ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΡΗΤΗΣ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΝΙΚΗΣ ΠΑΡΑΡΤΗΜΑ ΧΑΝΙΑ

ΣΧΕΔΙΑΣΙΑΣΜΟΣ ΚΑΙ ΥΛΟΠΟΙΗΣΗ ΣΥΜΜΕΤΡΙΚΟΥ ΚΡΥΠΤΑΛΓΟΡΙΘΜΟΥ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

Κωνσταντίνου Δ. Φραγκιαδάκη

Επιβλέπων : Αντωνιδάκης Μανώλης
Καθηγητής ΤΕΙ

Χανιά, Μάρτιος 2006

Αυτή η σελίδα είναι σκόπιμα αφημένη λευκή.

Πρόλογος

Η παρούσα πτυχιακής εργασία εκπονήθηκε κατά τη διάρκεια του εαρινού εξαμήνου του ακαδημαϊκού έτους 2005 από τον Φραγκιαδάκη Κων/νο. Το μεγαλύτερο μέρος της ανάπτυξης έγινε στο Εργαστήριο Μικροϋπολογιστών του τμήματος Ηλεκτρονικής στο ΤΕΙ Χανίων.

Ευχαριστώ τον υπεύθυνο για την εργασία καθηγητή κ. Αντωνιδάκη Μανώλη τόσο για το ενδιαφέρον που έδειξε όσο και για τις παρατηρήσεις και προτάσεις προς βελτίωση της εργασίας.

Ευχαριστώ, τέλος, την οικογένεια μου, που όλο αυτό το διάστημα στήριξε την προσπάθειά μου, σε όλες τις φάσεις της ανάπτυξης και υλοποίησης του έργου.

Αύγουστος 2005

Φραγκιαδάκης Κων/νος

Περίληψη

Ο σκοπός της διπλωματικής εργασίας είναι η μελέτη και η ανάπτυξη ενός καινούργιου αλγορίθμου κρυπτογράφησης συμμετρικού κλειδιού (Block cipher). Ο αλγόριθμός δημιουργήθηκε με προσανατολισμό την βελτιστοποίηση της ασφάλειας από την πλευρά των μαθηματικών ιδιοτήτων (αλγεβρικές δομές) όσο και από την πλευρά της συστημικής-διαδικαστικής ανάλυσης. Μελετήθηκαν μέθοδοι διάσπασης (Διαφορική και γραμμική) καθώς επίσης και μέθοδοι στατιστικών αναλύσεων για την αξιολόγηση ιδιοτήτων. Κατ' επέκταση, στόχος της εργασίας είναι η παρουσίαση του τρόπου δημιουργίας ενός συμμετρικού αλγορίθμου .Για την κατασκευή του αλγορίθμου μελετήθηκαν τα αντιπροσωπευτικά σχέδια αλγορίθμων όπως Blowfish, Cast-128, RC5, IDEA, FOX, DES για τις μαθηματικές ιδιότητες όσο και για την υπολογιστική ασφάλεια που προσφέρουν. Δημιουργήθηκε 1 Μοντέλο για την μελέτη και την ανάλυση του αλγορίθμου (DES). Το πρόγραμμα που χρησιμοποιήθηκε για την εξομοίωση των μοντέλων είναι το μαθηματικό εργαλείο mat lab.

Λέξεις κλειδιά: Δίκτυα Αντικατάστασης-Μετάθεσης (ΔΑΜ) , Στατιστικοί έλεγχοι, Γραμμική και διαφορική κρυπτανάλυση , Κρυπτογράφηση γινομένου, Φαινόμενο χιονοστιβάδας, Φαινόμενο ανεξαρτησίας Bit, Κριτήριο Αυστηρής Χιονοστιβάδας, Κουτιά αντικατάστασης , Κουτιά μετάθεσης, Ανάμειξη λειτουργιών από διαφορετικές αλγεβρικές ομάδες,

Abstract

The objective of this diploma thesis is the Design and the implementation of new encryption symmetric algorithm (Block cipher). The algorithm was created with orientation "optimization of security" from the side of mathematic attributes (algebraic structures) as from the side of systemic-procedural analysis. Were studied methods of attack (Differential and linear cryptanalysis) and methods of statistical analyses for the evaluation of attributes. At extension, objective of work is the presentation of way of creation of symmetric encryption algorithms. For the manufacture of algorithm were studied the representative drawings of algorithms as Blowfish, Cast-128, RC5, IDEA, FOX, DES for the mathematic attributes and for the calculating security that they offer. Were created 1 Model for the study and the analysis of algorithm (DES,).The program that was used for the simulation of models is the mathematic tool mat lab.

Words keys: Substitution-Permutation Networks (SPN), Statistical Tests, Linear and Differential cryptanalysis, Product ciphers, Avalanche effect, Bit Independence Criterion, Strict avalanche Criterion, Substitution Box(S-box), Permutation Box, Mix operation from different algebraic groups.

Πίνακας Περιεχομένων

1

Εισαγωγή

Η λέξη κρυπτολογία αποτελείται από την ελληνική λέξη κρύπτος – κρυφός και την λέξη λόγος. Είναι ο τομέας που ασχολείται με την μελέτη της ασφαλής επικοινωνίας. Ο κύριος στόχος είναι να παρέχει μηχανισμούς για 2 ή περισσότερα μέλη να επικοινωνήσουν χωρίς κάποιος άλλος να είναι ικανός να διαβάζει την πληροφορία εκτός από τα μέλη.

Η κρυπτολογία χωρίζεται σε 2 επιμέρους ενότητες:

- Κρυπτογραφία
- Κρυπταναλυση.

Η κρυπτογραφία είναι η επιστήμη που ασχολείται με τους μαθηματικούς μετασχηματισμούς για την εξασφάλιση της ασφάλειας της πληροφορίας..
Η κρυπτανάλυση είναι η επιστήμη που ασχολείται με την ανάλυση και την διάσπαση των κρυπτοσυστημάτων.

Ιστορικά η κρυπτογραφία χρησιμοποιήθηκε για την κρυπτογράφηση μηνυμάτων δηλαδή μετατροπή της πληροφορίας από μια κανονική κατανοητή μορφή σε ένα ακατάληπτο σχήμα που χωρίς την γνώση του κρυφού μετασχηματισμού το αποτέλεσμα ήταν ακατανόητο. Κύριο χαρακτηριστικό των παλαιότερων μορφών κρυπτογράφησης ήταν το ενδιαφέρων κυρίως για τα σχέδια-μοτίβα μέσα στην γλώσσα. Στις νεότερες μορφές , η έμφαση έχει

μεταφερθεί, η κρυπτογραφία κάνει εκτενής χρήση από αρκετά πεδία των μαθηματικών , όπως διακριτά μαθηματικά, θεωρία αριθμών, θεωρία πληροφορίας, υπολογιστική πολυπλοκότητα, στατιστική και συνδυαστική ανάλυση.

Η κρυπτογραφία παρέχει 4 βασικές λειτουργίες (αντικειμενικοί σκοποί):

Εμπιστευτικότητα: Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.

Ακεραιότητα: Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.

Μη απάρνηση: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.

Πιστοποίηση: Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητες τους καθώς και την αρχή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι η ταυτότητες τους δεν είναι πλαστές

ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

Ο αντικειμενικός στόχος της κρυπτογραφίας είναι να δώσει την δυνατότητα σε 2 πρόσωπα Έστω τον Κώστα και την Βασιλική να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε ένας αντίπαλος να μην μπορεί να παρέβλειθει ή να καταλάβει το περιεχόμενο των μηνυμάτων.

Ένα κρυπτοσύστημα(σύνολο διαδικασιών κρυπτογράφησης-αποκρυπτογράφησης) αποτελείται από 5 ζευγάρια(P,C,k,E,D)

- Το P είναι ο χώρος όλων των δυνατών μηνυμάτων ή αλλιώς ανοικτών κείμενων

- Το C είναι ο χώρος όλων τον δυνατών κρυπτογραφημένων μηνυμάτων ή αλλιώς κρυπτοκειμένων
- Το k είναι ο χώρος όλων τον δυνατών κλειδιών ή αλλιώς κλειδοχώρος
- Η E είναι ο κρυπτογραφικός μετασχηματισμός ή κρυπτογραφική συνάρτηση
- Η D είναι η αντίστροφη συνάρτηση ή μετασχηματισμός αποκρυπτογράφησης

Η συνάρτηση κρυπτογράφησης E δέχεται δύο παραμέτρους , μέσα από τον χώρο P
και τον χώρο k και παράγει μία ακολουθία που ανήκει στον χώρο C

$$E_k(P) = C \qquad (1.1)$$

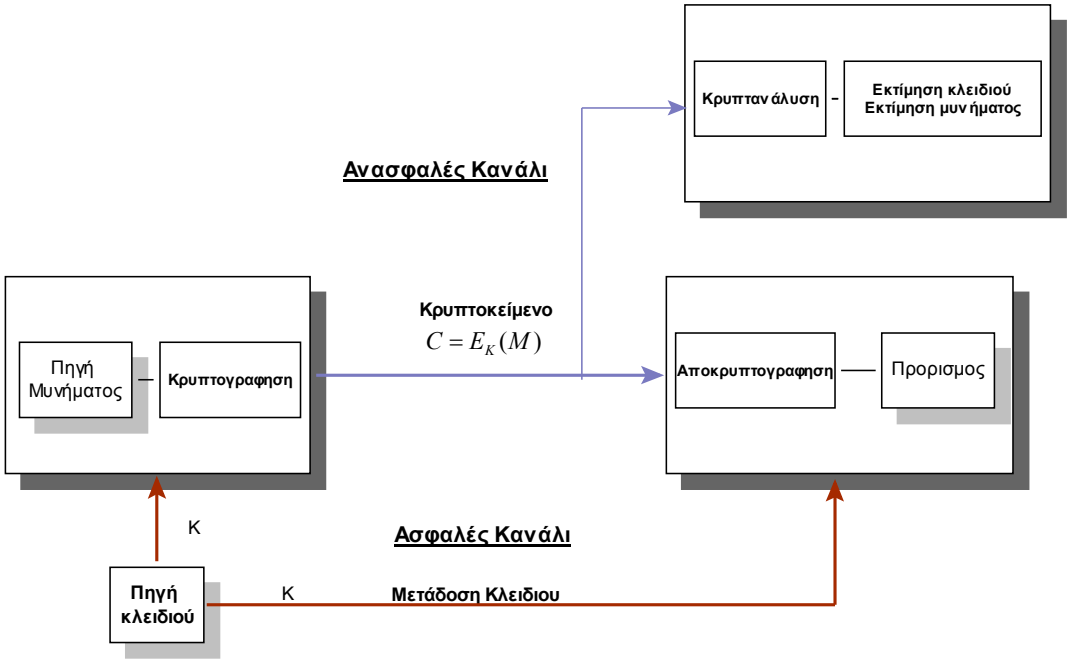
Η συνάρτηση αποκρυπτογράφησης D δέχεται 2 παραμέτρους , τον χώρο C και τον χώρο k και παράγει μια ακολουθία που ανήκει στον χώρο P

$$D_k(C) = P \qquad (1.2)$$

Το Σύστημα του Σχ1.1 λειτουργεί με τον ακόλουθο τρόπο :

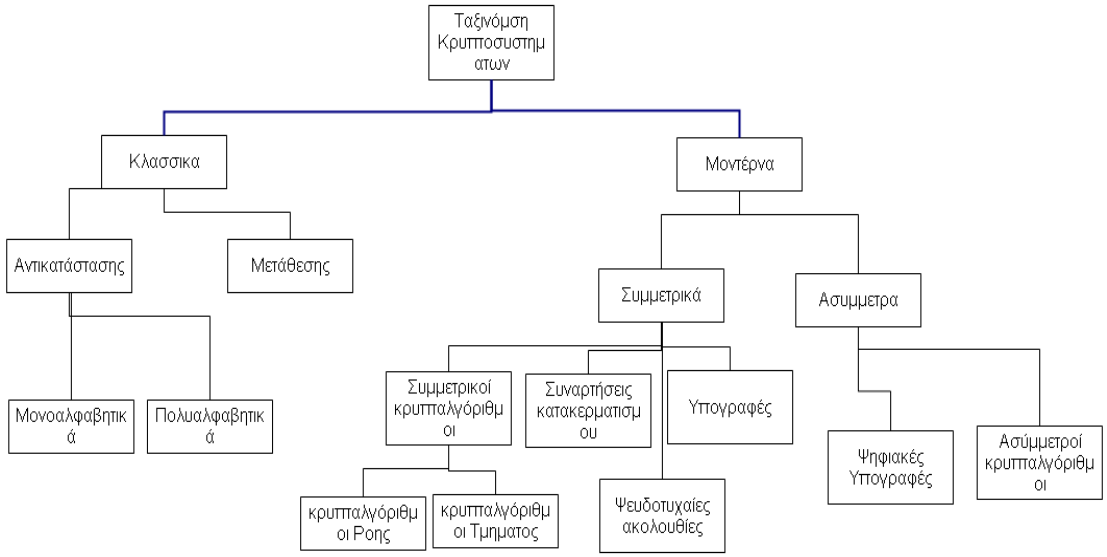
1 ο αποστολέας επιλέγει ένα κλειδί $K = [k_1, k_2, k_3 ... k_n]$ μήκους n όπου $n \geq 1$, από τον χώρο κλειδιών με τυχαίο τρόπο όπου τα n στοιχεία του K είναι στοιχεία από ένα πεπερασμένο αλφάβητο .
2 Αποστέλλει την ακολουθία στον παραλήπτη μέσο από ασφαλές κανάλι
3 Η πηγή δημιουργεί ένα μήνυμα από τον χώρο μηνυμάτων $M \in P$ $M = [m_1, m_2, m_3 ... m_i]$ όπου $i \geq 1$
4 Η συνάρτηση κρυπτογράφησης παίρνει τις δυο εισόδους και παράγει μια κρυπτοακολουθία συμβόλων $C = [c_1, c_2, c_3 ... c_j]$ όπου $j \geq 1$ οπού η ακολουθία αυτή αποστέλλεται διαμέσου ενός μη ασφαλούς καναλιού.
5 Η συνάρτηση αποκρυπτογράφησης παίρνει ως όρισμα της 2 τιμές και παράγει την ισοδύναμη ακολουθία μηνύματος $M = [m_1, m_2, m_3 ... m_i]$

Ο αντίπαλος παρακολουθεί την επικοινωνία ενημερώνεται για την κρυπτοακολουθία αλλά δεν έχει γνώση για το μήνυμα και την κλείδα που χρησιμοποιήθηκε .Αν ο αντίπαλος επιλέξει να παρακολουθεί όλα τα μηνύματα θα προσανατολιστεί στην εξεύρεση του κλειδιού .Αν ο αντίπαλος ενδιαφέρεται μόνο για το υπάρχων μήνυμα θα παράγει μια εκτίμηση για την πληροφορία του μηνύματος.



Σχήμα 1.1 Μοντέλο Τυπικού Κρυποσυστήματος

Είδη Κρυπτοσυστημάτων



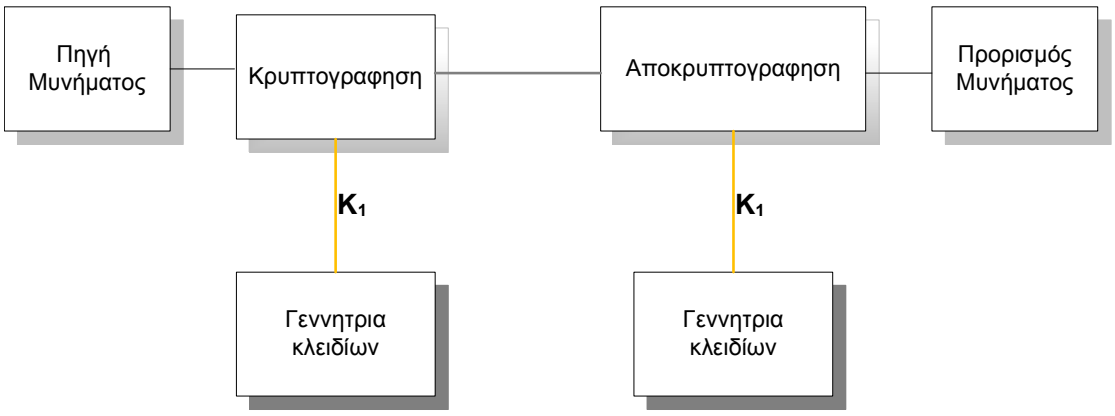
Σχήμα 1.2 Χάρτης Ταξινόμησης Κρυπτοσυστημάτων

Τα κρυπτοσυστήματα χωρίζονται σε 2 μεγάλες κατηγορίες τα κλασσικά και τα μοντέρνα. Στα μοντέρνα κρυπτοσυστήματα διακρίνονται δύο κατηγορίες (Συμμετρικά, Ασύμμετρα).

Συμμετρικά κρυπτοσυστήματα

Συμμετρικό κρυπτοσύστημα είναι το σύστημα εκείνο το οποίο χρησιμοποιεί κατά την διαδικασία της κρυπτογράφησης αποκρυπτογράφησης ένα κοινό κλειδί Σχ 1.3.Η ασφάλεια αυτών των αλγορίθμων βασίζεται στην μυστικότητα του κλειδιού

Συμμετρικό Μοντέλο



Σχήμα 1.3 Συμμετρικό κρυπτοσύστημα

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 καθίστα δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων.

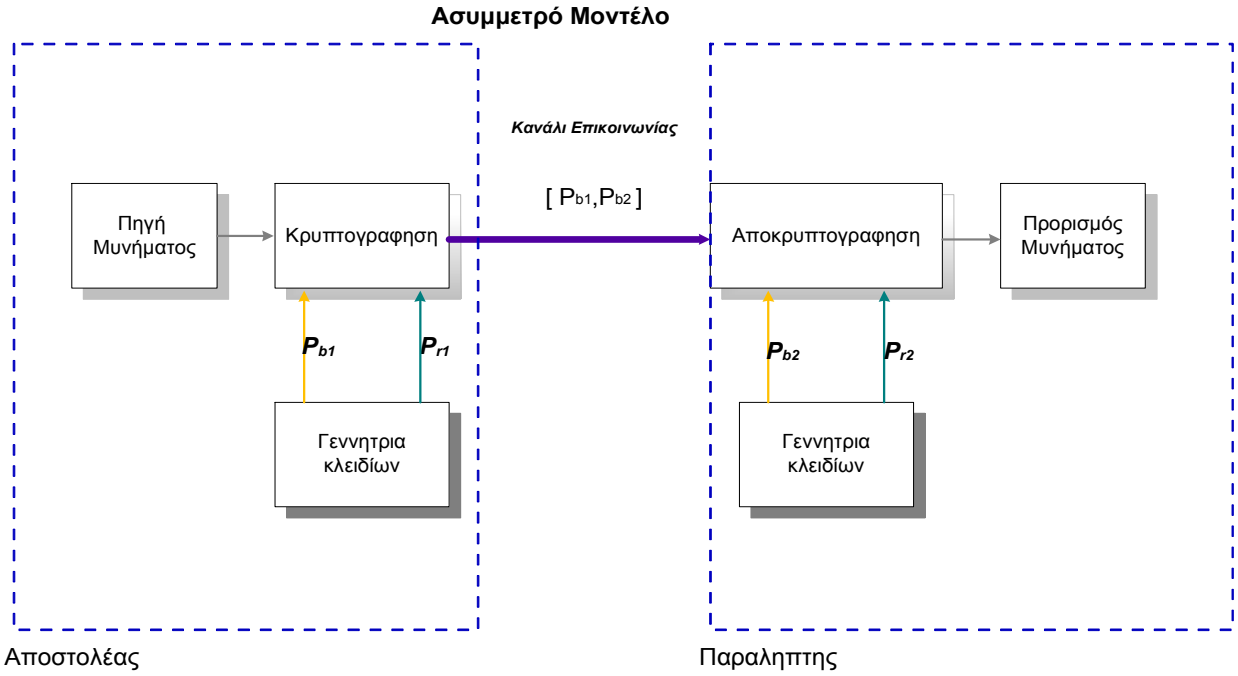
Ασύμμετρα κρυπτοσυστήματα

Το ασύμμετρο κρυπτοσύστημα ή κρυπτοσύστημα δημοσίου κλειδιού δημιουργήθηκε από 3 φοιτητές στο πανεπιστήμιο MIT .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 τα αποκρυπτογράφηση μόνο το άλλο (αχ 1.4) .

Τα στάδια της επικοινωνίας είναι τα ακόλουθα:

1. Η γεννήτρια κλειδιών του Κώστα παράγει 2 ζεύγη κλειδιών, P_{r2} P_{b1}, P_{r1}

2. Η γεννήτρια κλειδιών της Βασιλικής παράγει 2 ζεύγη κλειδιών P_{b2}, P_{r2}
3. Η Βασιλική και ο Κώστας ανταλλάσσουν τα δημόσια ζεύγη P_{b2}, P_{b1}
4. Ο Κώστας δημιουργεί ένα μήνυμα $M = [m_1, m_2, m_3 ... m_i]$ όπου τα σύμβολα m ανήκουν στον χώρο των μηνυμάτων.
5. Κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί της Βασιλικής P_{b2} η παραγόμενη κρυπτοσυμβολοσειρά $C = [c_1, c_2, c_3 ... c_j]$ αποστέλλεται
6. Η Βασιλική λαμβάνει την κρυπτοσυμβολοσειρά και στην συνέχεια με το ιδιωτικό της κλειδί P_{r2} την αποκρυπτογραφεί και η έξοδος που παράγεται είναι το μήνυμα $M = [m_1, m_2, m_3 ... m_i]$.



Σχήμα 1.4 Κρυπτοσύστημα δημοσίου κλειδιού

Είδη Επιθέσεων

Κρυπταναλυτικές επιθέσεις σε αλγορίθμους

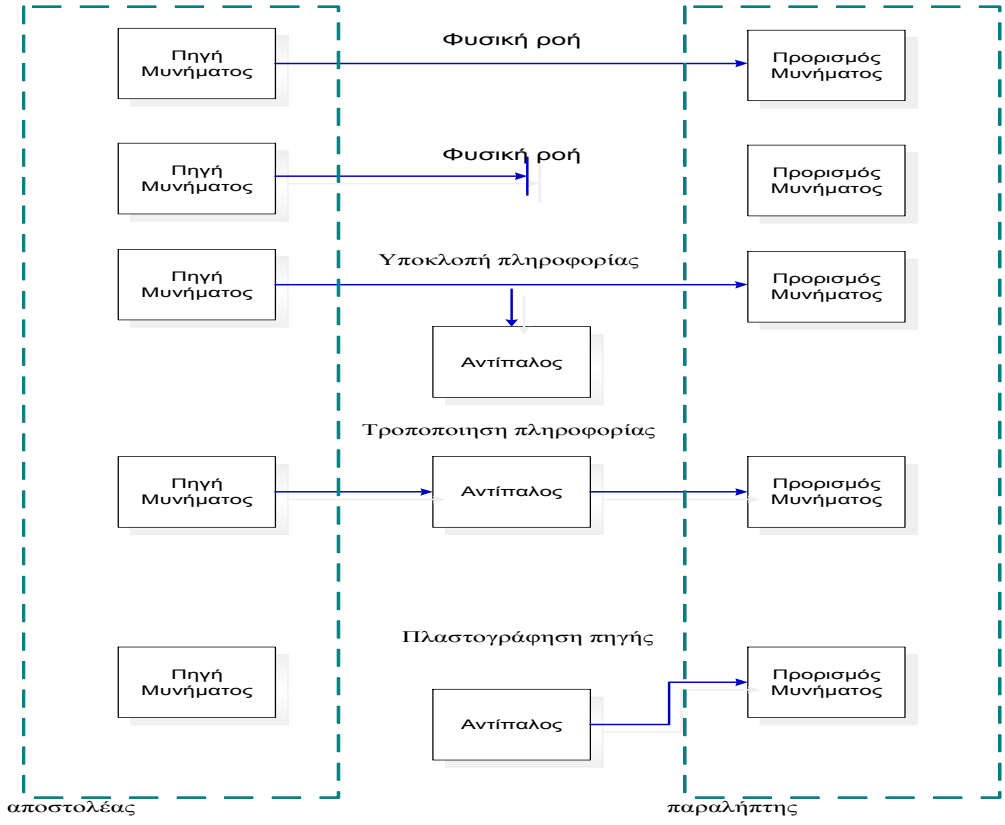
Υπάρχουν 6 βασικές κρυπταναλυτικές επιθέσεις κατηγοριοποιημένες ανάλογα με την ικανότητα του αντιπάλου (πόρους(Υπολογιστική Ισχύ) και το επίπεδο πρόσβασης που έχει

1. Επίθεση βασισμένη στο κρυπτοκείμενο : Ο κρύπταναλυτής έχει στην διάθεση του N κρυπτομυνήματα δεδομένου τής γνώσης του αλγορίθμου. Σκοπός είναι να ανακαλύψει τα μηνύματα που περικλείουν τα κρυπτοκείμενα ή να εξάγει το κλειδί που χρησιμοποιήθηκε.
2. Επίθεση βασισμένη στην γνώση μυνημάτων,κρυπτοκειμένων : Ο κρυπταναλυτής μερικά ζευγάρια (μνημάτων, κρυπτοκειμένων).Ο στόχος είναι η εξαγωγή κλειδιού ή ένα αλγόριθμό για την αποκρυπτογράφηση νέων μνημάτων (προσσεγιστικός αλγόριθμος) με το ίδιο κλειδί.
3. Επίθεση βασισμένη στην επιλογή μνημάτων : Ο κρυπταναλυτής έχει καταφέρει να αποκτήσει πρόσβαση στη επιλογή του μνήματος που θα κρυπτογραφηθεί. Στόχος είναι η εξαγωγή του κλειδιού ή ενός προσσεγιστικού αλγορίθμου.
4. Προσαρμόσιμη επίθεση βασισμένη στην επιλογή μνημάτων : Ο κρυπταναλυτής μπορεί να επιλέξει όχι μόνο μία συστάδα μνημάτων αλλά μπορεί να επιλέξει πιο επόμενο μήνυμα θα κρυπτογραφηθεί(Κατάλληλη επιλογή ζευγαριών προσδίδει περισσότερη πιθανότητα για την τιμή του κλειδιού). Στόχος είναι η εξαγωγή του κλειδιού ή ενός προσσεγιστικού αλγορίθμου.
5. Επίθεση βασισμένη στην επιλογή κρυπτοκειμένων: Ο κρυπταναλυτής μπορεί να επιλέξει κρυπτοκείμενα για αποκρυπτογράφηση(μελετάει πως συμπεριφέρεται ο αλγόριθμος στην αποκρυπτογράφηση) και έχει πρόσβαση στα αποκρυπτογραφημένα κείμενα.
6. Προσαρμόσιμη επίθεση βασισμένη στην επιλογή μνημάτων - κλειδιών: Ο κρυπταναλυτής επιλέγει μια σχέση μεταξύ του άγνωστου κλειδιού και του δικό του κλειδιού και βάση των συμπερασμάτων που βγάζει από την ανάλυση (Είσοδος/έξοδος) στο σύστημά στόχου και στο δικό του αντίγραφο (κρυπταλγόριθμος) προσσεγκίζει μετά από κάποιες δοκιμές το σωστό κλειδί.

Επιθέσεις στο κανάλι επικοινωνίας

Υπάρχουν 4 βασικές απειλές στο κανάλι επικοινωνίας κατηγοριοποιημένες με κριτήριο την ενεργή ή παθητική συμπεριφορά του αντιπάλου.

1. Διακοπή γραμμής : Ο αντίπαλος έχει διακόψει την ροή της πληροφορίας από τον αποστολέα στον παραλήπτη(ενεργή συμπεριφορά)
2. Υποκλοπή πληροφορίας από το κανάλι : Ο αντίπαλος αντιγράφει τις πληροφορίες που διαβιβάζονται στο κανάλι επικοινωνίας (παθητική συμπεριφορά – μη ανιχνεύσιμη) .
3. Τροποποίηση πληροφορίας στο κανάλι : Ο αντίπαλος τροποποιεί τις πληροφορίες που διαβιβάζονται στο κανάλι με τέτοιο τρόπο ώστε να αλλάξει το περιεχόμενο ή να αναγεννά δική του πληροφορία. (ενεργή συμπεριφορά)
4. Πλαστογράφηση πηγής : Ο Αντίπαλος προσποιείται ότι είναι ένα από τα μέλη



Σχήμα 1.5 Είδη επιθέσεων στο κανάλι επικοινωνίας

Ασφάλεια κρυπταλγορίθμων

Ταξινόμηση Μοντέλων αξιολόγησης ασφάλειας

Υπάρχουν 4 βασικά μοντέλα για την αξιολόγηση των αλγορίθμων

1. Ασφάλεια άνευ όρων(Τέλεια Ασφάλεια):

Αυτή η μέτρηση εστιάζεται στην διάκριση αν ένα κρυπτοσύστημα έχει ασφάλεια άνευ όρων βασική υπόθεση είναι ότι όσο και αν κρυπτοκείμενο και αν κατέχει ο αντίπαλος δεν υπάρχει αρκετή πληροφορία για να ανάκτηση το ανοικτό κείμενο(μοναδική λύση) όσο υπολογιστική ισχύ (άπειρη) και αν έχει στην διάθεση του. Χαρακτηριστικό παράδείγμα το σημειωματάριο μίας χρήσης(one time pad).

2. Υπολογιστική ασφάλεια(Πρακτική Ασφάλεια)

Αύτη η μέτρηση εστιάζεται στην υπολογιστική προσπάθεια (παράγοντας εργασίας) που χρειάζεται για να διασπαστεί ένα κρυπτοσύστημα. Στόχος των σύγχρονων συστημάτων να έχουν μεγάλο παράγοντα δυσκολίας ώστε να μην είναι χρονικά δυνατό να διασπαστούν με τα διαθέσιμα ή τα <μελλοντικά> μέσα.

3. Ασφάλεια – θεωρεία πολυπλοκότητας.

Αυτή η μέτρηση εστιάζει στην ταξινόμηση της υπολογιστικής ικανότητας του αντιπάλου υπολογιστικών προβλημάτων ανάλογα με τους πόρους που απαιτούνται για την επίλυση τους. Οι πόροι αναφέρονται

- Το μεγέθους δεδομένων που χρειάζονται σαν είσοδο στην επίθεση
- Τον υπολογιστικό χρόνο που χρειάζεται για να εκτελεστεί η επίθεση
- Το μέγεθος του χώρου αποθήκευσης που χρειάζεται για την επίθεση
- Το πλήθος των επεξεργαστών

4. Αποδείξιμη ασφάλεια.

Αυτή η μέτρηση εστιάζεται στην απόδειξή ισοδυναμίας του μαθηματικού μοντέλου του κρυποσυστήματος με κάποιο πολύ γνωστό δύσκολο στην

επίλυση του πρόβλημα (θεωρίας αριθμών).χαρακτηριστικό παράδειγμα η παραγοντοποίηση μεγάλων ακεραίων

Παράγοντας εργασίας (Work Factor)

Ο παράγοντας εργασίας W_f μετράει την λιγότερη ποσότητα δουλείας που χρειάζεται για τον υπολογισμό του κλειδιού σε ένα κρυπταλγόριθμο. Οι μονάδες μέτρησης του παράγοντα είναι σε χρονικές μονάδες (t) ή σε λειτουργίες (clock cycles).

Αν ο πιο βέλτιστός προσσεγκιστικός αλγόριθμος για την διάσπαση χρειάζεται το λιγότερο ν λειτουργίες ή t(χρόνια) και το ν ή το t είναι αρκετά μεγάλο τότε το κρυπτοσύστημα θεωρείται ασφαλές.

Εφαρμογές κρυπτογραφίας

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

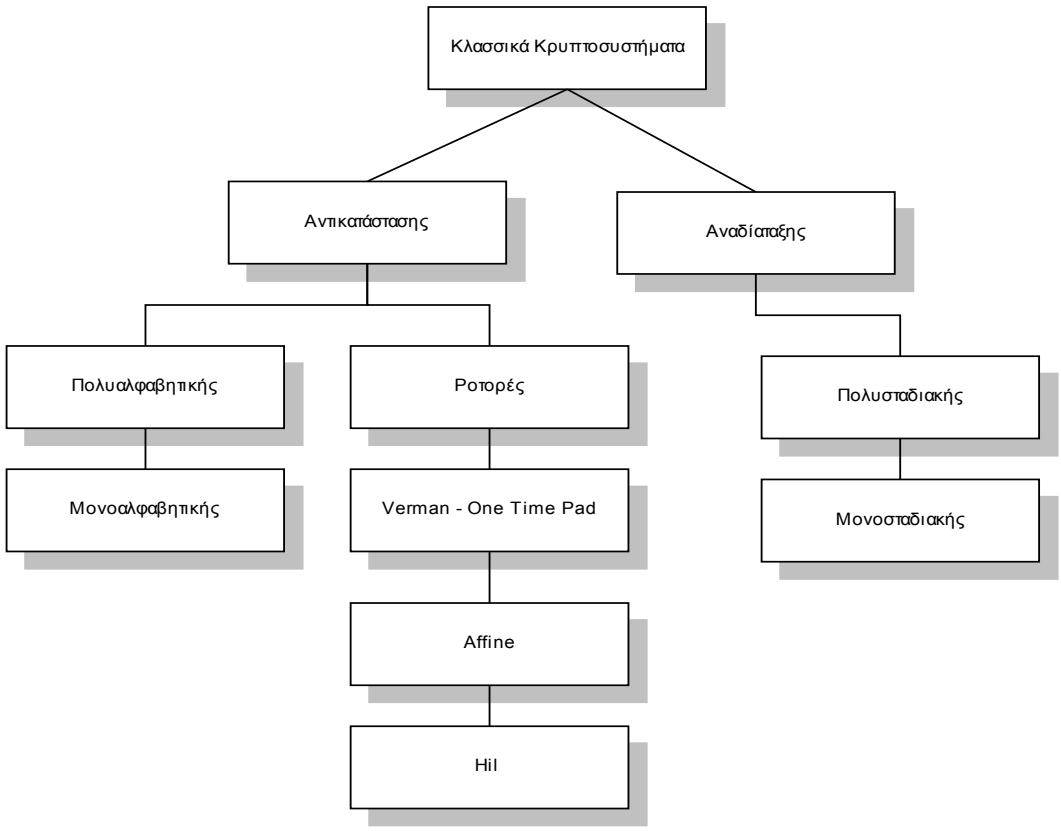
1. *Ασφάλεια συναλλαγών σε τράπεζες δίκτυα - ATM*
2. Κινητή τηλεφωνία (ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM)
3. Σταθερή τηλεφωνία (crypto phones)
4. Διασφάλιση Εταιρικών πληροφοριών
5. Στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)
6. Διπλωματικά δίκτυα (Τηλεγραφήματα)
7. Ηλεκτρονικές επιχείρησης (πιστωτικές κάρτες, πληρωμές)
8. Ηλεκτρονική ψηφοφορία
9. Ηλεκτρονική δημοπρασία
10. Συστήματα συναγερμών (αυτοκινήτου –σπιτιού)
11. Συστήματα βιομετρικής αναγνώρισης.
12. Έξυπνες κάρτες
13. Ιδιωτικά δίκτυα
14. Word Wide Web
15. Δορυφορικές εφαρμογές(δορυφορική τηλεόραση)
16. Ασύρματα δίκτυα (Hipperlan,bluthooth,802.11A)
17. Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων.
18. Τηλεσυνδίασκεψη

2

2.1 Εισαγωγή

Τα κλασσικά κρυπτοσυτήματα βασίστηκαν στην επεξεργασία της γλωσσικής δομής του μηνύματος Οι λέξεις που είναι η μικρότερη μονάδα αποτελείται από μία μη τυχαία ακολουθία από γράμματα τα όποια συνδέονται με συγκεκριμένο νοητικά τρόπο.
Η επεξεργασία γινόταν τόσο στην μορφή των γραμμάτων όσο και στην σειρά-θέση που εμφανιζόντουσαν σε μία λέξη. Χαρακτηριστικά ξεχωρίζουν δύο βασικοί τύποι κρυπτοσυστήμάτων αχ 2.1.

- Κρυπτοσυστήματα Αντικατάστασης
- Κρυπτοσυστήματα Αναδιάταξης



Σχήμα 2.1. Χάρτης Κρυπτοσυστημάτων

2.2 Κρυπτοσυστήματα Αντικατάστασης

Οι τεχνικές αντικατάστασης είναι εκείνες στις οποίες τα γράμματα αντικαθίστανται από άλλα γράμματα ή σύμβολα ή αριθμούς .

Κρυπτοσύστημα καίσαρα :

Έστω κείμενο P και κρυπτοκείμενο C και όπου τα κείμενα εκφράζονται με το αριθμητικό τους ισοδύναμο και επιλογή γλώσσας η αγγλική (26 σύμβολα) $P = C \;\; P, C \in Z_{26}$ και επιλογή κλειδιού μέσα από ένα κλειδοχώρο K όπου $K \in Z_{26}$ όπου για το καίσαρα κ=3 . θεωρώ δείκτη ι ο οποίος ορίζει την θέση. Για λόγους κλειστότητας αριθμών χρησιμοποιείται η modular αριθμητική

Ορίζω αριθμητικό Ισοδύναμο πίν 2.1

Πιν

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Ορίζω συνάρτηση κρυπτογράφησης $E_k : P \to C \;\; c_i = E_k(p_i) = p_i + k \bmod n$

Ορίζω συνάρτηση αποκρυπτογράφησης $D_k : C \to P \;\; p_i = D_k(c_i) = c_i - k \bmod n$

Παράδειγμα :

Μήνυμα : Landing in Blue Coast
Κρυπτοκείμενο : odqglqj lq eoxh frdvw

Το παραπάνω σύστημα μπορώ να το γενικεύσω για $k \in Z_{26}$

Κρυπτανάλυση κρυπτοσυστημάτων τύπου καίσαρα :

Ο αντίπαλός αν γνωρίζει το σύστημα πρέπει να δοκιμάσει όλα τα πιθανά κλειδιά μέχρι να φθάσει σε ένα κείμενο που να έχει νόημα

Παράδειγμα
Έστω ο κρυπταναλυτής έχει αποκτήσει το κρυπτοκείμενο **odqglqj lq eoxh frdvw**
Ο κρυπταναλυτής δημιουργεί τον πίν 2.2 και μετά από την εξαντλητική εξερεύνηση καταλήγει σε μία μοναδική λύση με το κλειδί κ=3.Τα στοιχεία που ξεχωρίζουν είναι ο μικρός χώρος κλειδιών K=26 κλειδιά και το κρυπτοαλφάβητο είναι μία μετατόπιση του αλφαβήτου του μηνύματος το οποίο σημαίνει ότι τα γράμματα διατηρούν την φυσική τους σειρά

Πίνακας 2.2 Εξαντλητική Μέθοδος

Κλειδί	Κρυπτοκείμενο

1	ncpfkpi kp dnwg eqcuv
2	mboejoh jo cmvf dpbtu
3	landing in blue coast
4	kzmchmf hm aktd bnzrs
5	jylbgle gl zjsc amyqr
6	ixkafkd fk yirb zlxpq
7	hwjzejc ej xhqa ykwop
8	gviydib di wgpz xjvno
9	fuhxcha ch vfoy wiumn
10	etgwbgz bg uenx vhtlm
11	dsfvafy af tdmw ugskl
12	creuzex ze sclv tfrjk
13	bqdtydw yd rbku seqij
14	apcsxcv xc qajt rdphi
15	zobrwbu wb pzis qcogh
16	ynaqvat va oyhr pbnfg
17	xmzpuzs uz nxgq oamef
18	wlyotyr ty mwfp nzlde
19	vkxnsxq sx lveo mykcd
20	ujwmrwp rw kudn lxjbc
21	tivlqvo qv jtcm kwiab
22	shukpun pu isbl jvhza
23	rgtjotm ot hrak iugyz
24	qfsinsl ns gqzj htfxy
25	perhmrk mr fpyi gsewx
26	odqglqj lq eoxh frdvw

Μονοαλφαβητικά κρυπτοσυστήματα :

Κάθε γράμμα του μηνύματος το αντικαθιστώ με ένα άλλο σύμβολο ορίζω δηλαδή ένα πίνακα αντιστοίχησης 1-1 από το αλφάβητο της γλώσσας σε ένα καινούργιο αλφάβητο ανακατεμένο ή μη φυσικό αλφάβητο

Έστω κείμενο P και κρυπτοκείμενο C και όπου τα κείμενα εκφράζονται με το αριθμητικό τους ισοδύναμο και επιλογή γλώσσας η αγγλική (26 σύμβολα) $P, C \in Z_{26}$ και επιλογή κλειδιού ορίζει την αντιστοίχηση 1-1 .θεωρώ δείκτη ι ο οποίος ορίζει την θέση.

Ορίζω αριθμητικό Ισοδύναμο γλώσσας πίν 2.1

Ορίζω συνάρτηση κρυπτογράφησης $E_k : P^n \to C^m \quad c_i = E_k(p_i) = p_i + k \bmod n$

Ορίζω συνάρτηση αποκρυπτογράφησης $D_k : C^m \to P^n \quad p_i = D_k(c_i) = c_i - k \bmod n$

Ο κλειδοχώρος έχει αυξηθεί από 25 κλειδιά σε $n!$-1 δηλαδή 6.2045 *10^{23} - 1 όπου n!

εκφράζει όλους τους πιθανούς συνδυασμούς αλφαβήτων. Είναι πρακτικά αδύνατον να καταφέρει ο κρυπταναλυτής να δοκιμάσει όλους τους συνδυασμούς μέσα σε λογικό διάστημα
Εμφανίζεται ότι το συγκεκριμένο σύστημα είναι ασφαλές

Παράδειγμα :
Παράγω ένα τυχαίο αλφάβητο με σύμβολα τα γράμματα της αγγλικής γλώσσας

Πχ COXETKMUGDAVLHJSYZRWIBPNFQ
GTIJENKPXVBMRDOHSUQWZLYAFC
FDPXMAYBGZKRJEVOCHWINSQLUT

Ορίζω Αντιστοίχηση 1-1

Αλφάβητο Μυνήματος ABCDEFGHIJKLMNOPQRSTUVWXYZ
Κρυπτοαλφάβητο ZHQPDMFCOREJWNSUGAVYIXLBKT

Έστω το μήνυμα : Landing in Blue Coast
Το παραγόμενο κρυπτοκείμενο είναι : JZNPONFONHJIDQSZVY

Κρυπτανάλυση Μονοαλφαβητικής Αντικατάστασης :
Ο κρυπταναλυτής χρησιμοποιεί μία μέθοδο που λέγεται ανάλυση συχνότητας η οποία διασπά την μονοαλφαβητική αντικατάσταση τεχνική αυτή μελετάει την στατιστική δομή της γλώσσας του κρυπτομηνύματος σχ 2.2 πιν 2.2.Η ανάλυση συχνότητας βασίζεται στο γεγονός ότι οι περισσότερες γλώσσες παρουσιάζουν στην δομή (γράμματα ή συνδυασμούς γραμμάτων) τους κάποια ορισμένη κατανομή με μέγιστα και ελάχιστα. τα οποία μπορούν να χαρακτηρίσουν την γλώσσα αυτή. Με τον υπολογισμό της κατανομής των γραμμάτων μέσα στην γλώσσα βρίσκουμε ένα μέτρο που το ακολουθούν όλα τα κείμενα της γλώσσας αυτής. Για την αγγλική γλώσσα το Ε τείνει να είναι το πιο κοινό γράμμα (με της περισσότερες επαναλήψεις σε ένα οποιοδήποτε κείμενο) ενώ το Z τείνει να είναι το πιο σπάνια συναντούμενο γράμμα. Σε μερικά κρυπτοσυστήματα τέτοιες ιδιότητες της φυσικής γλώσσας συντηρούνται στο κρυπτογράφημα, και αυτά οι κατανομές δίνουν τη δυνατότητα μίας επίθεσης κρυπτοκειμένου. Χρησιμοποιώντας την κατανομή χαρακτήρων ψάχνουμε να βρούμε για τον πιο επαναλαμβανόμενο κρυπτοχαρακτήρα. και τον αντικαθιστούμε από τον πιο επαναλαμβανόμενο χαρακτήρα της φυσικής γλώσσας. και συνεχίζουμε την ανάλυση έως φθάσουμε σε μία μοναδική λύση(Το εξαγόμενο μήνυμα να έχει γλωσσικό νόημα).

Βοηθητικά εργαλεία είναι:
1. Ν-γραμματική πιθανοτική ανάλυση
2. Ανάλυση δομής Γλώσσας
3. Ακολουθιακή Γραμματική Ανάλυση κατά Μαρκοφ

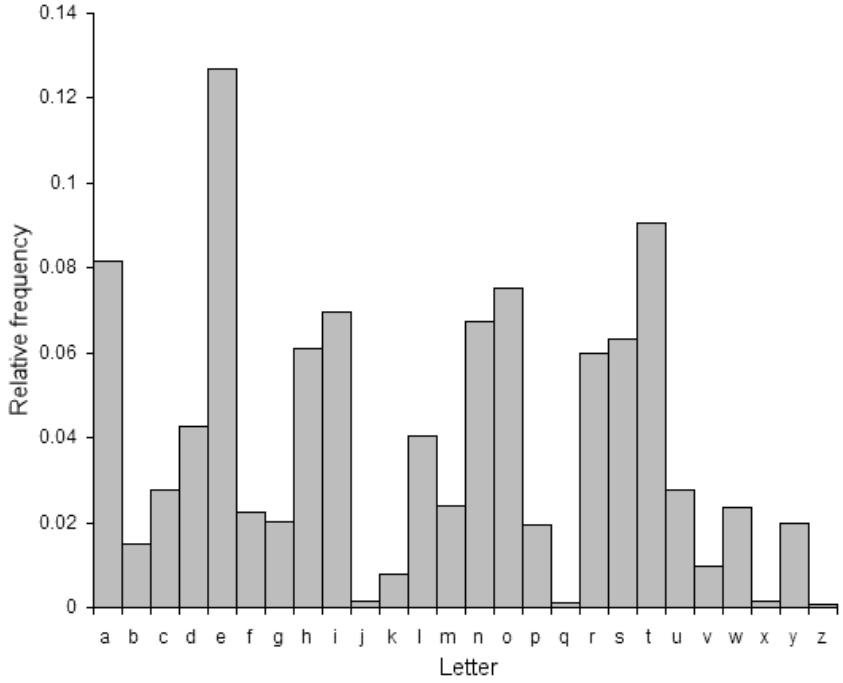
Πινακας 2.2 Σχετικές Συχνότητες Γραμμάτων Αγγλικής-Ελληνικής

A	B	C	D	E	F	G	H	I	J	K	L	M
8.2	1.4	2.8	3.8	12.7	2.9	2.0	5.3	6.3	0.1	0.4	3.4	2.3

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7.1	8.0	2.0	0.1	6.8	6.1	10.5	2.5	0.9	1.5	0.2	2.0	0.1

Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν
12	0.8	2	1.7	8	0.5	2.9	1.3	7.8	4.2	3.3	4.4	7.9

Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Υ	Ω		
0.6	9.8	5.024	5.009	4.9	9.1	4.3	1.2	1.4	0.2	1.6		



Σχήμα 2.2 Ιστόγραμμα με τις σχετικές συχνότητες της Αγγλικής γλώσσας

Ανάλυση Δομής Γλώσσας :

1. Το πίο κοινό πρώτο γράμμα μέσα σε λέξεις T, O, A, W, B, C, D, S, F, M, R, H, I, Y, E, G, L, N, O, U, J, K
2. Το πίο κοινό δεύτερο γράμμα μέσα σε λέξεις H, O, E, I, A, U, N, R, T
3. Το πίο κοινό τρίτο γράμμα μέσα σε λέξεις E, S, A, R, N, I
4. Το πίο κοινό τελευτέο γράμμα μέσα σε λέξεις E, S, T, D, N, R, Y, F, L, O, G, H, A, K, M, P, U, W
5. Οι περισσότερες λέξεις τελείωνουν με E ,T, D, S
6. Τα γράμματα που ακολοθούν το E R,S,N,D
7. Τα πίο κοινά διπλά γράμματα SS, EE, TT, FF, LL, MM, OO

Η Τριγραμματική ανάλυση σε ένα Αγγλικό κείμενο 763 λέξεων

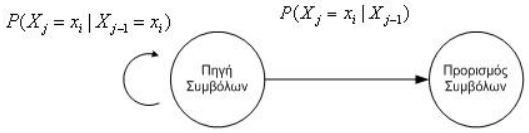
Λεξεις	Εμφάνιση	Συχνότητα
The	91	11.9%
And	27	3.5%
Had	19	2.5%
Was	15	2%
That	13	1.7%

Διακριτή Στατιστική πηγή Μαρκόφ :

Μπορούμε να παραστήσουμε το μήνυμα σαν μία ακολουθία γραμμάτων Αυτές οι ακολουθίες γραμμάτων δεν είναι τυχαίες αλλά έχουν μια στατιστική εξάρτηση δηλαδή η εμφάνιση ενός γράμματος επηρεάζει την εμφάνιση ενός άλλου γράμματος .πχ Η εμφάνιση του του Q συνεπάγει ότι το αμέσως πιθανότερο γράμμα είναι το U. Η πηγή εκπέμπει γράμματα απο ένα πεπερασμένο αλφάβητο έστω το Αγγλικό σύμφωνα με κάποιες πιθανότητες που εξαρτώνται από το τρέχων γράμμα και από τα προηγούμενα γράμματα .Η πιθανότητα εμφάνισης ενός γράμματος εξαρτάται από το συγκεκριμένο γράμμα και από το αμέσως προηγούμενο πχ

P(Xj=b,Xj-1=a) = 0.0228302.

Σχηματίζεται επομένως ένας πίνακας 26x26 με όλους τους συνδυασμούς και τις πιθανότητες για κάθε συνδυασμό. Συμπεραίνουμε ότι το μήνυμα σαν ακολουθία περιέχει μνήμη την οποία μπορούμε να ποσοτικοποιήσουμε



Παράδειγμα

Έστω ο κρυπταναλυτής έχει αποκτήσει πρόσβαση στο κρυπτοκείμενο.
WSADSXDAONVOPDDZQCQSINYAKAOQCZNPUSSAZJOEDYZEDVUJZ
QDZNZNZJSFSIVPDXDJSUWDNYONMZXSASMYCDAOQCDVYUZAYS
MYCDUSUIJZYOSNYCZYVYCDQIAADNYUASFADVVSMCIWZNOYKV
YZNPHDCONPZJJHJZHJZHJZAOQCFDYAOQCDAUSSAFDYUSSADAZN

OQDVSQODYKONPDDPCDZPDPZYMIJJVUDDPZFZONVYZHAOQELZJJ
OZPXOQDKSIYSMZVYDNKSIAVDZYHDJYZNPYSVDZYNDBYYSZND
WDAFDNQKDBOYJOEDQAZQEONFLSAELDJJSAQ

Το πρώτο βήμα που κάνει ο κρυπταναλυτής είναι να μετρήσει την συχνότητα που εμφανίζονται τα γράμματα(πιν 2.3) στο κρυπτοκείμενο και μετά να τα συσχετίσει με το ιστόγραμμα 2.2 Το πιο εμφανιζόμενο γράμμα μέσα στο κρυπτοκείμενο είναι το γράμμα D το οποίο τείνει να είναι το γράμμα Ε αλλά αυτό δεν είναι σίγουρο. Ο κρυπταναλυτής οδηγείται σε διάφορους συσχετισμούς ανάλογα με την συχνότητα γραμμάτων.

Πίνακας 2.3 Μετρήσεις κατανομής γραμμάτων

Νούμερο.	χαρακτήρας	Συχνότητες(%)	Μέτρηση Συχνότητας
1	D	12.5000	41
2	Z	9.7561	32
3	Y	8.5366	28
4	S	8.2317	27
5	A	7.3171	24
6	N	6.4024	21
7	O	6.4024	21
8	J	5.4878	18
9	Q	4.8780	16
10	V	4.2683	14
11	C	3.6585	12
12	P	3.6585	12
13	U	3.0488	10
14	I	2.4390	8
15	F	2.1341	7
16	E	1.8293	6
17	H	1.8293	6
18	K	1.8293	6
19	M	1.8293	6
20	W	1.2195	4
21	X	1.2195	4
22	L	0.9146	3
23	B	0.6098	2

Διγραματική Ανάλυση

1	ZN	2.4465	8
2	OQ	2.1407	7

3	**SA**	**2.1407**		**7**	
4	**AO**	**1.8349**		**6**	
5	**CD**	**1.8349**		**6**	
6	**ON**	**1.8349**		**6**	
7	**DA**	**1.5291**		**5**	
8	**DZ**	**1.5291**		**5**	
9	**JZ**	**1.5291**		**5**	
10	**NP**	**1.5291**		**5**	
11	**QC**	**1.5291**		**5**	
12	**VY**	**1.5291**		**5**	
13	**ZY**	**1.5291**		**5**	
14	**AD**	**1.2232**		**4**	
15	**DN**	**1.2232**		**4**	
16	**DV**	**1.2232**		**4**	
17	**DY**	**1.2232**		**4**	
18	**JJ**	**1.2232**		**4**	
19	**NY**	**1.2232**		**4**	
20	**PD**	**1.2232**		**4**	
21	**SI**		**1.2232**		**4**
22	**SM**	**1.2232**		**4**	
23	**US**	**1.2232**		**4**	
24	**YC**	**1.2232**		**4**	
25	**YS**	**1.2232**		**4**	
26	**YZ**	**1.2232**		**4**	

Αντικαθιστά μέσα στο κρυπτοκείμενο το D με το E

wsaEsxEaonvopEEzqcqsinyakaoqcznpussazjoeEyzeEvujzqEznznzj sfsivpExEjsuwEnyonmzxsasmycEaoqcEvyuzaysmycEusuijzyosnyc zyvycEqiaaEnyuasfaEvvsmciwznoykvyznphEconpzjjhjzhjzhjzaoqcf EyaoqcEaussafEyussaEaznoqEvsqoEykonpEEpcEzpEpzymijjvuEE pzfzonvyzhaoqelzjjozpxoqEksiysmzvyEnksiavEzyhEjyznpysvEzyn EbyysznEwEafEnqkEboyjoeEqazqeonflsaelEjjsaq

Συνεχίζει επιλέγοντας σαν ζευγάρι το Z να το αντικαταστήσει με το T ή το A κλπ.. Μελετάει την διγραμματική κατανομή.

Σύμφωνα με το σχέδιο του Ναυτικού τμήματος των ΗΠΑ η γενική λύση για τα κρυπτοσυστήματα μονοαλφαβητικής αντικατάστασης είναι η εξής

Ανάλυση Κρυπτοκειμένου

- Προετοιμασία του πίνακα συχνοτήτων
- Αναζήτηση για επαναλήψεις

- Προσδιορισμός του τύπου του συστήματος που χρησιμοποιήθηκε
- Προετοιμασία φύλλου εργασίας
- Προετοιμασία αλφαβήτων κρυπτοκειμένου (Αν έχει χρησιμοποιηθεί παραπάνω από ένα)
- Δημιουργία πίνακα με μεγάλου μήκους επαναλήψεις και κατανομές ασυνήθιστων γραμμάτων

Ταξινόμηση σύμφωνων και φωνήεντων μελετώντας
- Συχνότητες
- Κενά
- Συνδυασμούς γραμμάτων
- Επαναλήψεις

Προσδιορισμός ταυτότητας γραμμάτων
- Διάσπαση ή διεξαγωγή της wedge διαδικασίας
- Επαλήθευση των υποθέσεων
- Τοποθέτηση σωστών τιμών από την αρχή έως το τέλος του μηνύματος
- Ανάκτηση νέων τιμών για την ολοκλήρωση της λύσης Ανακατασκευή του συστήματος
- Ανακατασκευή του πίνακα κρυπτογράφησης
- Ανάκτηση του κλειδιού που χρησιμοποιήθηκε στην λειτουργία του συστήματος
- Ανάκτηση του κλειδιού ή της φράσης κλειδιού που χρησιμοποιήθηκε για να κατασκευαστεί η αλφαβητική ακολουθία.

Πολύαλφαβητικά κρυπτοσυστήματα τετραγώνου Viginere :

Στα πολυαλφαβητικά κρυπτοσυστήματα κάθε γράμμα του μηνύματος αντικαθίσταται με ένα σύμβολο κάθε φορά από διαφορετικό αλφάβητο .Κάθε γράμμα του μηνύματος το αντικαθιστώ με περσότερα από ένα σύμβολα ορίζω δηλαδή ένα πίνακα αντιστοίχησης 1-1 από το αλφάβητο της γλώσσας σε πολλά διαφορετικά αλφάβητα ανακατεμένα ή μη φυσικά αλφάβητα τα οποία αλλάζουν κάθε φορά ανάλογα με τα γράμματα της κλείδας πιν 2.4.Το τετράγωνο viginere περιέχει ουσιαστικά μια λίστα μετατοπισμένων αλφαβήτων της κάθε γλώσσας

Υπάρχουν δύο τύποι μικτών αλφαβήτων

- Κλείδα και ακολουθία
- Κλείδα και αναδιάταξη

Στην μέθοδο κλείδα και ακολουθία γράφουμε την κλείδα αφαιρώντας τα επαναλαμβανόμενα γράμματα και μετά συμπληρώνουμε τα υπόλοιπα γράμματα του αλφαβήτου. Ενώ στην μέθοδο κλείδα και αναδιάταξη γράφουμε την κλείδα χωρίς επαναλαμβανόμενα γράμματα και γράφουμε από κάτω τα υπόλοιπα γράμματα σε γραμμές κάτω από τα αρχικά και διαβάζουμε τις στήλες που δημιουργούνται και τις τοποθετούμε στην στήλη κλειδιών. Οι μέθοδοι αυτές αύξησαν την πολυπλοκότητα του κρυπτοσυστήματος .Το μέγεθος τάξης κλειδιού είναι πολύ μεγάλο $|K| = 26^{26} = 6.1561 * 10^{36}$

Πίνακας 2.4 Τετράγωνο Vigenere

Γράμματα κλειδιού	**Γράμματα Μυνήματος**																								
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Έστω κείμενο P και κρυπτοκείμενο C , όπου τα κείμενα εκφράζονται με το αριθμητικό τους ισοδύναμο και επιλογή γλώσσας η αγγλική (26 σύμβολα) $P, C \in Z_{26}$ και επιλογή κλειδιού $K = k_1, k_2, k_3, ...k_n$ που ορίζει το αλφάβητο που θα χρησιμοποιηθεί κάθε φορά.

Ορίζω αριθμητικό Ισοδύναμο γλώσσας πίν 2.1

Ορίζω συνάρτηση κρυπτογράφησης $E_k : P^n \to C^m$

$$E_k(p) = (p_1 + k_1 \bmod n) + (p_2 + k_2 \bmod n) + (p_n + k_n \bmod n) + (p_{n+1} + k_1 \bmod n) + (p_{n+2} + k_2 \bmod n)$$

Ορίζω συνάρτηση αποκρυπτογράφησης $D_k : C^m \to P^n$

$$D_k(c) = (c_1 - k_1 \bmod n) + (c_2 - k_2 \bmod n) + (c_n - k_n \bmod n) + (c_{n+1} - k_1 \bmod n)$$

Η ασφάλεια του κρυπτοαλγορίθμου βασίζεται στην διάχυση των στατιστικών δεδομένων της γλώσσας η κατανομή γραμμάτων του κρυπτοκειμένου πλέον δεν παρουσιάζει μέγιστα και ελάχιστα αλλά τείνει να γίνει επίπεδη. Το γράμμα Ε στην αγγλική γλώσσα διαμοιράζεται σε n διαφορετικά αλφάβητα δηλαδή κωδικοποιείται με n διαφορετικά γράμματα. Άρα η συχνότητα του καταμερίζεται σε n διαφορετικά γράμματα. Όπου ν είναι οι χαρακτήρες του κλειδιού. Πιο επίπεδη κατανομή σε ένα κρυπτόγραμμα σημαίνει μεγάλο παράγοντα εργασία και οδηγεί σε μία πρώτη σχεδιαστική αρχή.

Παράδειγμα :

Επιλέγουμε σαν λέξη κλειδί την AVALANCHE και την γράφουμε επαναληπτικά πάνω από το κείμενο του μηνύματος. .Το πρώτο γράμμα του μηνύματος είναι το L πηγαίνουμε στην στήλη που ο δείκτης είναι το L και στην γραμμή που δείχνει το γράμμα κλειδιού Α στον πιν 2.4 το στοιχείο που δείχνουν είναι το γράμμα L όπου είναι το παραγόμενο κρυπτόγραμμα. Η διαδικασία επαναλαμβάνεται για τα επόμενα γράμματα του μηνύματος.. Η αντίστροφη διαδικασία οδηγεί στην αποκρυπτογράφηση.

Κωδική λέξη AVALANCHEAVALANCHE
Έστω το μήνυμα : LANDINGINBLUECOAST
Το παραγόμενο κρυπτοκείμενο είναι : LVNOIAIPRBGUPCBCZX

Κρυπτανάλυση Πολυαλφαβητικής Αντικατάστασης :

Μέθοδος Kasiski :

Η εξέταση Kasiski ή αλλιώς Τεστ kasiski είναι μια μέθοδος για την διάσπαση πολυαλφαβητικών κρυπτοσυστημάτων.Η βασική ιδέα είναι η παρατήρηση ότι λόγω της επανάληψης κάποιων λέξεων μέσα στο μήνυμα κρυπτογραφούνται και παράγουν ίδια κρυπτοκείμενα όταν είναι ευθυγραμμισμένα με το κλειδί. Τα επαναλαμβανόμενα συμπλέγματα θα πρέπει να είναι τουλάχιστον τρία. Μετρώντας την απόσταση ανάμεσα στα επαναλαμβανόμενα μοτίβα δημιουργείται μια λίστα από αποστάσεις και ο ΜΚΔ όλων αυτών είναι συνήθως το μήκος του κλειδιού. Αν ο κρυπταναλυτης βρει το μήκος του κλειδιού έστω 5 τότε σε ένα κρυπτογραφημένο κείμενο τα γράμματα στην θέση [1,1+n*5] όπου δημιουργούν μία λίστα μιας μονοαλφαβητικης αντικατάστασης η οποία αναλύεται εύκολα με την ανάλυση συχνότητας γραμμάτων . Καταλήγουμε με τόσες λίστες όσα είναι τα στοιχεία του κλειδιού και αντιμετωπίζουμε πλέον την πολυαλφαβητική αντικατάσταση σαν πολλές απλές μονοαλφαβητικες αντικαταστάσεις.

Τα βήματα για τον έλεγχο kasiski είναι

1. Αναγνώριση των επαναλαμβανόμενων μοτίβων τριών ή περισσότερων χαρακτήρων
2. Για κάθε μοτίβο γράφουμε την διεύθυνση που ξεκινάνε τα μοτίβα.
3. Υπολογίζουμε τη απόσταση μεταξύ των μοτίβων
4. Προσδιορίζουμε όλους τους παράγοντες των αποστάσεων ΜΚΔ
5. Επιλέγουμε τον παράγοντα που εμφανίζεται πιο συχνά

3

3 Εισαγωγή

Η μοντέρνα κρυπτογραφία βασίστηκε πάνω στην επεξεργασία του αριθμητικού ισοδύναμου της γλωσσικής δομής του μηνύματος. Ανακαλύφθηκαν τρόποι με τους οποίους μεγιστοποιήθηκε η ασφάλεια των κρυπτογραφικών χαρακτηριστικών τοσο από στατιστικής συμπεριφοράς όσο και από πλευράς επαναληψημότητας. Η κρυπτογραφία μηχανοποιείται και μεγιστοποιείται ο όγκος της κρυπτογράφησης δεδομένων .Η κλασσική μορφή του μηνύματος διευρύνεται πλέων έχουμε κρυπτογράφηση γενικά της πληροφορίας (Ηχός – Φωνή).Η μελέτη μεταφέρεται πάνω σε μαθηματικές δομές.

3.1 Κυρια σημεία της Θεωρίας Του Shannon

3.1.1 Εντροπία και αβεβαιότητα

Η πληροφοριακή θεωρία ορίζει την ποσότητα της πληροφορίας σε ένα μήνυμα ως τον ελάχιστο αριθμό bit που απαιτούνται για να απεικονίσουμε όλα τα δυνατά νοήματα του μηνύματος αυτού, θεωρώντας ότι όλα τα μηνύματα είναι το ίδιο πιθανά. Για παράδειγμα ένα πεδίο που αποθηκεύει τις μέρες της εβδομάδος δεν θα ήταν πάνω από 3 bit, γιατί η πληροφορία αυτή μπορεί να απεικονιστεί με 3 bit:

000 = Κυριακή
001 = Δευτέρα
010 = Τρίτη
011 = Τετάρτη
100 = Πέμπτη
101 = Παρασκευή
110 = Σάββατο
111 = Δεν χρησιμοποιείται

Ένα πεδίο που αποθηκεύει το φύλο περιέχει μόνο ένα bit πληροφορίας, παρόλο που μπορεί να αποθηκεύεται ως ένα string 7 byte.

Τυπικά, η ποσότητα της πληροφορίας σε ένα μήνυμα M μετριέται με την εντροπία του μηνύματος, που συμβολίζεται με H(M). Η εντροπία ενός μηνύματος που περιέχει το φύλο είναι 1 bit· η εντροπία ενός μηνύματος που αναφέρει την μέρα της εβδομάδος είναι κάτι λιγότερο από 3. Γενικά, η εντροπία ενός μηνύματος είναι $\log_2 n$, όπου n είναι ο αριθμός των δυνατών εννοιών, και μετριέται σε bit. Αυτός ο ορισμός θεωρεί ότι κάθε έννοια έχει την ίδια πιθανότητα.

Η εντροπία ενός μηνύματος μετράει και την αβεβαιότητά του.

$$H(M) = \sum_{i}^{n} p(m_i) * \log_2 \frac{1}{p(m_i)}$$

Η εντροπία γίνεται ελάχιστή όταν η πιθανότητα εμφάνισης ενός γεγονότος γίνεται μέγιστη και γίνεται μέγιστη όταν η πιθανότητα εμφάνισής ένος γεγονότος σε ένα σύνολο γεγονότων γίνει ισοπίθανη.

Αυτή είναι ο αριθμός των bit του αρχικού κειμένου που χρειάζεται να ανακτήσουμε, όταν το κείμενο είναι κρυπτογραφημένο, για να μάθουμε ποιο είναι το αρχικό κείμενο. Για παράδειγμα, αν το «*(&AT6» είναι κομμάτι ενός κρυπτογραφήματος που σημαίνει είτε «ΑΝΔΡΑΣ» είτε «ΓΥΝΑΙΚΑ», τότε η αβεβαιότητα του μηνύματος είναι 1. Χρειάζεται να ανακτήσουμε ένα καλά διαλεγμένο bit για να μάθουμε το μήνυμα

3.1.2 Η τάξη μιας γλώσσας

Για μια δεδομένη γλώσσα, ονομάζουμε τάξη της γλώσσας (rate of the language) το

$$r = H(M)/N$$

όπου N είναι το μήκος του μηνύματος. Η τάξη στα Αγγλικά παίρνει διάφορες τιμές, από 1,0 ως 1,5 bit/γράμμα, για μεγάλες τιμές του N. Γενικά, το 1,3 είναι μια αποδεκτή τιμή. Η απόλυτη τάξη (absolute rate) μιας γλώσσας είναι ο μέγιστος αριθμός bit που μπορούν να αντιστοιχούν σε ένα χαρακτήρα, θεωρώντας ότι κάθε ακολουθία χαρακτήρων είναι το ίδιο πιθανή. Αν υπάρχουν L χαρακτήρες σε μια γλώσσα, η απόλυτη τάξη είναι:

$$R = \log_2 L$$

Αυτή είναι η μέγιστη εντροπία των χαρακτήρων. Για τα Αγγλικά η απόλυτη τάξη είναι $\log_2 26$ ή περίπου 4,7 bit/γράμμα. Είναι φυσικό η πραγματική τάξη να είναι μικρότερη από την απόλυτη, γιατί οι γλώσσες είναι πλεονάζουσες.

Ο πλεονασμός (redundancy) μιας γλώσσας, D, ορίζεται ως:

$$D = R - r$$

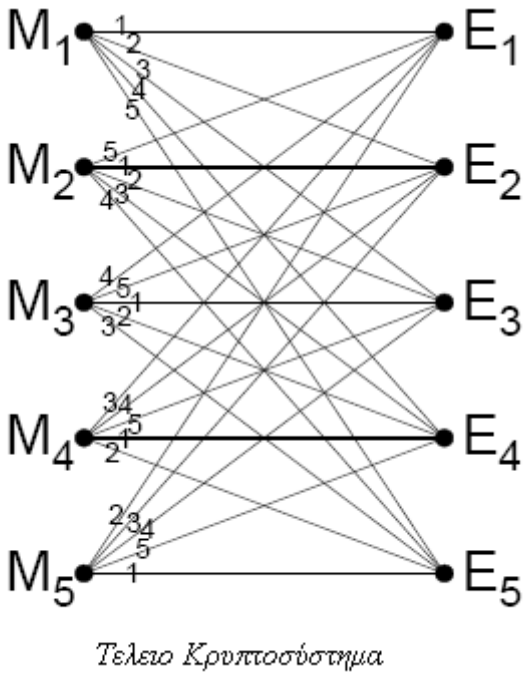
Για τα Αγγλικά, που έχουν τάξη 1,3, ο πλεονασμός είναι 3,4 bit/γράμμα. Ένα κείμενο ASCII, που είναι απλά ένα αγγλικό κείμενο, έχει 1,3 bit πληροφορίας ανά γράμμα, δηλαδή ανά byte. Αυτό σημαίνει ότι το κάθε byte έχει 8-1,3=6,7 bit πλεονάζουσας πληροφορίας και το κάθε bit έχει 6,7/8=0,84 bit πλεονάζουσας πληροφορίας. Η εντροπία είναι 0,16 bit πληροφορίας για κάθε bit ASCII κειμένου.

3.1.2 Ασφάλεια ενός κρυπτοσυστήματος

Ο Shannon καθόρισε ένα ακριβές μαθηματικό μοντέλο για το τι σημαίνει να είναι ασφαλές ένα κρυπτοσύστημα. Ο στόχος του κρυπταναλυτή είναι να ανακτήσει το κλειδί, K, το αρχικό κείμενο, P, ή και τα δύο. Όμως, μπορεί να είναι ικανοποιημένος με την απόκτηση κάποιας πιθανολογικής πληροφορίας σχετικής με το P: ότι είναι ψηφιοποιημένος ήχος..

Στις περισσότερες περιπτώσεις ο κρυπταναλυτής γνωρίζει εκ των προτέρων κάποια πιθανολογική πληροφορία. Καταρχήν, πιθανότατα γνωρίζει την γλώσσα (αν πρόκειται για κείμενο). Αν είναι ένα μήνυμα για την Βασιλική, τότε μάλλον θα αρχίζει με «Αγαπητή Βασιλική» κοκ. Στόχος του αναλυτή είναι να μεταβάλλει τις πιθανότητες που σχετίζονται με κάθε πιθανό κείμενο. Τελικά κάποιο κείμενο θα αναδειχτεί ως το πιθανότερο αρχικό κείμενο.

Για να παρέχει ένα κρυπτοσύστημα τέλεια ασφάλεια (perfect security) θα πρέπει το κρυπτογράφημα να μην φανερώνει καμία πληροφορία για το αρχικό κείμενο. Αυτό, είπε ο Shannon, μπορεί να γίνει μόνο αν ο αριθμός των πιθανών κλειδιών είναι τουλάχιστο όσο μεγάλος είναι και ο αριθμός των πιθανών μηνυμάτων σχ 3.1.



Σχήμα 3.1 Τέλειο Κρυπτοσύστημα

Με άλλα λόγια, θα πρέπει το κλειδί να έχει μήκος τουλάχιστο ίσο με το κείμενο, και κανένα κλειδί δεν θα πρέπει να χρησιμοποιείται ξανά. Περιέγραψε, δηλαδή, το on-time pad.

Γενικά, όμως, κάθε κρυπτογράφημα φανερώνει κάποια πληροφορία για το αρχικό κείμενο. Δουλειά ενός καλού κρυπτογραφικού αλγόριθμου είναι να ελαττώσει αυτήν την πληροφορία στο ελάχιστο· δουλειά του κρυπταναλυτή είναι να εκμεταλλευτεί την πληροφορία για να ανακτήσει το κείμενο.

Οι κρυπταναλυτές στηρίζονται στον πλεονασμό μιας γλώσσας για να μειώσουν τον αριθμό των πιθανών αρχικών κειμένων. Αυτός είναι και ο λόγος που πολλές κρυπτογραφικές εφαρμογές πρώτα συμπιέζουν το κείμενο και μετά το κρυπτογραφούν. Η συμπίεση μειώνει τον πλεονασμό της γλώσσας, και παράλληλα μειώνει το μέγεθος της εργασίας κρυπτογράφησης και αποκρυπτογράφησης

Η εντροπία ενός κρυπτοσυστήματος είναι συνάρτηση του μεγέθους του συνόλου των δυνατών κλειδιών, K. Υπολογίζεται προσεγγιστικά από τον τύπο:

$$H(K) = \log_2 K$$

Ένα κρυπτοσύστημα με μήκος κλειδιού 64 bit έχει εντροπία 64 bit. Γενικά, όσο πιο μεγάλη η εντροπία, τόσο δυσκολότερο είναι να σπάσει το κρυπτοσύστημα.

3.1.3 Θεωρητική Ασφάλεια

Προκειμένου ο Shannon να μελετήσει ένα κρυπτοσυστήμα με βάση την θεωρία πληροφορίας μοντελοποίησε τις βασικές έννοιες που εμφανιζόντουσαν στο σύστημα. Την πηγή κειμένου P ,την πηγή κρυπτοκειμένου C και την πηγή κλειδιού C

Σε ένα κρυπτοσύστημα εμφανίζονται οι ακόλουθες Αβεβαιότητες

- $H(K|P) \geq H(K)$
  Εμφανίζεται διαρροή ποσότητας του κλειδιού από την ανάγνωση του μηνύματος
- $H(K|C) \geq H(K)$
  Εμφανίζεται διαρροή ποσότητας του κλειδιού από την ανάγνωση του κρυπτοκειμένου
- $H(C|P) \geq H(C)$
  Εμφανίζεται διαρροή ποσότητας του κρυπτοκειμένου από την ανάγνωση του μηνύματος
- $H(C|K) \geq H(C)$
  Εμφανίζεται διαρροή ποσότητας του κρυπτοκειμένου από την ανάγνωση του κλειδιού
- $H(P|K) \geq H(P)$
  Εμφανίζεται διαρροή ποσότητας του μηνύματος από την ανάγνωση του κλειδιού
- $H(P|C) \geq H(P)$
  Εμφανίζεται διαρροή ποσότητας του μηνύματος από την ανάγνωση του κρυπτοκειμένου

3.1.4 Απόσταση μοναδικότητας (unicity distance)

Για ένα κρυπτογραφημένο μήνυμα μήκους n, ο αριθμός των διαφορετικών κλειδιών που το αποκωδικοποιούν σε κάποιο κείμενο, που να έχει νόημα στη γλώσσα στην οποία γράφτηκε, δίνεται από τον τύπο:

$$2^{H(K)-nD} - 1$$

Ο Shannon καθόρισε ως απόσταση μοναδικότητας, U, καλούμενη και σημείο μοναδικότητας, μια προσέγγιση της ποσότητας κρυπτογραφήματος, η οποία είναι τόση ώστε το άθροισμα της εντροπίας (πραγματικής πληροφορίας), που υπάρχει στο αρχικό κείμενο, και της εντροπίας του κλειδιού κρυπτογράφησης, να ισούται με τον αριθμό των bit του κρυπτογραφήματος που χρησιμοποιούμε. Έπειτα έδειξε ότι κρυπτογραφήματα με μήκος μεγαλύτερο της απόστασης αυτής, είναι σχεδόν σίγουρο ότι έχουν μία μοναδική λογική αποκρυπτογράφηση. Κρυπτογραφήματα αρκετά μικρότερα της απόστασης αυτής ενδέχεται να έχουν πολλαπλές, το ίδιο πιθανές αποκρυπτογραφήσεις. Ως εκ τούτου είναι πιο ασφαλή, καθώς ο αντίπαλος έχει δυσκολία να διαλέξει τη σωστή αποκρυπτογράφηση.

Η απόσταση μοναδικότητας υπολογίζεται, για τα περισσότερα κρυπτοσυστήματα, ως ο λόγος της εντροπίας του κρυπτοσυστήματος προς τον πλεονασμό της γλώσσας.

$$U = H(K)/D$$

Η απόσταση μοναδικότητας δεν παράγει απόλυτες προβλέψεις, αλλά δίνει πιθανολογικά αποτελέσματα. Η απόσταση μοναδικότητας υπολογίζει την ελάχιστη ποσότητα κρυπτογραφήματος για το οποίο το πιθανότερο είναι να υπάρχει ένα μοναδικό λογικό αρχικό κείμενο στο οποίο να αποκρυπτογραφείται. Γενικά, όσο μεγαλύτερη η απόσταση αυτή, τόσο καλύτερο είναι το κρυπτοσύστημα. Η κρυπτογράφηση αγγλικού κειμένου με τον DES (που έχει 56 bit κλειδί) έχει απόσταση μοναδικότητας περίπου 8,2 χαρακτήρες ή 66 bit. Ο πίνακας 3.1 δίνει την απόσταση μοναδικότητας για διάφορα κλειδιά.

Πίνακας 3.1
Αποστάσεις μοναδικότητας κειμένων ASCII κρυπτογραφημένα

Μήκος κλειδιού (σε bit)	Απόσταση μοναδικότητας (σε χαρακτήρες)
40	5,9
56	8,2
64	9,4
80	11,8
128	18,8
256	37,6

Η απόσταση μοναδικότητας δεν είναι μέτρο της ποσότητας κρυπτογραφήματος απαιτείται για κρυπτανάλυση, αλλά της ποσότητας κρυπτογραφήματος που

απαιτείται για να υπάρχει μία μοναδική λύση για την κρυπτανάλυση. Ένα κρυπτοσύστημα μπορεί να είναι υπολογιστικά δύσκολο να αναλυθεί, ακόμη κι αν είναι θεωρητικά δυνατόν να σπαστεί με μικρή ποσότητα κρυπτογραφήματος. Η απόσταση μοναδικότητας είναι αντιστρόφως ανάλογη προς τον πλεονασμό. Καθώς ο πλεονασμός πλησιάζει το μηδέν, ακόμη κι ένας απλός κώδικας μπορεί να είναι άσπαστος με μια επίθεση κρυπτογραφήματος.

Ο Shannon όρισε ότι ένα σύστημα παρέχει ιδανική μυστικότητα, όταν η απόσταση μοναδικότητάς του είναι άπειρη. Ένα ιδανικό κρυπτοσύστημα δεν είναι και τέλειο, αλλά ένα τέλειο κρυπτοσύστημα είναι σίγουρα ιδανικό. Αν ένα κρυπτοσύστημα παρέχει ιδανική μυστικότητα, ακόμη και η επιτυχής κρυπτανάλυσή του δεν μπορεί να καθορίσει με απόλυση σιγουριά αν το ανακτημένο κείμενο είναι το αρχικό κείμενο.

3.1.5 Σύγχυση και διάχυση

Οι δύο βασικές τεχνικές συγκάλυψης του πλεονασμού σε ένα κείμενο είναι, κατά τον Shannon, η σύγχυση και η διάχυση.

Η σύγχυση συγκαλύπτει την σχέση ανάμεσα στο αρχικό κείμενο και το κρυπτογράφημα. Στην ουσία δημιουργεί σύνθετες και περίπλοκές συναρτησιακά

σχέσεις του κρυπτοκειμένου και του κλειδιού για παράδειγμα σε ένα κρυπτοσύστημα μονοαλφαβητικής αντικατάστασης είναι εύκολο να περιγράψουμε το κλειδί δεδομένου του πιο συχνά επαναλαμβανόμενου γράμματος πχ για την αγγλική γλώσσα είναι το Ε. Αν η σύνδεση μεταξύ τους είναι αρκετά σύνθετη και περίπλοκη ο κρυπταναλυτής θα μπορούσε να εκτιμήσει το στατιστικό περιεχόμενο S1 για να περιορίσει το κλειδί σε μία περιοχή αλλά αυτό θα τον οδηγούσε σε ένα σύνθετο κλειδοχωρο πχ R μία καινούργια στατιστική ανάλυση θα τον οδηγούσε σε ένα καινούργιο περιεχόμενο S2 το οποίο θα περιόριζε το κλειδί σε μία καινούργια περιοχή πχ R2 αλλά η δυσκολία θα ήταν να εκτιμήσει σε ποια περιοχή θα ήταν. Ένα επιπλέων χαρακτηριστικό είναι ότι κάθε αλλαγή σε ένα χαρακτήρα είτε του κλειδιού είτε του μηνύματος θα επηρέαζε όλα τα στοιχεία του κρυπτοκειμένου και αυτή η αλλαγή στο κρυπτοκείμενο θα είχε χαρακτηριστικά τυχαιότητας .

$$c_1 = f_1(m_1, m_2, ...m_n; k_1..k_s)$$
$$c_2 = f_2(m_1, m_2, ...m_n; k_1..k_s)$$

Αυτό καθιστά δύσκολες τις προσπάθειες για ανάλυση του κρυπτογραφήματος ψάχνοντας για πλεονασμούς και στατιστικά χαρακτηριστικά.

Η διάχυση εξασθενει τον πλεονασμό του κειμένου, διαχέοντας τον μέσα στο κρυπτογράφημα. Το αποτέλεσμα είναι ότι ο κρυπταναλυτής χρειάζεται πολύ μεγάλο όγκο πληροφορίας για να σχηματίσει ξανά την στατιστική δομή του μηνύματος και αυτό έχει συμβεί γιατί οι σχετικές συχνότητες των γραμμάτων έχουν κατανεμηθεί με τρόπο που τείνει να γίνουν περίπου ισοπιθανες., το ίδιο και οι διαγραμματικές συχνότητες Ο ευκολότερος τρόπος να το πετύχουμε είναι με αντικατάσταση. Ένα απλό παράδειγμα σύγχυσης της στατιστικής ανάλυσης είναι η αθροιστική λειτουργία σε ένα μήνυμα.

$$y_n = \sum_{i=1}^{s} m_{n+i} \bmod 26$$

Προσθέτοντας s συνεχόμενα γράμματα για να πάρουμε ένα γράμμα y_n. Στην ουσία αυτή η πράξη καταστρέφει την στατιστική δομή της γλώσσας .Αυτές οι ακολουθίες γραμμάτων τείνουν να είναι τυχαίες χωρίς να έχουν μια στατιστική εξάρτηση δηλαδή η εμφάνιση ενός γράμματος δεν επηρεάζει την εμφάνιση ενός άλλου γράμματος .πχ Η εμφάνιση του του Q δεν συνεπάγει ότι το αμέσως πιθανότερο γράμμα είναι το U πλέον . Τα γράμματα δεν διατηρούν την φυσική τους σειρά άρα και τις διαγραμματικές πιθανότητες Ο απλούστερος τρόπος να πετύχουμε διάχυση είναι η μετάθεση (transposition ή permutation). Ένας απλός αλγόριθμος μετάθεσης απλά αλλάζει την θέση των γραμμάτων στο κείμενο. Οι σημερινοί αλγόριθμοι εφαρμόζουν αυτό το είδος μετάθεσης, αλλά χρησιμοποιούν και άλλες μορφές διάχυσης, όπου κομμάτια του κειμένου διαχέονται σε όλο το κείμενο. Οι αλγόριθμοι μπλοκ χρησιμοποιούν τόσο σύγχυση όσο και διάχυση. Γενικά, η διάχυση από μόνη της είναι εύκολο να αναλυθεί

3.1.6 Άλγεβρα Κρυπτοσυστημάτων

Έστω ένα κρυπτοσύστημα μπορεί να αναπαρασταθεί σαν ένα σύνολο μετασχηματισμών από ένα σύνολο σε ένα άλλο. Υπάρχουν δύο συνδετικές λειτουργίες οι οποίες σχηματίζουν ένα τρίτο κρυπτοσύστημα Τ από δύο άλλα .

Ο πρώτος τρόπος καλείται λειτουργία γινομένου κατά την οποία ένα μήνυμα κρυπτογραφείται από το πρώτο σύστημα R και στην συνέχεια το αποτέλεσμα λαμβάνεται σαν είσοδος από το δεύτερο κρυπτοσύστημα S. Τα κλειδιά μπορούν να επιλεγούν ανεξάρτητα .

$$T = S \times R$$

Ο δεύτερος τρόπος είναι η λειτουργία «Πρόσθεση βαρών» κατά την οποία προ-επιλέγονται ποιο σύστημα θα χρησιμοποιηθεί με πιθανότητες p,q αντίστοιχα.

$T = p*R + q*S$ $T = p*R + q*S$ όπου p+q=1.

Οι συνθετικές λειτουργίες μας δίνουν ένα νέο τρόπο για την σύνθεση νέων τύπων κρυπτοσυστημάτων από τα ήδη υπάρχοντα. Αυτή η νέα σύνθεση έχει ως αποτέλεσμα την ενίσχυση χαρακτηριστικών όπως η υψηλή σύγχυση και διάχυση. Τα πιο κοινά χρησιμοποιούμενα είναι τα κρυπτοσυστήματα γινομένου πχ Αντικατάσταση-Μετάθεση ή Μετάθεση –Τετράγωνο Viginere

Η λειτουργία του πολλαπλασιασμού έχει τα παρακάτω χαρακτηριστικά

- $R \times S \neq S \times R$ σε μερικές περιπτώσεις ισχύει η ισότητα πχ Αντικατάσταση και στην συνέχεια μετάθεση.
- $R*(S*T) = (R*S)*T = R*S*T$
- Αν οι εσωτερικοί μετασχηματισμοί Ri, Si και αντιμεταθετικοί τότε και τα συστήματα αντιμεταθετικά
- Αν T*T=T τότε το σύστημα είναι ισοδύναμο πχ Αντικατάσταση , Μετάθεση, Τετράγωνο Vigenere.

Ο Shannon πρότεινε την συνθετικη λειτοργία του πολλαπλασιασμού για την δημιουργία κρυπτοσυστημάτων με πίο ισχύρα χαρακτηριστικά δημιουργόντας τα με την επανάληψη κάποιων βασικών κρυπτοσυστημάτων πχ αντικατάστασης – αναδιάταξης.

Τα βασικά χαρακτηριστικά ενός σύνθετου κρυπτοσυστήματος είναι:

1. Το σύνθετο κρυπτοσύστημα δεν θα πρέπει να αποτελείται από ένα βασικό τύπο πχ Ενα κρυπτοσύστημα αναδιάταξης όταν χρησιμοποιειθει δύο φόρες δεν παρέχει μεγαλύτερη ισχύ. Δυο διαδοχικές αναδιατάξεις μπορούν να αντικατασταθούν από μία ισοδύναμη αναδιάταξη $T*T = T^2 = T$. Το ίδιο συμβαίνει με δύο διαδοχικές αντικαταστάσεις. Η λειτουργία του πολλαπλασιασμού δεν δημιουργεί ένα νέο κρυπτοσύστημα που ανήκει σε μια διαφορετική κλάση. Άρα επαναλαμβάνοντας την διαδικασία του πολλαπλασιασμού σε ένα ισοδύναμο κρυπτοσύστημα δεν προσθέτει περισσότερη ασφάλεια στο νέο κρυπτοσύστημα απλά χρησιμοποιεί επιπλέων τμήμα κλειδιών.
2. Τα απλά κρυπτοσυστήματα που χρησιμοποιούνται δεν θα πρέπει να τηρούν το κριτήριο της αντιμετάθεσης μεταξύ τους δηλαδή θα πρέπει $\text{ΚΣ}_1 \times \text{ΚΣ}_2 \neq \text{ΚΣ}_2 \times \text{ΚΣ}_1$.Το κριτήριο χρησιμεύει στην διάκριση ενός σύνθετου κρυπτοσυστήματος αν είναι ισοδύναμο ή όχι. πχ Τα περισσότερα βασικά κρυπτοσυστήματα πχ Αντικατάστασης-Αφινικό –Ηιλλ-Τετραγώνου-Μετατόπισης-Αναδιάταξης σχηματίζουν κλάσης ισοδυναμίας.. Έστω ότι έχω δύο κρυπτυοσυστήματα $\text{ΚΣ}_1, \text{ΚΣ}_2$ κάθε ένα σχηματίζει με την συνθετική λειτουργία ένα σύστημα ισοδυναμίας και τα δύο ικανοποιούν το κριτήριο της

αντιμετάθεσης $K\Sigma_1 \times K\Sigma_2 = K\Sigma_2 \times K\Sigma_1$ τότε το νέο σύνθετο κρυπτοσύστημα $(K\Sigma_1 \times K\Sigma_2)$ είναι ένα σύστημα ισοδυναμίας.

Ο τρόπος σύνθεσης που υπέδειξε ο Shannon είναι

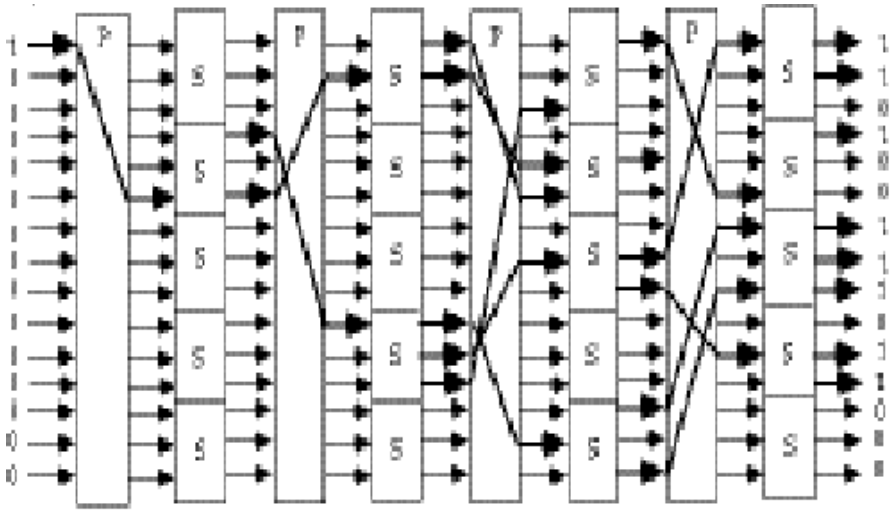
$F = LSLSLT$

Όπου L είναι μια γραμμική λειτουργία S είναι η αντικατάσταση και T είναι η αναδιάταξη.

3.2 Δίκτυα Αντικατάστασης – Μετάθεσης ΔΑΜ

Ο Shannon με την εργασία του **Communication Theory of Secrecy Systems** Υπέδειξε μία επαναληπτική συνάρτηση που τα στοιχεία ήταν μία αντικατάσταση ακολουθούμενη από μία αναδιάταξη ή αλλιώς μετάθεση .Ένας από τους λόγους που κάνει πιο ισχυρή την προηγούμενη διάταξη κρυπταναλυτικά είναι ότι ενώ ένα σύστημα αντικατάστασης μπορεί να αναλυθεί μέσω μιας στατιστικής ανάλυσης σε ένα σύστημα αναδιάταξης η στατιστική ανάλυση δεν έχει καμία επιτυχία. .Η δομή αυτή έχει στόχο την

- Υψηλή διάχυση (υλοποιείται με μεταθέσεις)
- Υψηλή σύγχυση (υλοποιείται με αντικαταστάσεις)



Σχήμα 3.2 Δίκτυο Αντικατάστασης Μετάθεσης

Ένας γύρος ορίζεται από μια σειρά κουτιών αντικατάστασης συνοδευμένο από μία συνάρτηση μετάθεση παράμετροι που ορίζουν ένα ΔΑΜ είναι το μήκος της εισόδου n ο αριθμός των γύρων r και το μέγεθος των κουτιών αντικατάστασης m*m

3.2.1 Κουτιά αντικατάστασής (S-boxes)

Τα κουτιά αντικατάστασης είναι ένα μη γραμμικό στοιχείο σε ένα κρυπταλγόριθμο. Το μέγεθος την κουτιών αντικατάστασης ορίζεται από των αριθμό των bits εισόδου και από τον αριθμό των bits εξόδου Adams και ο Traveres έθεσαν τα κρυπτογραφικά κριτήρια τα οποία πρέπει να τηρεί ένα κουτί αντικατάστασης

1. Μη γραμμικότητα(Non linearity) : Ορίζει το βαθμό της μη γραμμικότητας στην σχέση (εισόδου –εξόδου) . Προτάθηκαν η συμπλήρωση κουτιών με τιμές οι οποίες είναι τα παράγωγα ειδικών συναρτήσεων (Bent Boolean Functions).Το χαρακτηριστικό των τιμών αυτών είναι ότι έχουν ίδια απόσταση από όλες τις γραμμικές συναρτήσεις της ίδιας τάξης αυτό μεταφράζεται σαν μη γραμικκότητα δηλαδή πόσο μια τιμή των bent συναρτήσεων πλησιάζει κοντά σε μια γραμμική συνάρτηση. άρα η συνέλιξη με όλες τις γραμμικές συναρτήσεις δείχνει το είδος της συσχέτισης .
2. Αμφίεση(Bijection) : Το κριτήριο αυτό είναι απαραίτητο για να ορίζεται μονοσήμαντα η αποκρυπτογράφηση. Δεν μπορεί 2 διαφορετικές είσοδοι να βγάζουν την ίδια έξοδο.Οταν έχω δίκτυα τύπου Feistel δεν χρειάζεται τα κουτιά αντικατάστασης να τηρούν το κριτήριο αυτό.
3. Αυστηρή Χιονοστιβάδα (Strict Avalanche Criterion) Για οποιαδήποτε αλλαγή σε ένα ψηφίο εισόδου προκαλείται αντιστροφή σε κάθε bit εξόδου με πιθανότητα. Αυτό το κριτήριο δημιουργήθηκε για την μεγιστοποίηση του χαρακτηριστικού στης σύγχυσης.
4. Ανεξαρτησία των ψηφίων της εξόδου(Bit Independence effect) Αυτό το κριτήριο αναφέρει ότι δεν θα πρέπει να εμφανίζεται σχέσεις μεταξύ bits της εξόδου η αυτοσυσχετηση μεταξύ δύο η περισσότερων bits της εξόδου μειώνει τον χώρο αναζήτησης

Οι προσεγγίσεις για την δημιουργία των κουτιών αντικατάστασης είναι:

- Τυχαία
- Τυχαία με έλεγχο
- Δημιουργία από άνθρωπο
- Δημιουργία από μαθηματικά

3.2 Σκελετός τύπου Feistel

Οι περισσότεροι αλγόριθμοι μπλοκ είναι δίκτυα Feistel (Feistel networks). Η ιδέα εμφανίστηκε στις αρχές της δεκαετίας του ’70. Η λογική είναι η εξής: Παίρνουμε ένα μπλοκ μήκους n και το διαιρούμε σε δύο μισά μήκους n/2, L και R. Φυσικά το n πρέπει να είναι άρτιος αριθμός. Έπειτα ορίζουμε έναν επαναλαμβανόμενο αλγόριθμο μπλοκ, όπου το αποτέλεσμα του γύρου i εξαρτάται από το αποτέλεσμα του προηγούμενου γύρου: $L_i = R_{i-1}$

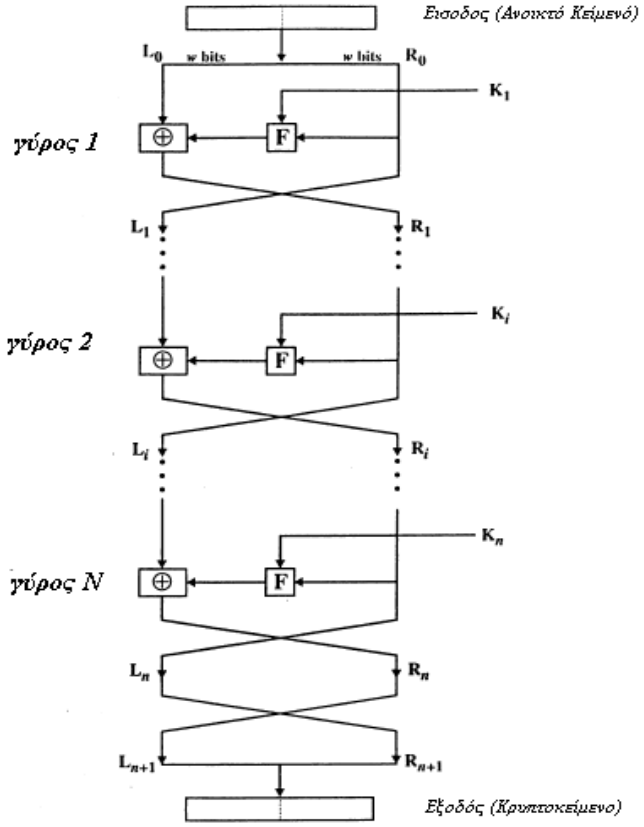
$$R_i = L_{i-1} \ f(R_{i-1}, K_i)$$

K_i είναι το υπο-κλειδί που χρησιμοποιείται κατά τον γύρο i και f είναι μια οποιαδήποτε επαναλαμβανόμενη συνάρτηση (round function).

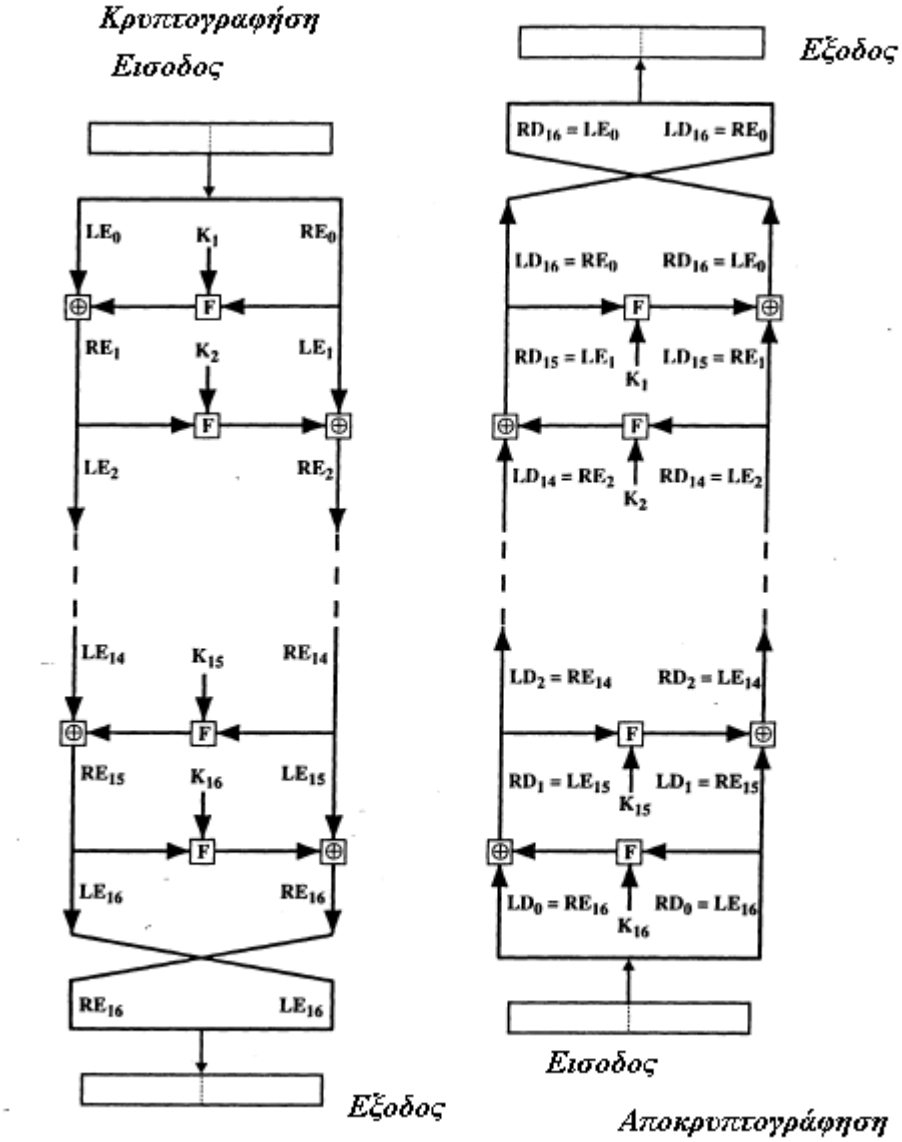
Η ιδέα αυτή εφαρμόζεται στον DES, αλλά και σε άλλους αλγόριθμους (Lucifer, FEAL, Khufu, Khafre, LOKI, GOST, CAST, Blowfish κα.) Έχει τόσο μεγάλη απήχηση, επειδή είναι αντιστρέψιμη συνάρτηση. Επειδή χρησιμοποιείται το XOR για να συνδυάσει το αριστερό μισό με το αποτέλεσμα της συνάρτησης f, ισχύει οπωσδήποτε ότι

$$L_{i-1} \; *f(R_{i-1}, K_i) * f(R_{i-1}, K_i) = L_{i-1}$$

Ένας αλγόριθμος που χρησιμοποιεί αυτή τη διάταξη είναι εγγυημένο ότι είναι αντιστρεπτός, αν η είσοδος της συνάρτησης f για κάθε γύρο μπορεί να δημιουργηθεί ξανά. Δεν έχει σημασία τι είναι η συνάρτηση f· δεν χρειάζεται να είναι αντιστρέψιμη. Μπορούμε να σχεδιάσουμε την f να είναι όσο πολύπλοκη θέλουμε, και δεν χρειάζεται να υλοποιήσουμε δύο διαφορετικούς αλγόριθμους για κρυπτογράφηση και αποκρυπτογράφηση



Σχήμα 3.3 Κλασική δομή feistel



Σχήμα 3.4 Σκελετός τύπου Feistel

Νούμερο Γύρων

Έχει αποδειχθεί ερευνητικά ότι όσο αυξάνουν οι γύροι σε ένα δίκτυο τύπου feistel αυξάνεται η δυσκολία της κρυπτανάλυσης.Το κριτήριο που εξάγεται είναι ότι το νούμερο των γύρων επιλέγεται ώστε ο παράγοντας εργασίας των μορφών κρυπταναλυσης να είναι συγκρίσιμος ή μεγαλύτερος από τον παράγοντα εργασίας της επίθεσης ωμής βίας(brute force attack)

4

4.1 Συμμετρικοί κρυπταλγόριθμοι

Οι συμμετρικοί αλγόριθμοι εμφανίστηκαν στην μηχανοποιημένη μορφή στην δεκαιτεία του 70.Χωρίζονται σε δυο μεγάλες κατηγορίες ανάλογα με τον τρόπο που χειρίζονται το κείμενο προς επεξεργασία

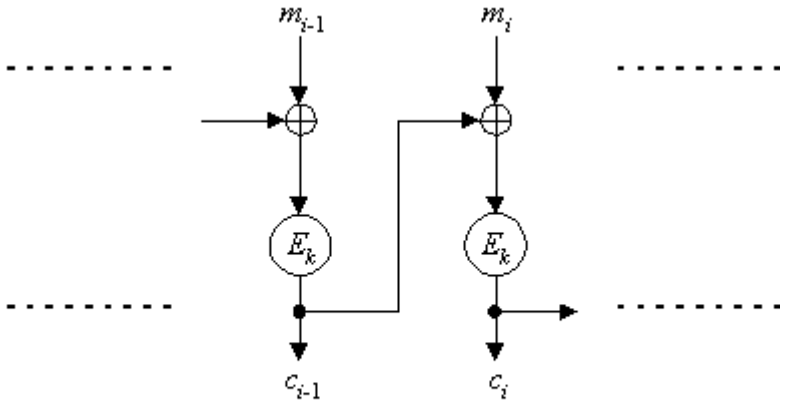
- Κρυπταλγόριθμοι ροής (Stream Ciphers)
- Κρυπταλγόριθμοι Τμήματος (Block Ciphers)

Οι αλγόριθμοι ροής εφαρμόζονται πάνω στην μικρότερη μονάδα ενός ψηφιακού συστήματος τα δυαδικά ψηφία (bits).Ενώ οι κρυπταλγόριθμοι τμήματος εφαρμόζονται με μονάδα επεξεργασία τις ψηφιακές λέξεις δηλαδή συστάδες από δυαδικά ψηφία μεγαλύτερη ασφάλεια των κρυπταλγορίθμων τμήματος τους καθιστούν πιο συχνά χρησιμοποιούμενους .Ένας κρυπταλγόριθμος τμήματος είναι μια επαναληπτική διαδικασία μίας κλάσης συναρτήσεων στις οποίες ρέει η πληροφορία διαδοχικά και μετασχηματίζεται. Το αποτέλεσμα αποτελεί την σύνθετη πολλαπλασιαστική δομή κατά Shannon.Η κάθε επανάληψη ονομάζεται γύρος του κρυπταλορίθμου Ο καινούργιος γύρος τροφοδοτείται με τα αποτέλεσμα του προηγούμενου καθώς επίσης και με ένα κλειδί που ονομάζεται κλειδί γύρου.Τα κλειδιά γύρου δημιουργούνται από ένα πρόγραμμα κλειδιού το οποίο συνήθως είναι εκτός του σκελετού του αλγορίθμου Η διαδικασία υπολογισμού των υποκλείδιων κάθε γύρου γίνεται στην αρχή για λόγους ταχύτητας

4.1.1 Τρόποι λειτουργίας

Ένας αλγόριθμος τύπου block cipher έχει διάφορους τρόπους λειτουργίας. Κάθε τρόπος λειτουργίας μπορεί να έχει τις δικές του ιδιότητες εκτός από αυτές που κληρονομεί από τον βασικό cipher. Οι βασικοί τρόποι λειτουργίας είναι: ο *Electronic Code Book (ECB)*, ο *Cipher Block Chaining (CBC)*, ο *Cipher Feedback (CFB)* και ο *Output Feedback (OFB)*.

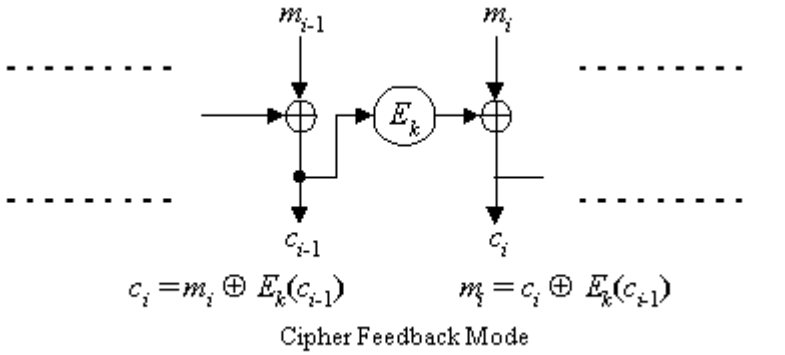
Σε ECB mode, το κείμενο χωρίζεται σε ισομήκη block. Κάθε μη κρυπτογραφημένο block κρυπτογραφείται ανεξάρτητα από την συνάρτηση του βασικού block cipher. Μειονέκτημα αυτού του τρόπου είναι ότι ομοιότητες του plaintext δεν καλύπτονται. Τα plaintext block που είναι ταυτόσημα, δίνουν ταυτόσημα ciphertext block και το κείμενο μπορεί εύκολα να τροποποιηθεί με την αφαίρεση, πρόσθεση ή και ανακατάταξη των όμοιων ciphertext block. Η ταχύτητα της κρυπτογράφησης κάθε plaintext block είναι ίδια με την ταχύτητα του block cipher. Ο ECB επιτρέπει την παράλληλη παραγωγή των ciphertext blocks για καλύτερη απόδοση.



Cipher Block Chaining

Σε CBC mode, κάθε μη κρυπτογραφημένο block συνδυάζεται μέσω της λογικής πράξης X-OR με το πρωτύτερα κρυπτογραφημένο block. Το αποτέλεσμα κρυπτογραφείται. Απαιτείται μια αρχική τιμή για την πρώτη X-OR πράξη που καλείται *Initialization Vector*, c_0. Τα όμοια plaintext blocks καλύπτονται με την χρήση της λογικής πράξης και αυξάνεται η ασφάλεια του αλγόριθμου. Η ταχύτητα της κρυπτογράφησης είναι ίδια με αυτή του block cipher, αλλά η διαδικασία δεν μπορεί να πραγματοποιηθεί παράλληλα παρ' όλο που η αποκρυπτογράφηση μπορεί.

Σε CFB mode, το προηγούμενο ciphertext block κρυπτογραφείται και το αποτέλεσμα που παράγεται συνδυάζεται με το επόμενο plaintext block με χρήση μιας X-OR. Η έξοδος της X-OR αποτελεί το νέο ciphertext block που θα κρυπτογραφηθεί, συνεχίζοντας την διαδικασία. Γίνεται η ποσότητα που χρησιμοποιείται για ανάδραση *(feedback)* να μην είναι ένα πλήρες block.Απαιτείται ένας Initialization Vector c_0 για την πρώτη X-OR πράξη.

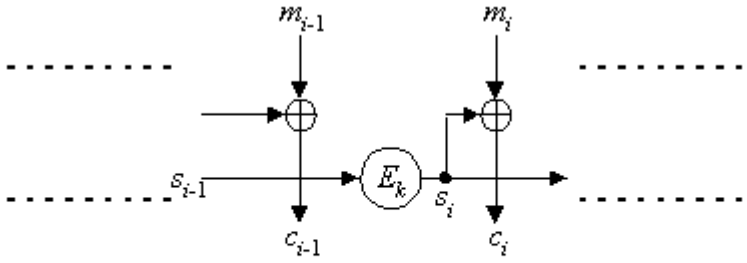


Cipher Feedback Mode

Με αυτόν τον τρόπο καλύπτονται πιθανές ομοιότητες στα plaintext blocks μέσω της X-OR. Γίνεται, όμως, στην πλήρη ανάδραση τα c_i και c_{i-1} να είναι ταυτόσημα. Σαν συνέπεια και το επόμενο ζεύγος κρυπτογραφημένων block θα είναι ταυτόσημα μεταξύ τους. Αυτό το πρόβλημα λύνεται με την χρήση μερικής ανάδρασης. Η ταχύτητα της κρυπτογράφησης είναι ίδια με αυτή του block cipher και δεν επιτρέπεται παράλληλη επεξεργασία.

Σε OFB mode, η διαδικασία είναι παρόμοια με αυτήν του CFB mode, με την διαφορά ότι η ποσότητα που συνδυάζεται με X-OR με κάθε plaintext block παράγεται ανεξάρτητα από τα plaintext και ciphertext. Ένας Initialization Vector s_0 χρειάζεται για να ξεκινήσει την διαδικασία και κάθε block s_i προκύπτει από την κρυπτογράφηση του προηγούμενου s_{i-1}. Η κρυπτογράφηση plaintext block γίνεται με τον συνδυασμό κάθε plaintext block μέσω μιας X-OR, με το κρυπτογραφημένο s.

Η ανάδραση με block όχι πλήρη δεν συνιστάται για λόγους ασφάλειας. Ο OFB mode έχει το εξής πλεονέκτημα σε σχέση με τον CFB. Τα πιθανά λάθη μετάδοσης δεν πολλαπλασιάζονται κατά την αποκρυπτογράφηση και έτσι δεν την επηρεάζουν. Το κείμενο, όμως, μπορεί εύκολα να αλλοιωθεί με την αφαίρεση, πρόσθεση ή και ανακατάταξη όμοιων ciphertext block. Δεν είναι δυνατή η παράλληλη επεξεργασία, αλλά η διαδικασία μπορεί να επιταχυνθεί με την παραγωγή των κρυπτογραφημένων s πριν τα δεδομένα να είναι διαθέσιμα για κρυπτογράφηση.



Output Feedback Mode

Άλλος ένας τρόπος λειτουργίας είναι ο *Propagating Cipher Block Chaining (PCBC)*. Χρησιμοποιείται με πρωτόκολλα όπως το Kerberos version 4, ενώ δεν έχει επίσημα τυποποιηθεί ούτε χαίρει παγκόσμιας αναγνώρισης. Είναι παρόμοιος με το CBC και έχει σχεδιασθεί με σκοπό να αναπαράγει το πιθανό λάθος μετάδοσης έτσι ώστε να γίνεται αντιληπτό και το κείμενο που προκύπτει να απορρίπτεται. Η μέθοδος της $c_i = E_k(m_i \oplus m_{i-1} \oplus c_{i-1})$ κρυπτογράφησης δίνεται από την εξίσωση:

και η αποκρυπτογράφηση επιτυγχάνεται με τον εξής υπολογισμό:

$m_0 \oplus c_0\ m_i = D_k(c_i) \oplus c_{i-1} \oplus m_{i-1}$ όπου είναι ο Initialization Vector.

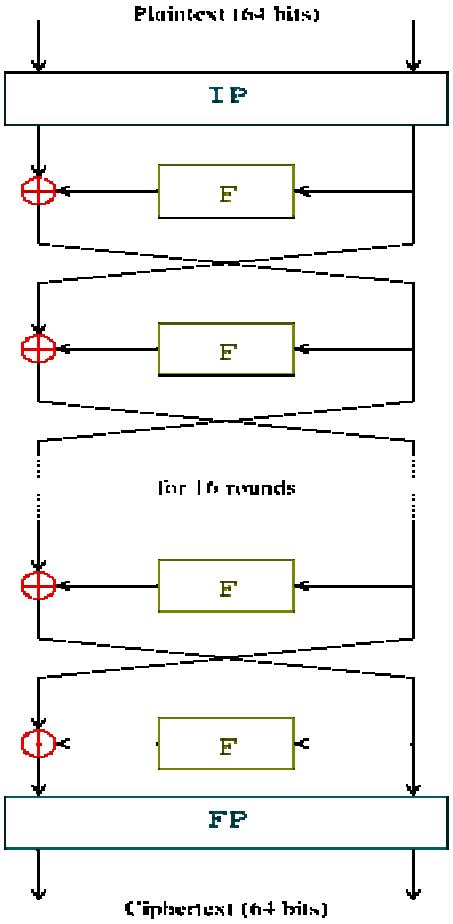
4.2 Κρυπταλγόριθμός DES

Ο Κρυπταλγόριθμος DES δημοσιεύτηκε το 1977 και σχεδιάστηκε με βάση τα κριτήρια σχεδιασμού τα οποία διατυπώθηκαν 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

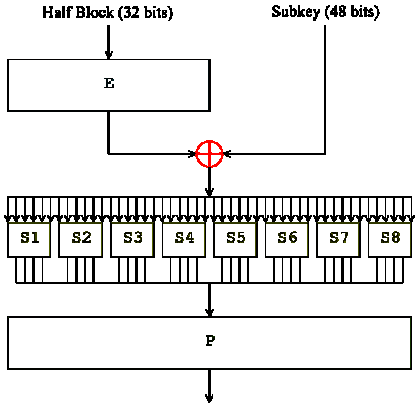
- Υψηλό επίπεδο ασφάλειας
- Πλήρεις και διαφανείς προδιαγραφές
- Η ασφάλεια δεν θα πρέπει να εξαρτάται από την μυστικότητα του αλγορίθμου
- Διαθέσιμο και προσβάσιμο από όλους τους χρήστες
- Κατάλληλο για ποικιλία εφαρμογών
- Χαμηλό κόστος Υλοποίησης
- Να επιτρέπεται η εξαγωγή του
- Να είναι δυνατή η αξιολόγηση του

4.2.1 Περιγραφή του DES

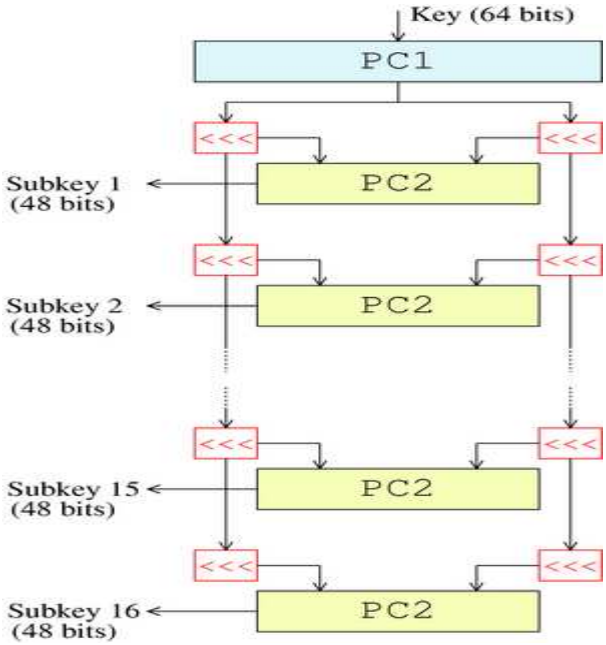
Ο DES είναι block cipher, πιο συγκεκριμένα Feistel cipher, με μέγεθος block 64 bit. Χρησιμοποιεί κλειδί 64 bits από τα οποία τα 8 αποτελούν bits ισοτιμίας. Όταν χρησιμοποιείται για την επικοινωνία, αποστολέας και παραλήπτης μοιράζονται το ίδιο κλειδί. Ο DES, εκτός από κρυπτογράφηση, μπορεί να χρησιμοποιηθεί στην παραγωγή MACs (σε CBC mode). Επίσης, μπορεί να χρησιμοποιηθεί για κρυπτογράφηση αρχείων αποθηκευμένα σε σκληρό δίσκο σε περιβάλλοντα ενός χρήστη. Για την διανομή των κλειδιών σε περιβάλλον πολλών χρηστών, συνδυάζεται με ασύμμετρο κρυπτοσύστημα



Σχήμα 4.1 Σκελετός DES αλγορίθμου



Σχήμα 4.2 Η συνάρτηση F του DES αλγορίθμου



Σχήμα 4.3 Πρόγραμμα κλειδιών DES

Triple-DES

Είναι μια παραλλαγή του DES όπου το μήνυμα κρυπτογραφείται και αποκρυπτογραφείται διαδοχικά με διαφορετικά κλειδιά για την ενίσχυση του βασικού αλγόριθμου. Υπάρχουν τέσσερις διαφορετικοί τρόποι για να επιτευχθεί αυτό:

- DES-EEE3 *(Encrypt-Encrypt-Encrypt)*: πραγματοποιούνται τρεις συνεχόμενες κρυπτογραφήσεις με το τρία διαφορετικά κλειδιά.
- DES-EDE3 *(Encrypt-Decrypt-Encrypt)*: το μήνυμα διαδοχικά κρυπτογραφείται, αποκρυπτογραφείται και τέλος κρυπτογραφείται με χρήση τριών διαφορετικών κλειδιών.
- DES-EEE2: είναι η ίδια με την πρώτη διαδικασία εκτός του ότι απαιτούνται δύο διαφορετικά κλειδιά.
- DES-EDE2: είναι η ίδια με την δεύτερη διαδικασία εκτός του ότι απαιτούνται δύο κλειδιά.

Τα επιπλέον κλειδιά δημιουργούνται από το κοινό μυστικό κλειδί με κατάλληλο αλγόριθμο. Από αυτούς τους τρόπους, ο πιο ασφαλής είναι ο DES-EEE3, με την τριπλή κρυπτογράφηση και τα τρία διαφορετικά κλειδιά.

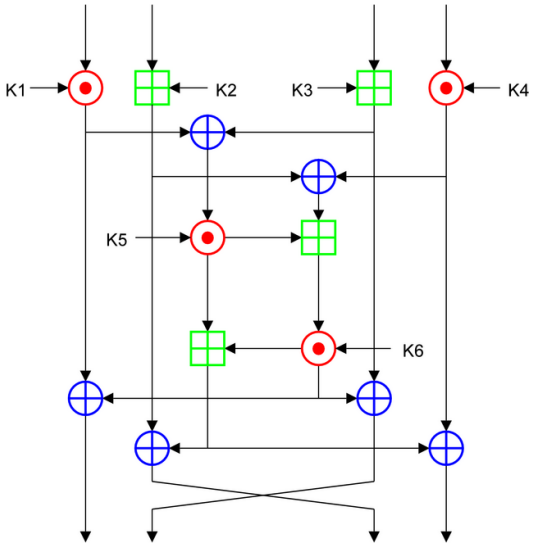
DESX

Ο DESX είναι μια άλλη παραλλαγή του DES. Η διαφορά του DES και του DESX είναι ότι η είσοδος στο DESX περνάει από μια X-OR πράξη με ένα επιπλέον κλειδί

64 bits και ομοίως η έξοδος της κρυπτογράφησης. Η αιτία ανάπτυξης του DESX είναι η δραματική αύξηση της αντοχής του DES σε γνωστές επιθέσεις.

IDEA (International Data Encryption Algorithm)

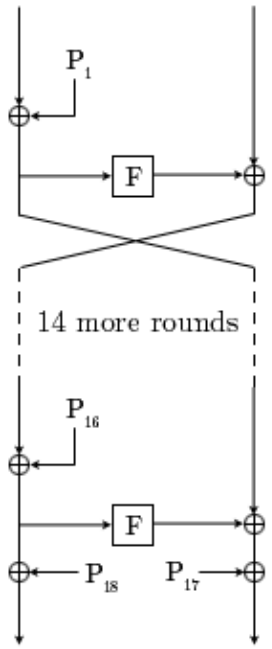
Ο IDEA είναι ένας block cipher που αναπτύχθηκε από τους Lai και Massey. Χρησιμοποιεί block μεγέθους 64 bits και κλειδιά 128 bits. Η διαδικασία της κρυπτογράφησης απαιτεί 8 σύνθετες επαναλήψεις. Παρ' όλο που δεν έχει την κατασκευή ενός Feistel cipher, η αποκρυπτογράφηση γίνεται με τον ίδιο τρόπο που γίνεται και η κρυπτογράφηση. Έχει σχεδιαστεί για να εύκολα εφαρμόσιμος τόσο hardware σε όσο και σε software. Μερικές, όμως, αριθμητικές διεργασίες που χρησιμοποιεί ο IDEA καθιστούν τις λογισμικές εφαρμογές αργές, παρόμοιες σε ταχύτητα με τον DES. Ο IDEA αποτελεί ένα πολύ δυνατό αλγόριθμο που είναι απρόσβλητος από τα περισσότερα είδη επιθέσεων.



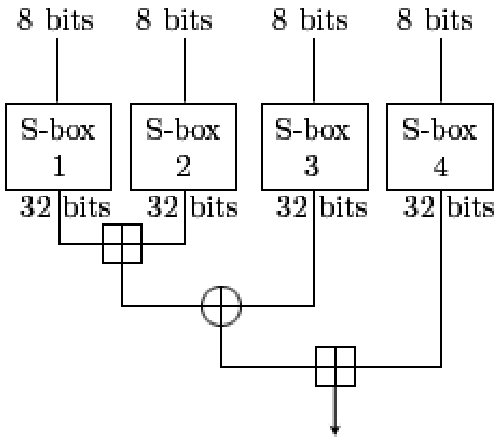
Σχήμα 4.4 Σκελετός IDEA αλγορίθμου

Blowfish

Ο Blowfish είναι ένας block cipher που κατασκευάστηκε από τον Schneier. Είναι ένας Feistel cipher με μέγεθος block 64 bits και μεταβλητό μήκος κλειδιού, με μέγιστο μήκος 448 bits. Όλες οι διεργασίες βασίζονται σε X-OR πράξεις και προσθέσεις λέξεων των 32 bits. Από το κλειδί παράγεται πίνακας με τα subkeys που χρησιμοποιούνται σε κάθε γύρο επανάληψης της κρυπτογράφησης. Έχει σχεδιασθεί για 32-bit μηχανές και είναι σημαντικά ταχύτερος από τον DES. Παρ' όλες τις αδυναμίες που έχουν ανακαλυφθεί καθ' όλη την διάρκεια της ύπαρξης του, θεωρείται ακόμα ασφαλής αλγόριθμος.



Σχήμα 4.5 Σκελετός Blowfish αλγορίθμου



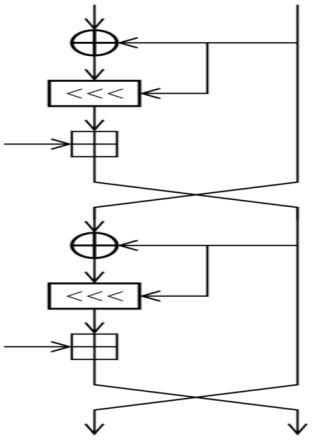
Σχήμα 4.6 Η συνάρτηση F του Blowfish αλγορίθμου

RC2, RC4, RC5

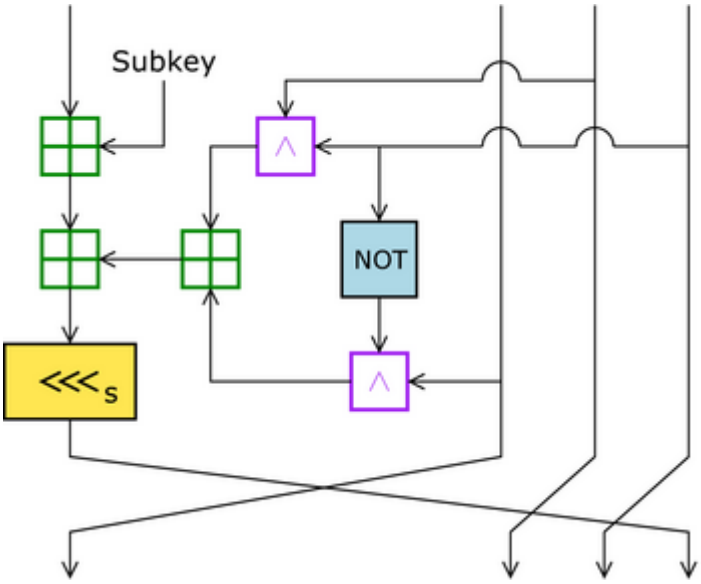
Ο RC2 είναι ένας block cipher με κλειδί μεταβλητού μήκους που σχεδιάστηκε από τον Ron Rivest για την RSA Inc. Τα αρχικά σημαίνουν "Ron's Code" ή "Rivest's Cipher". Είναι γρηγορότερος από τον DES και στόχος της σχεδίασης ήταν να λειτουργήσει για αντικατάσταση του DES. Μπορεί να γίνει περισσότερο ή λιγότερο ασφαλής από τον DES, ανάλογα με το μήκος του κλειδιού. Έχει μέγεθος block ίσο με 64 bits και είναι έως και τρεις φορές ταχύτερος από τον DES.

Ο RC4 είναι ένας stream cipher που σχεδιάστηκε πάλι από την Ron Rivest για λογαριασμό της RSA Inc. Έχει μεταβλητό μήκος κλειδιού και λειτουργεί στο επίπεδο του byte. Θεωρείται εξαιρετικά ασφαλής και οι υλοποιήσεις του σε λογισμικό τρέχουν πολύ γρήγορα. Χρησιμοποιείται για κρυπτογράφηση τοπικά αποθηκευμένων αρχείων και για την διασφάλιση της επικοινωνίας μεταξύ δύο απομακρυσμένων σημείων μέσω του πρωτοκόλλου SSL.

Ο RC5 είναι ένας γρήγορος block cipher από τον Ron Rivest για λογαριασμό της RSA Inc το 1994. Έχει πολλούς παραμέτρους: μεταβλητό μήκος κλειδιού, μεταβλητό μέγεθος block και μεταβλητό αριθμό επαναλήψεων. Τυπικές επιλογές για το μέγεθος του block είναι 32 bits (για πειραματικές εφαρμογές), 64 bits (για αντικατάσταση του DES) και 128 bits. Ο αριθμός των επαναλήψεων μπορεί να είναι από 0 έως και 255. Ο RC5 είναι πολύ απλός στην λειτουργία, πράγμα που τον κάνει εύκολο στην ανάλυση.



Σχήμα 4.7 Σκελετός RC5 αλγορίθμου



Σχήμα 4.8 Σκελετός RC2 αλγορίθμου

5

Ο Κρυπταλγόριθμος Hellas1

Ο hellas1 είναι μια πειραματική έκδοση ενός νέου αλγορίθμου που δημιουργήθηκε το 2005 για την ανάλυση χαρακτηριστικών τόσο της δομής feistel όσο και των επιμέρους στοιχείων.

5.1 Περιοχές Εφαρμογής

Ένας κρυπτογραφικός αλγόριθμος πρέπει να είναι κατάλληλος για ένα πλήθος εφαρμογών

- Κρυπτογράφησης δέσμης. Ο αλγόριθμος θα πρέπει να είναι αποτελεσματικός για κρυπτογράφηση αρχείων όσο και μιας συνεχόμενης ροής ψηφίων (bits)
- Γεννήτρια τυχαίων ψηφίων .Ο αλγόριθμος θα πρέπει να είναι αποτελεσματικός στην παραγωγή μια σειράς από τυχαία ψηφία(bits)
- Κρυπτογράφηση πακέτων . . Ο αλγόριθμος θα πρέπει να είναι αποτελεσματικός για την κρυπτογράφηση δεδομένα πακέτων
- Συνάρτηση κατακερματισμού . Ο αλγόριθμος θα πρέπει να είναι αποτελεσματικός στο να μετατρέπεται σε μονόδρομη συνάρτηση κατακερματισμού.

5.2 Πλατφόρμες Ανάπτυξης

Ένας κρυπτογραφικός αλγόριθμος πρέπει να υλοποιήσιμος σε μια ποικιλία διαφορετικών πλατφορμών ανάπτυξης.

- Ειδικό Υλικό(Hardware) . Ένας κρυπτογραφικός αλγόριθμος πρέπει να είναι αποδοτικός σε VLSI υλικό.
- Μεγάλους Επεξεργαστές. Ένας κρυπτογραφικός αλγόριθμος πρέπει να είναι αποδοτικός σε 32-bit επεξεργαστές με 4 kbyte πρόγραμμα .
- Μεσαίου μεγέθους Επεξεργαστές . Ένας κρυπτογραφικός αλγόριθμος πρέπει να μπορεί να τρέχει σε μικροελεκτές και άλλους μικροεπεξεργαστές
- Μικρούς Επεξεργαστές . Ένας κρυπτογραφικός αλγόριθμος πρεπει να μπορεί να υλοποιηθεί σε (Έξυπνες Κάρτες (smart cards).

5.3 Επιπλέων Απαιτήσεις

Ένας κρυπτογραφικός αλγόριθμος πρέπει να είναι κατάλληλος

- Ένας αλγόριθμος θα πρέπει να είναι απλός στον προγραμματισμό. Η εμπειρία με τον DES έδειξε ότι οι προγραμματιστές κάνουν συχνά λάθη υλοποίησης αν ο αλγόριθμος είναι πολύπλοκός.
- Ο αλγόριθμος πρέπει να έχει επίπεδη και ομοιόμορφη περιοχή κλειδοχώρου επιτρέποντας οποιαδήποτε τυχαία ψηφιοσειρά να μπορεί να είναι το πιθανό κλειδί .Δεν θα πρέπει να υπάρχουν αδύναμα κλειδιά
- Χρησιμοποίηση μίας σχεδίασης που είναι εύκολο να κατανοηθεί . Αυτό επιτρέπει την ανάλυση και αυξάνει την αυτοπεποίθηση στην ασφάλεια του αλγορίθμου.

5.4 Περιγραφή του αλγόριθμου - Αποφάσεις σχεδιασμού

Ο αλγόριθμός σχεδιάστηκε με μέγεθος πληροφορίας εισόδου 64 Bits ο λόγος που χρησιμοποίησα το μέγεθος αυτό είναι ότι ήθελα να είναι συμβατός με τους υπάρχων αλγορίθμους αλλά και να είναι εύκολο στο χειρισμό και να εμποδίζει την ανάλυση .Το μέγεθος του κλειδιού είναι 128bits το οποίο επιλέχθηκε σαν ελάχιστή πλέων τιμή ενός αλγορίθμου καθώς εμφανίζει μεγάλο παράγοντα εργασίας 2^{128} και καθιστά την επίθεση ωμής βίας μη πρακτική για τα τρέχων συστήματα . Από την πλευρά της σχεδίασης θα ήταν προτιμότερο για ένα μεταβλητό μήκος κλειδιού αλγόριθμό το οποίο θα εξυπηρετούσε διαφορετικές τάξης ασφάλειας εφαρμογές Επιλέχθηκε σαν σκελετός του αλγορίθμου ένα ισορροπημένο δίκτυο feistel δηλαδή τα δύο μισά του αλγορίθμου έχουν ίδιο μέγεθος ο λόγος που χρησιμοποίησα αυτή την δομή είναι ότι είναι η πιο αναλυμένη από πλευράς κρυπτανάλυσης και η πιο απλή και ο ίδιος αλγόριθμος χρησιμοποιείται για την κρυπτογράφηση και για την αποκρυπτογράφηση άρα από πλευράς υλικού δεν χρειάζεται άλλη σχεδίαση για την κρυπτογράφηση και άλλη για την αποκρυπτογράφηση. Τα ισορροπημένα δίκτυα από πλευράς κρυπτανάλυσης έχουν εμφανίσει καλύτερα κρυπτογραφικά στοιχεία ασφάλειας. Επέλεξα να έχει μεταβλητό αριθμό γύρων για να μπορέσω να μελετήσω κάποια χαρακτηριστικά όπως το φαινόμενο χιονοστιβάδας (κάθε δεξιό Bit εισόδου επηρεάζει κάθε αριστερό Bit εισόδου) και επιπλέων για να έχω την επιλογή διαφορετικών χρόνων εκτέλεσης του αλγορίθμου άρα και ταχύτητας του συνολικού αλγορίθμου. Η μη αναστρέψιμη συνάρτηση F σχεδιαστικέ για ασφάλεια και ταχύτητα Επέλεξα τέσσερα 8*32bit S-box αντί για ένα είναι για να αποφύγω το φαινόμενο της συμμετρίας πχ(Κάποια bytes της εισόδου είναι ίσα άρα και στην έξοδο εμφανίζει το S-box κάτι που διαδίδεται στους επόμενους γύρους το οποίο δημιουργεί την ικανότητα μιας στατιστικής επίθεσης). Ο λόγος που χρησιμοποίησα μέγεθος S-box 8*32 είναι διότι εμφανίζουν καλύτερη αντίσταση στην διαφορική κρυπτανάλυση από ότι κουτιά μικρότερου μεγέθους βέβαια αυτό τα κάνει πιο ευπρόσβλητα σε επιθέσεις γραμμικής κρυπτανάλυσης αλλά αυτή η αδυναμία μπορεί να αντιμετωπιστεί συνδυάζοντας την έξοδο των 4 κουτιών. Δεν χρησιμοποίησα παραπάνω μέγεθος διότι δεν θα ήταν αποδοτικά και πρακτικά σε υλοποίησης συστημάτων με μικρό χώρο αποθήκευσης όπως Έξυπνες κάρτες (κάθε κουτί έχει $2^8 = 256$ στοιχεία άρα

κάθε ψηφίο επιπλέων διπλασιάζει το μέγεθος) Τα στοιχεία των S-box είναι τα αποτελέσματα ειδικών συναρτήσεων bent τα οποία παρουσιάζουν υψηλή μη γραμμικότητα σύμφωνα με τον μετασχηματισμό Walsh-Hardmand .Επέλεξα τα S-box που χρησιμοποιήθηκαν στον σχεδιασμό του CAST αλγορίθμου σαν πρότυπο σχεδίασης. Η πύλη που χρησιμοποίησα για το συνδυασμό είναι η πύλη Xor ό λόγος που την χρησιμοποίησα σαν ένα στοιχείο συνδυασμού είναι ότι παρουσιάζει ισοπίθανη τιμή άσσων και μηδενικών 50% όταν έχω 0 στην είσοδο ή 1 από την πλευρά του παρατηρητή ενώ η πύλη And εμφανίζει μια ακολουθία μηδενικών με πιθανότητα 75% και η πύλη OR εμφανίζει με πιθανότητα 25% μηδενικά.. Ο αλγόριθμος παραγωγής κλειδιών σχεδιάστηκε για να διατηρήσει ολόκληρη την εντροπία του κλειδιού και για να διανείμει την εντροπία ομοιόμορφα στα υποκλειδιά .Η αρχική ιδέα ήταν να κάνω τον αλγόριθμό αυτών πιο πολύπλοκο με το να εισάγω Μετασχηματισμούς ανάμιξης που είναι η βασική καρδιά του IDEA (πολλαπλασιασμούς πρόσθεσης και Xor) και εξαρτημένες περιστροφές από τα δεδομένα και το κλειδί (DDR-KDR) του αλγορίθμου RC5 . Τελικά περιορίστηκα στο να φτιάξω ένα επαναληπτικό αλγόριθμο χρησιμοποιώντας σαν κρυπτογραφικό μετασχηματισμό την συνάρτηση F και της μεταβλητές περιστροφές επιλογής κλειδιού. Ανακάλυψα στην συνέχεια ότι αυτή το κριτήριο της σχεδίασης το είχαν χρησιμοποίηση άλλοι δημοφιλής κρυπταλγόριθμοι.. Χρησιμοποίησα την επαναληπτική δομή του αλγορίθμου (τέσσερις περιστροφές για την εξαγωγή κάθε υποκλειδιού) για να αυξήσω την σύγχυση και διάχυση των χαρακτηριστικών του κλειδιού στα υποκλειδια και για να εμποδίσω την κρυπτανάλυση του αλγορίθμου στην περίπτωση που ο κρυπταναλυτής έφθανε στην εξαγωγή του κλειδιού του τελευταίου γύρου (Διαφορική κρυπτανάλυση).Θα ήταν αδύνατο για αυτόν να προχωρήσει στην ανάκτηση των υποκλειδιών των προηγούμενων γύρων. Χρησιμοποίησα εξαρτημένες περιστροφές βάση των bytes του κλειδιού δανειζόμενος στοιχεία από τις M-sequence. Επέλεξα να προϋπολογίζεται πρώτα η μήτρα κλειδιών και μετά να τρέχει ο κύριο αλγόριθμος και αυτό το έκανα για λόγους ταχύτητας..

5.5 Τεστ χιονοστιβάδας(Avalanche) και Ασφάλεια Hellas1

Ο αλγόριθμος Hellas1 σχεδιάστηκε σε δύο μορφές με ιδιαίτερο χαρακτηριστικό την ικανοποίηση του κριτηρίου της χιονοστιβάδας. Το τεστ το έφτιαξα με το εργαλείο matlab γεμίζοντας ένα πίνακα με όλες τις πιθανές εισόδους και εξόδους .

Στην πρώτη σχεδίαση ο αλγόριθμος έφθασε να εκπλήρωση το κριτήριο αυτό στους 16 γύρους . Στην δεύτερη σχεδίαση του ο αλγόριθμός έφθασε για το συντριπτικό αριθμό Test vectors να εκπληρώσει το κριτήριο αυτό στους 9 γύρους. Αυτό είναι ικανοποιητικό σε σχέση με τον αλγόριθμό Des ο οποίος εμφανίζει το φαινόμενο αυτό στους 16 γύρους .

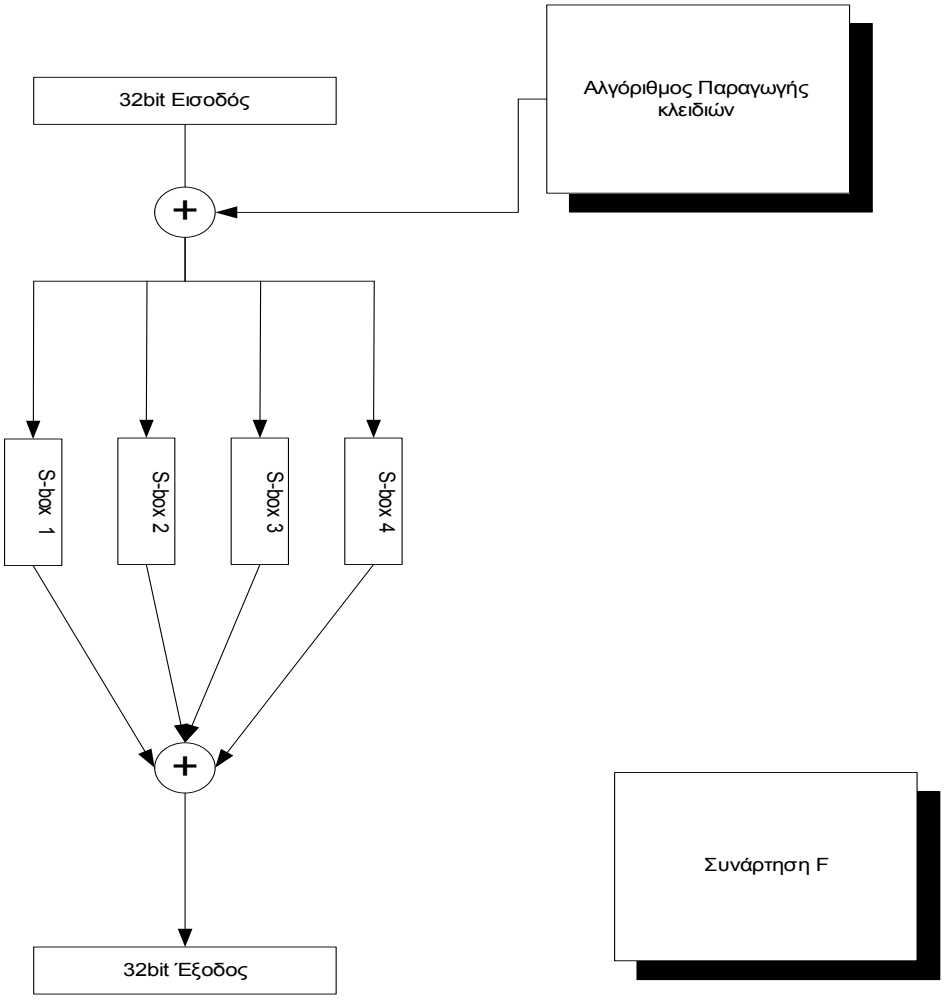
Για οποιαδήποτε μορφή κρυπτανάλυσης από την σχεδιαστική πλευρά απαιτείται η κατασκευή ενός μινι αλγόριθμου για απλοποίηση και μέτρηση καθώς επίσης και η φιλοσοφία της ανάλυσης κάθε κρυπτογραφικού στοιχείου ξεχωριστά και της λεγόμενης αφαιρετικής λειτουργίας (αφαιρούμε όλα τα στοιχεία εκτός από ένα και παρατηρούμε την ασφάλεια του αλγορίθμου

βασιζόμενη μόνο σε αυτό το στοιχείο αν τα υπόλοιπα έχουν παρακαμφτεί πχ Twofish)
Για την διαφορική κρυπτανάλυση τα S-box το οποία είναι το μόνο μη γραμμικό στοιχείο στον κρυπταλγόριθμο παρουσιάζουν υψηλή μη γραμμικότητα και επίπεδη κατανομή ζευγών εισόδου και εξόδου και αυτό δεν επιτρέπει την εύρεση ενός διαφορικού χαρακτηριστικού και ενός γραμμικού χαρακτηριστικού. Οι bent συναρτήσεις παρουσιάζουν την υψηλότερη μη γραμικκιτητα σε ένα S-box και αυτό καθιστά δύσκολή την γραμμική κρυπτανάλυση.

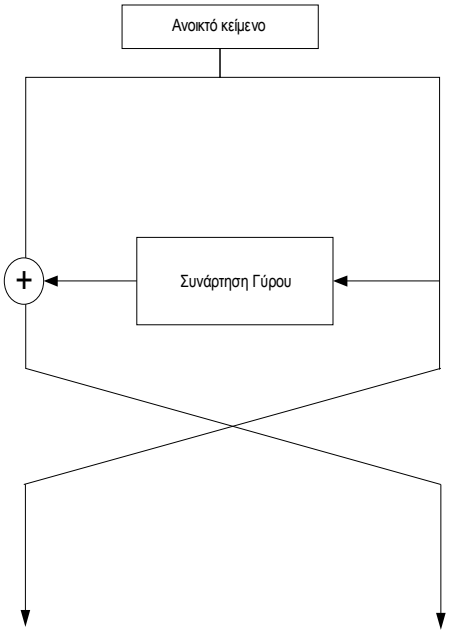
5.6 Συμπεράσματα

Ο Hellas1 αποτελεί ένα πειραματικό μοντέλο ενός σύγχρονου κρυπταλγορίθμου τμήματος. Δεν προτείνεται για χρησιμοποίηση μιας και δεν είναι ολοκληρωμένη έκδοση. Η κρυπτογραφική δύναμη ενός αλγορίθμου δεν βρίσκεται στην σχεδίαση του αλγορίθμου αλλά βρίσκεται στην ανάλυση του

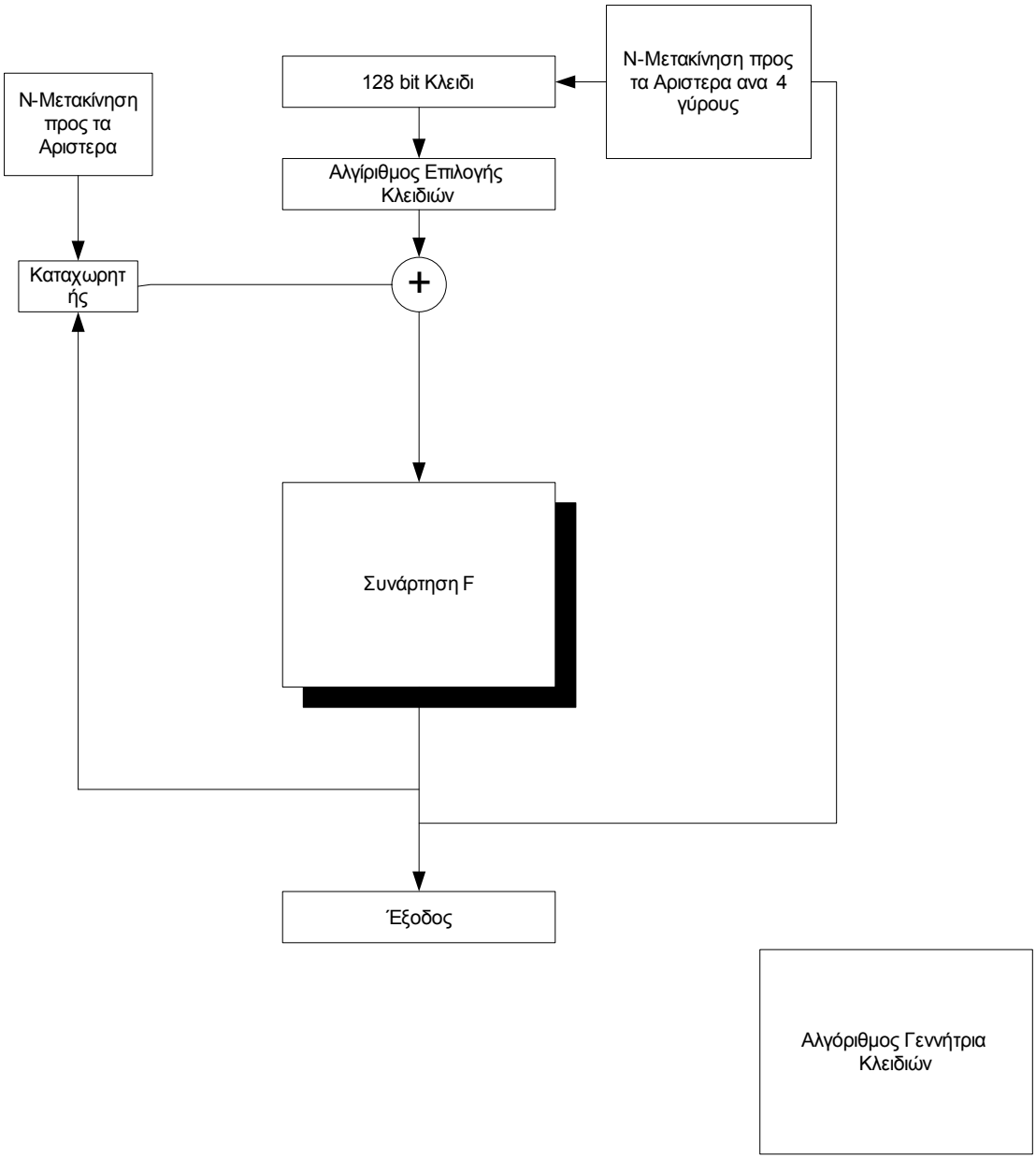
Σχεδίαση 1



Σχήμα 5.1 Συνάρτηση F

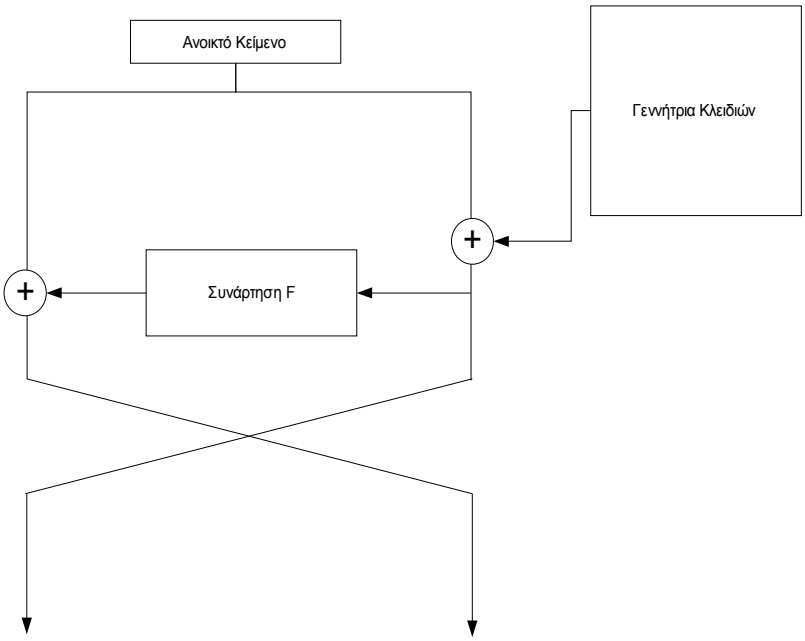


Σχήμα 5.2 Γύρος κρυπτογράφησης-αποκρυπτογράφησης

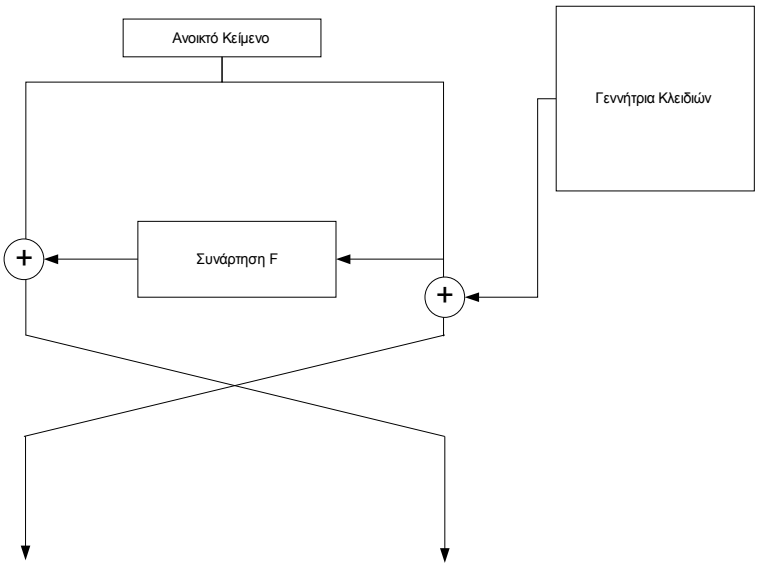


Σχήμα 5.3 Αλγόριθμος γεννήτριας κλειδιών

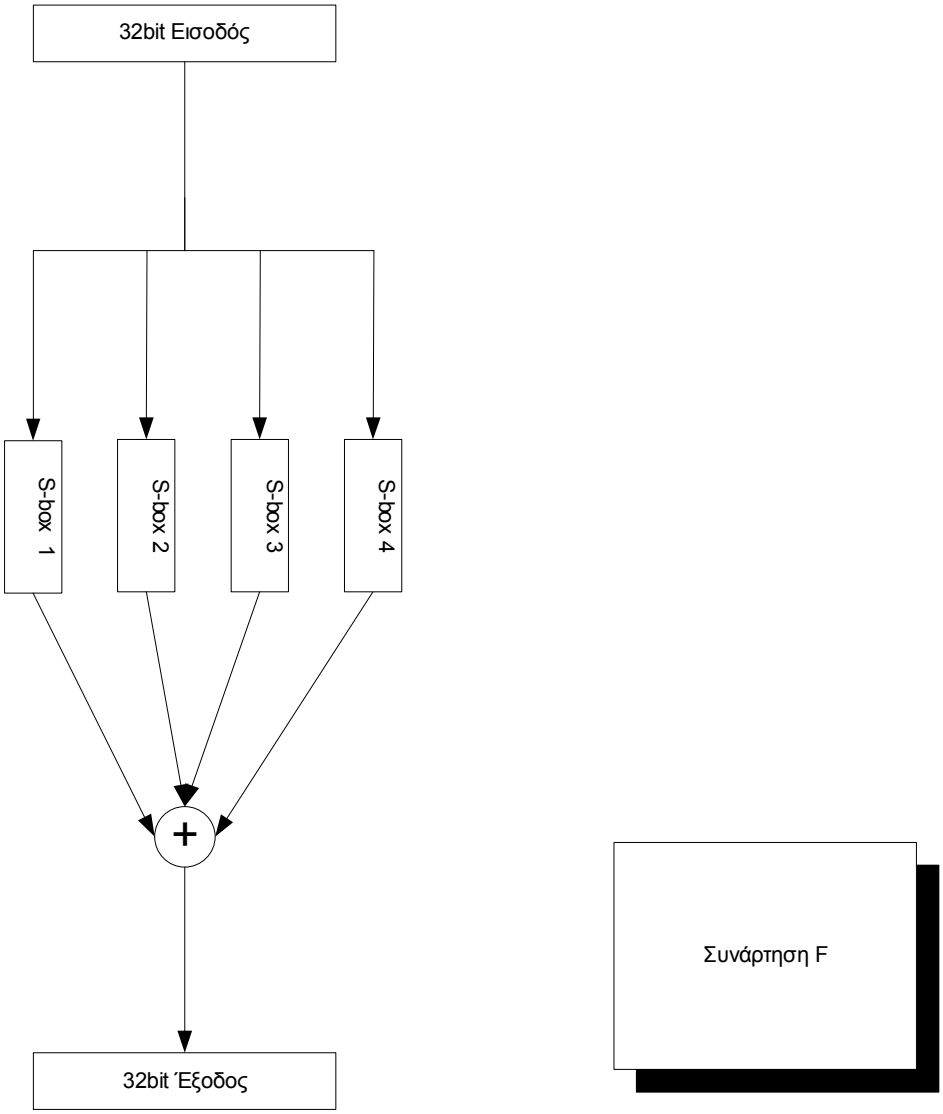
Σχεδίαση 2



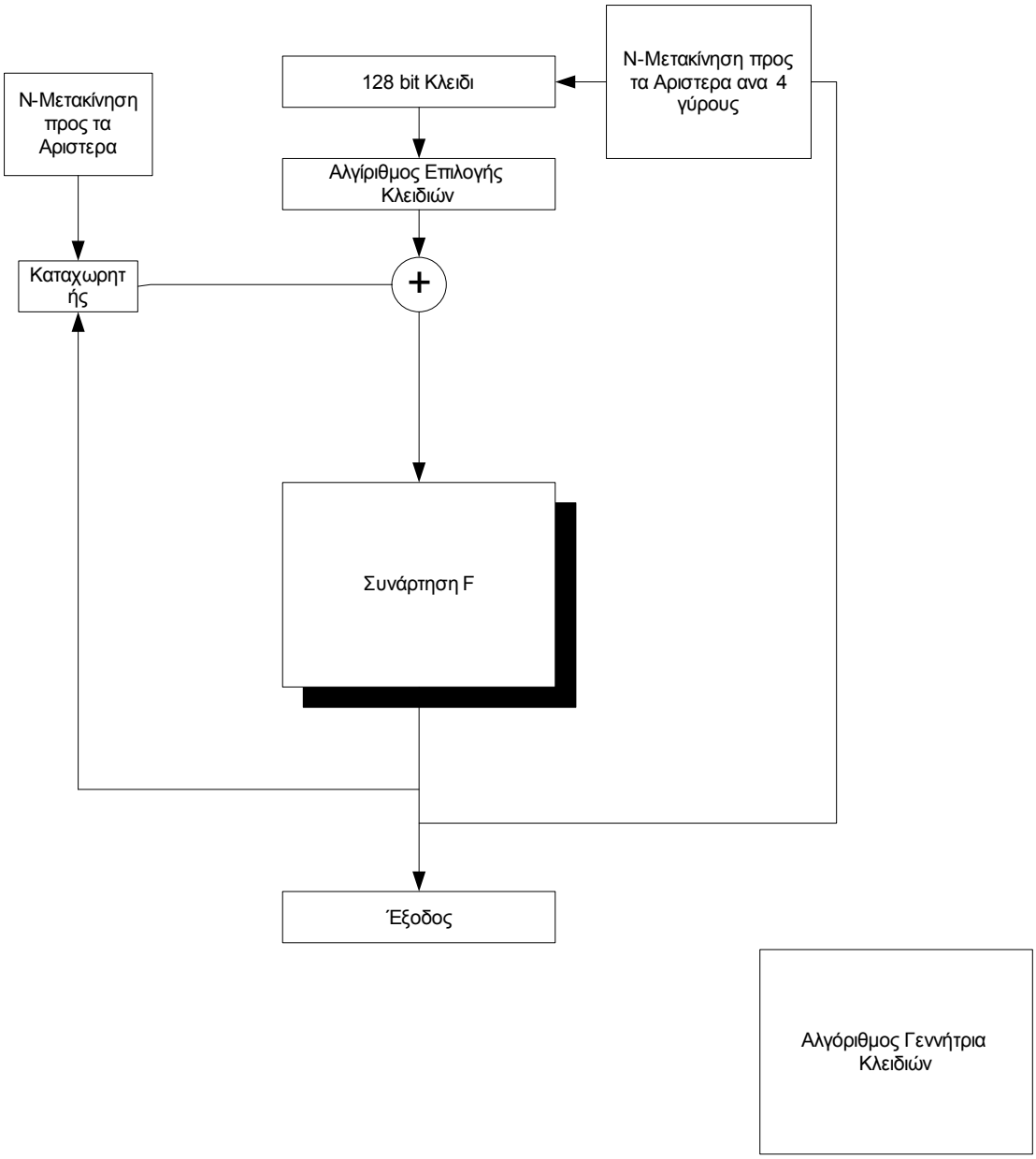
Σχήμα 5.4 Γύρος κρυπτογράφησης



Σχήμα 5.5 Γύρος αποκρυπτογράφησης



Σχήμα 5.6 Συνάρτηση F



Σχήμα 5.7 Αλγόριθμος γεννήτριας κλειδιών

5.7 Παράρτημα

Ο κώδικας έτρεξε σε matlab R14

Tc.m

```
% Αυτό είναι μια δοκιμαστική έκδοση ενός νέου κρυπτογραφικού αλγορίθμου

Ch=input('Πατηστε E για κρυπτογραφηση και D για αποκρυπτογραφηση   ','s');

% plaintext_hex = {'00' '11' '22' '33' '44' '55' '66' '77'};
  %       plaintext = hex2dec (plaintext_hex);
% plaintext =double('12345678')
%plaintext = [53,54,55,56,18,120,93,28]
plaintext = [165   146    10    37    30   158   155   138]
key = double('1111111111111111');

if (Ch == 'E')
   ciphertext = cipher (plaintext,key,Ch)
else

    dec_plaintext = cipher (plaintext,key,Ch)
end
```

Cipher.m

```
function ciphertext = cipher (plaintext,key,Ch)
global N
N= input('Posous girous ? ')

Skeys= Sbkeygeneration(key,Ch,N);

for i=1:1:4
    Bl(i)=plaintext(i);
    Br(i)=plaintext(i+4);
end
for i=1:1:N
    s=Skeys(i,:);
    xresult=F(Br,s);

    if length(xresult) == 1
        kxt=dec2hex(xresult);
k=0;

if length(kxt)<8
            kx=[zeros(1,8-(length(kxt))),kxt];
        else
            kx=kxt;
        end

for i=1:1:4
```

```
    for j=1:1:2
       k=k+1;
       b(i,j)=kx(k);
       end
       end

       for i=1:1:4
          b1(i)=hex2dec(b(i,:));
       end
       result=b1;
    else
      result=xresult;
    end

Blx=bitxor(result,Bl);
B=Br;
Br=Blx;
Bl=B;
end
ciphertext= [Br,Bl];
end
```

Sbkeygeneration.m

```
function Skeys = Sbkeygeneration(key,Ch,N)

global skys;
global tempx;
skys=key;
regist=[0,0,0,0];
for round=1:1:N

    if round>1
       rot1(skys);% rotate
    end

    for j=1:1:4
       key1=choicebitselction(skys,j);
     regist=bitxor(regist,key1);
       xresult=F(regist,key1);
    regist=xresult;
    regist= rot2(key1,regist);
end

    kx=dec2hex(xresult);
k=0;
for i=1:1:4
    for j=1:1:2
       k=k+1;
       b(i,j)=kx(k);
       end
       end
```

```
        for i=1:1:4
            tp(i)=hex2dec(b(i,:));
        end

Skeys(round,:)=tp;
end

if (Ch == 'D')
    j=1;
    if N == 1
    else

    for i=16:-1:1
        temp(j,:)=Skeys(i,:);
        j=j+1;
    end
    Skeys=temp;
end
end
end
```

rot1.m

```
function rot1(skys)

A=bitxor(skys(1),skys(4));
offset=bitxor(skys(16),A);

temp=dec2bin(skys);

k=0;
y=length(temp(1,:));
for i=1:1:16
    for j=1:1:length(temp(1,:))
        k=k+1;
        kx(k)=temp(i,j);
        end
        end

for i=1:1:offset

for j=1:1:length(kx)
    if j==length(kx)
        b(j)=kx(1);
    else
    b(j)=kx(j+1);
end
end
kx=b;
end

k=1;
```

```
for i=1:1:16
   for j=1:1:y
      tmp(i,j)=kx(k);
      k=k+1;
   end
end
skeys=bin2dec(tmp)';
end
```

choicebitselction.m

```
function key1 = choicebitselction(skys,j)

if j==1
    b=1;
 elseif j ==2
       b=5;
    elseif j==3
       b=9;
    elseif j==4
       b=13;
    end

key1(1)=skys(b);
key1(2)=skys(b+1);
key1(3)=skys(b+2);
key1(4)=skys(b+3);

end
```

rot2.m

```
function regist = rot2 (key1,regist)

A=bitxor(key1(1),key1(4));
offset= bitxor(bitor(key1(2),A),key1(3));


kxt=dec2hex(regist);
k=0;


if length(kxt)<8
          kx=[zeros(1,8-(length(kxt))),kxt];
       else
          kx=kxt;
       end

for i=1:1:4
   for j=1:1:2
      k=k+1;
```

```
        b(i,j)=kx(k);
        end
        end

        for i=1:1:4
            tp(i)=hex2dec(b(i,:));
        end
z=length(tp);
temp=dec2bin(tp);
k=0;
y=length(temp(1,:));

for i=1:1:4
    for j=1:1:length(temp(1,:))
        k=k+1;
        ky(k)=temp(i,j);
        end
        end

for i=1:1:offset

for j=1:1:length(ky)
    if j==length(ky)
        b(j)=ky(1);
    else
    b(j)=ky(j+1);
end
end
ky=b;
end

k=1;
for i=1:1:z
    for j=1:1:y
        tmp(i,j)=ky(k);
        k=k+1;
    end
end
regist=bin2dec(tmp)';
end
```

F.m

```
function xresult = F(Br,Skeys)
load C:\MATLAB6p5\work\ptix\sboxs1.mat
x=Br;
Br =bitxor(x,Skeys);
S=Br(1);
P=Br(2);
Q=Br(3);
R=Br(4);
if S == 0
    S=1;
end
```

```
if P == 0
   P=1;
end
if Q == 0
   Q=1;
end
if R == 0
   R=1;
end

sout1= sb1(S);
sout2=sb2(P);
sout3=sb3(Q);
sout4=sb4(R);
temp=bitxor(sout1,sout2);
temp1=bitxor(sout3,sout4);
xresult=bitxor(temp,temp1);
end
```

S-Box S1

30fb40d4 9fa0ff0b 6beccd2f 3f258c7a 1e213f2f 9c004dd3 6003e540 cf9fc949
bfd4af27 88bbbdb5 e2034090 98d09675 6e63a0e0 15c361d2 c2e7661d 22d4ff8e
28683b6f c07fd059 ff2379c8 775f50e2 43c340d3 df2f8656 887ca41a a2d2bd2d
a1c9e0d6 346c4819 61b76d87 22540f2f 2abe32e1 aa54166b 22568e3a a2d341d0
66db40c8 a784392f 004dff2f 2db9d2de 97943fac 4a97c1d8 527644b7 b5f437a7
b82cbaef d751d159 6ff7f0ed 5a097a1f 827b68d0 90ecf52e 22b0c054 bc8e5935
4b6d2f7f 50bb64a2 d2664910 bee5812d b7332290 e93b159f b48ee411 4bff345d
fd45c240 ad31973f c4f6d02e 55fc8165 d5b1caad a1ac2dae a2d4b76d c19b0c50
882240f2 0c6e4f38 a4e4bfd7 4f5ba272 564c1d2f c59c5319 b949e354 b04669fe
b1b6ab8a c71358dd 6385c545 110f935d 57538ad5 6a390493 e63d37e0 2a54f6b3
3a787d5f 6276a0b5 19a6fcdf 7a42206a 29f9d4d5 f61b1891 bb72275e aa508167
38901091 c6b505eb 84c7cb8c 2ad75a0f 874a1427 a2d1936b 2ad286af aa56d291
d7894360 425c750d 93b39e26 187184c9 6c00b32d 73e2bb14 a0bebc3c 54623779
64459eab 3f328b82 7718cf82 59a2cea6 04ee002e 89fe78e6 3fab0950 325ff6c2
81383f05 6963c5c8 76cb5ad6 d49974c9 ca180dcf 380782d5 c7fa5cf6 8ac31511
35e79e13 47da91d0 f40f9086 a7e2419e 31366241 051ef495 aa573b04 4a805d8d
548300d0 00322a3c bf64cddf ba57a68e 75c6372b 50afd341 a7c13275 915a0bf5
6b54bfab 2b0b1426 ab4cc9d7 449ccd82 f7fbf265 ab85c5f3 1b55db94 aad4e324
cfa4bd3f 2deaa3e2 9e204d02 c8bd25ac eadf55b3 d5bd9e98 e31231b2 2ad5ad6c
954329de adbe4528 d8710f69 aa51c90f aa786bf6 22513f1e aa51a79b 2ad344cc
7b5a41f0 d37cfbad 1b069505 41ece491 b4c332e6 032268d4 c9600acc ce387e6d
bf6bb16c 6a70fb78 0d03d9c9 d4df39de e01063da 4736f464 5ad328d8 b347cc96
75bb0fc3 98511bfb 4ffbcc35 b58bcf6a e11f0abc bfc5fe4a a70aec10 ac39570a
3f04442f 6188b153 e0397a2e 5727cb79 9ceb418f 1cacd68d 2ad37c96 0175cb9d
c69dff09 c75b65f0 d9db40d8 ec0e7779 4744ead4 b11c3274 dd24cb9e 7e1c54bd
f01144f9 d2240eb1 9675b3fd a3ac3755 d47c27af 51c85f4d 56907596 a5bb15e6
580304f0 ca042cf1 011a37ea 8dbfaadb 35ba3e4a 3526ffa0 c37b4d09 bc306ed9
98a52666 5648f725 ff5e569d 0ced63d0 7c63b2cf 700b45e1 d5ea50f1 85a92872
af1fbda7 d4234870 a7870bf3 2d3b4d79 42e04198 0cd0ede7 26470db8 f881814c

474d6ad7 7c0c5e5c d1231959 381b7298 f5d2f4db ab838653 6e2f1e23 83719c9e
bd91e046 9a56456e dc39200c 20c8c571 962bda1c e1e696ff b141ab08 7cca89b9
1a69e783 02cc4843 a2f7c579 429ef47d 427b169c 5ac9f049 dd8f0f00 5c8165bf

S-Box S2

1f201094 ef0ba75b 69e3cf7e 393f4380 fe61cf7a eec5207a 55889c94 72fc0651
ada7ef79 4e1d7235 d55a63ce de0436ba 99c430ef 5f0c0794 18dcdb7d a1d6eff3
a0b52f7b 59e83605 ee15b094 e9ffd909 dc440086 ef944459 ba83ccb3 e0c3cdfb
d1da4181 3b092ab1 f997f1c1 a5e6cf7b 01420ddb e4e7ef5b 25a1ff41 e180f806
1fc41080 179bee7a d37ac6a9 fe5830a4 98de8b7f 77e83f4e 79929269 24fa9f7b
e113c85b acc40083 d7503525 f7ea615f 62143154 0d554b63 5d681121 c866c359
3d63cf73 cee234c0 d4d87e87 5c672b21 071f6181 39f7627f 361e3084 e4eb573b
602f64a4 d63acd9c 1bbc4635 9e81032d 2701f50c 99847ab4 a0e3df79 ba6cf38c
10843094 2537a95e f46f6ffe a1ff3b1f 208cfb6a 8f458c74 d9e0a227 4ec73a34
fc884f69 3e4de8df ef0e0088 3559648d 8a45388c 1d804366 721d9bfd a58684bb
e8256333 844e8212 128d8098 fed33fb4 ce280ae1 27e19ba5 d5a6c252 e49754bd

c5d655dd eb667064 77840b4d a1b6a801 84db26a9 e0b56714 21f043b7 e5d05860
54f03084 066ff472 a31aa153 dadc4755 b5625dbf 68561be6 83ca6b94 2d6ed23b
eccf01db a6d3d0ba b6803d5c af77a709 33b4a34c 397bc8d6 5ee22b95 5f0e5304
81ed6f61 20e74364 b45e1378 de18639b 881ca122 b96726d1 8049a7e8 22b7da7b
5e552d25 5272d237 79d2951c c60d894c 488cb402 1ba4fe5b a4b09f6b 1ca815cf
a20c3005 8871df63 b9de2fcb 0cc6c9e9 0beeff53 e3214517 b4542835 9f63293c
ee41e729 6e1d2d7c 50045286 1e6685f3 f33401c6 30a22c95 31a70850 60930f13
73f98417 a1269859 ec645c44 52c877a9 cdff33a6 a02b1741 7cbad9a2 2180036f
50d99c08 cb3f4861 c26bd765 64a3f6ab 80342676 25a75e7b e4e6d1fc 20c710e6
cdf0b680 17844d3b 31eef84d 7e0824e4 2ccb49eb 846a3bae 8ff77888 ee5d60f6
7af75673 2fdd5cdb a11631c1 30f66f43 b3faec54 157fd7fa ef8579cc d152de58
db2ffd5e 8f32ce19 306af97a 02f03ef8 99319ad5 c242fa0f a7e3ebb0 c68e4906
b8da230c 80823028 dcdef3c8 d35fb171 088a1bc8 bec0c560 61a3c9e8 bca8f54d
c72feffa 22822e99 82c570b4 d8d94e89 8b1c34bc 301e16e6 273be979 b0ffeaa6
61d9b8c6 00b24869 b7ffce3f 08dc283b 43daf65a f7e19798 7619b72f 8f1c9ba4
dc8637a0 16a7d3b1 9fc393b7 a7136eeb c6bcc63e 1a513742 ef6828bc 520365d6
2d6a77ab 3527ed4b 821fd216 095c6e2e db92f2fb 5eea29cb 145892f5 91584f7f
5483697b 2667a8cc 85196048 8c4bacea 833860d4 0d23e0f9 6c387e8a 0ae6d249
b284600c d835731d dcb1c647 ac4c56ea 3ebd81b3 230eabb0 6438bc87 f0b5b1fa
8f5ea2b3 fc184642 0a036b7a 4fb089bd 649da589 a345415e 5c038323 3e5d3bb9
43d79572 7e6dd07c 06dfdf1e 6c6cc4ef 7160a539 73bfbe70 83877605 4523ecf1

S-Box S3

8defc240 25fa5d9f eb903dbf e810c907 47607fff 369fe44b 8c1fc644 aececa90
beb1f9bf eefbcaea e8cf1950 51df07ae 920e8806 f0ad0548 e13c8d83 927010d5
11107d9f 07647db9 b2e3e4d4 3d4f285e b9afa820 fade82e0 a067268b 8272792e
553fb2c0 489ae22b d4ef9794 125e3fbc 21fffcee 825b1bfd 9255c5ed 1257a240
4e1a8302 bae07fff 528246e7 8e57140e 3373f7bf 8c9f8188 a6fc4ee8 c982b5a5
a8c01db7 579fc264 67094f31 f2bd3f5f 40fff7c1 1fb78dfc 8e6bd2c1 437be59b
99b03dbf b5dbc64b 638dc0e6 55819d99 a197c81c 4a012d6e c5884a28 ccc36f71

b843c213 6c0743f1 8309893c 0feddd5f 2f7fe850 d7c07f7e 02507fbf 5afb9a04
a747d2d0 1651192e af70bf3e 58c31380 5f98302e 727cc3c4 0a0fb402 0f7fef82
8c96fdad 5d2c2aae 8ee99a49 50da88b8 8427f4a0 1eac5790 796fb449 8252dc15
efbd7d9b a672597d ada840d8 45f54504 fa5d7403 e83ec305 4f91751a 925669c2
23efe941 a903f12e 60270df2 0276e4b6 94fd6574 927985b2 8276dbcb 02778176
f8af918d 4e48f79e 8f616ddf e29d840e 842f7d83 340ce5c8 96bbb682 93b4b148
ef303cab 984faf28 779faf9b 92dc560d 224d1e20 8437aa88 7d29dc96 2756d3dc
8b907cee b51fd240 e7c07ce3 e566b4a1 c3e9615e 3cf8209d 6094d1e3 cd9ca341
5c76460e 00ea983b d4d67881 fd47572c f76cedd9 bda8229c 127dadaa 438a074e
1f97c090 081bdb8a 93a07ebe b938ca15 97b03cff 3dc2c0f8 8d1ab2ec 64380e51
68cc7bfb d90f2788 12490181 5de5ffd4 dd7ef86a 76a2e214 b9a40368 925d958f
4b39fffa ba39aee9 a4ffd30b faf7933b 6d498623 193cbcfa 27627545 825cf47a
61bd8ba0 d11e42d1 cead04f4 127ea392 10428db7 8272a972 9270c4a8 127de50b
285ba1c8 3c62f44f 35c0eaa5 e805d231 428929fb b4fcdf82 4fb66a53 0e7dc15b
1f081fab 108618ae fcfd086d f9ff2889 694bcc11 236a5cae 12deca4d 2c3f8cc5
d2d02dfe f8ef5896 e4cf52da 95155b67 494a488c b9b6a80c 5c8f82bc 89d36b45
3a609437 ec00c9a9 44715253 0a874b49 d773bc40 7c34671c 02717ef6 4feb5536
a2d02fff d2bf60c4 d43f03c0 50b4ef6d 07478cd1 006e1888 a2e53f55 b9e6d4bc

a2048016 97573833 d7207d67 de0f8f3d 72f87b33 abcc4f33 7688c55d 7b00a6b0
947b0001 570075d2 f9bb88f8 8942019e 4264a5ff 856302e0 72dbd92b ee971b69
6ea22fde 5f08ae2b af7a616d e5c98767 cf1febd2 61efc8c2 f1ac2571 cc8239c2
67214cb8 b1e583d1 b7dc3e62 7f10bdce f90a5c38 0ff0443d 606e6dc6 60543a49
5727c148 2be98a1d 8ab41738 20e1be24 af96da0f 68458425 99833be5 600d457d
282f9350 8334b362 d91d1120 2b6d8da0 642b1e31 9c305a00 52bce688 1b03588a
f7baefd5 4142ed9c a4315c11 83323ec5 dfef4636 a133c501 e9d3531c ee353783

S-Box S4

9db30420 1fb6e9de a7be7bef d273a298 4a4f7bdb 64ad8c57 85510443 fa020ed1
7e287aff e60fb663 095f35a1 79ebf120 fd059d43 6497b7b1 f3641f63 241e4adf
28147f5f 4fa2b8cd c9430040 0cc32220 fdd30b30 c0a5374f 1d2d00d9 24147b15
ee4d111a 0fca5167 71ff904c 2d195ffe 1a05645f 0c13fefe 081b08ca 05170121
80530100 e83e5efe ac9af4f8 7fe72701 d2b8ee5f 06df4261 bb9e9b8a 7293ea25
ce84ffdf f5718801 3dd64b04 a26f263b 7ed48400 547eebe6 446d4ca0 6cf3d6f5
2649abdf aea0c7f5 36338cc1 503f7e93 d3772061 11b638e1 72500e03 f80eb2bb
abe0502e ec8d77de 57971e81 e14f6746 c9335400 6920318f 081dbb99 ffc304a5
4d351805 7f3d5ce3 a6c866c6 5d5bcca9 daec6fea 9f926f91 9f46222f 3991467d
a5bf6d8e 1143c44f 43958302 d0214eeb 022083b8 3fb6180c 18f8931e 281658e6
26486e3e 8bd78a70 7477e4c1 b506e07c f32d0a25 79098b02 e4eabb81 28123b23
69dead38 1574ca16 df871b62 211c40b7 a51a9ef9 0014377b 041e8ac8 09114003
bd59e4d2 e3d156d5 4fe876d5 2f91a340 557be8de 00eae4a7 0ce5c2ec 4db4bba6
e756bdff dd3369ac ec17b035 06572327 99afc8b0 56c8c391 6b65811c 5e146119
6e85cb75 be07c002 c2325577 893ff4ec 5bbfc92d d0ec3b25 b7801ab7 8d6d3b24
20c763ef c366a5fc 9c382880 0ace3205 aac9548a eca1d7c7 041afa32 1d16625a
6701902c 9b757a54 31d477f7 9126b031 36cc6fdb c70b8b46 d9e66a48 56e55a79
026a4ceb 52437eff 2f8f76b4 0df980a5 8674cde3 edda04eb 17a9be04 2c18f4df
b7747f9d ab2af7b4 efc34d20 2e096b7c 1741a254 e5b6a035 213d42f6 2c1c7c26
61c2f50f 6552daf9 d2c231f8 25130f69 d8167fa2 0418f2c8 001a96a6 0d1526ab
63315c21 5e0a72ec 49bafefd 187908d9 8d0dbd86 311170a7 3e9b640c cc3e10d7

d5cad3b6 0caec388 f73001e1 6c728aff 71eae2a1 1f9af36e cfcbd12f c1de8417
ac07be6b cb44a1d8 8b9b0f56 013988c3 b1c52fca b4be31cd d8782806 12a3a4e2
6f7de532 58fd7eb6 d01ee900 24adffc2 f4990fc5 9711aac5 001d7b95 82e5e7d2
109873f6 00613096 c32d9521 ada121ff 29908415 7fbb977f af9eb3db 29c9ed2a
5ce2a465 a730f32c d0aa3fe8 8a5cc091 d49e2ce7 0ce454a9 d60acd86 015f1919
77079103 dea03af6 78a8565e dee356df 21f05cbe 8b75e387 b3c50651 b8a5c3ef
d8eeb6d2 e523be77 c2154529 2f69efdf afe67afb f470c4b2 f3e0eb5b d6cc9876
39e4460c 1fda8538 1987832f ca007367 a99144f8 296b299e 492fc295 9266beab
b5676e69 9bd3ddda df7e052f db25701c 1b5e51ee f65324e6 6afce36c 0316cc04
8644213e b7dc59d0 7965291f ccd6fd43 41823979 932bcdf6 b657c34d 4edfd282
7ae5290c 3cb9536b 851e20fe 9833557e 13ecf0b0 d3ffb372 3f85c5c1 0aef7ed2

S-Box S5

7ec90c04 2c6e74b9 9b0e66df a6337911 b86a7fff 1dd358f5 44dd9d44 1731167f
08fbf1fa e7f511cc d2051b00 735aba00 2ab722d8 386381cb acf6243a 69befd7a
e6a2e77f f0c720cd c4494816 ccf5c180 38851640 15b0a848 e68b18cb 4caadeff
5f480a01 0412b2aa 259814fc 41d0efe2 4e40b48d 248eb6fb 8dba1cfe 41a99b02
1a550a04 ba8f65cb 7251f4e7 95a51725 c106ecd7 97a5980a c539b9aa 4d79fe6a

f2f3f763 68af8040 ed0c9e56 11b4958b e1eb5a88 8709e6b0 d7e07156 4e29fea7
6366e52d 02d1c000 c4ac8e05 9377f571 0c05372a 578535f2 2261be02 d642a0c9
df13a280 74b55bd2 682199c0 d421e5ec 53fb3ce8 c8adedb3 28a87fc9 3d959981
5c1ff900 fe38d399 0c4eff0b 062407ea aa2f4fb1 4fb96976 90c79505 b0a8a774
ef55a1ff e59ca2c2 a6b62d27 e66a4263 df65001f 0ec50966 dfdd55bc 29de0655
911e739a 17af8975 32c7911c 89f89468 0d01e980 524755f4 03b63cc9 0cc844b2
bcf3f0aa 87ac36e9 e53a7426 01b3d82b 1a9e7449 64ee2d7e cddbb1da 01c94910
b868bf80 0d26f3fd 9342ede7 04a5c284 636737b6 50f5b616 f24766e3 8eca36c1
136e05db fef18391 fb887a37 d6e7f7d4 c7fb7dc9 3063fcdf b6f589de ec2941da
26e46695 b7566419 f654efc5 d08d58b7 48925401 c1bacb7f e5ff550f b6083049
5bb5d0e8 87d72e5a ab6a6ee1 223a66ce c62bf3cd 9e0885f9 68cb3e47 086c010f
a21de820 d18b69de f3f65777 fa02c3f6 407edac3 cbb3d550 1793084d b0d70eba
0ab378d5 d951fb0c ded7da56 4124bbe4 94ca0b56 0f5755d1 e0e1e56e 6184b5be
580a249f 94f74bc0 e327888e 9f7b5561 c3dc0280 05687715 646c6bd7 44904db3
66b4f0a3 c0f1648a 697ed5af 49e92ff6 309e374f 2cb6356a 85808573 4991f840
76f0ae02 083be84d 28421c9a 44489406 736e4cb8 c1092910 8bc95fc6 7d869cf4
134f616f 2e77118d b31b2be1 aa90b472 3ca5d717 7d161bba 9cad9010 af462ba2
9fe459d2 45d34559 d9f2da13 dbc65487 f3e4f94e 176d486f 097c13ea 631da5c7
445f7382 175683f4 cdc66a97 70be0288 b3cdcf72 6e5dd2f3 20936079 459b80a5
be60e2db a9c23101 eba5315c 224e42f2 1c5c1572 f6721b2c 1ad2fff3 8c25404e
324ed72f 4067b7fd 0523138e 5ca3bc78 dc0fd66e 75922283 784d6b17 58ebb16e
44094f85 3f481d87 fcfeae7b 77b5ff76 8c2302bf aaf47556 5f46b02a 2b092801
3d38f5f7 0ca81f36 52af4a8a 66d5e7c0 df3b0874 95055110 1b5ad7a8 f61ed5ad
6cf6e479 20758184 d0cefa65 88f7be58 4a046826 0ff6f8f3 a09c7f70 5346aba0
5ce96c28 e176eda3 6bac307f 376829d2 85360fa9 17e3fe2a 24b79767 f5a96b20
d6cd2595 68ff1ebf 7555442c f19f06be f9e0659a eeb9491d 34010718 bb30cab8
e822fe15 88570983 750e6249 da627e55 5e76ffa8 b1534546 6d47de08 efe9e7d4

S-Box S6

f6fa8f9d 2cac6ce1 4ca34867 e2337f7c 95db08e7 016843b4 eced5cbc 325553ac
bf9f0960 dfa1e2ed 83f0579d 63ed86b9 1ab6a6b8 de5ebe39 f38ff732 8989b138
33f14961 c01937bd f506c6da e4625e7e a308ea99 4e23e33c 79cbd7cc 48a14367
a3149619 fec94bd5 a114174a eaa01866 a084db2d 09a8486f a888614a 2900af98
01665991 e1992863 c8f30c60 2e78ef3c d0d51932 cf0fec14 f7ca07d2 d0a82072
fd41197e 9305a6b0 e86be3da 74bed3cd 372da53c 4c7f4448 dab5d440 6dba0ec3
083919a7 9fbaeed9 49dbcfb0 4e670c53 5c3d9c01 64bdb941 2c0e636a ba7dd9cd
ea6f7388 e70bc762 35f29adb 5c4cdd8d f0d48d8c b88153e2 08a19866 1ae2eac8
284caf89 aa928223 9334be53 3b3a21bf 16434be3 9aea3906 efe8c36e f890cdd9
80226dae c340a4a3 df7e9c09 a694a807 5b7c5ecc 221db3a6 9a69a02f 68818a54
ceb2296f 53c0843a fe893655 25bfe68a b4628abc cf222ebf 25ac6f48 a9a99387
53bddb65 e76ffbe7 e967fd78 0ba93563 8e342bc1 e8a11be9 4980740d c8087dfc
8de4bf99 a11101a0 7fd37975 da5a26c0 e81f994f 9528cd89 fd339fed b87834bf
5f04456d 22258698 c9c4c83b 2dc156be 4f628daa 57f55ec5 e2220abe d2916ebf
4ec75b95 24f2c3c0 42d15d99 cd0d7fa0 7b6e27ff a8dc8af0 7345c106 f41e232f
35162386 e6ea8926 3333b094 157ec6f2 372b74af 692573e4 e9a9d848 f3160289
3a62ef1d a787e238 f3a5f676 74364853 20951063 4576698d b6fad407 592af950
36f73523 4cfb6e87 7da4cec0 6c152daa cb0396a8 c50dfe5d fcd707ab 0921c42f
89dff0bb 5fe2be78 448f4f33 754613c9 2b05d08d 48b9d585 dc049441 c8098f9b

7dede786 c39a3373 42410005 6a091751 0ef3c8a6 890072d6 28207682 a9a9f7be
bf32679d d45b5b75 b353fd00 cbb0e358 830f220a 1f8fb214 d372cf08 cc3c4a13
8cf63166 061c87be 88c98f88 6062e397 47cf8e7a b6c85283 3cc2acfb 3fc06976
4e8f0252 64d8314d da3870e3 1e665459 c10908f0 513021a5 6c5b68b7 822f8aa0
3007cd3e 74719eef dc872681 073340d4 7e432fd9 0c5ec241 8809286c f592d891
08a930f6 957ef305 b7fbffbd c266e96f 6fe4ac98 b173ecc0 bc60b42a 953498da
fba1ae12 2d4bd736 0f25faab a4f3fceb e2969123 257f0c3d 9348af49 361400bc
e8816f4a 3814f200 a3f94043 9c7a54c2 bc704f57 da41e7f9 c25ad33a 54f4a084
b17f5505 59357cbe edbd15c8 7f97c5ab ba5ac7b5 b6f6deaf 3a479c3a 5302da25
653d7e6a 54268d49 51a477ea 5017d55b d7d25d88 44136c76 0404a8c8 b8e5a121
b81a928a 60ed5869 97c55b96 eaec991b 29935913 01fdb7f1 088e8dfa 9ab6f6f5
3b4cbf9f 4a5de3ab e6051d35 a0e1d855 d36b4cf1 f544edeb b0e93524 bebb8fbd
a2d762cf 49c92f54 38b5f331 7128a454 48392905 a65b1db8 851c97bd d675cf2f

S-Box S7

85e04019 332bf567 662dbfff cfc65693 2a8d7f6f ab9bc912 de6008a1 2028da1f
0227bce7 4d642916 18fac300 50f18b82 2cb2cb11 b232e75c 4b3695f2 b28707de
a05fbcf6 cd4181e9 e150210c e24ef1bd b168c381 fde4e789 5c79b0d8 1e8bfd43
4d495001 38be4341 913cee1d 92a79c3f 089766be baeeadf4 1286becf b6eacb19
2660c200 7565bde4 64241f7a 8248dca9 c3b3ad66 28136086 0bd8dfa8 356d1cf2
107789be b3b2e9ce 0502aa8f 0bc0351e 166bf52a eb12ff82 e3486911 d34d7516
4e7b3aff 5f43671b 9cf6e037 4981ac83 334266ce 8c9341b7 d0d854c0 cb3a6c88
47bc2829 4725ba37 a66ad22b 7ad61f1e 0c5cbafa 4437f107 b6e79962 42d2d816
0a961288 e1a5c06e 13749e67 72fc081a b1d139f7 f9583745 cf19df58 bec3f756
c06eba30 07211b24 45c28829 c95e317f bc8ec511 38bc46e9 c6e6fa14 bae8584a
ad4ebc46 468f508b 7829435f f124183b 821dba9f aff60ff4 ea2c4e6d 16e39264
92544a8b 009b4fc3 aba68ced 9ac96f78 06a5b79a b2856e6e 1aec3ca9 be838688

0e0804e9 55f1be56 e7e5363b b3a1f25d f7debb85 61fe033c 16746233 3c034c28
da6d0c74 79aac56c 3ce4e1ad 51f0c802 98f8f35a 1626a49f eed82b29 1d382fe3
0c4fb99a bb325778 3ec6d97b 6e77a6a9 cb658b5c d45230c7 2bd1408b 60c03eb7
b9068d78 a33754f4 f430c87d c8a71302 b96d8c32 ebd4e7be be8b9d2d 7979fb06
e7225308 8b75cf77 11ef8da4 e083c858 8d6b786f 5a6317a6 fa5cf7a0 5dda0033
f28ebfb0 f5b9c310 a0eac280 08b9767a a3d9d2b0 79d34217 021a718d 9ac6336a
2711fd60 438050e3 069908a8 3d7fedc4 826d2bef 4eeb8476 488dcf25 36c9d566
28e74e41 c2610aca 3d49a9cf bae3b9df b65f8de6 92aeaf64 3ac7d5e6 9ea80509
f22b017d a4173f70 dd1e16c3 15e0d7f9 50b1b887 2b9f4fd5 625aba82 6a017962
2ec01b9c 15488aa9 d716e740 40055a2c 93d29a22 e32dbf9a 058745b9 3453dc1e
d699296e 496cff6f 1c9f4986 dfe2ed07 b87242d1 19de7eae 053e561a 15ad6f8c
66626c1c 7154c24c ea082b2a 93eb2939 17dcb0f0 58d4f2ae 9ea294fb 52cf564c
9883fe66 2ec40581 763953c3 01d6692e d3a0c108 a1e7160e e4f2dfa6 693ed285
74904698 4c2b0edd 4f757656 5d393378 a132234f 3d321c5d c3f5e194 4b269301
c79f022f 3c997e7e 5e4f9504 3ffafbbd 76f7ad0e 296693f4 3d1fce6f c61e45be
d3b5ab34 f72bf9b7 1b0434c0 4e72b567 5592a33d b5229301 cfd2a87f 60aeb767
1814386b 30bcc33d 38a0c07d fd1606f2 c363519b 589dd390 5479f8e6 1cb8d647
97fd61a9 ea7759f4 2d57539d 569a58cf e84e63ad 462e1b78 6580f87e f3817914
91da55f4 40a230f3 d1988f35 b6e318d2 3ffa50bc 3d40f021 c3c0bdae 4958c24c
518f36b2 84b1d370 0fedce83 878ddada f2a279c7 94e01be8 90716f4b 954b8aa3

S-Box S8

e216300d bbddfffc a7ebdabd 35648095 7789f8b7 e6c1121b 0e241600 052ce8b5
11a9cfb0 e5952f11 ece7990a 9386d174 2a42931c 76e38111 b12def3a 37dddfc
de9adeb1 0a0cc32c be197029 84a00940 bb243a0f b4d137cf b44e79f0 049eedfd
0b15a15d 480d3168 8bbbde5a 669ded42 c7ece831 3f8f95e7 72df191b 7580330d
94074251 5c7dcdfa abbe6d63 aa402164 b301d40a 02e7d1ca 53571dae 7a3182a2
12a8ddec fdaa335d 176f43e8 71fb46d4 38129022 ce949ad4 b84769ad 965bd862
82f3d055 66fb9767 15b80b4e 1d5b47a0 4cfde06f c28ec4b8 57e8726e 647a78fc
99865d44 608bd593 6c200e03 39dc5ff6 5d0b00a3 ae63aff2 7e8bd632 70108c0c
bbd35049 2998df04 980cf42a 9b6df491 9e7edd53 06918548 58cb7e07 3b74ef2e
522fffb1 d24708cc 1c7e27cd a4eb215b 3cf1d2e2 19b47a38 424f7618 35856039
9d17dee7 27eb35e6 c9aff67b 36baf5b8 09c467cd c18910b1 e11dbf7b 06cd1af8
7170c608 2d5e3354 d4de495a 64c6d006 bcc0c62c 3dd00db3 708f8f34 77d51b42
264f620f 24b8d2bf 15c1b79e 46a52564 f8d7e54e 3e378160 7895cda5 859c15a5
e6459788 c37bc75f db07ba0c 0676a3ab 7f229b1e 31842e7b 24259fd7 f8bef472
835ffcb8 6df4c1f2 96f5b195 fd0af0fc b0fe134c e2506d3d 4f9b12ea f215f225
a223736f 9fb4c428 25d04979 34c713f8 c4618187 ea7a6e98 7cd16efc 1436876c
f1544107 bedeee14 56e9af27 a04aa441 3cf7c899 92ecbae6 dd67016d 151682eb
a842eedf fdba60b4 f1907b75 20e3030f 24d8c29e e139673b efa63fb8 71873054
b6f2cf3b 9f326442 cb15a4cc b01a4504 f1e47d8d 844a1be5 bae7dfdc 42cbda70
cd7dae0a 57e85b7a d53f5af6 20cf4d8c cea4d428 79d130a4 3486ebfb 33d3cddc
77853b53 37effcb5 c5068778 e580b3e6 4e68b8f4 c5c8b37e 0d809ea2 398feb7c
132a4f94 43b7950e 2fee7d1c 223613bd dd06caa2 37df932b c4248289 acf3ebc3
5715f6b7 ef3478dd f267616f c148cbe4 9052815e 5e410fab b48a2465 2eda7fa4
e87b40e4 e98ea084 5889e9e1 efd390fc dd07d35b db485694 38d7e5b2 57720101
730edebc 5b643113 94917e4f 503c2fba 646f1282 7523d24a e0779695 f9c17a8f
7a5b2121 d187b896 29263a4d ba510cdf 81f47c9f ad1163ed ea7b5965 1a00726e
11403092 00da6d77 4a0cdd61 ad1f4603 605bdfb0 9eedc364 22ebe6a8 cee7d28a

a0e736a0 5564a6b9 10853209 c7eb8f37 2de705ca 8951570f df09822b bd691a6c
aa12e4f2 87451c0f e0f6a27a 3ada4819 4cf1764f 0d771c2b 67cdb156 350d8384
5938fa0f 42399ef3 36997b07 0e84093d 4aa93e61 8360d87b 1fa98b0c 1149382c
e97625a5 0614d1b7 0e25244b 0c768347 589e8d82 0d2059d1 a466bb1e f8da0a82
04f19130 ba6e4ec0 99265164 1ee7230d 50b2ad80 eaee6801 8db2a283 ea8bf59e

Βιβλιογραφία

1. **Bruce Schneier**, *Applied Cryptography*, 2nd edition, Wiley, 758, 1996
2. **A. J. Menezes**, **P. C. van Oorschot**, and **S. A. Vanstone**, *Handbook of Applied Cryptography*, CRC Press, 780, 1996 δείγματα του βιβλίου.
3. **Douglas R. Stinson**, *Cryptography: Theory and Practice (Discrete Mathematics and Its Applications)*, 1st edition, CRC Press, 434, 1995.
4. **Wenbo Mao**, *Modern Cryptography: Theory and Practice*, 1st edition, Prentice Hall PTR, 740, 2003.
5. **William Stallings**, *Cryptography and Network Security: Principles and Practice*, 2nd Edition, Prentice Hall, 569, 1998.
6. **Henk C.A. van Tilborg**, *Fundamentals of Cryptology : A Professional Reference and Interactive Tutorial*, 1 edition, Springer, 512, 1999.
7. **David Kahn**, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, Scribner, 1200, 1996.
8. **Simon Singh**, *Κώδικες και Μυστικά*, Τραυλός, 606, 2001, ISBN 960-7990-42-0
9. **Β.Α. Κάτος - Γ.Χ. Στεφανίδης**, *Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης*, ΖΥΓΟΣ, 396, 2003.
10. **Δρ Ελευθέριος Μπότζιος** Σημείωσεις Εφαρμοσμένης ασφάλειας Πληροφοριακών Συστημάτων
11. CAST design Procedure
12. Κ.Μαγκος Α Νιξαρλιδης ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ
13. C.E Shannon Communication Theory of Secrecy Systems