημα οριακά από μια ενδεχόμενη επίθεση. Από το 1996 προτείνεται το μέγεθος του *p* να είναι τουλάχιστον 768 bits. Το πρότυπο FIPS 186 δεν επιτρέπει πρώτους αριθμούς p που το μέγεθός τους ξεπερνά τα 1024 bits.

Ένα σημαντικό πλεονέκτημα του DSA είναι ότι, η εκθετοποίηση ως διαδικασία μπορεί να προηγείται της δημιουργίας της ψηφιακής υπογραφής, κάτι που δεν είναι εφικτό με τον RSA.

## 1.9 Συναρτήσεις Κατακερματισμού (Hash Functions)

Ο όρος *συνάρτηση κατακερματισμού* (hash function) υποδηλώνει ένα μετασχηματισμό *H* ο οποίος παίρνει ως είσοδο ένα μήνυμα *m* ανεξαρτήτου μήκους και δίνει ως έξοδο μία ακολουθία χαρακτήρων h, είναι δηλαδή $h = H(m)$. Η έξοδος *h* μιας συνάρτησης κατακερματισμού ονομάζεται *τιμή κατακερματισμού (hash value)* ή *σύνοψη μηνύματος (message digest)* και ανάλογα με τον αλγόριθμο κατακερματισμού που χρησιμοποιείται έχει και συγκεκριμένο μέγεθος, συνήθως πολύ μικρότερο από αυτό του αρχικού μηνύματος. Μπορούμε να φανταστούμε την σύνοψη μηνύματος ως το “ψηφιακό αποτύπωμα” (“digital fingerprint”) του εγγράφου.




ΕΙΚΟΝΑ 57:32 ΣΥΝΑΡΤΗΣΗ ΚΑΤΑΚΕΡΜΑΤΙΣΜΟΥ

Οι σημαντικότερες ιδιότητες των συναρτήσεων κατακερματισμού με μορφή $y = H(x)$ είναι:

- Η είσοδος *x* μπορεί να έχει οποιοδήποτε μήκος
- Η έξοδος *y* έχει περιορισμένο μήκος
- Δεδομένου του x και της συνάρτησης Η είναι εύκολος ο υπολογισμός του *H*(*x*)
- Η *H*(*x*) είναι μονόδρομη (one way function)
- Η *H*(*x*) είναι αμφιμονοσήμαντη (συνάρτηση ένα προς ένα)

Μια **μονόδρομη συνάρτηση** κατακερματισμού ονομάζεται η συνάρτηση που δεν μπορεί να αποκαλυφτεί η αντιστροφή της, δηλαδή το αρχικό μήνυμα δεν μπορεί να ανακτηθεί από τη σύνοψή του. Όταν επιπλέον η συνάρτηση είναι αμφιμονοσήμαντη, τότε είναι πολύ δύσκολο να βρεθούν δύο διαφορετικά μηνύματα με την ίδια σύνοψη. Στην περίπτωση που κάτι τέτοιο συμβεί τότε υπάρχει *σύγκρουση* (collision) .

Οι πιο γνωστοί αλγόριθμοι κατακερματισμού είναι οι MD5 με σύνοψη 128 bit, ο SHA-1 με σύνοψη 160 bits και ο RIPEMD-160**Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.** με σύνοψη 160 bits. Οι νέες εκδόσεις του αλγορίθμου SHA, SHA-256, SHA-384 και SHA-512

**Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.** δίνουν σύνοψη μηνύματος 256, 384 και 512 bits αντίστοιχα.

### *1.9.1Αλγόριθμος Κατακερματισμού Secure Hash Algorithm-1 (SHA-1)*

Ο ασφαλής αλγόριθμος κατακερματισμού *SHA-1* (*Secure Hash Algorithm-1*)**Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.** αποτελεί μια βελτιωμένη έκδοση του αρχικού αλγορίθμου κατακερματισμού SHA. Αυτός ο αλγόριθμος κατακερματισμού (hash algorithm) σχεδιάστηκε αποκλειστικά για χρήση σε συνδυασμό με τον DSA και συνεπώς δεν μπορεί να χρησιμοποιηθεί με τον RSA ή οποιοδήποτε άλλο αλγόριθμο δημοσίου κλειδιού για ψηφιακή υπογραφή. Οι σχεδιαστικές αρχές του SHA-1 είναι παρεμφερείς με αυτές των συναρτήσεων κατακερματισμού MD2, MD4, και κυρίως της συνάρτησης MD5.

Ο αλγόριθμος μπορεί να έχει ως είσοδο μηνύματα μήκους μικρότερου από $2^{64}$ bits. Η έξοδος του αλγορίθμου ονομάζεται σύνοψη μηνύματος (message digest ή hash value ή message fingerprint) και έχει μήκος 160 bit. Είναι πιο αργός από τον MD5 αλλά το μεγαλύτερο message digest που παράγει (ο MD5 παράγει message digest μήκους 128 bits) τον καθιστούν πιο ισχυρό σε προσπάθειες αντιστροφής του.

### *1.9.4 Ψηφιακά πιστοποιητικά*

Τα ψηφιακά πιστοποιητικά ταυτοποιούν τους χρήστες στον ψηφιακό κόσμο και διανέμονται έναντι τρίτου από εταιρίες γνωστές ως «Αρχές Πιστοποίησης». Ένα ψηφιακό πιστοποιητικό περιέχει τον αριθμό έκδοσής του, τον σειριακό αριθμό χρήστη, τον αλγόριθμο κρυπτογράφησης που χρησιμοποιήθηκε για τη δημιουργία της υπογραφής του, το όνομα της Αρχής Πιστοποίησης που το εκδίδει, την ημερομηνία λήξης του πιστοποιητικού, το όνομα χρήστη, το δημόσιο κλειδί κρυπτογράφησης και την ψηφιακή υπογραφή του χρήστη. Τα πιστοποιητικά αυτά είναι αρκετά σημαντικά και βοηθούν στην ασφάλεια, αφού οι administrators διάφορων συστημάτων μπορούν να ελέγχουν με διάφορους τρόπους από ποιες Αρχές πιστοποίησης τα πιστοποιητικά θα δέχονται από τους servers και ποια όχι. Μια αρκετά γνωστή εταιρία που δρα ως «Αρχή πιστοποίησης» είναι η VeriSign.(www.VeriSign.com ).

Για να αυξηθεί περισσότερο η ασφάλεια στο Διαδίκτυο και να αξιοποιηθούν οι προαναφερθείσες μέθοδοι, έχουν αναπτυχθεί ειδικά πρωτόκολλα ασφαλούς επικοινωνίας που μπορούν να χειρίζονται μόνο την κρυπτογράφηση και την αποκρυπτογράφηση της πληροφορίας. Ένα παράδειγμα είναι το πρωτόκολλο στρώματος ασφαλούς σωλήνωσης (Secure Socket Layer Protocol – SSL), για το οποίο μπορείτε να βρείτε περαιτέρω πληροφορίες στο παράρτημα σχετικά με την κρυπτογραφία . Το πρωτόκολλο αυτό λειτουργεί ως εργαλείο πιστοποίησης και για άλλα πρωτόκολλα Διαδικτυακών εφαρμογών όπως το HTTP, SMTP, TELNET, FTP κλπ.

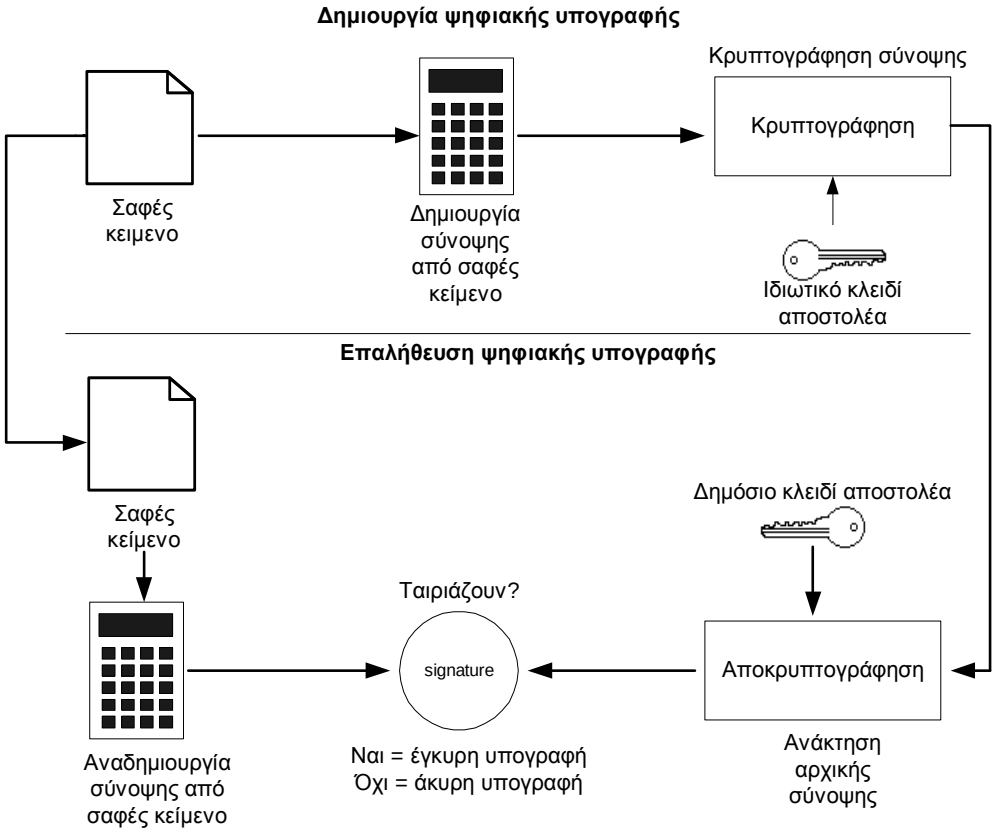
### *1.9.5 Ανταλλαγή κλειδιών (key exchange)*

Η κρυπτογραφία δημοσίου κλειδιού μπορεί να χρησιμοποιηθεί και για την ανταλλαγή κλειδιών μεταξύ δύο οντοτήτων. Αυτό σημαίνει ότι ένα πρωτόκολλο μπορεί να χρησιμοποιεί δημόσια κα ιδιωτικά κλειδιά έτσι ώστε, κατά τη λήξη του πρωτοκόλλου, οι δύο οντότητες να μοιράζονται ένα συμμετρικό κλειδί άγνωστο σε κάθε άλλη οντότητα.
Η ανταλλαγή κλειδιών μπορεί να πραγματοποιηθεί με δύο τρόπους:

- Κατά τη *μεταφορά κλειδιού (key transfer)* η μία οντότητα παράγει το συμμετρικό κλειδί και το στέλνει στην δεύτερη οντότητα. Η κρυπτογραφία δημοσίου κλειδιού μπορεί να χρησιμοποιηθεί για να προστατέψει το απόρρητο της συγκεκριμένης μεταφοράς.
- Κατά τη *συμφωνία κλειδιού (key agreement)* και οι δύο οντότητες συμβάλουν στη δημιουργία του συμμετρικού κλειδιού. Η κρυπτογραφία δημοσίου κλειδιού κάνει αυτή τη διαδικασία πολύ απλή σε σύγκριση με τη χρήση της συμμετρικής κρυπτογραφίας.

## 1.10 Ψηφιακές Υπογραφές (Digital Signatures)

Η *ψηφιακή υπογραφή* είναι για τον ηλεκτρονικό κόσμο ότι η χειρόγραφη υπογραφή για τον πραγματικό. Επιβεβαιώνει την ταυτότητα του υπογράφοντος αλλά και την ακεραιότητα των πληροφοριών που έχουν υπογραφεί. Επίσης η ψηφιακή υπογραφή μπορεί να θεωρηθεί πιο ασφαλής από την χειρόγραφή, αφού η πλαστογραφία στον ηλεκτρονικό κόσμο είναι υπολογιστικά αδύνατη. Η δημιουργία μιας ψηφιακής υπογραφής είναι δύσκολα επιτεύξιμη με την συμβατική, συμμετρική κρυπτογραφία. Γι' αυτό και η έννοια της ψηφιακής υπογραφής είναι άρρηκτα συνδεδεμένη με την έννοια της ασύμμετρης κρυπτογραφίας. Για να δημιουργηθεί λοιπόν, αλλά και για να επαληθευτεί μια ψηφιακή υπογραφή, χρειάζεται ένα ζεύγος κλειδιών, δημόσιο και ιδιωτικό του υπογράφοντος, και μια συνάρτηση κατακερματισμού.




ΕΙΚΟΝΑ 5833: ΔΗΜΙΟΥΡΓΙΑ ΚΑΙ ΕΠΑΛΗΘΕΥΣΗ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ

Όπως φαίνεται και στην εικόνα 58, αρχικά ο αποστολέας, και άρα ο υπογράφων του μηνύματος, δημιουργεί με χρήση μιας συνάρτησης κατακερματισμού μια σύνοψη του μηνύματος που θέλει να στείλει. Στη συνέχεια κρυπτογραφεί τη σύνοψη κάνοντας χρήση του ιδιωτικού του κλειδιού, που μόνο αυτός κατέχει. Το αποτέλεσμα της κρυπτογράφησης αυτής είναι η ψηφιακή υπογραφή του αποστολέα. Το αρχικό μήνυμα στέλνεται στον παραλήπτη μαζί με την ψηφιακή υπογραφή. Από την πλευρά του τώρα ο παραλήπτης παράγει επίσης μια σύνοψη του μηνύματος που έλαβε, κάνοντας χρήση της ίδιας συνάρτησης κατακερματισμού. Στη συνέχεια αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, που είναι ελευθέρα διαθέσιμο, την ψηφιακή υπογραφή και συγκρίνει τα αποτελέσματα με τη σύνοψη του μηνύματος που παρήγαγε. Αν ταιριάζουν, τότε η ψηφιακή υπογραφή έχει επαληθευτεί. Αν όχι τότε ή το περιεχόμενο του μηνύματος έχει αλλοιωθεί ή το δημόσιο κλειδί δεν ταιριάζει με το ιδιωτικό κλειδί του παραλήπτη, δηλαδή η ψηφιακή υπογραφή είναι ψεύτικη.

Η ψηφιακή υπογραφή είναι ένα εργαλείο που εξασφαλίζει την πιστοποίηση αυθεντικότητας του αποστολέα αλλά και την ακεραιότητα των δεδομένων που στέλνονται. Η πιστοποίηση αυθεντικότητας εξασφαλίζεται όμως με την προϋπόθεση ότι το ζεύγος δημόσιου-ιδιωτικού κλειδιού

που χρησιμοποιείται ανήκει πράγματι σε εκείνον που υποστηρίζει ότι είναι ο αποστολέας του μηνύματος.

Εκτός από την πιστοποίηση αυθεντικότητας και την εξασφάλιση της ακεραιότητας των δεδομένων που στέλνονται, στα προτερήματα της ψηφιακής υπογραφής θα πρέπει να προστεθεί και η δυνατότητα καθολικής επαλήθευσής της, αφού ο καθένας που έχει πρόσβαση στο δημόσιο κλειδί του αποστολέα μπορεί να την επαληθεύσει. Ένα ακόμη σημαντικό πλεονέκτημα είναι η ευκολία στη δημιουργία και την επαλήθευση της αφού και τα δύο επιτυγχάνονται με τη χρήση απλών και σχετικά εύκολων υπολογιστικών μηχανισμών.

Οι πιο ευρέως διαδεδομένοι αλγόριθμοι που χρησιμοποιούνται για τη δημιουργία και επαλήθευση των ψηφιακών υπογραφών είναι οι DSA και RSA.

## 1.11 Secure Socket Layer (SSL)

Σε ένα ανοιχτό περιβάλλον όπως το Διαδίκτυο, όπου εκτελούνται καθημερινά χιλιάδες συναλλαγές (ηλεκτρονικό εμπόριο, τραπεζικές πληρωμές κ.α.), το πιο σημαντικό είναι η προστασία των προσωπικών στοιχείων που μεταφέρονται(ονόματα, διευθύνσεις, αριθμούς πιστωτικών καρτών κ.α ). Για αυτό το λόγο δημιουργήθηκε από τη Netscape στις αρχές του 1990 το πρωτόκολλο SSL (Secure Socket Layer). Το SSL λειτουργεί ανάμεσα στο πρωτόκολλο TCP/IP και σε άλλα πρωτόκολλα υψηλότερου επιπέδου.

Στη σημερινή κοινωνία του Διαδικτύου, το SSL χρησιμοποιείται κυρίως για τη διασφάλιση της επικοινωνίας ανάμεσα σε ένα χρήστη του Διαδικτύου (πελάτης) και έναν εξυπηρετητή Ιστού. Για να το πετύχει αυτό το SSL διεκπεραιώνει τις παρακάτω διαδικασίες:

- Επιτρέπει σε έναν SSL εξυπηρετητή να πιστοποιήσει την αυθεντικότητα ενός SSL πελάτη.
- Επιτρέπει σε έναν SSL πελάτη να πιστοποιήσει την αυθεντικότητα ενός SSL εξυπηρετητή.
- Δημιουργεί ένα κρυπτογραφημένο κανάλι επικοινωνίας ανάμεσα στον SSL εξυπηρετητή και τον SSL πελάτη.

Για να πιστοποιήσει την αυθεντικότητα εξυπηρετητών και πελατών, το SSL χρησιμοποιεί μια πληθώρα κρυπτογραφικών αλγορίθμων. Οι αλγόριθμοι αυτοί μπορούν να χρησιμοποιηθούν για την έκδοση ψηφιακών πιστοποιητικών και τη δημιουργία ζεύγους κλειδιών. Ανάλογα με την πολιτική του οργανισμού και την έκδοση του SSL, οι πελάτες και οι εξυπηρετητές χρησιμοποιούν διαφορετικούς κρυπτογραφικούς αλγορίθμους. Οι κρυπτογραφικοί αυτοί αλγόριθμοι είναι:

- Key Exchange Algorithm (KEA)
- Data Encryption Standard (DES)
- Triple-DES
- Digital Signature Algorithm (DSA)
- Message Digest Algorithm (MD5)
- Secure Hash Algorithm (SHA-1)

Το πρότυπο SSL είναι πλέον ένα παγκοσμίως αποδεκτό πρωτόκολλο κρυπτογράφησης που χρησιμοποιείται στο Διαδίκτυο. Παρακάτω περιγράφονται κάποιοι από τους τομείς στους οποίους μπορεί να βρει εφαρμογή το πρωτόκολλο αυτό:

- Οργανισμοί οι οποίοι χρησιμοποιούν προγράμματα απομακρυσμένων τραπεζικών συναλλαγών.
- Σελίδες ηλεκτρονικού εμπορίου οι οποίες δέχονται on line πληρωμές από τους πελάτες τους.
- Μεγάλοι οργανισμοί έρευνας και ανάπτυξης για να διασφαλίσουν τα δεδομένα που ανταλλάσσουν.

**Επίλογος**

Στις μέρες μας η τεχνολογία αναπτύσσεται αλματωδώς, νέα τεχνολογικά προϊόντα εμφανίζονται καθημερινά . Οι λέξεις ηλεκτρονικά βιβλία, ηλεκτρονικοί αναγνώστες και προστασία πνευματικών δικαιωμάτων θα ακούγονται όλο ένα και περισσότερο όσο περνάει ο καιρός. Το παραδοσιακό βιβλίο έχει αρχίσει να διαδέχεται από τα ψηφιακά βιβλία. Εκδότες, πανεπιστήμια βιβλιοθήκες προσπαθούν να εκμεταλλευτούν αυτή τη νέα τεχνολογία.

Τα ηλεκτρονικά βιβλία σε συνδυασμό με την ανοδική αύξηση των πωλήσεων των ηλεκτρονικών αναγνωστών έχουν κερδίσει το ενδιαφέρον αρκετών εταιρών στο χώρο τις τεχνολογίας. Τα ψηφιακά βιβλία βοηθούν και θα βοηθήσουν αρκετά στην ευκολότερη ενημέρωση, εκμάθηση ακόμα και στην εύκολη και γρήγορη μεταφορά πολλών βιβλίων μαζί. Επιπλέον, οι ηλεκτρονικοί αναγνώστες το πιο πιθανόν θα έχουν την πορεία των κινητών τηλεφώνων όπου όλοι θα έχουν στην κατοχή και από ένα και θα αντικαταστήσει το κινητό τηλέφωνο με την πάροδο του χρόνου.

Όμως, με την ανάπτυξη των τεχνολογιών και την εξάπλωση του ίντερνετ δεν επέτρεψε την καθιέρωση των εμπορικών δομών που διέπουν τις καθημερινές μας συναλλαγές πριν την εξάπλωση του ηλεκτρονικού εμπορίου. Για το λόγο αυτό οι εταιρίες άρχισαν να εφαρμόζουν μέτρα προστασίας με το σκοπό να προστατέψουν τους εκδότες, τα έργα αλλά και τα οικονομικά τους συμφέροντα.

Στην παρούσα εργασία, πραγματοποιήθηκε εκτενής μελέτη πάνω στα πρότυπα των ηλεκτρονικών βιβλίων. Τα πρότυπα αυτά είναι πολλά, μιας και κάθε εταιρία στο χώρο προσπαθεί να δημιουργήσει και να προωθήσει το δικό της. Για το λόγο αυτό στο κεφάλαιο τρία και τέσσερα, παρουσιάστηκαν αναλυτικά το κάθε ένα πρότυπο ξεχωριστά με επεξηγήσεις πάνω στον τρόπο λειτουργίας. Επίσης, στο κεφάλαιο τέσσερα έγινε μία σύγκριση όλων των προτύπων που είχαν προαναφερθεί με την βοήθεια συγκριτικών πινάκων και σχεδιαγραμμάτων.

Στην συνέχεια παρουσιάστηκαν οι πιο γνώστες εταιρίας στο χώρο κατασκευής και πώλησης συσκευών ανάγνωσης ηλεκτρονικών βιβλίων. Αναλύθηκαν και συγκρίθηκαν λεπτομερώς τα τελευταία μοντέλα της κάθε εταιρίας και για να γίνει και ευκολότερη η περιγραφή τους προστέθηκε και αναλυτικός συγκριτικός πίνακας μεταξύ των συσκευών ώστε να υπάρχει μία πιο συγκεκριμένη άποψη ανάμεσα στους ηλεκτρονικούς αναγνώστες.

Ένα σημαντικό κομμάτι της εργασίας ήταν η παρουσίαση γενικά του ορισμού προστασία πνευματικών δικαιωμάτων αλλά και οι αναλύσει των πιο διαδεδομένων συστημάτων προστασίας ψηφιακών έργων. Επίσης, έγινε αναφορά και στα creative commons, ως μία εναλλακτική λύση πάνω στα πνευματικά δικαιώματα. Όλες οι αναφορές πλαισιώθηκαν από χαρακτηριστικά παραδείγματα για να γίνουν κατανοητές και στον μη μυημένο χρήστη.

Τέλος, ως παράρτημα παρουσιάστηκε η τεχνολογία της κρυπτογραφίας, ένα από τα συστήματα προστασίας των δικαιωμάτων. Στο παράρτημα έγινε η προσπάθεια να αναφερθούν σχεδόν όλες οι τεχνολογίες και συστήματα κρυπτογραφίας, όπου και με την βοήθεια παραδειγμάτων και εικόνων να γίνουν αρκετά κατανοητά.

**Βιβλιογραφία**


1. Paul Mercieca Lecturer – Information Management And Digital Publishing RMIT University, "*E-book acceptance: what will make users read on screen? "*, 2003, διαθέσιμο εδώ
2. Blair A. Smith JOHN LATHAM, Ph.D., Faculty Mentor and Chair JOHN DENIGRIS, Ph.D., Committee Member RICHARD SCHUTTLER, Ph.D., Committee Member Kurt Linberg, Ph.D., Dean, School of Business & Technology, Quantitative analysis of the impact of e-book format on student acceptance, usage and satisfaction, "A Dissertation Presented in Partial Fulfillment Of the Requirements for the Degree Doctor of Philosophy", 2008
3. Kyong-Ho Lee *, Nicholas Guttenberg, Victor McCrary, *Standardization aspects of eBook content formats*", 2002
4. Peggy Johnson University of Minnesota, "*Library Resources &Technical Services*" ISSN 0024-2527 October 2004 Volume 48, No. 4 http://www.lib.umn.edu/.../peggy-johnson
5. Αλέξανδρος Καπανιάρης, Γιολα Βαλάτσου, "Παρουσίαση της δράσης e-book: διαβάζω ψηφιακά για την εισαγωγή ηλεκτρονικών αναγνωστών σε σχολεία του Ν. Μαγνησίας στο πλαίσιο του προγράμματος Ψηφιακής Μαγνησίας".
6. Παιδαγωγικό ινστιτούτο διακομματική επιτροπή για τη μορφωτική αυτοτέλεια του λυκείου και τον διάλογο για την παιδεία. "Πρόταση για τον σχεδιασμό και την εισαγωγή του «ηλεκτρονικού βιβλίου» στην εκπαίδευση", 2009
7. Heather MacFadyen, The Reader's Devices: The Affordances of Ebook Readers" Volume 7 – Spring 2011, διαθέσιμο στο djim.management.dal.ca
8. Terence Cavanaugh, *TEACHING Exceptional Children*", Vol. 35, No. 2,.σελίδες 56-61. Copyright 2002 CEC.
9. E-Text Subcommittee Membe rs, Frank Bulk (chair); ASC members Lois Jaeck Dave Bocking, Christine Soteros, Daniel McCullough (USSU); Library David Fox; Bookstore Mark Jagoe; Additional information from Shari Furniss (EMAP) and Angie Gerrard (Library), Towards the Digital University: "A *brief introduction to E-Texts and Open Access*".
10. Lisa Mary Moore, At your leisure: "*Assessing ebook reader functionality and interactivity*" Project report submitted in partial fulfilment of the requirements for the degree of Master of Science (Human-Computer Interaction with Ergonomics) in the Faculty of Life Sciences, University College London, 2009. Διαθέσιμο στο www.uclic.ucl.ac.uk/distinction-projects/2009-Moore.pdf
11. Wilson, R. (2003). "*Ebook Readers in Higher Education. Educational Technology & Society*", 6 (4), 8-17, Διαθέσιμο στο http://ifets.ieee.org/periodical/6_4/3.pdf
12. Geir Ugletveit, Jakub Norek, Andrea Gasparini, UNIVERSITY OF OSLO Department of informatics "*Ebook reader*" inf4260
13. Eberhard Becker Willms Buhse Dirk G¨unnewig Niels Rump (Eds.) *Digital Rights Management Technological, Economic, Legal and Political Aspects*" ISBN 3-540-40465-1 Springer-Verlag Berlin Heidelberg NewYork
14. Yooki Park and Suzanne Scotchmer, "*Digital Rights Management and the Pricing of Digital Products*", July 2005
15. W. Zeng, H. Yu, and C.-Y. Lin, "*Multimedia security technologies for digital rights management*" , Academic Press, 2006
16. Καπαρού Μαρία, "*Αξιολόγηση της υφιστάμενης κατάστασης και υλοποίηση συστήματος διαχείρισης ψηφιακών δικαιωμάτων(DRMS), με ένα σύστημα διαχείρισης ανοιχτού κώδικα*", Διπλωματική εργασία, Ιούλιος 2008
17. Federal Information Processing Standards Publication 46-3, "*Data Encryption Standard*", U.S Department of Commerce/National Institute of Standards and Technology, 1999. http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
18. Federal Information Processing Standards Publication 186-2, "*Digital Signature Standard*." U.S Department of Commerce/National Institute of Standards and Technology, 2000
19. Βασίλης Κάτος, Γιώργος Στεφανίδης, "*Η Κρυπτογραφία*" Φεβρουάριος 2003 Διαθέσιμο στο http://utopia.duth.gr/~vkatos/documents/the_book/

20. Βασίλειος Ζορκάδης Θεματική Ενότητα ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ Τόμος Γ' "*Κρυπτογραφία*" 2002
21. Δημήτριος Π. Μεϊδάνη, "*Τα Δικαιώματα Πνευματικής Ιδιοκτησίας στην Ψηφιακή Εποχή: Ζητήματα Προστασίας και Διαχείρισης. Ένα Πρότυπο Σύστημα Ψηφιακής Διαχείρισης των Πνευματικών Δικαιωμάτων*", Διπλωματική Εργασία στα Πλαίσια του Μεταπτυχιακού Διπλώματος Ειδίκευσης: Επιστήμη, Δεκέμβριος 2006
22. Άννα Φράγκου, "*ΠΝΕΥΜΑΤΙΚΗ ΙΔΙΟΚΤΗΣΙΑ ΚΑΙ ΣΥΓΓΕΝΙΚΑ ΔΙΚΑΙΩΜΑΤΑ ΣΤΗΝ ΕΛΛΑΔΑ*", Μάιος 2001
23. Μουμούζιας Εμμανουήλ, "*Η πνευματική ιδιοκτησία στον Ψηφιακό χώρο*", Μάρτιος 2009
24. Adobe Systems Incorporated, "*EPUB INDUSTRY-STANDARD FILE FORMAT FOR DIGITAL REFLOWABLE PUBLICATIONS*", 2008 Διαθέσιμο στο http://www.adobe.com/content/dam/Adobe/en/devnet/digitalpublishing/pdfs/EPUB_datasheet.pdf
25. S THOLKAPPIAN D CHANDRAN, "*ROLE OF E-BOOKS IN ACADEMIC LIBRARIES : TOWARDS VIRTUAL LIBRARY*", 5th International CALIBER -2007, Panjab University, Chandigarh, 08-10 February, 2007, Διαθέσιμο στο http://shodhganga.inflibnet.ac.in/dxml/bitstream/handle/1944/1441/663-677.pdf?sequence=1
26. Μάγδα Βασιλείου, " *Επισκόπηση της αγοράς των ηλεκτρονικών βιβλίων: εκδότες και διαθέτες*" Διαθέσιμο στο http://eprints.rclis.org/bitstream/10760/14781/1/5A.1.pdf
27. Αθανάσιου Ν. Σκόδρα, ΕΛΛΗΝΙΚΟ ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ, "*Πολιτισμός, Ψηφιοποίηση & Πνευματικά Δικαιώματα*".2004. Διαθέσιμο στο http://www.infosoc.gr/meletes/
28. http://students.ceid.upatras.gr/~mprokala/techarticles/cryptography/AES/aes.htm
29. http://gmoutzou.blogspot.com/2008/11/blog-post_27.html
30. http://www.wikipedia.org/
31. http://wiki.mobileread.com/wiki/Main_Page
32. http://edutechwiki.unige.ch/en/Main_Page
33. http://elektronikosanagnostis.blogspot.com/
34. http://www.the-ebook-reader.com/
35. http://www.creativecommons.gr/
36. http://creativecommons.org/