ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ & ΠΛΗΡΟΦΟΡΙΚΗΣ

ΕΡΓΑΣΙΑ ΕΞΑΜΗΝΟΥ

ΓΙΑ ΤΟ ΜΑΘΗΜΑ

ΔΙΚΤΥΑ ΔΗΜΟΣΙΑΣ ΧΡΗΣΗΣ ΚΑΙ

ΔΙΑΣΥΝΔΕΣΗ ΔΙΚΤΥΩΝ

ΚΡΥΠΤΑΛΓΟΡΙΘΜΟΣ DES

ΚΑΝΤΑΣ ΠΑΝΑΓΙΩΤΗΣ

Α.Μ 5777

ΔΙΔΑΣΚΩΝ: ΧΡΗΣΤΟΣ ΜΠΟΥΡΑΣ

ΠΑΤΡΑ 2018

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΕΧΟΜΕΝΑ……I

ΑΚΡΩΝΥΜΙΑ…….…….III

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ…….1

1.1 ΕΙΣΑΓΩΓΗ……...5

1.2 ΤΙ ΕΙΝΑ Η ΚΡΥΠΤΟΓΡΑΦΙΑ……..5

1.3 ΙΣΤΟΡΙΑ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ……....7

1.3.1 ΠΡΩΤΗ ΠΕΡΙΟΔΟΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ (1900 Π.Χ. – 1900 Μ.Χ.)……....7

1.3.2 ΔΕΥΤΕΡΗ ΠΕΡΙΟΔΟΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ (1900 Μ.Χ. – 1950 Μ.Χ.)……....8

1.3.3 ΤΡΙΤΗ ΠΕΡΙΟΔΟΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ (1950 Μ.Χ. - ΣΗΜΕΡΑ)……....9

1.4 ΣΤΟΧΟΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ……..…...10

ΚΕΦΑΛΑΙΟ 2: ΕΙΔΗ ΣΥΓΧΡΟΝΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ……11

2.1 ΕΙΣΑΓΩΓΗ……11

2.2 ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ…….....11

2.2.1 ΠΛΕΟΝΕΚΤΗΜΑΤΑ - ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΣΥΜΜΕΤΡΙΚΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ.....14

2.3 ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΙΑ……..14

2.3.1 ΠΛΕΟΝΕΚΤΗΜΑΤΑ – ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΑΣΥΜΜΕΤΡΗΣ

ΚΡΥΠΤΟΓΡΑΦΙΑΣ……....17

ΚΕΦΑΛΑΙΟ 3: Ο ΚΡΥΠΤΑΛΓΟΡΙΘΜΟΣ DES……19

3.1 ΕΙΣΑΓΩΓΗ…….....19

3.2 ΙΣΤΟΡΙΑ ΤΟΥ DES……..……..….20

3.3 ΔΙΚΤΥΑ FEISTEL……..……22

3.4 ΠΕΡΙΓΡΑΦΗ ΤΟΥ DES……...……...26

3.5 ΑΣΦΑΛΕΙΑ ΤΟΥ DES…….....34

3.6 TRIPLE DES(3DES)……..…..37

3.7 AES…….…39

ΚΕΦΑΛΑΙΟ 4: ΣΥΜΠΕΡΑΣΜΑΤΑ……..44

ΒΙΒΛΙΟΓΡΑΦΙΑ……...…45

ΑΚΡΩΝΥΜΙΑ

AES: Advanced Encryption Standard

DES: Data Encryption Standard

EFF: Electronic Frontier Foundation

FIPS: Federal Information Processing Standards

IBM: International Business Machines Corporation

NBS: National Bureau of Standards

NSA: National Security Agency

NIST: National Institute of Standards and Technology

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1 Εισαγωγή

Στην εποχή της παγκόσμιας ηλεκτρονικής συνδεσιμότητας, των ιών και των χάκερ, της ηλεκτρονικής παρακολούθησης, και της ηλεκτρονικής απάτης, δεν υπάρχει καμία στιγμή στην οποία η ασφάλεια δεν έχει σημασία. Πρώτον, η εκρηκτική ανάπτυξη των υπολογιστικών συστημάτων και η σύνδεση τους μέσω δικτύων έχει αυξήσει την εξάρτηση των οργανισμών ,όσο και των μεμονωμένων χρηστών από τις πληροφορίες που αποθηκεύονται και ανταλλάσσονται μέσω αυτών των συστημάτων. Το γεγονός αυτό έχει οδηγήσει σε μια αυξημένη ανάγκη προστασίας των δεδομένων και των πόρων από την παράνομη αποκάλυψη, καθώς και την ανάγκη διασφάλισης της αυθεντικότητας των δεδομένων και των μηνυμάτων, αλλά και της προστασίας των συστημάτων από επιθέσεις μέσω δικτύων. Δεύτερον, οι αρχές της κρυπτογραφίας και της ασφάλειας δικτύων έχουν ωριμάσει, οδηγώντας στην ανάπτυξη πρακτικών και άμεσα διαθέσιμων εφαρμογών που βελτιώνουν την ασφάλεια των δικτύων.[1]

1.2 Τι είναι η Κρυπτογραφία

Η λέξη κρυπτογραφία προέρχεται από τα συνθετικά «κρυπτός» + «γράφω» και είναι ένα διεπιστημονικό γνωστικό πεδίο που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης.[3]

Στη διεθνή βιβλιογραφία προτείνονται διάφοροι ορισμοί για την κρυπτογραφία ωστόσο ο πιο διαδεδομένος αναφέρεται στο πρόβλημα της μυστικής επικοινωνίας:

Ορισμός 1.1 – Η κρυπτογραφία μελετά τρόπους με τους οποίους μπορούμε να μετασχηματίσουμε ένα μήνυμα σε φαινομενικά ακατάληπτη μορφή.

Μπορεί να γίνει εύκολα αντιληπτό πως ο παραπάνω ορισμός αν και μπορεί να καλύψει στο μέγιστο βαθμό τη χρήση της κρυπτογραφίας από την απαρχή της μέχρι

και τη Βιομηχανική Επανάσταση, στην εποχή της πληροφορικής έχει σαφείς ελλείψεις.

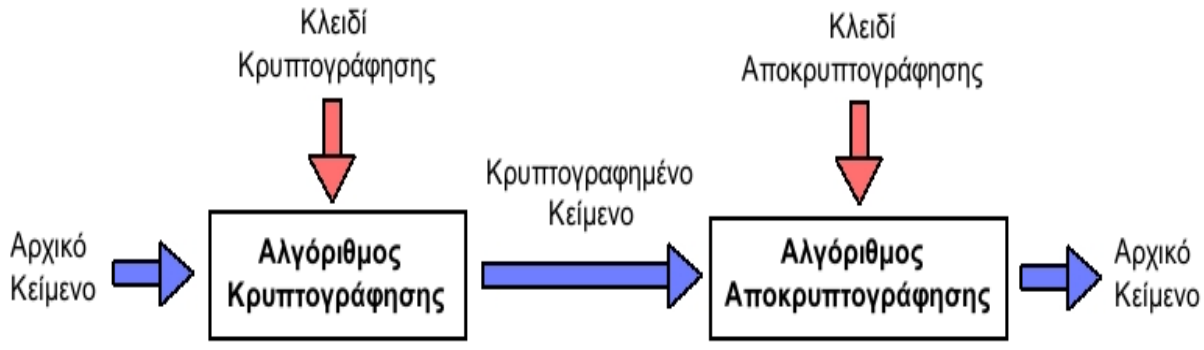
Ο ορισμός που δόθηκε μετέπειτα από τον Rivest (1990) εισήγαγε την έννοια του αντιπάλου και θεωρείται ίσως ο πιο ακριβής και πλήρης ορισμός που έχει δοθεί. Άρα καταλήγοντας με τον ορό κρυπτογραφία θα εννοείται το εξής:

Ορισμός 1.2 – Η κρυπτογραφία ασχολείται με την επικοινωνία παρουσία αντιπάλων.

Όντως η ύπαρξη αντιπάλου σε κάποια επικοινωνία αποτελεί τη βασική αιτία ύπαρξης και εφαρμογής της κρυπτογραφίας.

Η αρχική μορφή του μηνύματος, αποτελεί το απλό κείμενο (plaintext), ενώ το κρυπτογραφημένο κείμενο αποτελεί το κρυπτοκείμενο (ciphertext). Ο μετασχηματισμός του απλού κειμένου σε κρυπτοκείμενο ονομάζεται κρυπτογράφηση (encryption), ενώ ο μετασχηματισμός του κρυπτοκειμένου σε απλό κείμενο ονομάζεται αποκρυπτογράφηση (decryption). Οι διαδικασίες της κρυπτογράφησης και της αποκρυπτογράφησης υλοποιούνται με αλγόριθμο κρυπτογράφησης και αποκρυπτογράφησης αντίστοιχα. Οι δύο αυτοί αλγόριθμοι συνιστούν τον κρυπταλγόριθμο (cipher). Η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης απαιτεί μια επιπλέον ποσότητα πληροφορίας που ονομάζεται κλειδί (key).[2]

Η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης φαίνεται στο παρακάτω σχήμα.



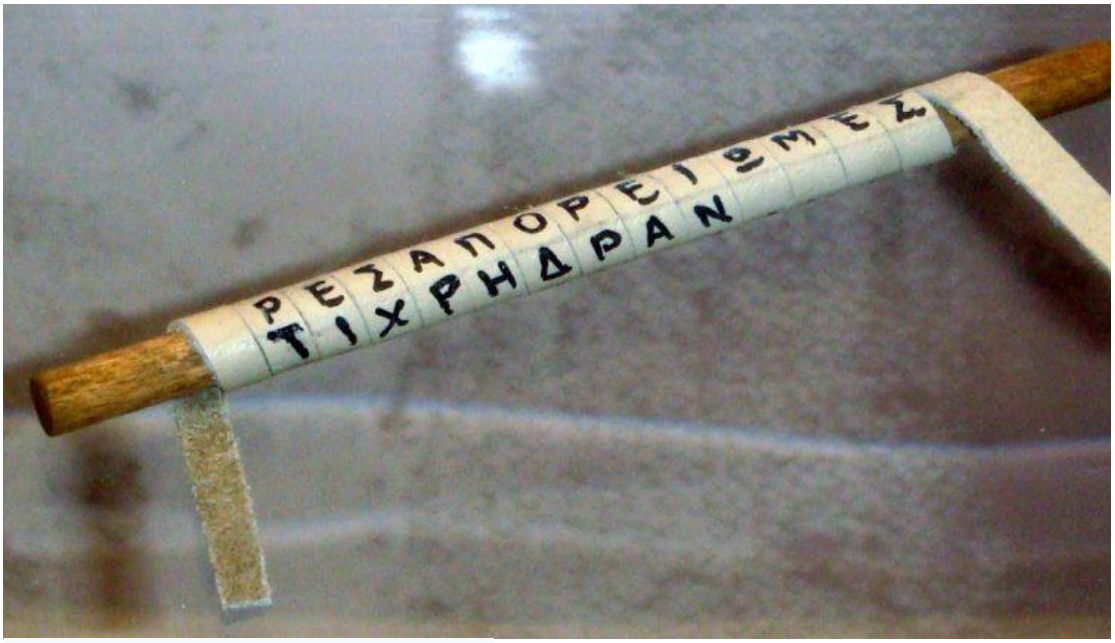
Εικόνα 1: Ένα τυπικό σύστημα κρυπτογράφησης - αποκρυπτογράφησης.[4]

1.3 Ιστορία της Κρυπτογραφίας

Ιστορικά, η κρυπτογραφία χρησιμοποιήθηκε για τη μετατροπή της πληροφορίας μηνυμάτων από μια κανονική, κατανοητή μορφή σε ένα «γρίφο», που χωρίς τη γνώση του κρυφού μετασχηματισμού θα παρέμενε ακατανόητος. Η ιστορία της κρυπτογραφίας μπορεί κατά προσέγγιση να διαιρεθεί σε τρείς περιόδους. Την πρώτη περίοδο κρυπτογραφίας (1900 π.Χ. – 1900 μ.Χ.), τη δεύτερη περίοδο κρυπτογραφίας (1900 μ.Χ. – 1950 μ.Χ.), και την τρίτη περίοδο κρυπτογραφίας (1950 μ.Χ. - Σήμερα).[3]

1.3.1 Πρώτη Περίοδος Κρυπτογραφίας (1900 π.Χ. – 1900 μ.Χ.)

Κατά τη διάρκεια της πρώτης περιόδου αναπτύχθηκε μεγάλο πλήθος μεθόδων και αλγορίθμων κρυπτογράφησης, που βασίζονταν κυρίως σε απλές αντικαταστάσεις γραμμάτων. Όλες αυτές δεν απαιτούσαν εξειδικευμένες γνώσεις και πολύπλοκες συσκευές, αλλά στηρίζονταν στην ευφυΐα και την ευρηματικότητα των δημιουργών τους. Η πρώτη στρατιωτική χρήση της κρυπτογραφίας αποδίδεται στους Σπαρτιάτες. Γύρω στον $5^{ο}$ αιώνα π.Χ. εφηύραν τη «σκυτάλη», την πρώτη κρυπτογραφική συσκευή, στην οποία χρησιμοποίησαν για την κρυπτογράφηση τη μέθοδο της μετάθεσης. Όπως αναφέρει ο Πλούταρχος, η «Σπαρτιατική Σκυτάλη» ήταν μιά ξύλινη ράβδος, ορισμένης διαμέτρου, γύρω από την οποία ήταν τυλιγμένη ελικοειδώς μια λωρίδα περγαμηνής. Το κείμενο ήταν γραμμένο σε στήλες, ένα γράμμα σε κάθε έλικα, όταν ξετύλιγαν τη λωρίδα, το κείμενο ήταν ακατάληπτο εξαιτίας της αναδιάταξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της σκυτάλης.[5]



Εικόνα 2: Η Σπαρτιατική Σκυτάλη.[6]

1.3.2 Δεύτερη Περίοδος Κρυπτογραφίας (1900 μ.Χ. – 1950 μ.Χ.)

Η δεύτερη περίοδος της κρυπτογραφίας καλύπτει τους δύο παγκόσμιους πολέμους, και λόγω της μεγάλης ανάγκης που υπήρξε για ασφάλεια, κατά τη μετάδοση ζωτικών πληροφοριών μεταξύ των στρατευμάτων των χωρών, αναπτύχθηκε σε πολύ μεγάλο βαθμό η κρυπτογραφία. Τα κρυπτοσυστήματα αυτής της περιόδου αρχίζουν να γίνονται πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάζονται «κρυπτομηχανές». Οι Γερμανοί έκαναν εκτενή χρήση ενός συστήματος γνωστού ως Enigma το οποίο εν τέλει «έσπασε» με τη συνεργασία του Alan Turing και άλλων επιστημόνων καθώς και ενός υπολογιστή, που κατασκεύασαν οι Βρετανοί επιστήμονες, ο οποίος ονομάσθηκε Colossus. [5]

Εικόνα 3: Η μηχανή Enigma.[7]

1.3.3 Τρίτη Περίοδος Κρυπτογραφίας (1950 μ.Χ. - Σήμερα)

Αυτή η περίοδος χαρακτηρίζεται από την έξαρση της ανάπτυξης στους επιστημονικούς κλάδους των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων. Η εποχή της σύγχρονης κρυπτογραφίας αρχίζει ουσιαστικά με τον Claude Shannon, αναμφισβήτητα θεωρείται ο πατέρας των μαθηματικών συστημάτων κρυπτογραφίας. Εκείνη την εποχή η κρυπτογραφία εξαφανίζεται και φυλάσσεται από τις μυστικές υπηρεσίες κυβερνητικών επικοινωνιών όπως η NSA. Πολύ λίγες εξελίξεις δημοσιοποιήθηκαν ξανά μέχρι τα μέσα της δεκαετίας του '70, όταν όλα άλλαξαν με τη δημοσίευση του σχεδίου προτύπου κρυπτογράφησης DES στον ομοσπονδιακό κατάλογο της Αμερικής στις 17 Μαρτίου 1975.[5]

1.4 Στόχος Κρυπτογραφίας

Όπως αναφέρθηκε και προηγουμένως η κρυπτογραφία ασχολείται με την επικοινωνία παρουσία αντιπάλων και παρέχει 4 βασικές λειτουργίες (Αντικειμενικούς Στόχους) :

- **Εμπιστευτικότητα :** Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη της συνομιλίας. Η εμπιστευτικότητα θα πρέπει να προσφέρεται με τέτοιο τρόπο ώστε να είναι αδύνατη η αποκάλυψη και πολλές φορές η ύπαρξη της ίδιας της πληροφορίας σε μη εξουσιοδοτημένα άτομα. Για παράδειγμα, κατά την κρίση στον Περσικό Κόλπο, η πληροφορία ότι η στρατιωτική ηγεσία των Ηνωμένων Πολιτειών προετοίμαζε επιχειρήσεις διέρρεε λόγω του αυξημένου αριθμού παραγγελιών σε πιτσαρία γειτονική του Πενταγώνου κατά τις νυχτερινές ώρες.

- **Ακεραιότητα :** Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης. Η ακεραιότητα θα πρέπει να παρέχει στον παραλήπτη και γενικότερα στον κάτοχο ενός μηνύματος τη δυνατότητα να μπορεί να ανιχνεύσει πιθανές αλλαγές στο μήνυμα από μη εξουσιοδοτημένα άτομα. Στο χώρο των τηλεπικοινωνιών και δικτύων, η ακεραιότητα είναι γνωστή ως ανίχνευση σφαλμάτων, οπού ένα μήνυμα μπορεί να υποστεί τροποποίηση λόγω του θορύβου του καναλιού επικοινωνίας.

- **Αυθεντικοποίηση :** Ο αποστολέας και ο παραλήπτης είναι σε θέση να εξακριβώσουν τις ταυτότητες τους, καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητες τους δεν είναι πλαστές. Αυθεντικοποίηση δεδομένων είναι η εξασφάλιση ότι ένα μήνυμα προέρχεται πράγματι από τον αποστολέα ο οποίος το έστειλε.

- **Μη Απάρνηση :** Ο παραλήπτης ή ο αποστολέας δεν μπορούν να αρνηθούν για την αποστολή ή τη λήψη του μηνύματος.[2]

ΚΕΦΑΛΑΙΟ 2: ΕΙΔΗ ΣΥΓΧΡΟΝΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

2.1 Εισαγωγή

Η κρυπτογραφία είναι με διαφορά το σημαντικότερο αυτοματοποιημένο εργαλείο για την ασφάλεια δικτύων και επικοινωνιών. Χρησιμοποιούνται κατά κύριο λόγο δύο μορφές κρυπτογραφίας: η συμβατική ή συμμετρική κρυπτογραφία, και η κρυπτογραφία δημόσιου κλειδιού ή ασύμμετρη κρυπτογραφία.[1]

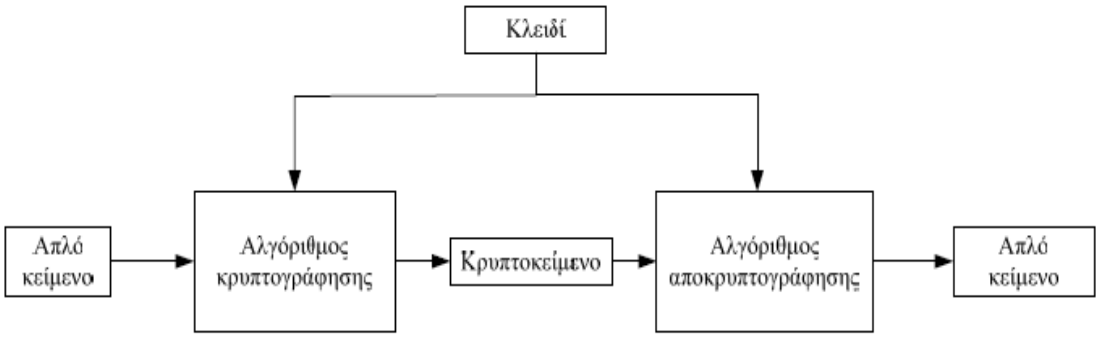
2.2 Συμμετρική Κρυπτογραφία

Η Συμμετρική κρυπτογραφία ήταν ο μόνος χρησιμοποιούμενος τύπος κρυπτογραφίας μέχρι τα τέλη της δεκαετίας του 1970. Αυτή η μορφή κρυπτογραφίας παραμένει με διαφορά ο ευρύτερα χρησιμοποιούμενος τύπος κρυπτογραφίας.

Οι συμμετρικοί κρυπτογραφικοί αλγόριθμοι μπορούν να χωριστούν σε δύο διαφορετικές κατηγορίες με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων:

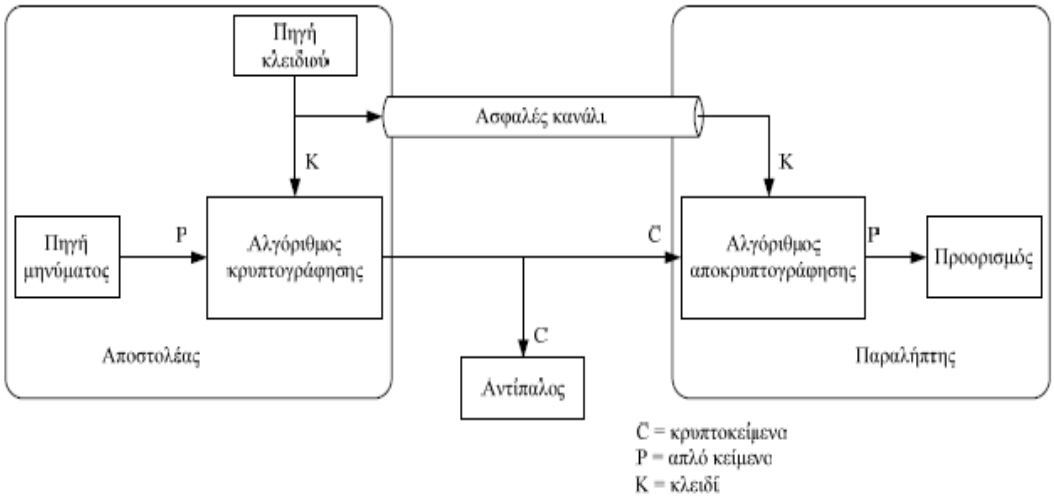
1. Δέσμης (Block Ciphers), οι οποίοι χωρίζουν το μήνυμα σε κομμάτια και κρυπτογραφούν κάθε ένα από τα κομμάτια αυτά χωριστά.
2. Ροής (Stream Ciphers), οι οποίοι κρυπτογραφούν μία ροή μηνύματος (stream) χωρίς να τη διαχωρίζουν σε τμήματα.

Το βασικό χαρακτηριστικό της συμμετρικής κρυπτογραφίας είναι ότι το κλειδί της κρυπτογράφησης είναι το ίδιο με αυτό της αποκρυπτογράφησης.



Εικόνα 4: Ένα συμμετρικό κρυπτοσύστημα.[2]

Το απλό κείμενο εισάγεται μαζί με το κλειδί στον αλγόριθμο κρυπτογράφησης. Το κλειδί είναι ανεξάρτητο του απλού κειμένου. Το αποτέλεσμα του αλγορίθμου κρυπτογράφησης είναι το κρυπτό-κείμενο. Για δεδομένο απλό κείμενο, δύο διαφορετικά κλειδιά παράγουν δύο διαφορετικά κρυπτοκείμενα. Ο αλγόριθμος αποκρυπτογράφησης δέχεται ως είσοδο το κρυπτοκείμενο και το κλειδί το οποίο είναι το ίδιο με αυτό του αλγορίθμου κρυπτογράφησης. Ο αλγόριθμος αποκρυπτογράφησης εφαρμόζει τους αντίστροφους μετασχηματισμούς από αυτούς του αλγορίθμου κρυπτογράφησης και επαναφέρει το κείμενο στην αρχική του μορφή, αυτή του απλού κειμένου.



Εικόνα 5: Μοντέλο επικοινωνίας συμμετρικού κρυπτοσυστήματος.[2]

Υπάρχουν δύο απαιτήσεις για την ασφαλή χρήση της συμμετρικής κρυπτογραφίας:

1. Χρειάζεται ένας ισχυρός αλγόριθμος κρυπτογράφησης. Ο αλγόριθμος πρέπει να είναι τέτοιος ώστε ένας αντίπαλος που τον γνωρίζει και έχει πρόσβαση σε ένα η περισσότερα κρυπτογραφημένα μηνύματα να μη μπορεί να αποκρυπτογραφήσει το μήνυμα, ούτε να καταλάβει ποιό είναι το μυστικό κλειδί. Αυτή η απαίτηση δηλώνεται συνήθως με ακόμα πιο ισχυρή μορφή: Ο αντίπαλος πρέπει να μην είναι ικανός να αποκρυπτογραφήσει το μήνυμα ή να αποκαλύψει το μυστικό κλειδί ακόμα και στην περίπτωση που έχει στην κατοχή του πολλά κρυπτογραφημένα μηνύματα, καθώς και τα αρχικά μηνύματα από τα οποία προήλθαν τα κρυπτογραφημένα.
2. Αποστολέας και παραλήπτης θα πρέπει να έχουν παραλάβει αντίγραφα του μυστικού κλειδιού με ασφαλή τρόπο, και να διατηρούν το κλειδί σε ασφαλές μέρος. Αν κάποιος ανακαλύψει το κλειδί και γνωρίζει τον αλγόριθμο, τότε όλη η επικοινωνία με αυτό το κλειδί είναι αναγνώσιμη.

Είναι σημαντικό να σημειωθεί ότι η ασφάλεια της συμμετρικής κρυπτογράφησης βασίζεται στη μυστικότητα του κλειδιού, και όχι στη μυστικότητα του αλγορίθμου που χρησιμοποιείται. Αυτό σημαίνει ότι θεωρείται πρακτικά αδύνατο να αποκρυπτογραφήσει κανείς ένα μήνυμα όταν έχει στη διάθεση του το κρυπτογράφημα και γνωρίζει μόνο τον αλγόριθμο κρυπτογράφησης/ αποκρυπτογράφησης που χρησιμοποιείται. Με άλλα λόγια, δε χρειάζεται να κρατείται μυστικός ο αλγόριθμος κρυπτογράφησης, το μόνο που πρέπει να μείνει μυστικό είναι το κλειδί.

Αυτό το χαρακτηριστικό γνώρισμα της συμμετρικής κρυπτογραφίας την καθιστά κατάλληλη για ευρεία χρήση. Το γεγονός ότι ο αλγόριθμος δεν είναι απαραίτητο να μείνει μυστικός σημαίνει ότι οι κατασκευαστές μπορούν να αναπτύξουν χαμηλού κόστους υλοποιήσεις αλγορίθμων κρυπτογράφησης. Με τη χρήση συμμετρικής κρυπτογραφίας, το πρωταρχικό πρόβλημα ασφαλείας είναι η διατήρηση της μυστικότητας του κλειδιού.[1],[2],[9]

2.2.1 Πλεονεκτήματα - Μειονεκτήματα Συμμετρικής Κρυπτογραφίας

Το βασικό πλεονέκτημα των αλγόριθμων συμμετρικού κλειδιού είναι ότι η διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης είναι πολύ γρήγορη και δεν καταναλώνει σημαντική υπολογιστική ισχύ.

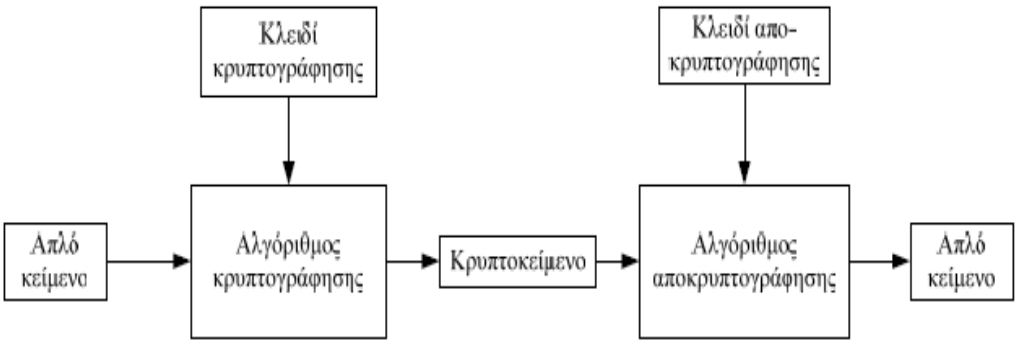
Από την άλλη μεριά η συμμετρική κρυπτογραφία έχει και ορισμένα μειονεκτήματα: Έστω ότι n μέλη επικοινωνούν μεταξύ τους χρησιμοποιώντας συμμετρική κρυπτογραφία. Τότε, ανά δύο θα πρέπει να μοιράζονται κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση. Το κάθε μέλος θα πρέπει να αποθηκεύσει n-1 διαφορετικά κλειδιά, προκειμένου να μπορεί να επικοινωνήσει με οποιοδήποτε από τα άλλα μέλη. Συνολικά θα πρέπει να μοιραστούν $(n^2 – n)/2$ κλειδιά. Εκτός από το γεγονός ότι μισό εκατομμύριο ασφαλή κανάλια επικοινωνίας είναι οικονομικώς ασύμφορα (αν όχι αδύνατο), τίθεται και το θέμα της αποθήκευσης των κλειδιών. Αυτή η αδυναμία αναφέρεται ως το πρόβλημα του τετραγώνου. Η απαίτηση του κρυπτοσυστήματος να χρησιμοποιείται το ίδιο κλειδί στην κρυπτογράφηση και αποκρυπτογράφηση, προϋποθέτει ότι ο αποστολέας και ο παραλήπτης έχουν κάποιον ασφαλή τρόπο να μοιραστούν αυτή την πληροφορία, το οποίο δεν είναι εφικτό σε οποιαδήποτε περίσταση.[2]

2.3 Ασύμμετρη Κρυπτογραφία

Η Ασύμμετρη κρυπτογραφία ή δημόσιου κλειδιού (Public Key Cryptography) επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman και παρέχει ένα εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης από την προγενέστερη κρυπτογράφηση συμμετρικού κλειδιού.Είναι η πρώτη πραγματικά επαναστατική εξέλιξη στην κρυπτογραφία εδώ και κυριολεκτικά χιλιάδες χρόνια.

Πρώτα από όλα, οι αλγόριθμοι δημόσιου κλειδιού βασίζονται σε μαθηματικές συναρτήσεις και όχι σε απλές πράξεις σε bit. Το πιό σημαντικό είναι ότι η ασύμμετρη κρυπτογραφία περιλαμβάνει τη χρήση δύο ξεχωριστών κλειδιών, ένα κλειδί που ονομάζεται δημόσιο (public key) και ένα κλειδί που ονομάζεται ιδιωτικό (private

key). Η χρήση δύο κλειδιών έχει βαθιές συνέπειες στους τομείς της εμπιστευτικότητας, της διανομής κλειδιών, και της πιστοποίησης της αυθεντικότητας.

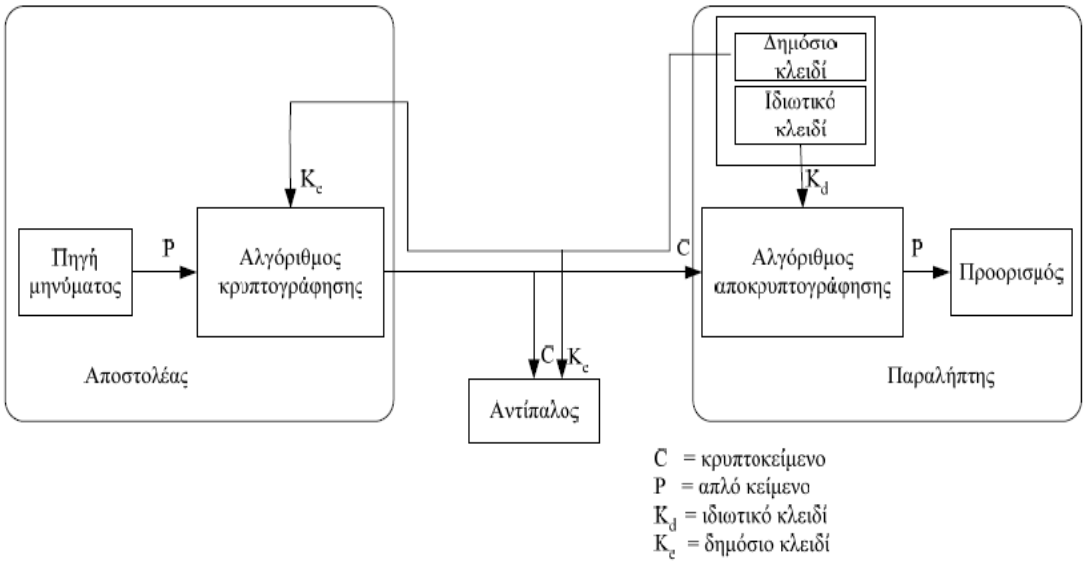


Εικόνα 8: Ένα ασύμμετρο κρυπτοσύστημα.[2]

Σύμφωνα με την ασύμμετρη κρυπτογραφία, το κλειδί κρυπτογράφησης δεν μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση, ή ακόμα καλύτερα, εάν χρησιμοποιηθεί το κλειδί κρυπτογράφησης για αποκρυπτογράφηση, το αποτέλεσμα δεν θα είναι το αρχικό απλό κείμενο. Το κλειδί αποκρυπτογράφησης είναι γνωστό μόνο στον παραλήπτη του μηνύματος. Έτσι σε αντίθεση με τα συμμετρικά κρυπτοσυστήματα, τα κλειδιά δημιουργούνται στον παραλήπτη, ο οποίος είναι ο μόνος που μπορεί να παράγει και να συσχετίσει ένα ζευγάρι ασύμμετρων κλειδιών. Το κλειδί για την κρυπτογράφηση ονομάζεται δημόσιο κλειδί γιατί μπορεί να διατεθεί ελεύθερα χωρίς να απαιτείται ασφαλές κανάλι για τη μετάδοση του. Το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση είναι το ιδιωτικό κλειδί και παραμένει υπό την κατοχή του παραλήπτη.

Έτσι το μοντέλο επικοινωνίας ενός ασύμμετρου κρυπτοσυστήματος δεν περιλαμβάνει ασφαλές κανάλι, αλλά η μετάδοση του μηνύματος περιλαμβάνει τα ακόλουθα στάδια:

1. Ο αποστολέας ζητάει από τον παραλήπτη το δημόσιο κλειδί Ke.
2. Ο παραλήπτης στέλνει το δημόσιο κλειδί μέσω του μη ασφαλούς καναλιού επικοινωνίας.
3. Ο αποστολέας κρυπτογραφεί το μήνυμα P με το δημόσιο κλειδί του παραλήπτη και στέλνει το κρυπτοκείμενο C στον παραλήπτη.
4. Ο παραλήπτης αποκρυπτογραφεί το κρυπτοκείμενο χρησιμοποιώντας το ιδιωτικό κλειδί Kd.



Εικόνα 9: Μοντέλο επικοινωνίας ασύμμετρου κρυπτοσυστήματος.[2]

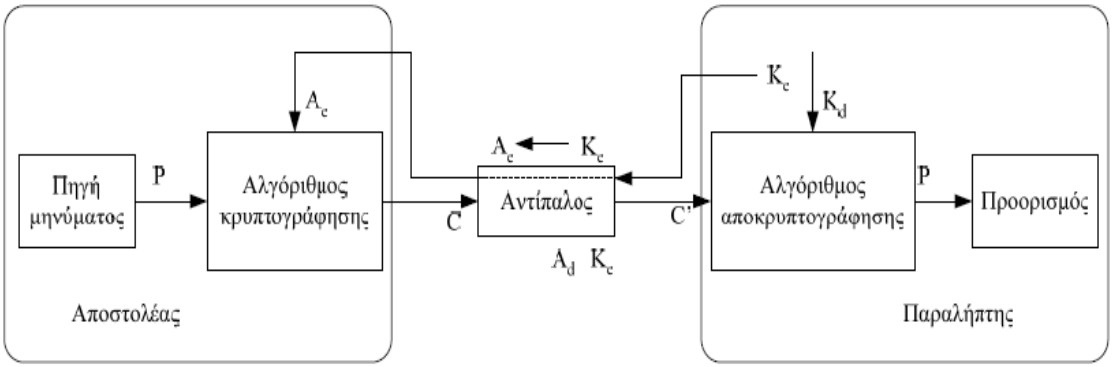
Υπάρχουν πέντε απαιτήσεις για τη χρήση της ασύμμετρης κρυπτογραφίας:

1. Πρέπει να είναι υπολογιστικά εύκολο για ένα μέλος B να δημιουργεί ένα ζεύγος κλειδιών (δημόσιο κλειδί K_c , ιδιωτικό κλειδί K_d).
2. Πρέπει να είναι υπολογιστικά εύκολο για τον αποστολέα A, με δεδομένο το δημόσιο κλειδί και το μήνυμα M που πρέπει να κρυπτογραφηθεί, να δημιουργήσει το αντίστοιχο κρυπτογράφημα.
3. Πρέπει να είναι υπολογιστικά εύκολο για τον παραλήπτη B να αποκρυπτογραφήσει το κρυπτογράφημα χρησιμοποιώντας το ιδιωτικό κλειδί ώστε να ανακτήσει το αρχικό μήνυμα.
4. Πρέπει να είναι υπολογιστικά αδύνατο για κάποιο δυνητικό επιτιθέμενο, ο οποίος γνωρίζει το δημόσιο κλειδί, να βρεί το ιδιωτικό κλειδί.
5. Πρέπει να είναι υπολογιστικά αδύνατο για κάποιο δυνητικό επιτιθέμενο, ο οποίος γνωρίζει το δημόσιο κλειδί και ένα κρυπτογράφημα, να ανακτήσει το αρχικό μήνυμα.[1],[2],[8]

2.3.1 Πλεονεκτήματα – Μειονεκτήματα Ασύμμετρης Κρυπτογραφίας

Τα πλεονεκτήματα της ασύμμετρης κρυπτογραφίας είναι ότι κάνει ευκολότερη τη διανομή κλειδιών σε σχέση με την συμμετρική γιατί όλοι μπορούν να γνωρίζουν το δημόσιο κλειδί αλλά όχι και το ιδιωτικό, ενώ στη συμμετρική χρησιμοποιείται το ίδιο κλειδί στην επικοινωνία. Επιπλέον, χρειάζονται λιγότερα κλειδιά O(n) στην ασύμμετρη από ότι στη συμμετρική που χρειάζεται ένα κλειδί για κάθε ζευγάρι που επικοινωνεί $O(n^2)$.

Από την άλλη μεριά η ασύμμετρη κρυπτογραφία είναι πολύ πιό αργή μέθοδος κρυπτογραφίας από τη συμμετρική. Επίσης παρότι δεν τίθεται το πρόβλημα της διανομής του κλειδιού, υπάρχει το πρόβλημα του «ενδιάμεσου ατόμου» (man in the middle). Συγκεκριμένα ο αποστολέας και ο παραλήπτης επικοινωνούν με ψηφιακά μέσα στέλνοντας μόνο μηνύματα, ο αντίπαλος έχει τη δυνατότητα στο μοντέλο του ασύμμετρου κρυπτοσυστήματος να συμμετέχει ενεργά, προκειμένου να αποκρυπτογραφήσει το μήνυμα. Ο αντίπαλος παρεμβάλλεται μεταξύ του αποστολέα και του αποδέκτη και αναλαμβάνει να δρομολογεί τα μηνύματα που ανταλλάσσονται μεταξύ του αποστολέα και του αποδέκτη. Έτσι, κατά την περίοδο της αποστολής του δημόσιου κλειδιού, ο αντίπαλος αντικαθιστά το δημόσιο κλειδί του παραλήπτη K_e με το δικό του δημόσιο κλειδί A_e, εφόσον γνωρίζει και το ιδιωτικό του κλειδί A_d. Ο αποστολέας πιστεύει ότι το δημόσιο κλειδί που έλαβε είναι του παραλήπτη του μηνύματος, ενώ το κλειδί αυτό στην πραγματικότητα είναι του αντιπάλου. Συνεπώς, το μήνυμα κρυπτογραφείται (C) με το δημόσιο κλειδί του αντιπάλου. Στη συνέχεια, ο αντίπαλος αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί, το κρυπτογραφεί με το δημόσιο κλειδί του παραλήπτη και μεταβιβάζει το νέο κρυπτοκείμενο (C′) στον παραλήπτη, με αποτέλεσμα η παρεμβολή του να μη γίνει αντιληπτή από κανέναν από τους δύο συμμετέχοντες.[2],[9]



Εικόνα 10: Η επίθεση του «ενδιάμεσου ατόμου».[2]

ΚΕΦΑΛΑΙΟ 3:

ΚΡΥΠΤΑΛΓΟΡΙΘΜΟΣ DES

3.1 Εισαγωγή

Ο DES (Data Encryption Standard) έχει μελετηθεί εκτενώς από τη δημοσίευση του και είναι ο πιο ευρέως χρησιμοποιούμενος συμμετρικός αλγόριθμος στον κόσμο. Το αρχικό κείμενο έχει μήκος 64 bit και το κλειδί έχει μήκος 56 bit. Στην πραγματικότητα το αρχικό κλειδί έχει μέγεθος 64 bit, αλλά μόνον τα 56 από αυτά συμμετέχουν στην κρυπτογράφηση, τα υπόλοιπα 8 bit του κλειδιού χρησιμοποιούνται για αρτιότητα (parity bits). Κείμενα με μέγεθος μεγαλύτερο από 64 bit υφίστανται επεξεργασία σε τμήματα των 64 bit. Η δομή του αλγορίθμου DES αποτελεί μια μικρή παραλλαγή του δικτύου Feistel. Υπάρχουν 16 γύροι επεξεργασίας. Από το αρχικό κλειδί των 56 bit δημιουργούνται 16 υποκλειδιά, καθένα από τα οποία χρησιμοποιείται σε ένα γύρο. Γενικά λαμβάνει μια σειρά από bit απλού κειμένου (plaintext bits) σταθερού μήκους και την μετατρέπει, μέσω μιας σειράς πολύπλοκων ενεργειών, σε μια άλλη σειρά bit, το κρυπτοκείμενο (chiphertext) με το ίδιο μήκος.

Όταν χρησιμοποιείται για την επικοινωνία, τόσο ο αποστολέας όσο και ο παραλήπτης πρέπει να γνωρίζουν το ίδιο μυστικό κλειδί, το οποίο μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση και την αποκρυπτογράφηση του μηνύματος ή για τη δημιουργία και την επαλήθευση ενός κώδικα ταυτότητας μηνυμάτων. Ο DES μπορεί επίσης να χρησιμοποιηθεί για μεμονωμένους χρήστες κρυπτογράφησης, όπως για την αποθήκευση αρχείων σε ένα σκληρό δίσκο σε κρυπτογραφημένη μορφή. [1],[2],[9]

3.2 Ιστορία του DES

Ο DES είναι ο κρυπταλγόριθμος ο οποίος είχε επιλεγεί ως επίσημο ομοσπονδιακό πρότυπο επεξεργασίας πληροφοριών (FIPS) για τις Ηνωμένες Πολιτείες το 1976 και στη συνέχεια χρησιμοποιήθηκε διεθνώς. Ο αλγόριθμος αρχικά ήταν αμφισβητούμενος, με απόρρητα τα στοιχεία του σχεδιασμού του και ένα σχετικά μικρού μήκους κλειδί. Υπήρχαν υποψίες πως η δημιουργία του DES αποσκοπούσε στη δημουργία backdoor (κερκόπορτας) για την παραβίαση της ασφάλειας της Υπηρεσίας Εθνικής Ασφάλειας (NSA) των Ηνωμένων Πολιτειών. Ο DES υπέστη έντονη ακαδημαϊκή διερεύνηση και αποτέλεσε το κίνητρο για την κατανόηση των κρυπταλγόριθμων συμμετρικού κλειδιού και την ανάλυσή τους.

Η προέλευση του DES βρίσκεται στις αρχές της δεκαετίας του 1970. Το 1972, μετά την ολοκλήρωση μελέτης για την ασφάλεια των υπολογιστών της κυβέρνησης, το σώμα προτύπων των Η.Π.Α., γνωστό ως NBS, που τώρα ονομάζεται NIST, επισήμανε την ανάγκη για ένα κυβερνητικό πρότυπο με το οποίο θα μπορούσαν να κρυπτογραφηθούν μη απόρρητες, ευαίσθητες πληροφορίες. Στις 15 Μαΐου του 1973, μετά από διαβούλευση με την NSA, η NBS κάνει προτάσεις για έναν κρυπταλγόριθμο που θα ανταποκρίνεται σε κριτήρια αυστηρού σχεδιασμού. Εντούτοις, καμία από τις προτάσεις που υποβλήθηκαν δεν αποδείχθηκε κατάλληλη. Δημοσιεύθηκε μία δεύτερη πρόταση εκδήλωσης ενδιαφέροντος στις 27 Αυγούστου του 1974. Αυτή τη φορά, η IBM υπέβαλε έναν αλγόριθμο, ο οποίος κρίθηκε αποδεκτός: Ήταν κρυπταλγόριθμος που αναπτύχθηκε κατά τη διάρκεια της περιόδου 1973-1974 βασιζόμενος σε προϋπάρχοντα. Αυτός ήταν ο κρυπταλγόριθμος "Lucifer", τον οποίο δημιούργησε ο Horst Feistel. Η ομάδα της IBM συνέχισε το σχεδιασμό και την ανάλυση κρυπταλγόριθμων με τη βοήθεια των Feistel, Walter Tuchman, Don Coppersmith, Alan Konheim, Carl Meyer, Mike Matyas, Roy Adler, Edna Grossman, Bill Notz, Lynn Smith και Bryart Tuckerman.

Οι απόπειρες κρυπτανάλυσης του DES είχαν σαν αποτέλεσμα την ανακάλυψη και καθιέρωση ποικίλων αρχών σχεδίασης των κρυπταλγόριθμων τμήματος. Ο DES είναι βασισμένος στον κρυπταλγόριθμο Lucifer της IBM, του οποίου το τμήμα του απλού κειμένου, του κρυπτοκειμένου, καθώς και το μέγεθος του κλειδιού είναι 128bits. Ο DES σχεδιάσθηκε με βάση τα κριτήρια τα οποία διατυπώθηκαν το 1972 από το Υπουργείο Εμπορίου των ΗΠΑ, που επιζητούσε να βελτιωθεί η εθνική ασφάλεια με

κρυπτογραφικές μεθόδους για την αποθήκευση, επεξεργασία, και διανομή της πληροφορίας. Τα κριτήρια ήταν τα ακόλουθα:

- υψηλό επίπεδο ασφάλειας.
- πλήρεις και διαφανείς προδιαγραφές.
- η ασφάλεια δεν θα πρέπει να εξαρτάται από τη μυστικότητα του κρυπταλγορίθμου.
- διαθέσιμο σε, και προσβάσιμο από, όλους τους χρήστες.
- κατάλληλο για ποικιλία εφαρμογών.
- χαμηλό κόστος υλοποίησης.
- να είναι επιτρεπτή η εξαγωγή του.
- να είναι δυνατή η αξιολόγηση του.

Ωστόσο, στην πράξη συνέβησαν ορισμένα γεγονότα τα οποία ήρθαν σε αντίφαση με τα παραπάνω κριτήρια. Αρχικά, όσον αφορά το πρώτο κριτήριο της απαίτησης της υψηλής ασφάλειας, ο DES είχε πολύ μικρότερο κλειδί από αυτό του προκατόχου του, τον Lucifer. Στην περίπτωση του DES, ο κλειδοχώρος ορίζεται από $2^{56} \approx 72 \cdot 10^{15}$ κλειδιά, έναντι του κλειδοχώρου του Lucifer, ο οποίος περιέχει $2^{128} \approx 34 \cdot 10^{37}$ κλειδιά. Σε αυτό ευθύνεται η NSA, η οποία άσκησε πιέσεις για μικρό μήκος κλειδιού. Όσον αφορά το κριτήριο της διαφάνειας των προδιαγραφών, τα κριτήρια σχεδιασμού των κουτιών αντικατάστασης που περιέχονται στη συνάρτηση γύρου του DES αποκαλύφθηκαν στα μέσα περίπου της δεκαετίας του ’90. Τα κριτήρια σχεδιασμού των κουτιών περιείχαν ενδείξεις ότι η τεχνική διαφορικής κρυπτανάλυσης που ανακαλύφθηκε επίσημα στις αρχές της δεκαετίας του ’90, ήταν γνωστή 15 χρόνια πριν.

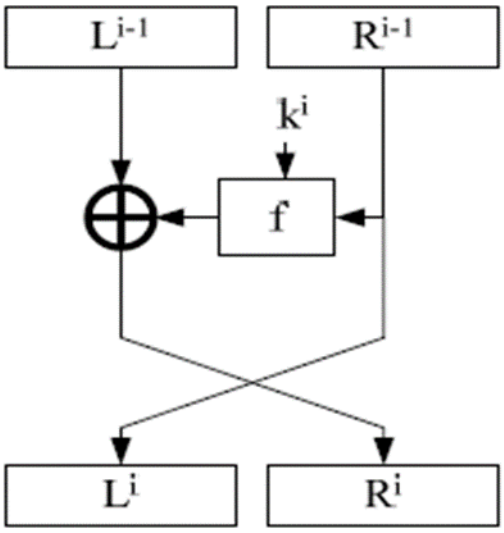
Η εισαγωγή του DES θεωρείται ότι ήταν καταλύτης για την ακαδημαϊκή μελέτη της κρυπτογραφίας, ιδιαίτερα των μεθόδων για να "σπάζουν" block κρυπταλγορίθμους. Μπορεί να ειπωθεί ότι το "αρχικό άλμα" του DES ξεπέρασε τις στρατιωτικές μελέτες και την ανάπτυξη των αλγόριθμων κρυπτογράφησης. Στη δεκαετία του 1970 υπήρχαν πολύ λίγοι κρυπτογράφοι, εκτός εκείνων των στρατιωτικών ή των μυστικών οργανώσεων, και ελάχιστη ήταν η ακαδημαϊκή έρευνα της κρυπτογραφίας. Υπάρχουν τώρα πολλοί δραστήριοι ακαδημαϊκοί κρυπτολόγοι

και τμήματα μαθηματικών με ισχυρά προγράμματα στην κρυπτογραφία και την ασφάλεια των πληροφοριών και των εμπορικών εταιρειών και συμβούλων. Μια γενιά κρυπταναλυτών έχει αναλύσει εξονυχιστικά τον αλγόριθμο DES προσπαθώντας να τον "σπάσει". Ανέφεραν πως ο DES έκανε περισσότερα για να γαλβανίσει τον τομέα της κρυπτανάλυσης από οτιδήποτε άλλο. Ένα εκπληκτικό μερίδιο της ανοιχτής βιβλιογραφίας στην κρυπτογραφία κατά τη δεκαετία του 1970 και του 1980 ασχολήθηκε με τον DES και ο DES είναι πρότυπο ενάντια σε όλους τους αλγορίθμους συμμετρικού κλειδιού μετά από σύγκριση.[2],[10]

3.3 Δίκτυα Feistel

Οι περισσότεροι συμμετρικοί αλγόριθμοι κρυπτογράφησης τμημάτων (block ciphers) έχουν τη δομή ενός δικτύου Feistel. Τα δίκτυα Feistel εμφανίστηκαν για πρώτη φορά στο εμπορικό σήμα του Lucifer της IBM, σχεδιασμένα από τους Horst Feistel και Don Coppersmith το 1973. Η ιδέα που είχε ο Feistel ήταν αρκετά απλή και είχε ως βασικό άξονα την απόδειξη της ασφάλειας ενός αλγορίθμου μέσω μη αντιστρέψιμων συναρτήσεων. Προσπάθησε να θέσει την ιδέα ότι τα μοντέλα των κρυπτογραφικών αλγορίθμων θα πρέπει να είναι όσο γίνεται πιο απλά. Το να προσθέτει κανείς μέρη τα οποία είναι ασφαλή, το καθένα ανεξάρτητα από το άλλο, δεν συνεπάγεται ότι το σύνολο είναι ασφαλές.

Η κρυπτογραφική πράξη τύπου Feistel παρατηρείται στην παρακάτω εικόνα η οποία αποτελεί και ένα γύρο σε κρυπτοσύστημα γινομένου. Το βασικό χαρακτηριστικό ενός δικτύου Feistel είναι η πλήρης ελευθερία στην επιλογή της συνάρτησης γύρου f.



Εικόνα 11: Ένας γύρος σε δίκτυο Feistel.[2]

Οι είσοδοι για τον αλγόριθμο κρυπτογράφησης είναι ένα τμήμα αρχικού κειμένου με μήκος 2w bit και ένα κλειδί K. Το τμήμα του αρχικού κειμένου διαιρείται σε δύο ίσα τμήματα L_0 και R_0. Τα δύο αυτά τμήματα περνούν από n γύρους επεξεργασίας και στη συνέχεια συνδυάζονται για την παραγωγή του τμήματος του κρυπτογραφήματος. Κάθε γύρος επεξεργασίας (βήμα) i δέχεται ως εισόδους τα Li_{-1} και Ri_{-1} ,τα οποία προέρχονται από τον προηγούμενο γύρο, καθώς επίσης και ένα υποκλειδί Ki το οποίο παράγεται από το κλειδί K. Γενικά, τα υποκλειδιά Ki είναι διαφορετικά τόσο μεταξύ τους όσο και με το K, και παράγονται από το κλειδί με έναν αλγόριθμο παραγωγής υποκλειδιών (subkey generation algorithm). Όλοι οι γύροι επεξεργασίας έχουν την ίδια δομή. Στο αριστερό μισό των δεδομένων γίνεται κάποια αντικατάσταση. Αυτό πραγματοποιείται με εφαρμογή μιας συνάρτησης γύρου (round fuction) F στο δεξιό μισό των δεδομένων και στη συνέχεια με συνδυασμό της εξόδου της συνάρτησης και του αριστερού μισού των δεδομένων με τον τελεστή αποκλειστικής διάζευξης (exclusive OR ,XOR). Η συνάρτηση γύρου έχει την ίδια γενική μορφή σε κάθε γύρο, αλλά πραγματοποιείται από το υποκλειδί Ki κάθε γύρου. Μετά από αυτή την αντικατάσταση εκτελείται μία μετάθεση, που αποτελείται από την εναλλαγή των δύο μισών του τμήματος δεδομένων.

Η ακριβής υλοποίηση του δικτύου Feistel εξαρτάται από τις επιλογές των παρακάτω παραμέτρων και σχεδιαστικών χαρακτηριστικών:

- Μέγεθος τμημάτων (block size): Όσο μεγαλύτερα είναι τα μεγέθη των τμημάτων τόσο αυξάνεται η ασφάλεια, όμως μειώνεται η ταχύτητα

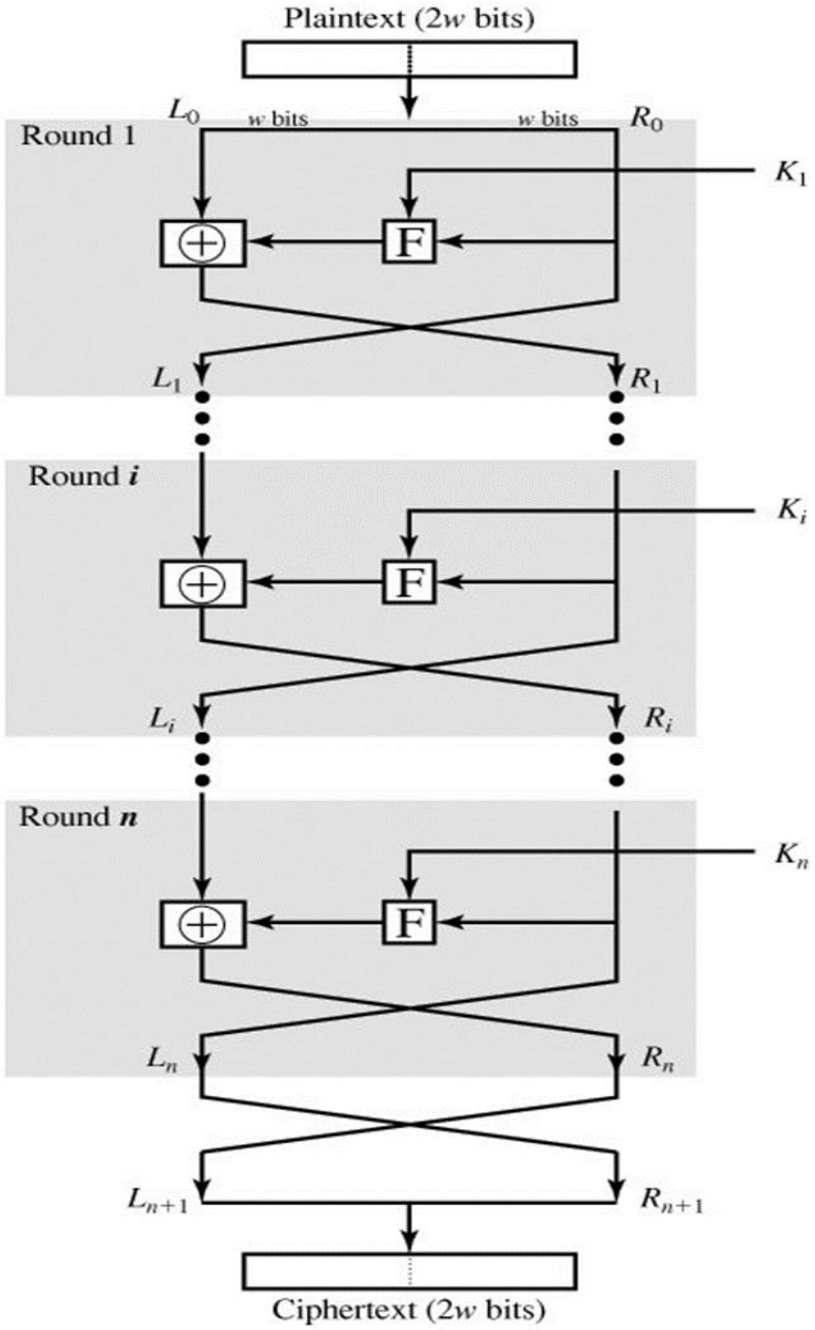
κωδικοποίησης και αποκωδικοποίησης. Ένα μέγεθος τμήματος ίσο με 64 bit δίνει μια εύλογη ισορροπία, και είναι σχεδόν καθολική επιλογή στο σχεδιασμό αλγόριθμων κρυπτογράφησης τμημάτων.

- Μέγεθος κλειδιού (key size): Μεγαλύτερο μέγεθος κλειδιού σημαίνει μεγαλύτερη ασφάλεια, αλλά μπορεί να μειώσει την ταχύτητα κωδικοποίησης και αποκωδικοποίησης. Το πιο συνηθισμένο μέγεθος κλειδιού στους σύγχρονους αλγορίθμους είναι τα 128 bit.
- Αριθμός γύρων (number of rounds): Η ουσία της κρυπτογράφησης Feistel είναι ότι μόνο ένας γύρος προσφέρει ανεπαρκή ασφάλεια αλλά πολλοί γύροι προσφέρουν αυξημένη ασφάλεια. Ο τυπικός αριθμός γύρων είναι 16.
- Αλγόριθμος παραγωγής υποκλειδιών (subkey generation algorithm): Η μεγαλύτερη πολυπλοκότητα ως προς αυτόν τον αλγόριθμο οδηγεί σε μεγαλύτερη δυσκολία στην κρυπτανάλυση.
- Συνάρτηση γύρου (round function): Και πάλι, μεγαλύτερη πολυπλοκότητα σημαίνει μεγαλύτερη ανθεκτικότητα στην κρυπτανάλυση.

Υπάρχουν επίσης δυο ακόμα ζητήματα στο σχεδιασμό μιας κρυπτογραφικής δομής Feistel:

- Ταχεία κρυπτογράφηση/αποκρυπτογράφηση μέσω λογισμικού (fast software encryption/decryption): Σε πολλές περιπτώσεις η κρυπτογράφηση έχει ενσωματωθεί σε εφαρμογές ή βοηθητικές συναρτήσεις με τέτοιο τρόπο ώστε να αποκλείεται η υλοποίηση της σε υλικό (hardware). Κατά συνέπεια, η ταχύτητα εκτέλεσης του αλγορίθμου αποτελεί σημαντικό ζήτημα.
- Ευκολία ανάλυσης (ease of analysis): Αν και θα επιθυμούσαμε να κάνουμε τον αλγόριθμο μας όσο το δυνατόν πιο δύσκολο στην κρυπτανάλυση, υπάρχει ένα σημαντικό πλεονέκτημα στο να κάνουμε τον αλγόριθμο εύκολο στην ανάλυση. Αν ένας αλγόριθμος μπορεί να εξηγηθεί εύκολα και με σαφή τρόπο, είναι ευκολότερο να αναλυθεί για την εύρεση κρυπταναλυτικών ευπαθειών και έτσι να αναπτυχθεί ένα υψηλότερο επίπεδο ασφάλειας ως προς την ανθεκτικότητα του.

- Η αποκρυπτογράφηση σε ένα σύστημα Feistel είναι στην ουσία η ίδια με την κρυπτογράφηση. Ο κανόνας που ακολουθείται είναι ο εξής: Χρήση του κρυπτογραφήματος ως είσοδο για τον αλγόριθμο, όμως χρησιμοποίηση των υποκλειδιών K_i με την αντίστροφη σειρά. Με άλλα λόγια, θα χρησιμοποιηθεί το κλειδί K_n στον πρώτο γύρο, το κλειδί K_{n-1} στο δεύτερο ,κ.ο.κ.,και το K_1 στον τελευταίο. Αυτό είναι ιδιαίτερα επιθυμητό χαρακτηριστικό, επειδή έτσι δεν είναι απαραίτητο να υλοποιηθούν δύο διαφορετικοί αλγόριθμοι – ένας για την κρυπτογράφηση και ένας για την αποκρυπτογράφηση.

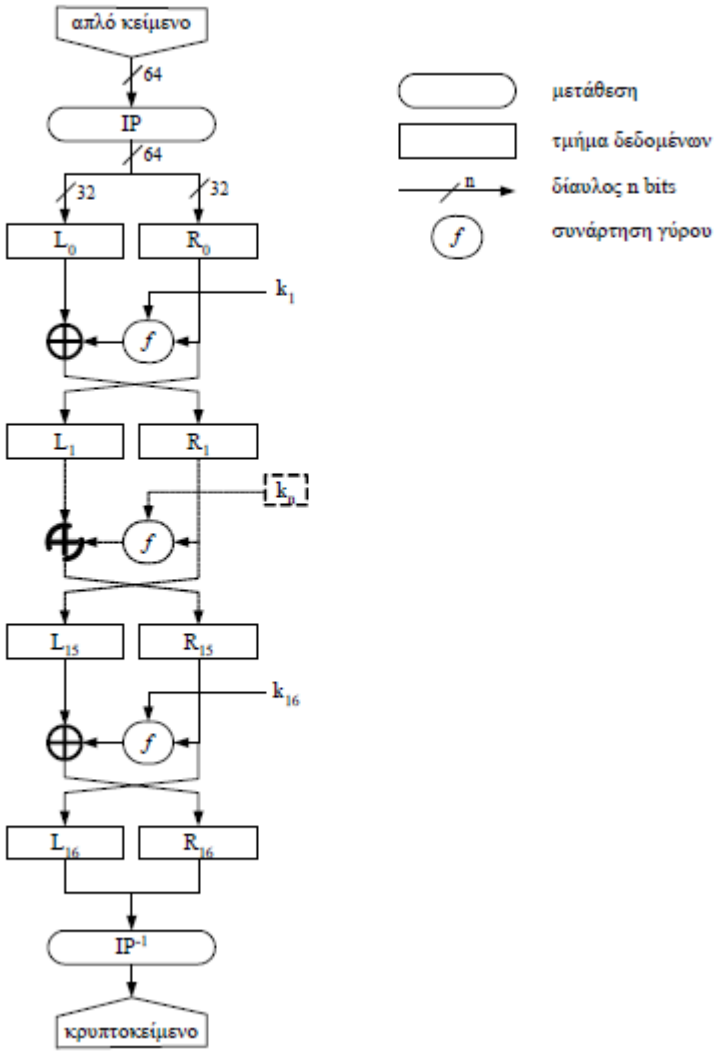


Εικόνα 12: Κλασσικό δίκτυο Feistel.[12]

Ο βασικός λόγος εκτενούς μελέτης των δικτύων Feistel είναι επειδή το πιο διαδεδομένο κρυπτοσύστημα DES, το οποίο θα μελετηθεί αργότερα, βασίζεται στα δίκτυα Feistel. [1],[2],[11]

3.4 Περιγραφή του DES

Ο κρυπταλγόριθμος DES παρουσιάζεται παρακάτω στην εικόνα 13 όπου διακρίνονται, η είσοδος του απλού κειμένου, η αρχική μετάθεση IP, η ακολουθία των 16 γύρων τύπου Feistel, η τελική μετάθεση IP^{-1} και τέλος η έξοδος του κρυπτοκειμένου(Οι IP,IP^{-1} είναι αντίστροφες συναρτήσεις). Ο κρυπταλγόριθμος DES έχει το χαρακτηριστικό ότι η κρυπτογράφηση και η αποκρυπτογράφηση μπορούν να υλοποιηθούν με την ίδια διαδικασία, με τη μόνη διαφορά ότι το πρόγραμμα κλειδιού της αποκρυπτογράφησης παράγει την αντίστροφη ακολουθία που παράγει το πρόγραμμα κλειδιού της κρυπτογράφησης. Αν δηλαδή κατά την κρυπτογράφηση το πρόγραμμα κλειδιού είναι $\{k_1,k_2,\ldots,k_{15}\}$, το πρόγραμμα κλειδιού κατά την αποκρυπτογράφηση θα είναι $\{k_{15},k_{14},\ldots,k_1\}$.



Εικόνα 13: Ο κρυπταλγόριθμος DES.[2]

Διαδικασία Μετάθεσης:

Η αρχική μετάθεση είναι η αντίστροφη της τελικής μετάθεσης και αντίστροφα. Ο λόγος που επιλέχθηκε αυτή η εξάρτηση των δύο μεταθέσεων είναι για να μπορεί να χρησιμοποιηθεί η ίδια διαδικασία και στην κρυπτογράφηση και στην αποκρυπτογράφηση, με τη μόνη διαφορά του προγράμματος των κλειδιών, όπως αναφέρθηκε παραπάνω. Στις δύο αυτές μεταθέσεις δε συμμετέχει το κλειδί, και επομένως δεν προσθέτουν ουσιαστικά περαιτέρω ασφάλεια στην κατασκευή. Η ύπαρξη της αρχικής και τελικής μετάθεσης έγινε για λόγους πρακτικούς, για να υπάρχει κάποιος χώρος αποθήκευσης (μνήμη) του απλού κειμένου και του κρυπτοκειμένου, πριν και μετά την εφαρμογή του δικτύου Feistel. Η ύπαρξη

αποθηκευτικών χώρων στην είσοδο και στα ηλεκτρονικά κυκλώματα είναι κοινή τακτική, και χρησιμοποιείται για να προσφέρει απομόνωση μεταξύ ενός ολοκληρωμένου κυκλώματος (microchip) και του υπόλοιπου ηλεκτρονικού κυκλώματος.

Ένας δεύτερος λόγος της επιλογής της συγκεκριμένης μετάθεσης είναι ότι δημιουργούνται ομαδοποιήσεις. Τα bit που βρίσκονται σε θέση πολλαπλάσια του αριθμού 8 δημιουργούν δυαδικές λέξεις. Έτσι στην περίπτωση που το απλό κείμενο αποτελείται από χαρακτήρες ASCII, διαχωρίζεται η πληροφορία του χαρακτήρα από το όγδοο bit αρτιότητας. Ωστόσο, δεν υπάρχουν ενδείξεις αν ο διαχωρισμός αυτός μειώνει ή αυξάνει την κρυπτογραφική δύναμη του DES. Γενικότερα, κατά την ανάλυση του DES δεν εξετάζονται η αρχική και η τελική μετάθεση, αλλά στην πράξη η συμμετοχή αυτών είναι υποχρεωτική λόγω της τυποποιημένης προδιαγραφής του κρυπταλγορίθμου.

Η αρχική μετάθεση παρουσιάζεται παρακάτω στην εικόνα 14. Ο πίνακας αριθμείται από αριστερά προς δεξιά και από επάνω προς τα κάτω. Η αρίθμηση καθορίζει το bit εξόδου, ενώ το περιεχόμενο του πίνακα καθορίζει το bit εισόδου. Έτσι, στο πρώτο bit της εξόδου της μετάθεσης θα εμφανισθεί το πεντηκοστό όγδοο (58) bit του απλού κειμένου, στο δεύτερο bit της εξόδου, το πεντηκοστό (50) bit, κ.ο.κ.

IP=

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

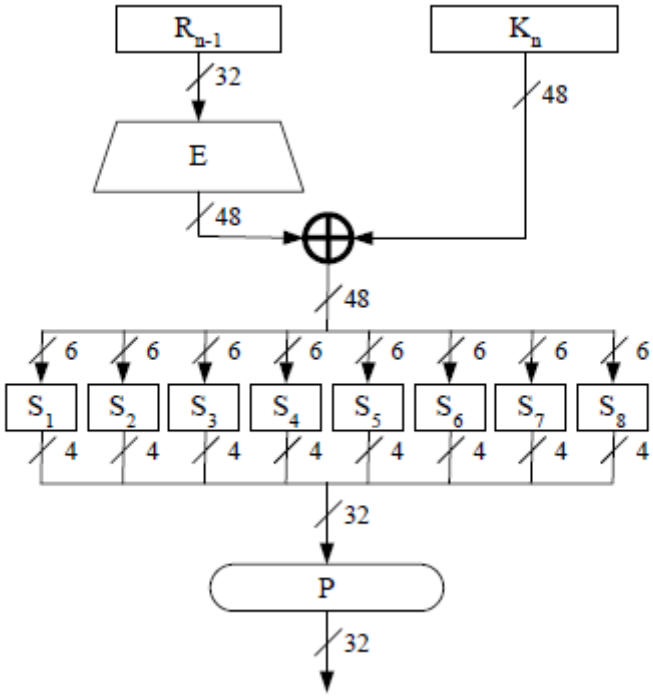
Εικόνα 14: Η αρχική αλληλομετάθεση IP.[2]

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

Έτσι η τελική μετάθεση θα είναι: IP^{-1}=| 40 8 48 … |

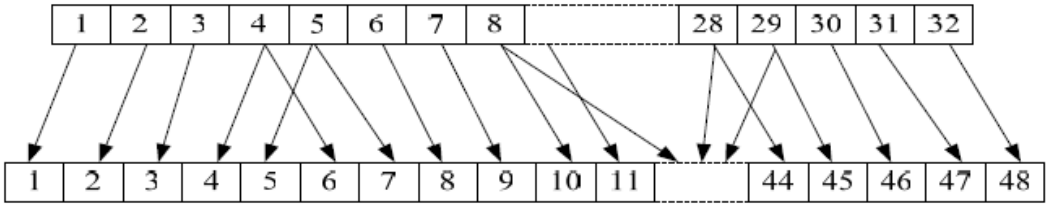
Συνάρτηση Γύρου f:

Η συνάρτηση γύρου αποτελείται από μια συνάρτηση επέκτασης $E:\{0,1\}^{32}\rightarrow\{0,1\}^{48}$, οκτώ κουτιά αντικατάστασης $Si:\{0,1\}^{6}\rightarrow\{0,1\}^{4}$, και μια τελική συνάρτηση μετάθεσης P των 32 bit. Η συνάρτηση γύρου παρουσιάζεται παρακάτω στην εικόνα 14.



Εικόνα 14: Η συνάρτηση γύρου του DES.[2]

Η συνάρτηση επέκτασης είναι μια μετάθεση στην οποία ορισμένα bit της εισόδου εμφανίζονται σε περισσότερες από μια θέσεις στην έξοδο. Πιο συγκεκριμένα, τα bit εισόδου στις θέσεις 4, 5, 8, 9, 12, 13, …, 28, 29 εμφανίζονται διπλά, όπως παρουσιάζεται παρακάτω στην εικόνα 15. Είναι προφανές ότι υπάρχει γραμμική σχέση μεταξύ των bit της εισόδου και των bit της εξόδου της συνάρτησης επέκτασης.



Εικόνα 15: Η συνάρτηση επέκτασης Ε.[2]

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

- Κάθε κουτί έχει είσοδο των 6 bit και έξοδο των 4 bit.
- Κανένα από τα bit της εξόδου δεν θα πρέπει να βρίσκεται σε γραμμική σχέση με οποιοδήποτε από τα bit της εισόδου.
- Αν τα δύο πρώτα bit και τα δύο τελευταία bit της εισόδου είναι σταθερά ενώ τα ενδιάμεσα bit αλλάζουν, οι έξοδοι που προκύπτουν θα πρέπει να είναι μοναδικές.
- Αν η απόσταση Hamming δύο εισόδων είναι ίση με 1, τότε η απόσταση Hamming των αντίστοιχων εξόδων θα πρέπει να είναι το λιγότερο ίση με 2.
- Αν δύο είσοδοι διαφέρουν στα δύο μεσαία bit, τότε οι αντίστοιχες έξοδοι θα πρέπει να διαφέρουν το λιγότερο σε 2 bit.
- Αν δύο είσοδοι έχουν τα δύο πρώτα bit διαφορετικά ενώ τα δύο τελευταία bit είναι ίδια, τότε οι αντίστοιχες έξοδοι θα πρέπει να είναι διαφορετικές.
- Για οποιαδήποτε μη μηδενική διαφορά των 6 bit της εισόδου, θα πρέπει το πολύ 8 από τα 32 ζευγάρια να προκαλούν την ίδια διαφορά εξόδου.
- Όμοια με το παραπάνω κριτήριο, αλλά θα πρέπει να εφαρμόζεται συγχρόνως σε οποιαδήποτε 3 από τα 8 κουτιά αντικατάστασης.

Με βάση τα κριτήρια αυτά σχεδιάσθηκαν τα κουτιά S_1-S_8 ,όπως φαίνονται στις παρακάτω εικόνες.

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

Εικόνα 16: Το κουτί αντικατάστασης S_2.[2]

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

Εικόνα 17: Το κουτί αντικατάστασης S_3.[2]

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

Εικόνα 18: Το κουτί αντικατάστασης S_4.[2]

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

Εικόνα 19: Το κουτί αντικατάστασης S_5.[2]

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

Εικόνα 20: Το κουτί αντικατάστασης S_6.[2]

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

Εικόνα 21: Το κουτί αντικατάστασης S_7.[2]

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

Εικόνα 22: Το κουτί αντικατάστασης S_8.[2]

Τέλος, οι έξοδοι των οκτώ κουτιών εισέρχονται σε μια τελική μετάθεση P των 32 bit η οποία παρουσιάζεται στην παρακάτω εικόνα.

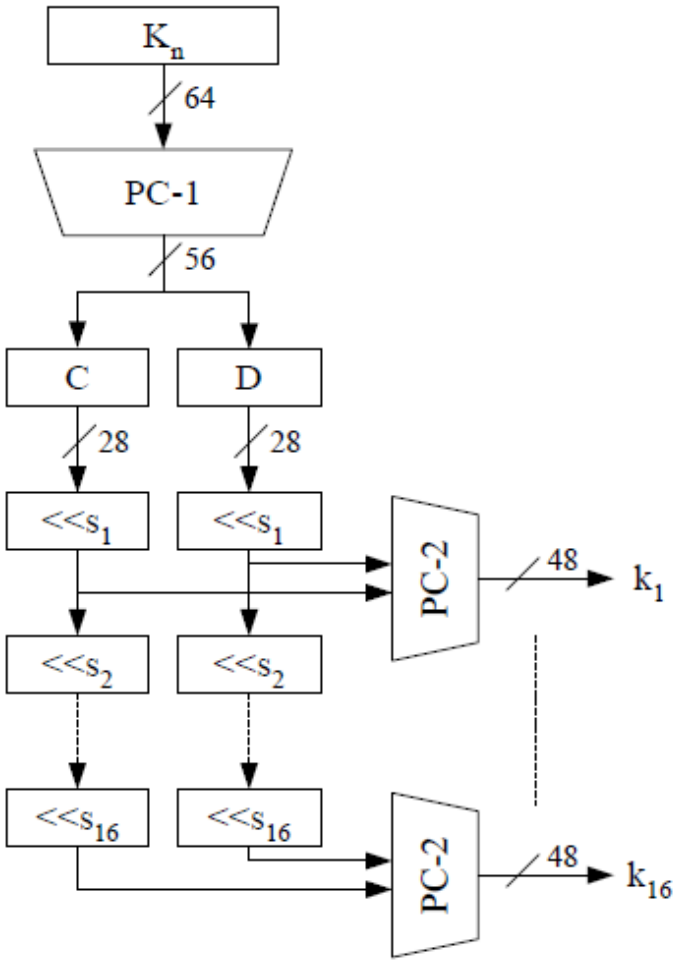
$$P=\begin{vmatrix} 16 & 7 & 20 & 21 & 29 & 12 & 28 & 17 \\ 1 & 15 & 23 & 26 & 5 & 18 & 31 & 10 \\ 2 & 8 & 24 & 14 & 32 & 27 & 3 & 9 \\ 19 & 13 & 30 & 6 & 22 & 11 & 4 & 25 \end{vmatrix}$$

Εικόνα 23: Η μετάθεση P πριν από την έξοδο της συνάρτησης γύρου.[2]

Το πρόγραμμα κλειδιού:

Η είσοδος της συνάρτησης γύρου απαιτεί 32 bit δεδομένων και 48 bit του κλειδιού. Σε κάθε γύρο το κλειδί προκύπτει από το πρόγραμμα κλειδιού όπως φαίνεται στην εικόνα 24. Το πρόγραμμα κλειδιού αποτελείται από δύο συναρτήσεις μετάθεσης επιλογής (permuted choice), PC-1:$\{0,1\}^{64}\rightarrow\{0,1\}^{56}$ και PC-2: $\{0,1\}^{56}\rightarrow\{0,1\}^{48}$, καθώς και από καταχωρητές ολίσθησης. Η μετάθεση επιλογής είναι μια μετάθεση κατά την οποία ορισμένα bit της εισόδου αγνοούνται και δεν εμφανίζονται στην έξοδο. Η PC-1 ξεχωρίζει όλα τα bit του αρχικού κλειδιού που θα συμμετάσχουν στο πρόγραμμα κλειδιού για τη δημιουργία των επιμέρους κλειδιών. Έτσι το κάθε όγδοο bit του αρχικού κλειδιού αγνοείται, με αποτέλεσμα να διατίθενται για την κρυπτογράφηση 64 – 8 = 56 bit.

Στη συνέχεια, τα 56 bit μοιράζονται σε δύο λέξεις των 28 bit και τροφοδοτούνται σε καταχωρητές ολίσθησης. Ανάλογα με το γύρο, πραγματοποιείται μια ολίσθηση n προκαθορισμένων θέσεων. Κατά την κρυπτογράφηση η ολίσθηση πραγματοποιείται προς την αριστερή φορά, ενώ κατά την αποκρυπτογράφηση η ολίσθηση εκτελείται προς τη δεξιά φορά. Ο αριθμός των ολισθήσεων έχει ως αποτέλεσμα το κλειδί να επανέλθει στην αρχική του θέση. Έτσι κατά την αποκρυπτογράφηση εκτελούνται οι αντίστροφες (δεξιές) ολισθήσεις, με αρχική τη μηδενική ολίσθηση, δηλαδή: 0, 1, 2, 2, …, 1.



n	s_n
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Εικόνα 24: Το πρόγραμμα κλειδιού του DES. [2]

Κατά την ολοκλήρωση της κάθε ολίσθησης επιλέγονται 48 από τα 56 bit που βρίσκονται στον καταχωρητή ολίσθησης σύμφωνα με τη μετάθεση επιλογής PC-2. Οι μεταθέσεις PC-1 και PC-2 παρουσιάζονται στις παρακάτω δύο εικόνες αντίστοιχα.[1],[9]

PC-1=

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

Εικόνα 25: Μετάθεση επιλογής PC-1. [2]

PC-2=

14	17	11	24	1	5
3	28	15	6	21	19
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Εικόνα 26: Μετάθεση επιλογής PC-2. [2]

3.5 Ασφάλεια του DES

Οι ανησυχίες για την ασφάλεια του αλγορίθμου εμπίπτουν σε δύο κατηγορίες: ανησυχίες σχετικά με τον ίδιο τον αλγόριθμο, και ανησυχίες σχετικά με τη χρήση του κλειδιού των 56 bit. Η πρώτη ανησυχία αναφέρεται στην πιθανότητα να είναι δυνατή η κρυπτανάλυση του αλγορίθμου με αξιοποίηση των χαρακτηριστικών του αλγορίθμου DES. Με το πέρασμα των χρόνων υπήρξαν διάφορες προσπάθειες για εύρεση και αξιοποίηση αδυναμιών του αλγορίθμου, καθιστώντας τον DES τον εκτενέστερα μελετημένο αλγόριθμο κρυπτογράφησης που υπάρχει.

Μια μεγαλύτερη ανησυχία είναι το μήκος του κλειδιού. Με μήκος κλειδιού 56 bit υπάρχουν 2^{56} πιθανά κλειδιά, δηλαδή περίπου $7{,}2 \times 10^{16}$. Με βάση αυτό μια επίθεση εξαντλητικής αναζήτησης κλειδιών φαινόταν να είναι πρακτικά ανέφικτη. Το μήκος του κλειδιού καθορίζει το πλήθος των πιθανών κλειδιών και ως εκ τούτου τη δυνατότητα πραγματοποίησης αυτής της προσέγγισης. Τέθηκαν από νωρίς ερωτήσεις για την επάρκεια του μήκους κλειδιού του DES, πριν ακόμα υιοθετηθεί ως πρότυπο. Το μικρό μήκος κλειδιού ήταν αυτό που, στην ουσία, υπαγόρευσε την ανάγκη για την αντικατάσταση του αλγορίθμου, παρά η θεωρητική κρυπτανάλυση.

Το πρώτο βήμα ανάλυσης του κρυπταλγορίθμου, είναι η εξέταση του μεγέθους του κλειδιού που ορίζει και το μέγεθος του κλειδοχώρου. Ο DES επιτρέπει 256 διαφορετικά κλειδιά. Αρχικά, ο DES ήταν σχεδιασμένος για 264 κλειδιά, αλλά

το μέγεθος αυτό μειώθηκε για να συμπεριληφθεί η πληροφορία των bit αρτιότητας. Μια άλλη παράμετρος η οποία είναι εξίσου κατακριτέα είναι το μικρό μέγεθος των κουτιών αντικατάστασης. Η διαδικασία καθορισμού των κουτιών αντικατάστασης ήταν κρυφή για αρκετά χρόνια και η παρέμβαση της NSA στο σχεδιασμό, δημιούργησε υποψίες ύπαρξης «μυστικής πόρτας» (trapdoor), η οποία επιτρέπει την αποκρυπτογράφηση χωρίς τη γνώση του κλειδιού. Ωστόσο, η ανάλυση των κουτιών έδειξε ότι η επιλογή αυτών έγινε με ιδιαίτερη προσοχή, αφού στην περίπτωση χρησιμοποίησης τυχαίων κουτιών, η ασφάλεια του DES μειωνόταν σημαντικά. Βέβαια, κάτι τέτοιο δεν αποδεικνύει την ύπαρξη ή όχι κάποιας μυστικής πόρτας.

Ιδιότητα των συμπληρωματικών μεταβλητών:

Μια ενδιαφέρουσα ιδιότητα είναι αυτή των συμπληρωματικών μεταβλητών. Μια δυαδική μεταβλητή Y ονομάζεται συμπληρωματική ως προς μια μεταβλητή X, όταν η Y είναι ίση με την αντίστροφη όλων των bit της X. Η συμπληρωματική μεταβλητή συμβολίζεται με X . Για παράδειγμα, 1001 = 0110 .Ο DES εμφανίζει τη συμπληρωματική ιδιότητα ως προς το απλό κείμενο, κλειδί και κρυπτοκείμενο. Αν η κρυπτογράφηση του DES ορίζεται από την: $\mathbf{c=e_k^{des}(p)}$, για οποιαδήποτε c, p και k, τότε ισχύει και $\mathbf{c`=e_{k`}^{des}(p)}$

Αυτό οφείλεται στην αποκλειστική διάζευξη του τμήματος της εισόδου με το κλειδί, πριν εισαχθούν στα κουτιά αντικατάστασης. Η αντιστροφή μιας μεταβλητής ισοδυναμεί με την αποκλειστική διάζευξη αυτής με το μοναδιαίο διάνυσμα. Επομένως η συμπληρωματική ιδιότητα του DES αποκαλύπτει την ύπαρξη απλών σχέσεων. Οι απλές σχέσεις είναι οι:

f (k) = k` ,

g1 (p, k) = p` και

g2 (c, k) = c`

τέτοιες ώστε: $e_k^{des}(p) = e_{f(k)}^{des}(g_1(p,k))= g_2(c,k)$.

Οι παραπάνω απλές σχέσεις μπορούν να χρησιμοποιηθούν για να μειωθεί ο χώρος αναζήτησης, από 256 σε 255, αφού σε κάθε κρυπτογράφηση (ή αποκρυπτογράφηση) μπορούν να δοκιμασθούν 2 κλειδιά.

Αδύναμα και ημιαδύναμα κλειδιά:

Το πρόγραμμα κλειδιού του DES είναι αδύναμο, όχι μόνον επειδή από οποιοδήποτε κλειδί γύρου μπορεί να βρεθεί με σχετική ευκολία το αρχικό κλειδί, αλλά και επειδή υπάρχουν κλειδιά τα οποία παράγουν το ίδιο πρόγραμμα κλειδιού κατά την κρυπτογράφηση και την αποκρυπτογράφηση. Υπό κανονικές συνθήκες, το πρόγραμμα κλειδιού της αποκρυπτογράφησης έχει αντίστροφη σειρά του προγράμματος κλειδιού της κρυπτογράφησης. Στην περίπτωση όμως που το κλειδί είναι κάποιο από τα κλειδιά της εικόνας 27, τότε το πρόγραμμα κλειδιών που προκύπτει είναι το ίδιο τόσο στην κρυπτογράφηση, όσο και στην αποκρυπτογράφηση. Αυτό σημαίνει ότι στην περίπτωση που ένα σύστημα χρησιμοποιεί διπλή κρυπτογράφηση, το κρυπτοκείμενο που προκύπτει θα είναι ίδιο με το απλό κείμενο. Δηλαδή, η δεύτερη κρυπτογράφηση θα αναιρεί την πρώτη. Τα κλειδιά αυτά ονομάζονται αδύναμα κλειδιά, και θα πρέπει να αποφεύγονται σε εφαρμογές που απαιτείται υψηλή ασφάλεια, όπως για παράδειγμα στη δημιουργία κλειδιών από ένα αρχικό κλειδί.

01	01	01	01	01	01	01	01
FE	FE	FE	FE	FE	FE	FE	FE
1F	1F	1F	1F	1F	1F	1F	1F
E0	E0	E0	E0	E0	E0	E0	E0

Εικόνα 27: Τα αδύναμα κλειδιά του DES.[2]

Εκτός από τα αδύναμα κλειδιά, υπάρχουν και τα ημιαδύναμα κλειδιά. Τα κλειδιά αυτά εμφανίζονται σε ζευγάρια, όπου το πρόγραμμα κλειδιού του ενός είναι ισοδύναμο με το πρόγραμμα κλειδιού του άλλου, με αντίστροφη σειρά. Έτσι, η κρυπτογράφηση του ενός κλειδιού ακολουθούμενη από την κρυπτογράφηση του δεύτερου κλειδιού που ορίζουν ζευγάρι, έχει ως αποτέλεσμα το κρυπτοκείμενο να είναι ίσο με το αρχικό απλό κείμενο. Η ύπαρξη τόσο των αδύναμων κλειδιών, όσο και των ζευγαριών των ημιαδύναμων κλειδιών, οφείλεται στην απλοϊκή κατασκευή του αλγορίθμου του προγράμματος κλειδιών.

01	FE	01	FE	01	FE	01	FE	1F	E0	1F	E0	0E	F1	0E	F1
FE	01	FE	01	FE	01	FE	01	E0	1F	E0	1F	F1	0E	F1	0E
01	E0	01	E0	01	F1	01	F1	1F	FE	1F	FE	0E	FE	0E	FE
E0	01	E0	01	F1	01	F1	01	FE	1F	FE	1F	FE	0E	FE	0E
01	1F	01	1F	01	0E	01	0E	E0	FE	E0	FE	F1	FE	F1	FE
1F	01	1F	01	0E	01	0E	01	FE	E0	FE	E0	FE	F1	FE	F1

Εικόνα 28: Τα ημιαδύναμα κλειδιά του DES.[2]

Το 1997, η εταιρεία RSA Security υποστήριξε μια σειρά διαγωνισμών με βραβείο $10.000 στην πρώτη ομάδα που θα "έσπαζε" ένα μήνυμα, το οποίο είχε κρυπτογραφηθεί με τον DES. Το διαγωνισμό κέρδισε το πρόγραμμα DESCHALL, που δημιουργήθηκε από τους Rocke Verser, Matt Curtin, και Justin Dolske, χρησιμοποιώντας το χρόνο που βρίσκονταν σε αδράνεια, χιλιάδων υπολογιστών σε ολόκληρο το Διαδίκτυο. Ο αλγόριθμος DES αποδείχθηκε τελικά και οριστικά ανασφαλής τον Ιούλιο του 1998, όταν το EFF ανακοίνωσε ότι κατάφερε να σπάσει ένα κρυπτογράφημα του DES χρησιμοποιώντας μια ειδική συσκευή με όνομα "DES cracker", η οποία κόστισε λιγότερα από 250.000 δολάρια. Η επίθεση κράτησε λιγότερο από τρεις μέρες. [1],[2],[10]

3.6 Triple DES (3DES)

Το 3DES δεν είναι τίποτα άλλο παρά τρία συστήματα DES σε σειρά. Η έξοδος δηλαδή του πρώτου συστήματος είναι η είσοδος του δευτέρου του οποίου η έξοδος είναι η είσοδος του τρίτου. Το 3DES χρησιμοποιεί τρία κλειδιά. Η συνάρτηση ακολουθεί μια διαδικασία κρυπτογράφησης-αποκρυπτογράφησης-κρυπτογράφησης όπως παρουσιάζεται στην εικόνα 29.

$C = E(K_3 , D(K_2 , E(K_1 , P)))$

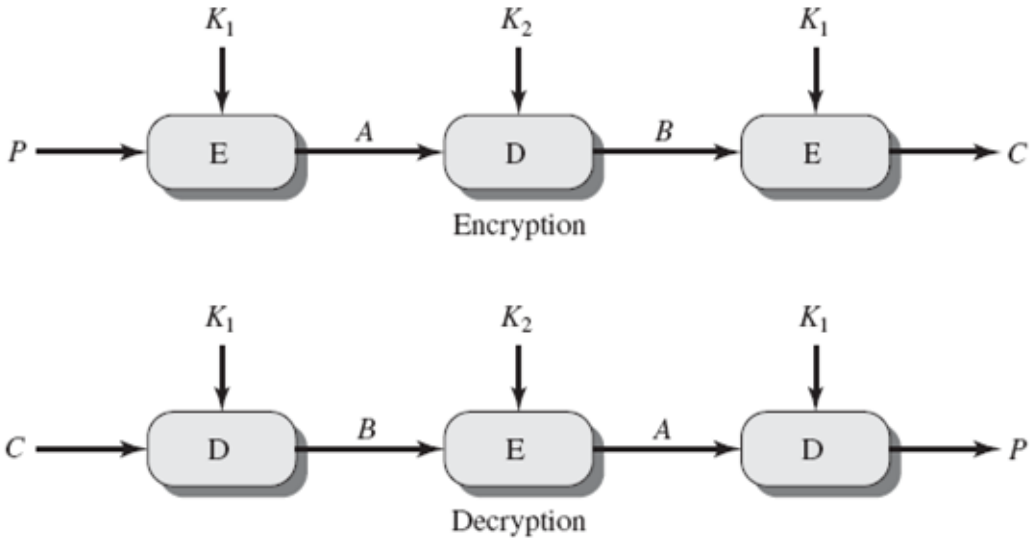
Όπου:

C = κρυπτογράφημα.

P = αρχικό κείμενο.

$E_K[X]$ = κρυπτογράφηση του X με χρήση του κλειδιού K.

$D_K[Y]$ = αποκρυπτογράφηση του Y με χρήση του κλειδιού K.



Εικόνα 29: Ο αλγόριθμος Τριπλού DES.[13]

Η αποκρυπτογράφηση είναι απλώς η ίδια με τα αντίστροφα κλειδιά. Δεν υπάρχει καμία κρυπτογραφική σπουδαιότητα στη χρήσης της αποκρυπτογράφησης για το δεύτερο στάδιο της κρυπτογράφησης 3DES. Το μόνο πλεονέκτημα της είναι ότι επιτρέπει στους χρήστες του 3DES να αποκρυπτογραφούν δεδομένα τα οποία είχαν κρυπτογραφηθεί με τον παλαιότερο αλγόριθμο απλού DES:

$C = E(K_1, D(K_1, E(K_1,P)))=E[K,P]$

Με τα τρία διαφορετικά κλειδιά, το 3DES έχει πραγματικό μέγεθος κλειδιού 168 bit. Είναι εύκολο να διαπιστώσει κανείς ότι ο 3DES είναι ένας εξαιρετικός αλγόριθμος αφού με μήκος κλειδιού 168 bit η επιτυχία των επιθέσεων εξαντλητικής αναζήτησης κλειδιών είναι ουσιαστικά αδύνατη.

Ο αλγόριθμος DES διαθέτει δυο στοιχεία που διασφαλίζουν την ευρεία χρήση του τα επόμενα χρόνια. Πρώτον, με μήκος κλειδιού 168 bit ξεπερνά όλες τις αδυναμίες του DES ως προς τις επιθέσεις εξαντλητικής αναζήτησης κλειδιών. Δεύτερον, ο πραγματικός αλγόριθμος κρυπτογράφησης που χρησιμοποιείται στον 3DES είναι ο ίδιος που υπάρχει και στον DES. Ο αλγόριθμος αυτός έχει υποστεί τον πιο εξονυχιστικό έλεγχο από οποιονδήποτε άλλον αλγόριθμο εδώ και μεγάλο χρονικό διάστημα, χωρίς να βρεθεί καμία αποδοτική μέθοδος κρυπτανάλυσης εκτός από την εξαντλητική αναζήτηση κλειδιών. Κατά συνέπεια, υπάρχει μεγάλη βεβαιότητα ότι ο 3DES είναι πολύ ανθεκτικός στην κρυπτανάλυση. Αν η ασφάλεια ήταν το μοναδικό πρόβλημα, τότε ο 3DES θα αποτελούσε την πιο κατάλληλη επιλογή

προτυποποιημένου αλγορίθμου κρυπτογράφησης για τις επόμενες δεκαετίες.[1],[2],[9]

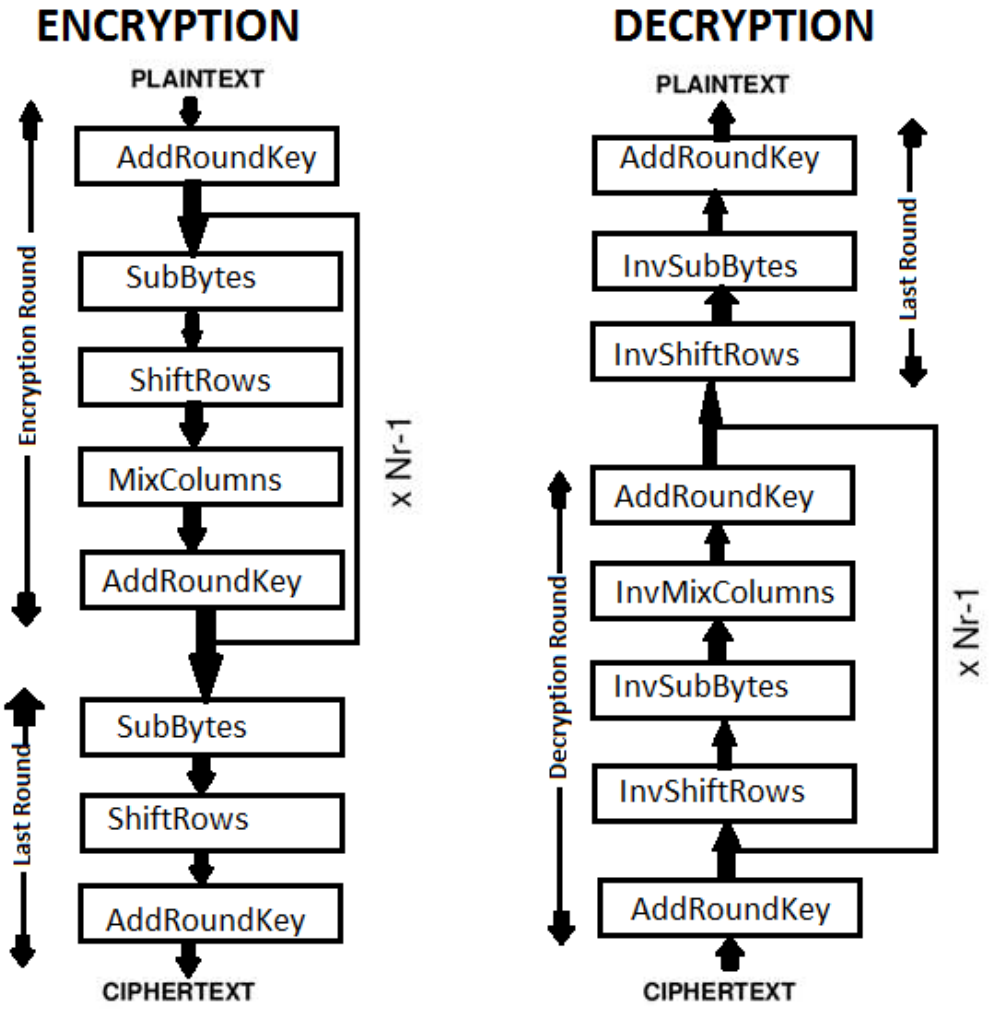
3.7 AES

Το βασικό μειονέκτημα του 3DES είναι ότι είναι σχετικά αργός σε υλοποιήσεις λογισμικού. Ο αρχικός αλγόριθμος DES είχε σχεδιαστεί για υλοποιήσεις υλικού στα μέσα της δεκαετίας του 70, και πλέον δε δίνει αποδοτικό κώδικα λογισμικού. Ο αλγόριθμος 3DES, που χρησιμοποιεί τριπλάσιο αριθμό γύρων, είναι αναλόγως πιο αργός. Ένα δεύτερο μειονέκτημα είναι ότι ο DES και ο 3DES χρησιμοποιούν μέγεθος τμήματος (block) 64 bit. Για λόγους απόδοσης και ασφάλειας θα ήταν επιθυμητό να έχουμε μεγαλύτερο μέγεθος τμήματος. Εξαιτίας αυτών των μειονεκτημάτων, ο 3DES δε μπορεί να θεωρηθεί κατάλληλος για μακροχρόνια χρήση.

Για την αντικατάσταση του, το NIST εξέδωσε το 1997 πρόσκληση για προτάσεις ενός εξελιγμένου προτύπου κρυπτογράφησης (Advanced Encryption Standard, AES), το οποίο θα έπρεπε να προσφέρει ίση ή μεγαλύτερη ασφάλεια με τον 3DES με σημαντικά βελτιωμένη απόδοση. Επιπρόσθετα ως προς αυτές τις γενικές απαιτήσεις, το NIST καθόρισε ότι ο AES θα πρέπει να είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης τμημάτων με μέγεθος τμήματος 128 bit και υποστήριξη για μεγέθη κλειδιών 128, 192, και 256 bit. Τα κριτήρια αξιολόγησης περιλάμβαναν την ασφάλεια, την υπολογιστική αποδοτικότητα, τις απαιτήσεις μνήμης, την καταλληλόλητα του υλικού και του λογισμικού, και την ευελιξία. Στον πρώτο κύκλο αξιολόγησης έγιναν δεκτές 15 προτάσεις αλγορίθμων. Ένας δεύτερος κύκλος μείωσε τον αριθμό στους πέντε. Το NIST ολοκλήρωσε τη διαδικασία αξιολόγησης και δημοσίευσε ένα τελικό πρότυπο (FIPS PUB 197) το Νοέμβριο του 2001. Το NIST επέλεξε ως προτεινόμενο αλγόριθμο AES τον αλγόριθμο Rijndael. Οι δύο ερευνητές που ανέπτυξαν και υπέβαλαν τον αλγόριθμο Rijndael για το πρότυπο AES είναι δύο κρυπτογράφοι από το Βέλγιο: οι Δρ. Joan Daemen και Δρ. Vincent Rijmen.

Περιγραφή του αλγορίθμου:

Ο AES χρησιμοποιεί μέγεθος τμήματος (block) 128 bit και μήκος κλειδιού που μπορεί να είναι 128, 192, ή 256 bit. Η υλοποίηση με μήκος κλειδιού 128 bit είναι η πιο συχνά χρησιμοποιούμενη και θα ασχοληθούμε έχοντας την ως πρότυπο.



Εικόνα 30: Η κρυπτογράφηση και αποκρυπτογράφηση στον αλγόριθμο AES.[14]

Η είσοδος στους αλγορίθμους κρυπτογράφησης και αποκρυπτογράφησης είναι ένα τμήμα των 128 bit. Στο FIPS PUB 197 αυτό το τμήμα απεικονίζεται ως ένας τετράγωνος πίνακας από byte. Αυτό το τμήμα αντιγράφεται στον **πίνακα αντικατάστασης** (state array), ο οποίος μεταβάλλεται σε κάθε βήμα της κρυπτογράφησης ή της αποκρυπτογράφησης. Μετά το τελευταίο στάδιο ο πίνακας αυτός αντιγράφεται σε έναν πίνακα εξόδου. Με τον ίδιο τρόπο, το κλειδί των 128 bit απεικονίζεται ως ένας τετράγωνος πίνακας από byte. Αυτό το κλειδί στη συνέχεια αναπτύσσεται σε έναν πίνακα λέξεων σχεδίου κλειδιών (key schedule words), κάθε

λέξη αποτελείται από τέσσερα byte και το συνολικό σχέδιο κλειδιών έχει μέγεθος σαράντα τεσσάρων λέξεων για ένα κλειδί 128 bit. Η ταξινόμηση των byte μέσα στον πίνακα γίνεται ανά στήλη. Έτσι, για παράδειγμα, τα πρώτα τέσσερα byte ενός αρχικού κειμένου των 128 bit, που αποτελεί την είσοδο του συστήματος κρυπτογράφησης, καταλαμβάνουν την πρώτη στήλη του πίνακα in, τα επόμενα τέσσερα byte καταλαμβάνουν τη δεύτερη στήλη, κ.ο.κ. Ομοίως, τα τέσσερα πρώτα byte του επεκταμένου κλειδιού, τα οποία αποτελούν μια λέξη, καταλαμβάνουν την πρώτη στήλη του πίνακα w.

Τα επόμενα σχόλια μας δίνουν μια καλύτερη εικόνα για τον αλγόριθμο AES:

1. Ένα αξιοσημείωτο στοιχείο αυτής της δομής είναι ότι δεν αποτελεί δομή Feistel. Ο AES δε χρησιμοποιεί δομή Feistel, αλλά επεξεργάζεται παράλληλα ολόκληρο το τμήμα των δεδομένων κατά τη διάρκεια κάθε γύρου, χρησιμοποιώντας αντικαταστάσεις και μετάθεση.
2. Το κλειδί που δίνεται ως είσοδος επεκτείνεται σε έναν πίνακα από σαράντα τέσσερις λέξεις των 32 bit, τον w[i]. Τέσσερις διαφορετικές λέξεις (128 bit) χρησιμοποιούνται ως κλειδί γύρου για κάθε γύρο.
3. Χρησιμοποιούνται τέσσερα διαφορετικά στάδια - ένα στάδιο μετάθεσης και τρία στάδια αντικατάστασης:
   - Αντικατάσταση byte (substitute bytes): Χρησιμοποιείται ένας πίνακας, που αναφέρεται ως S-box, ώστε να εκτελεστεί μια byte προς byte αντικατάσταση του τμήματος.
   - Μετατόπιση γραμμών (shift rows): Μια απλή μετάθεση που εκτελείται γραμμή προς γραμμή.
   - Ανάμιξη στηλών (mix columns): Μια αντικατάσταση, η οποία εναλλάσσει κάθε byte της στήλης ως συνάρτηση όλων των byte της στήλης.
   - Προσθήκη κλειδιού γύρου (add round key): Μια απλή πράξη XOR bit προς bit του τρέχοντος τμήματος με ένα κομμάτι του επεκταμένου κλειδιού.
4. Η δομή είναι αρκετά απλή. Και για την κρυπτογράφηση αλλά και την αποκρυπτογράφηση το κρυπτογραφικό σύστημα ξεκινά από το στάδιο προσθήκης του κλειδιού γύρου, ακολουθούμενο από εννέα άλλους γύρους,

καθένας από τους οποίους περιέχει και τα τέσσερα στάδια, και τέλος ακολουθεί ένας δέκατος γύρος τριών σταδίων.

5. Μόνο το στάδιο “Προσθήκης κλειδιού γύρου” χρησιμοποιεί το κλειδί. Για το σκοπό αυτό η κρυπτογράφηση ξεκινά και τελειώνει με ένα τέτοιο στάδιο. Κάθε άλλο στάδιο που εφαρμόζεται στην αρχή ή το τέλος είναι αντιστρέψιμο χωρίς γνώση του κλειδιού, και έτσι δεν θα πρόσθετε καθόλου ασφάλεια.

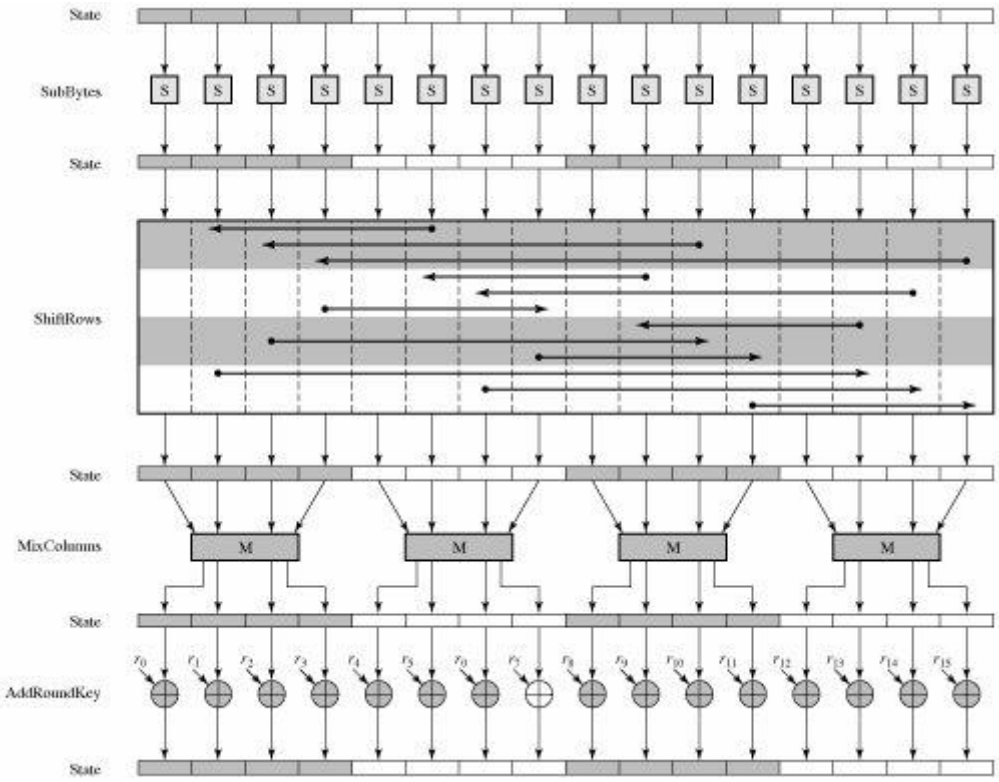
6. Το στάδιο προσθήκης κλειδιού γύρου δε θα είχε σημασία από μόνο του. Τα υπόλοιπα τρία στάδια τροποποιούν τα bit, αλλά μόνα τους δε θα παρείχαν καμία ασφάλεια επειδή δε χρησιμοποιούν το κλειδί. Μπορούμε να δούμε το σύστημα ως εναλλασσόμενες λειτουργίες κρυπτογράφησης ενός τμήματος με τον τελεστή XOR (φάση προσθήκης του κλειδιού γύρου), ακολουθούμενες από μια τροποποίηση του τμήματος (οι άλλες τρεις φάσεις), ακολουθούμενες από μια κρυπτογράφηση με τον τελεστή XOR ,κ.ο.κ. Αυτή η δομή είναι και αποδοτική, αλλά και ιδιαίτερα ασφαλής.

7. Κάθε στάδιο είναι εύκολα αντιστρέψιμο. Για τα στάδια αντικατάστασης των byte, μετατόπισης των γραμμών, και αναδιάταξης των στηλών χρησιμοποιείται μια αντίστροφη συνάρτηση στον αλγόριθμο αποκρυπτογράφησης. Για τη φάση προσθήκης του κλειδιού γύρου η αντιστροφή επιτυγχάνεται με εφαρμογή του τελεστή XOR μεταξύ του ίδιου κλειδιού γύρου και του τμήματος με χρήση της σχέσης A XOR A XOR B = B.

8. Όπως συμβαίνει με τα περισσότερα συστήματα κρυπτογράφησης, ο αλγόριθμος αποκρυπτογράφησης χρησιμοποιεί το επεκταμένο κλειδί με αντεστραμμένη σειρά. Ωστόσο, ο αλγόριθμος αποκρυπτογράφησης δεν είναι ακριβώς ίδιος με εκείνον της κρυπτογράφησης. Αυτό αποτελεί συνέπεια της συγκεκριμένης δομής του αλγορίθμου AES.

9. Αν αποδείξουμε ότι και τα τέσσερα στάδια είναι αντιστρέψιμα, είναι εύκολο να επαληθεύσουμε ότι η αποκρυπτογράφηση όντως ανακτά το αρχικό κείμενο. Στην εικόνα 30 φαίνονται οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης να κατευθύνονται σε αντίθετες κατακόρυφες κατευθύνσεις. Σε κάθε οριζόντιο σημείο, η κατάσταση (state) είναι η ίδια για την κρυπτογράφηση και την αποκρυπτογράφηση.

10. Ο τελικός γύρος της κρυπτογράφησης και της αποκρυπτογράφησης αποτελείται από τρία στάδια. Και πάλι, αυτό είναι συνέπεια της συγκεκριμένης δομής του αλγορίθμου AES και απαιτείται έτσι ώστε να είναι το σύστημα αντιστρέψιμο.[1]



Εικόνα 31: Ο γύρος κρυπτογράφησης AES. [15]

ΚΕΦΑΛΑΙΟ 4: ΣΥΜΠΕΡΑΣΜΑΤΑ

Η κρυπτογραφία έχει γίνει πλέον αναπόσπαστο κομμάτι της προστασίας της πληροφορίας και για αυτό το λόγο έχουν επινοηθεί πλήθος αλγορίθμων κρυπτογράφησης. Ορισμένοι από τους πιο βασικούς αλγορίθμους στην ιστορία της κρυπτογραφίας είναι ο DES, 3DES, AES οι οποίοι έχουν διαμορφώσει και θα διαμορφώσουν τη μοντέρνα και μελλοντική εποχή της κρυπτογραφίας.

Οι φόβοι των περισσότερων για αδυναμίες του DES δεν έχουν επαληθευτεί ακόμα και σήμερα. Το μόνο μειονέκτημα πλέον του κρυπτοσυστήματος αυτού είναι η εξαντλητική αναζήτηση, η οποία με τα σημερινά δεδομένα και λόγω του σχετικά μικρού μήκους κλειδιού είναι υπολογιστικά δυνατή.

Στη συνέχεια δημιουργήθηκε ο 3DES ως διάδοχος του DES, ο οποίος είναι εξαιρετικός αλγόριθμος που προέρχεται από τον DES λύνοντας το πρόβλημα του μικρού μήκους κλειδιού του προκατόχου του. Παρ' όλα αυτά είναι σχετικά αργός σε υλοποιήσεις λογισμικού και σε συνδυασμό με το μέγεθος block το οποίο είναι μόνο 64 bit δε θα προσφέρει για πολύ καιρό ακόμα την απαιτούμενη ασφάλεια και απόδοση.

Για αυτό το λόγο σχεδιάστηκε ένα νέο εξελιγμένο πρότυπο κρυπτογράφησης γνωστό ως AES το οποίο προσφέρει ίση ή μεγαλύτερη ασφάλεια με τον 3DES με σημαντικά βελτιωμένη απόδοση έχοντας μέγεθος block 128 bit και μήκος κλειδιού 128,192,και 256 bit γεγονός που τον κάνει τον πρώτο (και μόνο) δημόσιο κρυπταλγόριθμο που έχει εγκριθεί από την NSA για άκρως απόρρητες πληροφορίες.[9],[16]

ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλία:

[1] William Stallings - Βασικές Αρχές Ασφάλειας Δικτύων, Εφαρμογές και Πρότυπα Τρίτη αμερικανική έκδοση.

[2] Βιβλία: Β.Α.Κάτος , Γ.Χ.Στεφανίδης - Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης.

URLs:

[3] Wikipedia: https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1

[4] Wikipedia:

https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1#/media/File:Encryption_and_decryption_system.png

[5] Wikipedia:

https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1

[6] http://www.historyrunsparta.gr/wp-content/uploads/2017/02/spartatiki_skitali-750x430.jpg

[7] Wikipedia:

http://2.bp.blogspot.com/-EzZbvRy1Okw/VUdIFpVwnjI/AAAAAAAAAII/XKgT6t-tZCk/s1600/enigma-machine.jpg

[8] Wikipedia:

https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7_%CE%94

%CE%B7%CE%BC%CF%8C%CF%83%CE%B9%CE%BF%CF%85_%CE%9A%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CE%BF%CF%8D

[10] Wikipedia:

https://el.wikipedia.org/wiki/Data_Encryption_Standard

[11] Wikipedia:

https://translate.google.gr/translate?hl=el&sl=en&u=https://en.wikipedia.org/wiki/Feistel_cipher&prev=search

[12] http://flylib.com/books/3/190/1/html/2/images/03fig02.jpg

[13] http://book.transtutors.com/qimage/image08222014058.png

[14] http://nevonprojects.com/wp-content/uploads/2015/06/aes-image.png

[15] http://flylib.com/books/3/190/1/html/2/images/05fig03.jpg

[16] Wikipedia:

https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#Security

Δημοσιεύσεις:

[9] Διπλωματική Εργασία.

URLs:

http://dspace.lib.ntua.gr/dspace2/bitstream/handle/123456789/5545/kokkinosg_des.pdf?sequence=1