ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΚΡΥΠΤΟΓΡΑΦΙΑ ΣΥΜΜΕΤΡΙΚΩΝ ΚΑΙ ΑΣΥΜΜΕΤΡΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΕΦΑΡΜΟΓΕΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΜΑΝΩΛΑ ΠΗΝΕΛΟΠΗ
Α.Μ. 09104073

ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ: Παπαϊωάννου Αλέξανδρος (Επιβλέπων)
Αναπληρωτής Καθηγητής Ε.Μ.Π.
Κουκουβίνος Χρήστος Καθηγητής Ε.Μ.Π.
Στεφανέας Πέτρος Λέκτορας Ε.Μ.Π.

ΑΘΗΝΑ 2012

ΠΡΟΛΟΓΟΣ

Αντικείμενο της διπλωματικής εργασίας είναι η κρυπτογραφία και οι εφαρμογές της. Αρχικά δίνονται κάποιοι απαραίτητοι ορισμοί καθώς και χρήσιμη ορολογία όπως τι σημαίνει «κρυπτογράφηση», «αποκρυπτογράφηση» , «απλό» και «κρυπτογραφημένο» κείμενο, για την καλύτερη κατανόηση των όσων έπονται.

Στο πρώτο κεφάλαιο γίνεται μια ιστορική αναδρομή κατά την οποία βλέπουμε την πορεία της κρυπτογραφίας από το 1900π.Χ. μέχρι σήμερα. Παρατίθενται παραδείγματα από διάφορα κλασσικά κρυπτοσυστήματα που χρησιμοποιήθηκαν στο παρελθόν για στρατιωτική χρήση όπως η μέθοδος της σκυτάλης , το σύστημα αντικατάστασης του Καίσαρα και το τετράγωνο Vigenere. Αργότερα, τα κρυπτοσυστήματα αρχίζουν να γίνονται πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάζονται «κρυπτομηχανές». Μια από αυτές τις κρυπτομηχανές , και η πιο γνωστή, ήταν η μηχανή Αίνιγμα η οποία χρησιμοποιήθηκε ευρέως στη Γερμανία. Όπως ήταν αναμενόμενο, ανάλογη πρόοδο εμφανίστηκε την ίδια περίοδο και στον τομέα της κρυπτανάλυσης. Από το 1949μ.Χ αρχίζει η τρίτη περίοδος της κρυπτογραφίας η οποία σηματοδοτείται από την ανάπτυξη της μικροηλεκτρονικής και των υπολογιστικών συστημάτων και τον Claude Shannon, πατέρα των μαθηματικών συστημάτων κρυπτογραφίας, περίοδος που διαρκεί μέχρι σήμερα. Αφήνονται πίσω τα κλασσικά κρυπτοσυστήματα και το ενδιαφέρον στρέφεται σε αυτά που αποκαλούμε «μοντέρνα», τα οποία χωρίζονται σε «συμμετρικού» και «ασύμμετρου» κλειδιού. Στα μέσα της δεκαετίας του '70 δημοσιεύεται ο DES, ο πρώτος δημόσια προσιτός αλγόριθμος κρυπτογράφησης συμμετρικού κλειδιού που εγκρίνεται από μια εθνική αντιπροσωπεία όπως η NSA. Η απελευθέρωση της προδιαγραφής της από την NBS υποκινεί μια έκρηξη δημόσιου και ακαδημαϊκού ενδιαφέροντος για τα συστήματα κρυπτογραφίας.

Στο δεύτερο κεφάλαιο, περιγράφονται οι κατηγορίες συμμετρικών κρυπταλγορίθμων και αναπτύσσονται κυρίως οι κρυπταλγόριθμοι τμήματος στους οποίους ανήκει ο DES. Αρχικά γίνεται μια σύντομη αναφορά στην προέλευση του DES και ύστερα αναλύεται η δομή του, ο τρόπος κατασκευής του αλγορίθμου του, η ταχύτητα του καθώς και οι αιτίες αντικατάστασής του. Περιγράφονται κάποιες από τις κρυπταναλυτικές επιθέσεις που έγιναν εναντίον του καθώς και κάποιοι από τους αντικαταστάτες του DES όπως είναι ο double-DES, ο triple-DES και ο DESX.

Στο τρίτο κεφάλαιο, παρατίθενται κάποια διπλώματα ευρεσιτεχνίας γνωστά και ως «πατέντες» και πρότυπα τα οποία αφορούν σε κρυπτογραφικές τεχνικές. Λόγω του ότι η αρχειοθέτηση των περισσότερων διπλωμάτων ευρεσιτεχνίας γίνεται στις Ηνωμένες Πολιτείες της Αμερικής, δίνονται οι αριθμοί Αμερικάνικων πατεντών καθώς και σχετικές πληροφορίες σχετικές με τους εφευρέτες τους.

PROLOGUE

The purpose of this thesis is cryptography and its applications. First we give some necessary definitions and useful terminology as "encryption", "decryption", "plain text" and "cipher text" for a better understanding of what is to come.

The first chapter gives a historical overview in which we see the development of cryptography from 1900 BC. till today. Here are several examples of classical cryptosystems used in the past for military use such as the “scytale method”, “replacement system of Caesar” and “square Vigenere”. Later, the cryptosystems are becoming complex, and consist of mechanical and electromechanical construction, called "kryptomichanes." One of these kryptomichanes, and the most famous was the Enigma machine which was used widely in Germany. Unsurprisingly, such progress occurred in the same period in cryptanalysis. From 1949 AD. begins the third period of cryptography, which is marked by the development of microelectronics and computer systems and Claude Shannon, father of mathematical cryptography, a period that lasts until today. The classical cryptosystems are left behind and attention turns to what we call "modern" cryptosystems, which are divided into those of "symmetric" and "asymmetric" key. In the mid-70s DES was published. It was the first publicly accessible symmetric key encryption algorithm approved by a national agency like the NSA. The release of the specification of the NBS stimulates a burst of public and academic interest in cryptography.

The second chapter describes the types of symmetric ciphers and those that are mainly developed are the block ciphers in which belongs the DES. First there is a brief reference to the origin of the DES and then we analyze its structure, the structure of the algorithm, its speed and the causes of its replacement. Then some of the cryptanalytic attacks made against it are described as well as some of DES’s replacements such as double-DES, triple-DES and DESX.

The third chapter presents some patents and standards that deal with cryptographic techniques. Because the filing of patents takes place in the United States of America, the number of American patents and information related to their inventors are given.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω ιδιαιτέρως τον καθηγητή μου και επιβλέποντα κύριο Αλέξανδρο Παπαϊωάννου, Αναπληρωτή Καθηγητή του Ε.Μ.Π. για την πολύτιμη βοήθεια του και καθοδήγηση κατά την εκπόνηση της διπλωματικής μου εργασίας.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Η κρυπτογραφία είναι ένας κλάδος της επιστήμης της κρυπτολογίας, η οποία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Ο κύριος στόχος της 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 λέξη κρυπτολογία αποτελείται από την ελληνική λέξη "κρυπτός" και τη λέξη "λόγος" και χωρίζεται σε δύο κλάδους: Την Κρυπτογραφία και την Κρυπτανάλυση. Η λέξη κρυπτογραφία προέρχεται από τα συνθετικά "κρυπτός" + "γράφω" και είναι ένας επιστημονικός κλάδος που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων.

Η κρυπτογραφία παρέχει τέσσερις 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 ταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

Ορολογία

Κρυπτογράφηση (*encryption*) ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με τη χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη.

Αποκρυπτογράφηση (*decryption*) ονομάζεται η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα.

Κρυπτογραφικός αλγόριθμος (cipher) είναι η μέθοδος μετασχηματισμού δεδομένων σε μία μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος είναι μία πολύπλοκη μαθηματική συνάρτηση.

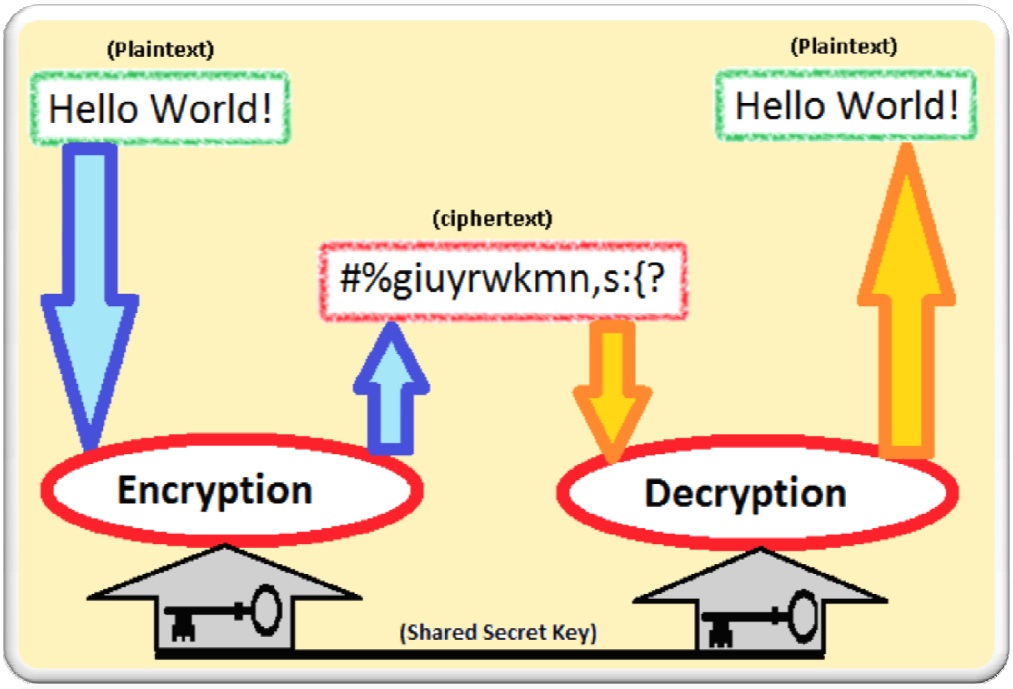
Αρχικό κείμενο (*plaintext*) είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.

Κλειδί (*key*) είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στη συνάρτηση κρυπτογράφησης.

Κρυπτογραφημένο κείμενο (*ciphertext*) είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.

Κρυπτανάλυση (*cryptanalysis*) είναι μία επιστήμη που ασχολείται με το "σπάσιμο" κάποιας κρυπτογραφικής τεχνικής ούτως ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί.

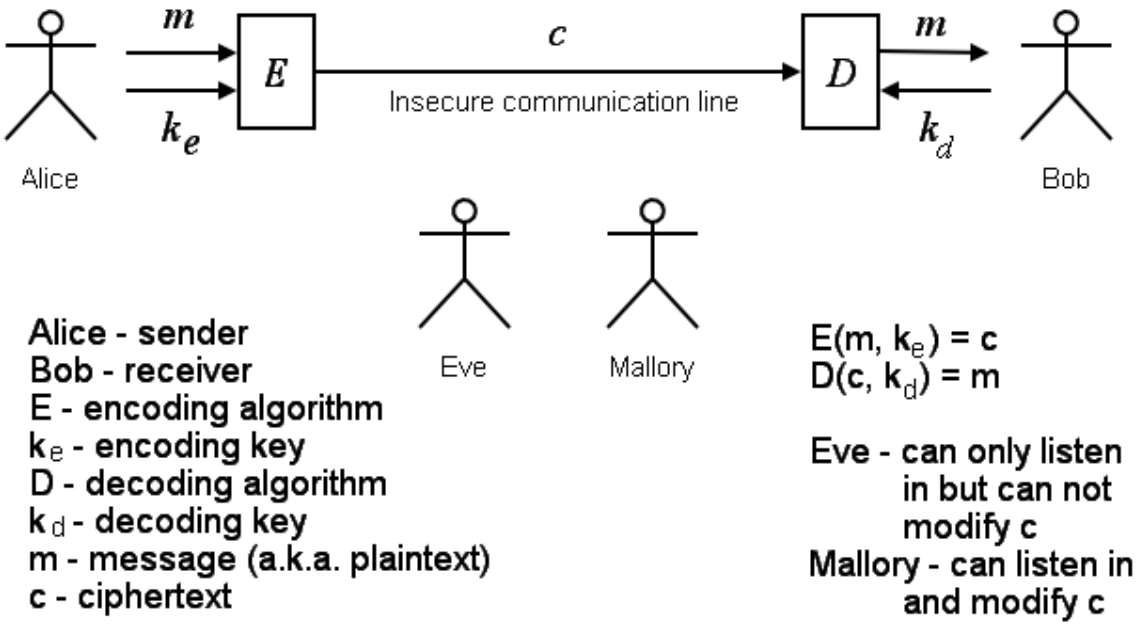
Η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης φαίνεται στο παρακάτω σχήμα.



Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης (cipher) και ενός κλειδιού κρυπτογράφησης (key). Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος που μεταδίδεται βασίζεται ως επί το πλείστον στη μυστικότητα του κλειδιού κρυπτογράφησης. Το μέγεθος του κλειδιού κρυπτογράφησης μετριέται σε αριθμό bits. Γενικά ισχύει ο εξής κανόνας: όσο

μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς. Διαφορετικοί αλγόριθμοι κρυπτογράφησης απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης.

Βασικές Έννοιες



Ο αντικειμενικός στόχος της κρυπτογραφίας είναι να δώσει τη δυνατότητα σε δύο πρόσωπα, έστω την Alice και τον Bob, να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε ένα τρίτο πρόσωπο, μη εξουσιοδοτημένο (ένας αντίπαλος), να μην μπορεί να παρεμβληθεί στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων.

Ένα κρυπτοσύστημα (σύνολο διαδικασιών κρυπτογράφησης - αποκρυπτογράφησης) αποτελείται από μία πεντάδα (P,C,k,E,D):

- Το P (ή m) είναι ο χώρος όλων των δυνατών μηνυμάτων ή αλλιώς απλών κειμένων
- Το C είναι ο χώρος όλων των δυνατών κρυπτογραφημένων μηνυμάτων ή αλλιώς κρυπτοκειμένων
- Το k είναι ο χώρος όλων των δυνατών κλειδιών ή αλλιώς κλειδοχώρος
- Η E είναι ο κρυπτογραφικός μετασχηματισμός ή κρυπτογραφική συνάρτηση
- Η D είναι η αντίστροφη συνάρτηση της E ή μετασχηματισμός αποκρυπτογράφησης

Η συνάρτηση κρυπτογράφησης E δέχεται δύο παραμέτρους, μέσα από τον χώρο P (ή m) και τον χώρο k και παράγει μία ακολουθία που ανήκει στον χώρο C. Η συνάρτηση αποκρυπτογράφησης D δέχεται 2 παραμέτρους, τον χώρο C και τον χώρο k και παράγει μια ακολουθία που ανήκει στον χώρο P (ή m).

Το Σύστημα του Σχήματος λειτουργεί με τον ακόλουθο τρόπο :

1. Ο αποστολέας επιλέγει ένα κλειδί μήκους *n* από τον χώρο κλειδιών με τυχαίο τρόπο, όπου τα n στοιχεία του k είναι στοιχεία από ένα πεπερασμένο αλφάβητο.
2. Αποστέλλει το κλειδί στον παραλήπτη μέσα από ένα ασφαλές κανάλι.
3. Ο αποστολέας δημιουργεί ένα μήνυμα από τον χώρο μηνυμάτων m.
4. Η συνάρτηση κρυπτογράφησης παίρνει τις δυο εισόδους (κλειδί και μήνυμα) και παράγει μια κρυπτοακολουθία συμβόλων (έναν γρίφο) και η ακολουθία αυτή αποστέλλεται διαμέσου ενός μη ασφαλούς καναλιού.
5. Η συνάρτηση αποκρυπτογράφησης παίρνει ως όρισμα τις δύο τιμές (κλειδί και γρίφο) και παράγει την ισοδύναμη ακολουθία μηνύματος.

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

Ο αντίπαλος μπορεί να είναι είτε παθητικός όπως η Eve, είτε κακόβουλος όπως ο Mallory. Η Eve, ένας ωτακουστής, ενώ μπορεί να συνδεθεί στα μηνύματα μεταξύ της Alice και του Bob δεν μπορεί να τα τροποποιήσει. Στην κβαντική κρυπτογραφία η Eve μπορεί να εκπροσωπεί και το περιβάλλον. Ο Mallory, μπορεί να τροποποιήσει τα μηνύματα, να τα υποκαταστήσει με δικά του, να αναπαράγει παλαιότερα μηνύματα κ.ο.κ. Η δυσκολία διατήρησης της ασφάλειας ενός συστήματος ενάντια στον Mallory είναι πολύ μεγαλύτερη από ότι ενάντια στην Eve.

"There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files. This book is about the latter"

Bruce Schneier, Applied cryptograpfy: Protocols, Algorithms, and Source code in C

ΚΕΦΑΛΑΙΟ 1 : ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Ιστορικά η κρυπτογραφία χρησιμοποιήθηκε για την κρυπτογράφηση μηνυμάτων δηλαδή μετατροπή της πληροφορίας από μια κανονική κατανοητή μορφή σε έναν γρίφο, που χωρίς τη γνώση του κρυφού μετασχηματισμού θα παρέμενε ακατανόητος. Κύριο χαρακτηριστικό των παλαιότερων μορφών κρυπτογράφησης ήταν ότι η επεξεργασία γινόταν πάνω στη γλωσσική δομή. Στις νεότερες μορφές η κρυπτογραφία κάνει χρήση του αριθμητικού ισοδύναμου, η έμφαση έχει μεταφερθεί σε διάφορα πεδία των μαθηματικών, όπως διακριτά μαθηματικά, θεωρία αριθμών, θεωρία πληροφορίας, υπολογιστική πολυπλοκότητα, στατιστική και συνδυαστική ανάλυση.

Η ιστορία της κρυπτογραφίας μπορεί κατά προσέγγιση να διαιρεθεί σε τρία στάδια [Bellare, 2005]. Στο πρώτο στάδιο οι διαδικασίες κρυπτογράφησης αφορούσαν τον τρόπο της έντυπης απεικόνισης (μελάνι και χαρτί). Έλαβαν τη μορφή αντικατάστασης και αναδιάταξης των γραμμάτων της αλφαβήτου (ενδεικτικά ο κρυπτογραφικός αλγόριθμος του Καίσαρα). Σαν δεύτερο στάδιο αναφέρεται αυτό των κρυπτογραφικών μηχανών, ιδίως στην περίοδο του Β' παγκοσμίου πολέμου (η γερμανική μηχανή Enigma). Τελευταίο στάδιο θεωρείται το σύγχρονο κρυπτογραφικό σύστημα, απόρροια της αμοιβαίας αλληλεπίδρασης των μαθηματικών και των υπολογιστών (οι υπολογιστές επέτρεψαν τη χρήση περιπλοκότερων αλγορίθμων κρυπτογράφησης και τα μαθηματικά προσέφεραν το υπόβαθρο).

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

Κατά τη διάρκεια αυτής της 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. Όλα αυτά τα συστήματα έχουν στις μέρες μας κρυπταναλυθεί και έχει αποδειχθεί ότι, εάν είναι γνωστό ένα μεγάλο κομμάτι του κρυπτογραφημένου μηνύματος, τότε το αρχικό κείμενο μπορεί σχετικά εύκολα να επανακτηθεί.

1.1.1 Το αρχαιότερο κρυπτογραφημένο κείμενο

Όπως προκύπτει από μία μικρή σφηνοειδή επιγραφή, που ανακαλύφθηκε στις όχθες του ποταμού Τίγρη, οι πολιτισμοί που αναπτύχθηκαν στη Μεσοποταμία ασχολήθηκαν με την κρυπτογραφία ήδη από το **1500 π.Χ.** Η επιγραφή αυτή περιγράφει μία μέθοδο κατασκευής σμάλτων για αγγειοπλαστική και θεωρείται ως το αρχαιότερο κρυπτογραφημένο κείμενο (με βάση τον Kahn). Επίσης, ως το αρχαιότερο βιβλίο κρυπτοκωδίκων στον κόσμο, θεωρείται μία σφηνοειδής επιγραφή στα Σούσα της Περσίας. η οποία περιλαμβάνει τους αριθμούς 1 έως 8 και από το 32 έως το 35, τοποθετημένους τον ένα κάτω από τον άλλο, ενώ απέναντι τους βρίσκονται τα αντίστοιχα για τον καθένα σφηνοειδή σύμβολα.

1.1.2 Στρατιωτική χρήση – Η μέθοδος της σκυτάλης

Η πρώτη στρατιωτική χρήση της κρυπτογραφίας αποδίδεται στους Σπαρτιάτες. Γύρω στον **5ο π.Χ.** αιώνα εφηύραν την «σκυτάλη», την πρώτη κρυπτογραφική συσκευή, στην οποία χρησιμοποίησαν για την κρυπτογράφηση τη μέθοδο της αντικατάστασης. Όπως αναφέρει ο Πλούταρχος, η «Σπαρτιατική Σκυτάλη», ήταν μια 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 δε ξετύλιγαν τη λωρίδα, το κείμενο ήταν ακατάληπτο εξαιτίας της ανάμειξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της σκυτάλης.

Σχήμα: Η Σπαρτιατική Σκυτάλη, μια πρώιμη συσκευή για την κρυπτογράφηση

Για παράδειγμα έστω ότι θέλουμε να κρυπτογραφήσουμε το μήνυμα : "HELP ME I AM UNDER ATTACK". Αφού τυλίξουμε μια λωρίδα δέρματος γύρω από τη σκυτάλη, γράφουμε το μήνυμά μας.

	H	E	L	P	M
	E	I	A	M	U
N	D	E	R	A	
T	T	A	C	K	

Ξετυλίγοντας το δέρμα θα πάρουμε το εξής κρυπτογραφημένο μήνυμα : "HENTEIDTLAEAPMRCMUAK".
Η αποκρυπτογράφηση γίνεται με τον ίδιο τρόπο. Ο παραλήπτη του μηνύματος αφού τυλίξει τη λωρίδα δέρματος γύρω από μια σκυτάλη ίδιας διαμέτρου με αυτή του αποστολέα θα μπορέσει να διαβάσει το αρχικό κείμενο "HELP ME I AM UNDER ATTACK".

1.1.3 Το σύστημα αντικατάστασης του Καίσαρα

Οι Έλληνες συγγραφείς δεν αναφέρουν αν και πότε χρησιμοποιήθηκαν συστήματα γραπτής αντικατάστασης γραμμάτων, αλλά τα βρίσκουμε στους Ρωμαίους, κυρίως την εποχή του Ιουλίου Καίσαρα. Ο Ιούλιος Καίσαρας έγραφε στον Κικέρωνα και σε άλλους φίλους του, αντικαθιστώντας τα γράμματα του κειμένου, με γράμματα, που βρίσκονται 3 θέσεις μετά, στο Λατινικό Αλφάβητο. Έτσι, σήμερα, το σύστημα κρυπτογράφησης που στηρίζεται στην αντικατάσταση των γραμμάτων του αλφαβήτου με άλλα που βρίσκονται σε καθορισμένο αριθμό θέσης πριν ή μετά, λέγεται κρυπτοσύστημα αντικατάστασης του Καίσαρα. Ο Καίσαρας χρησιμοποίησε και άλλα, πιο πολύπλοκα συστήματα κρυπτογράφησης, για τα οποία έγραψε ένα βιβλίο ο Valerius Probus, το οποίο δυστυχώς δεν διασώθηκε, αλλά αν και χαμένο, θεωρείται το πρώτο βιβλίο κρυπτολογίας. Το σύστημα αντικατάστασης του Καίσαρα, χρησιμοποιήθηκε ευρύτατα και στους επόμενους αιώνες.

Μια στρατηγική χρησιμοποιεί την περιστροφή : γυρίζοντας τον εσωτερικό τροχό και στη συνέχεια αντικαθιστώντας τα εξωτερικά γράμματα (απλό κείμενο) με εκείνα του εσωτερικού τροχού(κρυπτοκείμενο):

Π.χ. απλό κείμενο: CAESAR

κρυπτοκείμενο: PNRFNE

Ο Καίσαρας αντικαθιστούσε κάθε γράμμα του μηνύματος με κάποιο επόμενο, συνήθως το τρίτο κατά σειρά. Έτσι, για παράδειγμα, το όνομά του θα γραφόταν ως «Μσψμσφ Νδμφδυδφ». Η αντικατάσταση του Καίσαρα μπορεί να περιγραφεί από τον μετασχηματισμό $C=p+3 \bmod 26$, όπου p η αριθμητική τιμή του γράμματος του απλού κειμένου και C η αντίστοιχη τιμή στο κρυπτογραφημένο κείμενο. Ο αντίστροφος μετασχηματισμός είναι ο $p=C-3 \bmod 26$ και γενικότερα ο μετασχηματισμός $C=p+k \bmod 26$, $0 \leq k \leq 25$ και ο αντίστροφος του $p=C-k \bmod 26$ αποτελούν το προσθετικό σύστημα ή σύστημα αντικατάστασης του Καίσαρα. Ο αριθμός k περιγράφει το μέγεθος της μετατόπισης και λέγεται κλειδί. Επιτρέπεται $k=0$ αλλά δεν έχει ενδιαφέρον ένας τέτοιος μετασχηματισμός.

Η μέθοδος της αντικατάστασης είναι ευαίσθητη στη στατιστική ανάλυση του κρυπτογραφημένου μηνύματος, όπως πρώτος ανακάλυψε ο άραβας μαθηματικός Αλ Κιντί (ελληνικά Αλκιντος) τον 9ο αιώνα μ.Χ. Για παράδειγμα, από το κρυπτογραφημένο όνομα του Καίσαρα είναι εύκολο να φανταστεί κανείς ότι το «φ» αντιστοιχεί στο τελικό «ς» και ότι το «δ» αντιστοιχεί στο «α», το γράμμα με τη μεγαλύτερη συχνότητα στις περισσότερες γλώσσες (και στα ελληνικά, όπως θα γνωρίζουν οι φανατικοί λύτες σταυρολέξων). Για τον λόγο αυτόν από την εποχή του Καίσαρα η μεγάλη προσπάθεια των κρυπτογράφων ήταν να πετύχουν μεθόδους αντικατάστασης που να «καλύπτουν» τη συχνότητα εμφάνισης των γραμμάτων, έτσι

ώστε ο μοναδικός τρόπος για να διαβαστεί ένα κρυπτογραφημένο μήνυμα να είναι η γνώση του «κλειδιού» της αντικατάστασης.

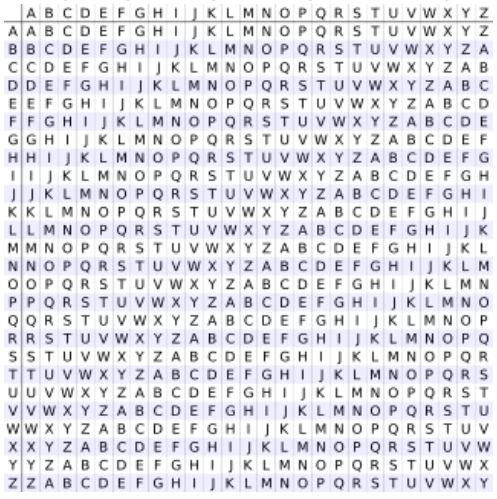
Στη διάρκεια του **Μεσαίωνα**, η κρυπτολογία ήταν κάτι το απαγορευμένο στην Ευρώπη και αποτελούσε μια μορφή αποκρυφισμού και μαύρης μαγείας, κάτι που συντέλεσε στην καθυστέρηση της ανάπτυξης της.

1.1.4 Οι Άραβες και οι συχνότητες των γραμμάτων

Η εξέλιξη, τόσο της κρυπτολογίας, όπως και των μαθηματικών, συνεχίζεται στον Αραβικό κόσμο. Στο γνωστό μυθιστόρημα «Χίλιες και μία νύχτες» κυριαρχούν οι λέξεις-αινίγματα, οι γρίφοι, τα λογοπαίγνια και οι αναγραμματισμοί. Έτσι, εμφανίστηκαν βιβλία που περιείχαν κρυπταλφάβητα, όπως το αλφάβητο «Dawoudi» που πήρε το όνομα του από τον βασιλιά Δαυίδ. Οι Άραβες είναι οι πρώτοι που επινόησαν αλλά και χρησιμοποίησαν μεθόδους κρυπτανάλυσης. Το κυριότερο εργαλείο στην κρυπτανάλυση, η χρησιμοποίηση των συχνοτήτων των γραμμάτων κειμένου, σε συνδυασμό με τις συχνότητες εμφάνισης στα κείμενα των γραμμάτων της γλώσσας, επινοήθηκε από αυτούς γύρω στον **14ο αιώνα**.

1.1.5 Το τετράγωνο Vigenere

Η κρυπτογραφία, λόγω των στρατιωτικών εξελίξεων, σημείωσε σημαντική ανάπτυξη στους επόμενους αιώνες. Ο Ιταλός *Giovanni Batista della Porta*, το 1563, δημοσίευσε το περίφημο για την κρυπτολογία βιβλίο «*De furtivis literarum notis*», με το οποίο έγιναν γνωστά τα πολυαλφαβητικά συστήματα κρυπτογράφησης και τα διγραφικά κρυπτογραφήματα, στα οποία, δύο γράμματα αντικαθίστανται από ένα. Σημαντικός εκπρόσωπος εκείνης της εποχής είναι και ο Γάλλος *Vigenere*, του οποίου ο πίνακας πολυαλφαβητικής αντικατάστασης, χρησιμοποιείται ακόμη και σήμερα.



Πρόκειται για έναν πίνακα που αποτελείται από το αλφάβητο γραμμένο 26 φορές σε διαφορετικές γραμμές. Σε κάθε γραμμή το αλφάβητο είναι μετατοπισμένο προς τα αριστερά σε σχέση με το αλφάβητο της προηγούμενης γραμμής.
Η κρυπτογράφηση ενός μηνύματος γίνεται ως εξής :
Επιλέγεται η λέξη κλειδί “CAT”και επαναλαμβάνεται όσες φορές χρειάζεται για να καλύψει το μήκος του μηνύματος.

plaintext: ATTACK AT DAWN
keyword: CATCATCATCATCA

Το πρώτο γράμμα του μηνύματος είναι το A πηγαίνουμε στην στήλη που ο δείκτης είναι το A και στην γραμμή που δείχνει το γράμμα της λέξης-κλειδί πχ C. Στον πίνακα το στοιχείο που δείχνουν είναι το γράμμα C όπου είναι το παραγόμενο κρυπτόγραμμα. Η διαδικασία επαναλαμβάνεται για τα επόμενα γράμματα του μηνύματος.

ciphertext: CTMCCD AM DTYN

Η αντίστροφη διαδικασία οδηγεί στην αποκρυπτογράφηση.

Για δεδομένα που είναι δυαδική ακολουθία από bits χρησιμοποιείται η πράξη **xor** (exclusive or η οποία συμβολίζεται και με ⊕) . Για παράδειγμα:

Plaintext: 01100001010100001111010010101010100100000001111101
Key: 00000111000001110000011100000111000001110000001110
Ciphertext: 01100110010101111111001110101101100101110011100011

1.1.5.1 Auto-Key Vigenere

Ο Vigenere δημιούργησε έναν ισχυρότερο κώδικα κρυπτογράφησης που ποτέ δεν επαναλαμβάνει το κλειδί. Αντ 'αυτού το "κλειδί" αποτελείται από τη λέξη κλειδί (εδώ QUARK) ακολουθούμενη από το απλό κείμενο, όπως φαίνεται στο παράδειγμα παρακάτω:

Plaintext: TAKEACOPYOFYOURPOLICYTONORMAWILCOXONTHETHIRDFLOOR
Κλειδί: **QUARK**TAKEACOPYOFYOURPOLICYTONORMAWILCOXONTHETHIRD
Ciphertext: JUKVKVOZCOHMDSFUMZCTNHZVQPFOJWCOOTWYVVBHUBYHYSWFU

1.1.6 Ιερογλυφική Γραφή

Ο *C.Wheatstone*, γνωστός από τις μελέτες του στον ηλεκτρισμό, παρουσίασε την πρώτη μηχανική κρυπτοσυσκευή, η οποία απετέλεσε τη βάση για την ανάπτυξη των κρυπτομηχανών της δεύτερης ιστορικής περιόδου της κρυπτογραφίας. Η σημαντικότερη αποκρυπτογράφηση ήταν αυτή των αιγυπτιακών ιερογλυφικών τα οποία, επί αιώνες, παρέμεναν μυστήριο και οι αρχαιολόγοι μόνο εικασίες μπορούσαν να διατυπώσουν για τη σημασία τους. Ωστόσο, χάρη σε μία κρυπταναλυτική εργασία, τα ιερογλυφικά εν τέλει αναλύθηκαν και έκτοτε οι αρχαιολόγοι είναι σε θέση να διαβάζουν ιστορικές επιγραφές. Τα αρχαιότερα ιερογλυφικά χρονολογούνται περίπου από το **3000 π.Χ.** Τα σύμβολα των ιερογλυφικών ήταν υπερβολικά πολύπλοκα για την καταγραφή των συναλλαγών εκείνης της εποχής. Έτσι, παράλληλα με αυτά, αναπτύχθηκε για καθημερινή χρήση η ιερατική γραφή, που ήταν μία συλλογή

συμβόλων, τα οποία ήταν εύκολα τόσο στο γράψιμο όσο και στην ανάγνωση. Τον **17ο αιώνα** αναθερμάνθηκε το ενδιαφέρον για την αποκρυπτογράφηση των ιερογλυφικών, έτσι το 1652 ο Γερμανός Ιησουΐτης Αθανάσιος Κίρχερ εξέδωσε ένα λεξικό ερμηνείας τους, με τίτλο «*Oedipus Aegyptiacus*». Με βάση αυτό προσπάθησε να ερμηνεύσει τις αιγυπτιακές γραφές, αλλά η προσπάθεια του αυτή ήταν κατά γενική ομολογία αποτυχημένη. Για παράδειγμα, το όνομα του Φαραώ Απρίη, το ερμήνευσε σαν «τα ευεργετήματα του θεϊκού Όσιρι εξασφαλίζονται μέσω των ιερών τελετών της αλυσίδας των πνευμάτων, ώστε να επιδαψιλεύσουν τα δώρα του Νείλου». Παρόλα αυτά, η προσπάθεια του άνοιξε τον δρόμο προς τη σωστή ερμηνεία των ιερογλυφικών, που προχώρησε χάρη στην ανακάλυψη της «Στήλης της Ροζέτας». Ήταν μια πέτρινη στήλη που βρήκαν τα στρατεύματα του Ναπολέοντα στην Αίγυπτο και είχε χαραγμένο πάνω της το ίδιο κείμενο τρεις φορές. Μια με ιερογλυφικά, μια στα ελληνικά και μια σε ιερατική γραφή. Δύο μεγάλοι αποκρυπτογράφοι της εποχής, ο Γιάνγκ και κυρίως ο Σαμπολιόν, μοιράστηκαν τη δόξα της ερμηνείας τους.

Οι προϊστορικοί πληθυσμοί χρησιμοποίησαν τρεις γραφές μέχρι να επινοήσουν αλφάβητο, γύρω στο 850 π.Χ.

Χρονολογικά, οι γραφές αυτές κατατάσσονται ως εξής

- 3000 1600 π.Χ. : Εικονογραφική (Ιερογλυφική) γραφή
- 1850 1450 π.Χ.: Γραμμική γραφή Α
- 1450 1200 π.Χ.: Γραμμική γραφή Β

Η Κρητική εικονογραφική (ή ιερογλυφική) γραφή δεν μας έχει αποκαλύψει τον κώδικα της, γνωρίζουμε ωστόσο ότι δεν πρόκειται για γραφή που χρησιμοποιεί εικόνες ως σημεία, αλλά για φωνητική γραφή, η οποία εξαντλείται σε περίπου διακόσιους σφραγιδόλιθους και συνυπήρχε με τη γραμμική γραφή Α, τόσο χρονικά όσο και τοπικά, όπως προκύπτει από τις ανασκαφές στο ανάκτορο των Μαλίων της Κρήτης. Εμφανίζεται στον Δίσκο της Φαιστού, που ανακαλύφθηκε το 1908 στη νότια Κρήτη. Πρόκειται για μια κυκλική πινακίδα, που χρονολογείται γύρω στο **1700 π.Χ**. και φέρει γραφή με τη μορφή δύο σπειρών. Τα σύμβολα δεν είναι χειροποίητα, αλλά έχουν χαραχθεί με τη βοήθεια μίας ποικιλίας σφραγίδων, καθιστώντας τον Δίσκο ως το αρχαιότερο δείγμα στοιχειοθεσίας. Δεν υπάρχει άλλο ανάλογο εύρημα και έτσι η αποκρυπτογράφηση στηρίζεται σε πολύ περιορισμένες πληροφορίες. Μέχρι σήμερα δεν έχει αποκρυπτογραφηθεί και παραμένει η πιο μυστηριώδης αρχαία ευρωπαϊκή γραφή.

Σχήμα: Ο Δίσκος της Φαιστού

1.1.7 Γραμμική Γραφή

Οι πρώτες επιγραφές με Γραμμική γραφή ανακαλύφθηκαν από τον Άρθουρ Έβανς (Sir Arthur Evans), τον μεγάλο Άγγλο αρχαιολόγο, που ανάσκαψε συστηματικά την Κνωσό το **1900**. Ο ίδιος ονόμασε αυτή τη γραφή γραμμική, επειδή τα γράμματα της είναι γραμμές (ένα γραμμικό σχήμα) και όχι σφήνες, όπως στη σφηνοειδή γραφή ή εικόνες όντων, όπως στην αιγυπτιακή ιερατική. Η γραμμική γραφή Α είναι μάλλον η γραφή των Μινωιτών (από το μυθικό Μίνωα, βασιλιά της Κνωσού), των κατοίκων της αρχαίας Κρήτης και από αυτή ίσως να προήλθε το σημερινό ελληνικό αλφάβητο. Τα γράμματα της γραμμικής γραφής χαράζονταν με αιχμηρό αντικείμενο πάνω σε πήλινες πλάκες, οι οποίες κατόπιν ξεραίνονταν σε φούρνους. Οι περισσότερες από τις επιγραφές με Γραμμική γραφή Α (περίπου 1500) είναι λογιστικές και περιέχουν εικόνες ή συντομογραφίες των εμπορεύσιμων προϊόντων και αριθμούς για υπόδειξη της ποσότητας ή οφειλής.

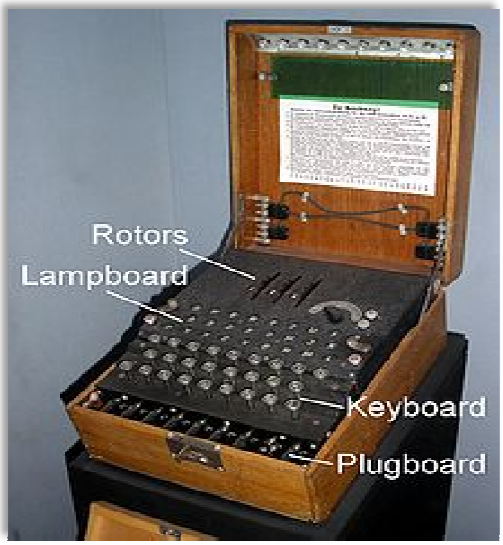
Ο Έβανς κατέγραψε 135 σύμβολα της. Χρησιμοποιήθηκε κυρίως στην Κρήτη, αν και ορισμένα πρόσφατα ευρήματα καταδεικνύουν ότι μπορεί να αποτέλεσε μέσο γραφής και αλλού, αφού επιγραφές με Γραμμική Α έχουν βρεθεί στην Κνωσό και Φαιστό της Κρήτης, αλλά και στη Μήλο και τη Θήρα. Πλάκες με επιγραφές σε γραμμική Α, εκτίθενται στο Μουσείο Ηρακλείου. Παρά την πρόοδο που έχει σημειωθεί, η γραμμική γραφή Α δεν έχει αποκρυπτογραφηθεί ακόμη. Ο Evans έδωσε και την ονομασία στη Γραμμική Γραφή Β, επειδή αναγνώρισε ότι πρόκειται για συγγενική γραφή με τη γραμμική Α, πιο πρόσφατη ωστόσο και εξελιγμένη. Με βάση όσα γνωρίζουμε σήμερα, η γραφή αυτή υιοθετήθηκε αποκλειστικά για λογιστικούς σκοπούς. Πινακίδες χαραγμένες με τη γραμμική γραφή Β βρέθηκαν στην Κνωσό, στα Χανιά αλλά και στην Πύλο, τις Μυκήνες, τη Θήβα και την Τίρυνθα. Σήμερα αποτελούν ένα σύνολο 10.000 τεμαχίων. Τα σχήματα των πινακίδων της γραφής αυτής ποικίλουν, επικρατούν όμως οι φυλλοειδείς και «σελιδόσχημες», οι οποίες διαφέρουν ως προς τις διαστάσεις, ανάλογα με τις προτιμήσεις του κάθε γραφέα. Έπλαθαν πηλό σε σχήμα κυλίνδρου, τον τοποθετούσαν σε λεία επιφάνεια και την πίεζαν μέχρι να γίνει επίπεδη, επιμήκης και συμπαγής πινακίδα, σαφώς διαφοροποιημένη σε δύο επιφάνειες: μία επίπεδη λειασμένη, που επρόκειτο να αποτελέσει την κύρια γραφική επιφάνεια και μία κυρτή, που συνήθως έμενε άγραφη. Πολλές φορές, όταν τα κείμενα απαιτούσαν περισσότερες από μία πινακίδες, έχουμε τις αποκαλούμενες «ομάδες» ή «πολύπτυχα» πινακίδων, οι οποίες εμφανίζουν κοινά χαρακτηριστικά και ως προς την αποξήρανση και το μίγμα του πηλού και κυρίως, ως προς το γραφικό χαρακτήρα του ίδιου του γραφέα. Τα πολύπτυχα αυτά φυλάσσονταν σε αρχειοφυλάκια και ταξινομούνταν κατά θέματα σε ξύλινα κιβώτια. Για να γνωρίζει ο ενδιαφερόμενος το περιεχόμενο των καλαθιών, κυρίως, χρησιμοποιούσαν ετικέτες: ένα σφαιρίδιο πηλού, εντυπωμένο στην πρόσθια πλευρά, στο οποίο καταγράφονταν συνοπτικές πληροφορίες. Συστηματικά, με τη γραφή αυτή, με την οποία είχε πραγματικό πάθος, ασχολήθηκε ο Άγγλος αρχιτέκτονας και ερασιτέχνης αρχαιολόγος Μ. Βέντρις. Ήταν ο πρώτος που κατάλαβε ότι επρόκειτο για κάποιο είδος ελληνικής γραφής, αλλά η άποψη του αυτή δεν έγινε δεκτή αρχικά από τους ειδικούς. Στη συνέχεια, όμως, αρκετοί προσχώρησαν στην άποψή του. Ένας από αυτούς ήταν ο κρυπταναλυτής Τζον Τσάντγουικ, ο οποίος, στη διάρκεια του πολέμου, είχε εργασθεί στην ανάλυση της γερμανικής κρυπτομηχανής Enigma.

Προσπάθησε να μεταφέρει την πείρα του στην κρυπτανάλυση της Γραμμικής Β, αλλά χωρίς επιτυχία μέχρι τότε. Όμως, ο συνδυασμός των δύο επιστημόνων έφερε το πολυπόθητο αποτέλεσμα. Το 1953 κατέγραψαν τα συμπεράσματά τους στο μνημειώδες έργο «Μαρτυρίες για την ελληνική διάλεκτο στα μυκηναϊκά αρχεία», που έγινε το πιο διάσημο άρθρο κρυπτανάλυσης. Η αποκρυπτογράφηση της Γραμμικής Β απέδειξε ότι επρόκειτο για ελληνική γλώσσα, ότι οι Μινωίτες της Κρήτης μιλούσαν ελληνικά και ότι η δεσπόζουσα δύναμη εκείνη την εποχή ήταν οι Μυκήνες. Η αποκρυπτογράφηση της Γραμμικής Β θεωρήθηκε επίτευγμα ανάλογο της κατάκτησης του Έβερεστ, που συνέβη την ίδια ακριβώς εποχή. Για αυτό και έγινε γνωστή σαν το «Έβερεστ της Ελληνικής αρχαιολογίας».

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

Η δεύτερη περίοδος της κρυπτογραφίας όπως προαναφέρθηκε τοποθετείται στις αρχές του 20ου αιώνα και φτάνει μέχρι το 1950. Καλύπτει, επομένως, τους δύο παγκόσμιους πολέμους, εξαιτίας των οποίων (λόγω της εξαιρετικά μεγάλης ανάγκης που υπήρξε για ασφάλεια κατά τη μετάδοση ζωτικών πληροφοριών μεταξύ των στρατευμάτων των χωρών) αναπτύχθηκε η κρυπτογραφία τόσο όσο δεν είχε αναπτυχθεί τα προηγούμενα 3000 χρόνια. Τα κρυπτοσυστήματα αυτής της περιόδου αρχίζουν να γίνονται πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάζονται «κρυπτομηχανές». Η κρυπτανάλυση τους, απαιτεί μεγάλο αριθμό προσωπικού, το οποίο εργαζόταν επί μεγάλο χρονικό διάστημα ενώ ταυτόχρονα γίνεται εξαιρετικά αισθητή η ανάγκη για μεγάλη υπολογιστική ισχύ. Παρά την πολυπλοκότητα που αποκτούν τα συστήματα κρυπτογράφησης κατά τη διάρκεια αυτής της περιόδου η κρυπτανάλυση τους είναι συνήθως επιτυχημένη. Οι Γερμανοί έκαναν εκτενή χρήση (σε διάφορες παραλλαγές) ενός συστήματος γνωστού ως Enigma .

1.2.1 Η μηχανή Enigma



Η **μηχανή Αίνιγμα** χρησιμοποιήθηκε ευρέως στη Γερμανία. Ο Marian Rejewski, στην Πολωνία, προσπάθησε και, τελικά, παραβίασε την πρώτη μορφή του γερμανικού στρατιωτικού συστήματος Enigma (που χρησιμοποιούσε μια ηλεκτρομηχανική κρυπτογραφική συσκευή) χρησιμοποιώντας θεωρητικά μαθηματικά το 1932. Ήταν η μεγαλύτερη σημαντική ανακάλυψη στην κρυπτολογική ανάλυση της εποχής. Οι Πολωνοί συνέχισαν να αποκρυπτογραφούν τα μηνύματα που βασίζονταν στην κρυπτογράφηση με το Enigma μέχρι το 1939. Τότε, ο γερμανικός στρατός έκανε

ορισμένες σημαντικές αλλαγές και οι Πολωνοί δεν μπόρεσαν να τις παρακολουθήσουν, επειδή η αποκρυπτογράφηση απαιτούσε περισσότερους πόρους από όσους μπορούσαν να διαθέσουν αλλά και διότι η Πολωνία κατακτήθηκε από τους Γερμανούς το 1939. Έτσι, εκείνο το καλοκαίρι μεταβίβασαν τη γνώση τους, μαζί με μερικές μηχανές που είχαν κατασκευάσει, στους Βρετανούς και τους Γάλλους. Ακόμη και ο Rejewski και οι μαθηματικοί και κρυπτογράφοι, του γραφείου σημάτων (Biuro Szyfrow), κατέληξαν σε συνεργασία με τους Βρετανούς και τους Γάλλους μετά από αυτή την εξέλιξη. Η συνεργασία αυτή συνεχίστηκε από τον Άλαν Τούρινγκ (Alan Turing), τον Γκόρντον Ουέλτσμαν (Gordon Welchman) και από πολλούς άλλους στο Μπλέτσλεϊ Παρκ (Bletchley Park), κέντρο της Βρετανικής Υπηρεσίας απο/κρυπτογράφησης και οδήγησε σε συνεχείς αποκρυπτογραφήσεις των διαφόρων παραλλαγών του Enigma, με τη βοήθεια και ενός υπολογιστή, που κατασκεύασαν οι Βρετανοί επιστήμονες, ο οποίος ονομάσθηκε Colossus και, δυστυχώς, καταστράφηκε με το τέλος του Πολέμου. Οι κρυπτογράφοι του αμερικανικού ναυτικού (σε συνεργασία με Βρετανούς και Ολλανδούς κρυπτογράφους μετά από το 1940) έσπασαν αρκετά κρυπτοσυστήματα του Ιαπωνικού ναυτικού. Το σπάσιμο ενός από αυτά, του JN-25, οδήγησε στην αμερικανική νίκη στη Ναυμαχία της Μιντγουέι καθώς και στην εξόντωση του Αρχηγού του Ιαπωνικού Στόλου Ιζορόκου Γιαμαμότο.

Το Ιαπωνικό Υπουργείο Εξωτερικών χρησιμοποίησε ένα τοπικά αναπτυγμένο κρυπτογραφικό σύστημα, (που καλείται Purple), και χρησιμοποίησε, επίσης, διάφορες παρόμοιες μηχανές για τις συνδέσεις μερικών ιαπωνικών πρεσβειών. Μία από αυτές αποκλήθηκε "Μηχανή-Μ" από τις ΗΠΑ, ενώ μια άλλη αναφέρθηκε ως «Red» (Κόκκινη). Μια ομάδα του αμερικανικού στρατού, η αποκαλούμενη SIS, κατάφερε να σπάσει το ασφαλέστερο ιαπωνικό διπλωματικό σύστημα κρυπτογράφησης (μια ηλεκτρομηχανική συσκευή, η οποία αποκλήθηκε "Purple" από τους Αμερικανούς) πριν καν ακόμη αρχίσει ο Β΄ Παγκόσμιος Πόλεμος. Οι Αμερικανοί αναφέρονται στο αποτέλεσμα της κρυπτανάλυσης, ειδικότερα της μηχανής Purple, αποκαλώντας το ως Magic (Μαγεία).

Οι συμμαχικές κρυπτομηχανές που χρησιμοποιήθηκαν στον δεύτερο παγκόσμιο πόλεμο περιλάμβαναν το βρετανικό TypeX και το αμερικανικό SIGABA . Και τα δύο ήταν ηλεκτρομηχανικά σχέδια παρόμοια στο πνεύμα με το Enigma, με σημαντικές εν τούτοις βελτιώσεις. Κανένα δεν έγινε γνωστό ότι παραβιάστηκε κατά τη διάρκεια του πολέμου. Τα στρατεύματα στο πεδίο μάχης χρησιμοποίησαν το M-209 και τη λιγότερη ασφαλή οικογένεια κρυπτομηχανών M-94. Οι Βρετανοί πράκτορες της Υπηρεσίας "SOE" χρησιμοποίησαν αρχικά ένα τύπο κρυπτογραφίας που βασιζόταν σε ποιήματα (τα απομνημονευμένα ποιήματα ήταν τα κλειδιά). Οι Γερμανοί, ώρες πριν την Απόβαση της Νορμανδίας συνέλαβαν ένα μήνυμα - ποίημα του Πολ Βερλέν, για το οποίο, χωρίς να το έχουν αποκρυπτογραφήσει, ήταν βέβαιοι πως προανήγγελλε την απόβαση. Η Γερμανική ηγεσία δεν έλαβε υπόψη της αυτή την προειδοποίηση.

Οι Πολωνοί είχαν προετοιμαστεί για την εμπόλεμη περίοδο κατασκευάζοντας την κρυπτομηχανή LCD Lacida, η οποία κρατήθηκε μυστική ακόμη και από τον Rejewski. Όταν. τον Ιούλιο του 1941 ελέγχθηκε από τον Rejewski η ασφάλειά της, του χρειάστηκαν μερικές μόνον ώρες για να την "σπάσει" και έτσι αναγκάστηκαν να την αλλάξουν βιαστικά. Τα μηνύματα που εστάλησαν με Lacida δεν ήταν, εντούτοις,

συγκρίσιμα με αυτά του Enigma, αλλά η παρεμπόδιση θα μπορούσε να έχει σημάνει το τέλος της κρίσιμης κρυπταναλυτικής Πολωνικής προσπάθειας.

1.3 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 ο πατέρας των μαθηματικών συστημάτων κρυπτογραφίας. Το **1949** δημοσίευσε το έγγραφο «Θεωρία επικοινωνίας των συστημάτων μυστικότητας» (*Communication Theory of Secrecy Systems*) στο τεχνικό περιοδικό Bell System και λίγο αργότερα στο βιβλίο του, «Μαθηματική Θεωρία της Επικοινωνίας» (*Mathematical Theory of Communication*), μαζί με τον Warren Weaver. Αυτά, εκτός από τις άλλες εργασίες του επάνω στη θεωρία δεδομένων και επικοινωνίας καθιέρωσε μια στερεά θεωρητική βάση για την κρυπτογραφία και την κρυπτανάλυση. 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.

1.3.1 DES – Data Encryption Standard και AES – Advanced Encryption Standard

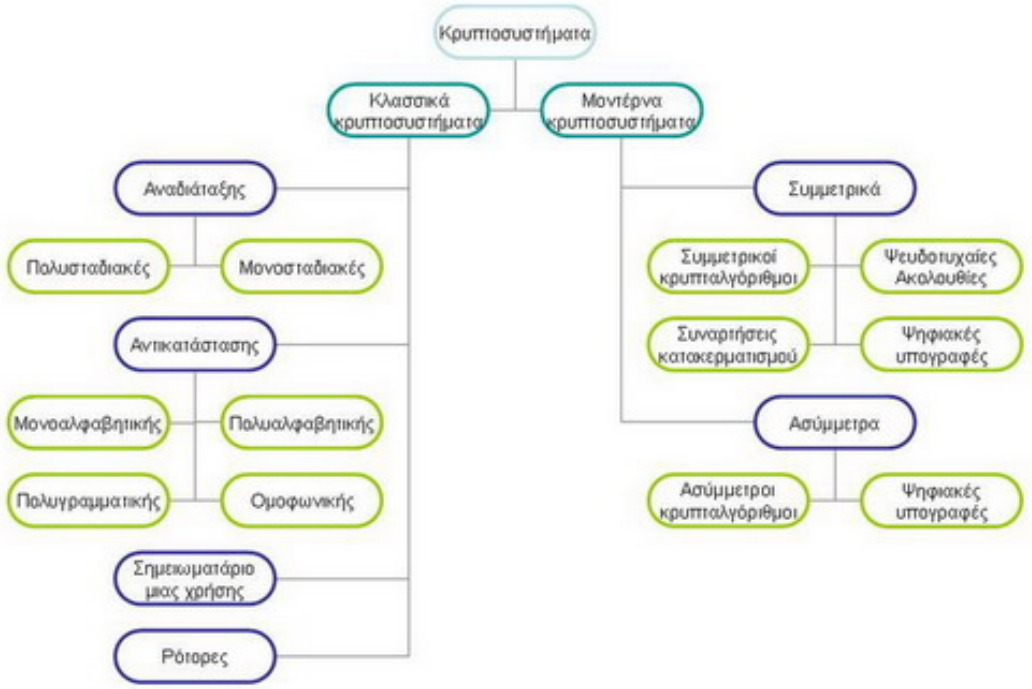
Στα μέσα της δεκαετίας του '70 έγιναν δύο σημαντικές δημόσιες (δηλ. μη-μυστικές) πρόοδοι. Πρώτα ήταν η δημοσίευση του σχεδίου προτύπου κρυπτογράφησης DES (Data Encryption Standard) στον ομοσπονδιακό κατάλογο της Αμερικής στις 17 Μαρτίου 1975. Το προτεινόμενο DES υποβλήθηκε από την IBM, στην πρόσκληση του Εθνικού Γραφείου των Προτύπων (τώρα γνωστό ως NIST), σε μια προσπάθεια να αναπτυχθούν ασφαλείς ηλεκτρονικές εγκαταστάσεις επικοινωνίας για επιχειρήσεις όπως τράπεζες και άλλες μεγάλες οικονομικές οργανώσεις. Μετά από τις συμβουλές και την τροποποίηση από την NSA, αυτό το πρότυπο υιοθετήθηκε και δημοσιεύθηκε ως ένα ομοσπονδιακή τυποποιημένο πρότυπο επεξεργασίας πληροφοριών το 1977 (αυτήν την περίοδο αναφέρεται σαν FIPS 46-3). Ο DES ήταν ο πρώτος δημόσια προσιτός αλγόριθμος κρυπτογράφησης που εγκρίνεται από μια εθνική αντιπροσωπεία όπως η NSA. Η απελευθέρωση της προδιαγραφής της από την NBS υποκίνησε μια έκρηξη δημόσιου και ακαδημαϊκού ενδιαφέροντος για τα συστήματα κρυπτογραφίας.

Ο DES αντικαταστάθηκε επίσημα από τον AES το 2001 διότι ο NIST τον θεώρησε πια ανεπαρκή. Μετά από έναν ανοικτό διαγωνισμό, ο NIST επέλεξε τον αλγόριθμο Rijndael, που υποβλήθηκε από δύο Φλαμανδούς κρυπτογράφους, για να είναι το AES. Ο DES και οι ασφαλέστερες παραλλαγές του όπως ο 3DES ή TDES χρησιμοποιούνται ακόμα σήμερα, ενσωματωμένος σε πολλά εθνικά και οργανωτικά πρότυπα. Εντούτοις, το βασικό μέγεθος των 56-bit έχει αποδειχθεί ότι είναι ανεπαρκές να αντισταθεί στις επιθέσεις ωμής βίας (μια τέτοια επίθεση πέτυχε να σπάσει τον DES σε 56 ώρες ενώ το άρθρο που αναφέρεται ως το σπάσιμο του DES δημοσιεύτηκε από τον O'Reilly and Associates). Κατά συνέπεια, η χρήση απλής

κρυπτογράφησης με τον DES είναι τώρα χωρίς αμφιβολία επισφαλής για χρήση στα νέα σχέδια των κρυπτογραφικών συστημάτων και μηνύματα που προστατεύονται από τα παλαιότερα κρυπτογραφικά συστήματα που χρησιμοποιούν DES, και όλα τα μηνύματα που έχουν αποσταλεί από το 1976 με τη χρήση DES, διατρέχουν επίσης σοβαρό κίνδυνο αποκρυπτογράφησης. Ανεξάρτητα από την έμφυτη ποιότητά του, το βασικό μέγεθος του DES (56-bit) ήταν πιθανά πάρα πολύ μικρό ακόμη και το 1976, πράγμα που είχε επισημάνει ο Whitfield Diffie. Υπήρξε επίσης η υποψία ότι κυβερνητικές οργανώσεις είχαν ακόμα και τότε ικανοποιητική υπολογιστική δύναμη ώστε να σπάσουν μηνύματα που είχαν κρυπτογραφηθεί με τον DES.

1.4 Κατηγορίες Κρυπτοσυστημάτων

Τα κρυπτοσυστήματα χωρίζονται σε 2 μεγάλες κατηγορίες τα Κλασσικά Κρυπτοσυστήματα και τα Μοντέρνα Κρυπτοσυστήματα (Συμμετρικά κρυπτοσυστήματα και Ασύμμετρα κρυπτοσυστήματα).



1.4.1 Κλασσικά Κρυπτοσυστήματα

Κλασσικά κρυπτοσυστήματα αποκαλούνται συνήθως τα κρυπτοσυστήματα αντικατάστασης και τα κρυπτοσυστήματα αναδιάταξης όπως είναι το σύστημα αντικατάστασης του Καίσαρα και ο αλγόριθμος Vigenere τα οποία αναλύσαμε παραπάνω.

Επίσης στα κλασσικά εντάσσονται συνήθως τα γραμμικά κρυπτοσυστήματα, το αφινικό ή ομοπαραλληλικό κρυπτοσύστημα, το Hill κρυπτοσύστημα, τα συνδυαστικά κρυπτοσυστήματα (πχ κρυπτοσύστημα Playfair), το ADFGVX Κρυπτοσύστημα, οι "μηχανές με ρότορες".

1.4.1.1 Playfair

Αυτό είναι ένα παράδειγμα ενός πολυαλφαβητικού συστήματος κρυπτογράφησης αντικατάστασης. Αντικαθιστά ζεύγη χαρακτήρων. Το κλειδί είναι μια μετάθεση του {A...I, K... Z}. Για παράδειγμα:

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

Για την κρυπτογράφηση, γράφεται το απλό κείμενο (χωρίς κενά ή σημεία στίξης), προσθέτοντας ένα X ανάμεσα σε διπλά γράμματα και στο τέλος αν χρειάζεται για να έχει το κείμενο άρτιο μήκος. Στη συνέχεια, για κάθε ζεύγος των γραμμάτων:

Έστω (a,b) είναι η σειρά και στήλη του πρώτου χαρακτήρα και (c,d) είναι η σειρά και στήλη του δεύτερου.
Αν a ≠ c και b≠ d τότε επιστρέφεται (a,d) (b,c).
Αν a = c τότε επιστρέφεται (a, (b +1)) (c, (d +1)) mod5
Αν b = d τότε επιστρέφεται ((a +1), b) ((c +1), d) mod5

Παράδειγμα"THEN ATTACK FROM THE EAST" ⇒ "TH EN AT XT AC KF RO MT HE XE AS TX" ⇒ "UT HW GO FO DB TV YK ZK NH NA DX OF"
Για την αποκρυπτογράφηση χρησιμοποιείται ο αλγόριθμος αντίστροφα. Το κρυπτοσύστημα Playfair είναι αρκετά ανασφαλές.

1.4.1.2 Four-square

Κρυπτογραφεί ζεύγη χαρακτήρων όπως το Playfair, αλλά είναι ελαφρά ισχυρότερο επειδή επιτρέπεται για διπλά γράμματα και δεν αποδίδει αντεστραμμένα διγράμματα κρυπτοκειμένου για αντεστραμμένα διγράμματα απλού κειμένου. Για παράδειγμα:

a b c d e G I V E M
f g h i k L B R T Y
l m n o p O D A H C
q r s t u F K N P Q
v w x y z S U W X Z

P R E M A a b c d e
T U O I Z f g h i k
N S H F L l m n o p

V B C D G q r s t u
K Q W X Y v w x y z

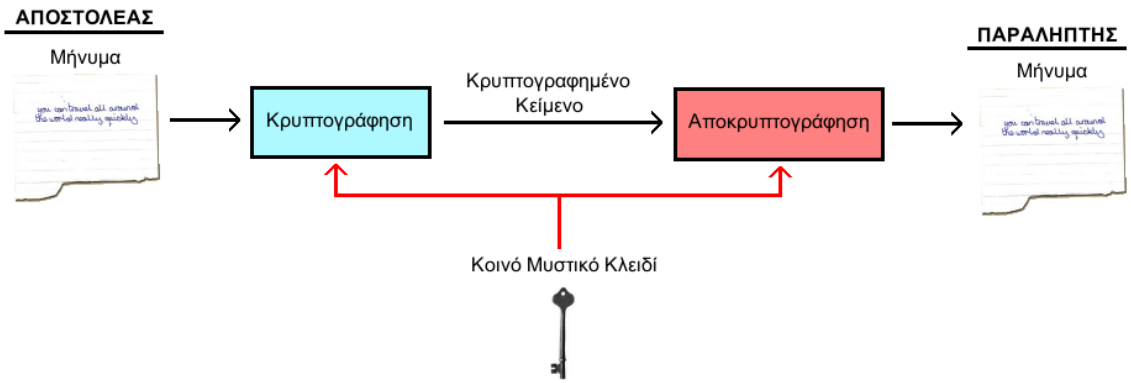
Για τα οποία έχουμε : "THEN ATTACK FROM THE EAST" ⇒ "TH EN AT TA CK FR OM TH EE AS TX" ⇒ "NI VL EV FM MO BV DF NI MA VV NX".

1.4.2 Μοντέρνα Κρυπτοσυστήματα

Τα μοντέρνα κρυπτοσυστήματα χωρίζονται με βάση τα κλειδιά σε :

- **Μυστικού ή Συμμετρικού Κλειδιού (Symmetric Key)**, στα οποία χρησιμοποιείται το ίδιο μυστικό κλειδί για την κρυπτογράφηση και αποκρυπτογράφηση. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα συναλλασσόμενα μέρη.
- **Δημόσιου ή Ασύμμετρου Κλειδιού (Public or Asymmetric Key)**, στα οποία χρησιμοποιείται διαφορετικό κλειδί για κρυπτογράφηση (δημόσιο κλειδί παραλήπτη) και διαφορετικό για αποκρυπτογράφηση (προσωπικό κλειδί παραλήπτη).

1.4.2.1 Συμμετρική Κρυπτογραφία

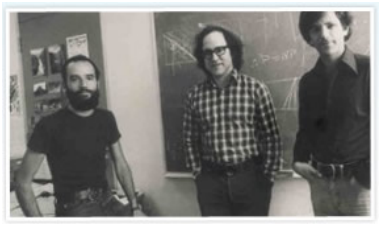


Ένα πρόβλημα το οποίο υφίσταται στους αλγόριθμους κρυπτογράφησης είναι η **αδυναμία ανταλλαγής του κλειδιού με κάποιον ασφαλή τρόπο**. Στην σύγχρονη ψηφιακή εποχή ο αποστολέας και ο παραλήπτης του μηνύματος πολλές φορές δεν γνωρίζονται, οπότε για την μετάδοση του κλειδιού από τον έναν στον άλλο θα πρέπει να υπάρχει κάποιο ασφαλές κανάλι επικοινωνίας. Φυσικά το διαδίκτυο δεν μπορεί να αποτελέσει κανάλι ασφαλούς επικοινωνίας, οπότε η χρήση της συμμετρικής κρυπτογράφησης σε εφαρμογές ηλεκτρονικού εμπορίου, ανταλλαγής ηλεκτρονικών μηνυμάτων κοκ ουσιαστικά δεν υφίσταται.

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

Οι πιο γνωστοί αλγόριθμοι αυτού του είδους είναι οι DES, Triple DES, IDEA, RC2, RC4, AES.

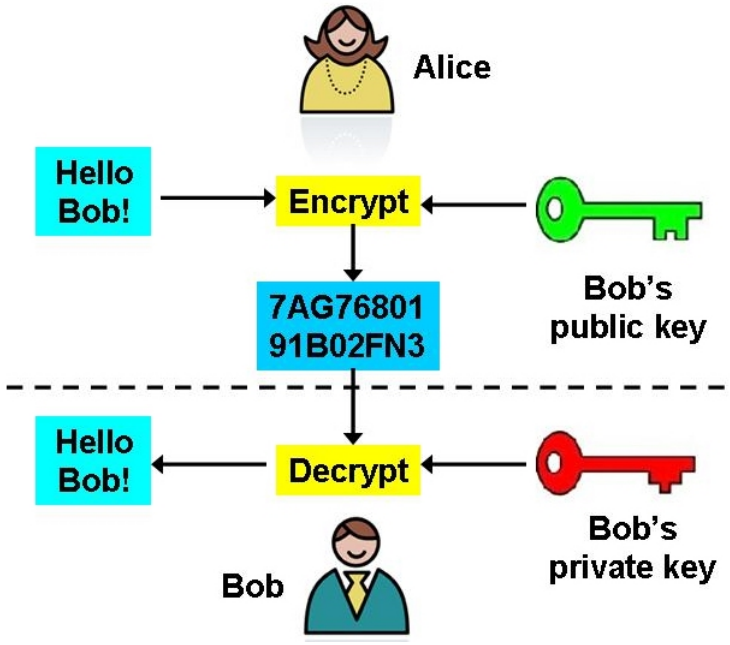
1.4.2.2 Ασύμμετρη Κρυπτογραφία (Δημοσίου Κλειδιού)



Το 1976, οι Whitfield Diffie και Martin Hellman έλυσαν το πρόβλημα της διακίνησης ενός κοινόχρηστου ιδιωτικού κλειδιού μέσω ενός μη ασφαλούς καναλιού, μια εφεύρεση γνωστή ως «Ανταλλαγή κλειδιού Diffie-Hellman». Ένα χρόνο αργότερα, τρεις καθηγητές του Massachusetts Institute of Technology (MIT) οι Iron Rivest, Adi Shamir και Leonard Adleman δημιούργησαν την πρώτη πρακτική εφαρμογή της κρυπτογράφησης **Δημόσιου Κλειδιού**, γνωστή ως μέθοδο RSA.

Οι βασικές ιδέες της κρυπτογράφησης Δημόσιου Κλειδιού:

• Αντί για ένα κλειδί, έχετε δύο: ένα για την κρυπτογράφηση (δημόσιο) και ένα διαφορετικό για την αποκρυπτογράφηση (ιδιωτικό)
• Το κλειδί κρυπτογράφησης μπορεί να είναι δημόσιο
• Η γνώση του κλειδιού κρυπτογράφησης, δεν βοηθάει στην εύρεση του κλειδιού αποκρυπτογράφησης



Ο Bob γνωρίζει ότι η Alice θέλει να του στείλει ένα μήνυμα, και δημιουργεί ένα ζευγάρι κλειδιών. Καθιστά γνωστό το δημόσιο κλειδί του, ίσως στην ιστοσελίδα του! Η Alice το βλέπει, και το ίδιο κάνει και η Eve. Η Alice χρησιμοποιεί το δημόσιο κλειδί

για να κρυπτογραφήσει το μήνυμά της, και το στέλνει στον Bob. Η Eve παρακολουθήσει το μήνυμα, αλλά δεν μπορεί να το αποκρυπτογραφήσει - μόνο ο Bob μπορεί να αποκρυπτογραφήσει το μήνυμα, γιατί μόνο ο Bob έχει το ιδιωτικό κλειδί.

1.5 Κλειδιά Κρυπτογράφησης

Δημιουργία κλειδιού:

Ένα κλειδί πρέπει να ανθίσταται σε επιθέσεις λεξικού (dictionary attack). Ένα «ισχυρό» κλειδί αποτελείται από μια «τυχαία» συμβολοσειρά bit, που δημιουργείται από μια αυτοματοποιημένη διαδικασία (γεννήτορας) παραγωγής ψευδο-τυχαίων αριθμών (pseudo-randomness generator). Κάθε bit ενός κλειδιού πρέπει να είναι εξίσου πιθανό.

Μήκος κλειδιού:

Ο μόνος τρόπος να παραβιαστεί ένας "ισχυρός" κρυπτογραφικός αλγόριθμος, είναι η αποκαλούμενη και ως επίθεση *ωμής βίας* (**brute-force**). Σε αυτήν την επίθεση, ο Mallory δοκιμάζει όλα τα πιθανά κλειδιά ώστε να βρει κάποιο που ταιριάζει με το κλειδί που χρησιμοποιήθηκε κατά την κρυπτογράφηση. Για να εξαπολύσει αυτού του είδους την επίθεση, ο κρυπταναλυτής πρέπει πρώτα να υποκλέψει ένα κρυπτογράφημα Η πολυπλοκότητα της επίθεσης υπολογίζεται ως εξής. Εαν το κλειδί έχει μήκος 8 bits, τότε υπάρχουν 2^8 , ή 256 πιθανά κλειδιά. Επομένως, θα χρειαστούν 256 προσπάθειες προκειμένου να βρεθεί το σωστό κλειδί, με πιθανότητα 50% να βρεθεί το κλειδί μετά τις μισές προσπάθειες. Οι χρόνοι μπορούν να συντομευθούν με κατανεμημένη επεξεργασία. Αν το κλειδί έχει μήκος 128 bit, τότε ο κρυπταναλυτής θα πρέπει να δοκιμάσει κατά μέσο όρο 2^{127} κλειδιά, πριν βρει το σωστό. Η επίθεση αυτή είναι πρακτικώς αδύνατη.
Σημείωση: Σε έναν συμμετρικό αλγόριθμο, το ελάχιστα αποδεκτό μήκος κλειδιού είναι 128 bit. Σε έναν αλγόριθμο δημόσιου κλειδιού, το ελάχιστα αποδεκτό μήκος κλειδιού είναι 1024 bit.

Ανταλλαγή κλειδιού:

Σε μεγάλα ιδίως δίκτυα, ο τρόπος με τον οποίο τα κλειδιά μεταφέρονται ή τίθενται υπό διαπραγμάτευση μεταξύ των χρηστών, πρέπει να είναι ασφαλής. Έχουν προταθεί πολλά πρωτόκολλα *ανταλλαγής κλειδιών* (π.χ Diffie Hellman), η επιλογή ενός εκ των οποίων πρέπει να γίνεται με μεγάλη προσοχή.

Αποθήκευση:

Ένα μυστικό (ιδιωτικό) κλειδί πρέπει να φυλάσσεται σε ασφαλές σημείο. Για παράδειγμα, η φύλαξη του σε φορητό αποθηκευτικό μέσο ή στο σκληρό δίσκο ενός Η/Υ θα πρέπει να συνεπικουρείται από μηχανισμούς ταυτοποίησης χρήστη (κωδικός πρόσβασης ή/και βιομετρικά συστήματα). Το πλέον ενδεδειγμένο από τη σκοπιά της ασφάλειας σημείο φύλαξης ενός κλειδιού είναι μια έξυπνη κάρτα (smart card): η πρόσβαση στο κλειδί ελέγχεται με τη χρήση κωδικού PIN ή/και με βιομετρικά αποτυπώματα. Η κάρτα μπορεί επίσης να φέρει το ψηφιακό πιστοποιητικό του κλειδιού και να εκτελεί το λογισμικό κρυπτογράφησης-αποκρυπτογράφησης καθώς και ψηφιακής υπογραφής για λογαριασμό του κατόχου της. Σε μια τέτοια

περίπτωση η κάρτα μπορεί να χρησιμοποιηθεί σε οποιοδήποτε τερματικό διαθέτει αναγνώστη έξυπνων καρτών.

1.6 Κρυπτανάλυση και Μέθοδοι Επιθέσεων

Κρυπτανάλυση είναι η μελέτη των μαθηματικών τεχνικών που επιχειρούν την αναίρεση των τεχνικών της κρυπτογραφίας και γενικότερα την αναίρεση της ασφαλούς μετάδοσης πληροφοριών. Η κρυπτανάλυση βασίζεται, πέραν των μαθηματικών και στο εμπειρικό γεγονός, ότι στην πράξη, ο κρυπταναλυτής έχει στη διάθεσή του πάρα πολύ μεγάλο αριθμό κρυπτογραφημένων κειμένων, τα οποία κρυπτογραφήθηκαν με τον ίδιο τρόπο. Ενώ επίσης θεωρούμε δεδομένο το γεγονός ότι ο κρυπταναλυτής γνωρίζει πλήρως τη διαδικασία κρυπτογράφησης-αποκρυπτογράφησης που χρησιμοποιήθηκε. Οι διαδικασίες κρυπτανάλυσης ονομάζονται επιθέσεις (attacks) :

Σκοπός του κρυπταναλυτή είναι να αποκτήσει:

- Ένα μέρος ή ολόκληρο το αρχικό κείμενο (plain text)
- Ένα μέρος ή ολόκληρο το κρυπτογραφημένο κείμενο (cipher text)
- Συνδυασμό των προηγουμένων από ένα μήνυμα ή από διαφορετικά μηνύματα
- Τα κλειδιά κρυπτογράφησης

Ανάλογα με τις μεθόδους που χρησιμοποιούνται, κατηγοριοποιούνται οι διάφορες μέθοδοι επιθέσεων. Οι δυνατότητες επίθεσης σε ένα κρυπτοσύστημα χωρίζονται στις ακόλουθες κατηγορίες :

- Επίθεση στο κρυπτοκείμενο (cipher-text only).
  Ο αντίπαλος έχει πρόσβαση μόνο σε ορισμένα τμήματα του κρυπτοκειμένου και ο αντικειμενικός σκοπός του είτε η αποκρυπτογράφηση του κρυπτοκειμένου αυτού ή η ανακάλυψη του αντίστοιχου κλειδιού. Κρυπτοκείμενο ευάλωτο σε μια τέτοια επίθεση θεωρείται ανασφαλές.

- Επίθεση με γνωστό αρχικό κείμενο (known-plaintext)
  Ο αντίπαλος γνωρίζει αντιστοιχίες κρυπτοκειμένου με απλό κείμενο και ο αντικειμενικός σκοπός του είναι η ανακάλυψη του αντίστοιχου κλειδιού. Στον κόσμο των δικτύων υπολογιστών τα πρωτόκολλα επικοινωνίας εμφανίζουν συστηματικά τυποποιημένα μηνύματα.

- Επίθεση με επιλεγμένο αρχικό κείμενο (chosen-plaintext)
  Ο αντίπαλος έχει τη δυνατότητα πρόσβασης στο κρυπτοσύστημα όπου δεν γνωρίζει το κλειδί και μπορεί να ζητά την κρυπτογράφηση μηνυμάτων. Με

αυτόν τον τρόπο μπορεί να ανακαλύψει την αντιστοιχία του απλού κειμένου με το άγνωστο κρυπτοκείμενο.

- Επίθεση με επιλεγμένο κρυπτοκείμενο (chosen-ciphertext)
  Υποθέτοντας ότι ο αντίπαλος έχει πρόσβαση στον αλγόριθμο αποκρυπτογράφησης, ο αντικειμενικός σκοπός του είναι να ανακαλύψει το κλειδί αποκρυπτογράφησης προκειμένου να μπορεί στο μέλλον να αποκρυπτογραφεί τα νέα κρυπτοκείμενα, όταν δε θα έχει πρόσβαση στον αλγόριθμο αποκρυπτογράφησης. Στα περισσότερα συμμετρικά κρυπτοσυστήματα η επίθεση αυτή έχει την ίδια ισχύ με την επίθεση του επιλεγμένου κειμένου. Η επίθεση με επιλεγμένο κρυπτοκείμενο θεωρείται ως η πιο αυστηρή επίθεση.

- Επίθεση προσαρμόσιμου επιλεγμένου κρυπτοκειμένου (adaptive chosen-ciphertext). Η επίθεση αυτή είναι αντίστοιχη του προσαρμόσιμου επιλεγμένου απλού κειμένου, με τη διαφορά ότι ο αντίπαλος έχει πρόσβαση στον αλγόριθμο αποκρυπτογράφησης.

1.6.1 Κρυπτανάλυση Κλασσικών Κρυπτοσυστημάτων

- Μέθοδος Ωμής Βίας (Brute Force)
- Ανάλυση Συχνότητας της γλώσσας
- Μέθοδος Kasiski
- Μέθοδος Δείκτη Σύμπτωσης
- Μέθοδος Αμοιβαίου Δείκτη Σύμπτωσης

1.6.2 Κρυπτανάλυση Σύγχρονων Κρυπτοσυστημάτων

- Διαφορική Κρυπτανάλυση (Differential Cryptanalysis)
- Γραμμική Κρυπτανάλυση (Linear Cryptanalysis)
- Κρυπτανάλυση στο Επίπεδο Υλικού (Side- channel Cryptanalysis)
- Κλειδοσχεσιακή Κρυπτανάλυση (Related Key Cryptanalysis)
- Κρυπτανάλυση Ισοτίμων (Cryptanalysis mod n)
- Κρυπτανάλυση Τετραγώνου (Square Cryptanalysis)
- Στατιστική Κρυπτανάλυση (Statistical Cryptanalysis)

1.7 Εφαρμογές της Κρυπτογραφίας

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

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

ΚΕΦΑΛΑΙΟ 2: ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ -DES

Σχήμα: Μοντέλο Συμμετρικού Κρυπτοσυστήματος

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

Τα στάδια της επικοινωνίας του σχήματος είναι τα ακόλουθα:

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

2.1 Κατηγορίες Συμμετρικών Κρυπταλγορίθμων

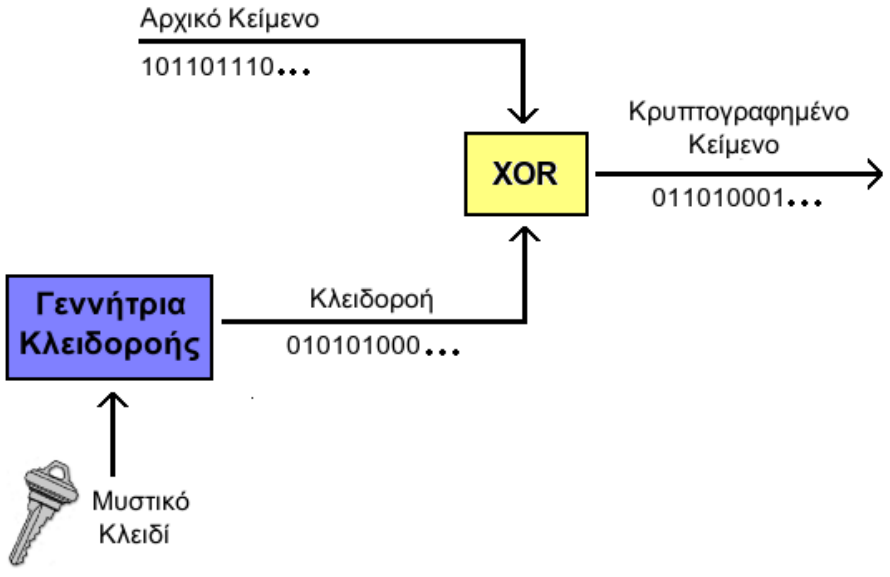
Οι συμμετρικοί κρυπτογραφικοί αλγόριθμοι μπορούν να χωριστούν σε δύο διαφορετικές κατηγορίες με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων:

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

2.1.1 Συμμετρικοί Κρυπταλγόριθμοι ροής (Stream Ciphers) :

- ORYX
- RC4
- SEAL

Οι **κρυπτογραφικοί αλγόριθμοι ροής (stream ciphers)** χρησιμοποιούνται για την κρυπτογράφηση μίας συνεχούς ροής δεδομένων (data stream). Για την κρυπτογράφηση επιλέγεται αρχικά μία *γεννήτρια κλειδορροής (keystream generator)*, η οποία δέχεται ως είσοδο το μυστικό κλειδί και παράγει στην έξοδό της μία ψευδοτυχαία ακολουθία bits, η οποία ονομάζεται κλειδορροή (keystream). Στην συνέχεια εφαρμόζεται η συνάρτηση XOR ανάμεσα στο αρχικό κείμενο και στην κλειδορροή και το αποτέλεσμα της συνάρτησης είναι η τελική κρυπτογραφημένη ροή δεδομένων. Η διαδικασία που μόλις περιγράφηκε φαίνεται πιο καθαρά στο σχήμα που παρατίθεται.



Σχηματικό διάγραμμα του τρόπου λειτουργίας των κρυπτογραφικών αλγορίθμων ροής.

Η αποκρυπτογράφηση γίνεται με την ακριβώς αντίστροφη διαδικασία. Εάν χρησιμοποιηθεί το ίδιο κλειδί ως είσοδο στην γεννήτρια κλειδοροής, τότε η δεύτερη θα παράγει ακριβώς την ίδια ακολουθία bits (κλειδοροή) όπως και προηγουμένως κατά την διαδικασία της κρυπτογράφησης. Εφαρμόζοντας την συνάρτηση XOR ανάμεσα στην κρυπτογραφημένη ακολουθία δεδομένων και την κλειδοροή παράγεται τελικά το αρχικό κείμενο.

Για να είναι ασφαλής ο κρυπτογραφικός αλγόριθμος ροής, θα πρέπει να πληρούνται ορισμένες προϋποθέσεις όσον αφορά την γεννήτρια κλειδοροής και την ψευδοτυχαία ακολουθία bits που αυτή παράγει. Συγκεκριμένα η ασφάλεια του αλγορίθμου εξαρτάται από τις εξής παραμέτρους:

- **Η ψευδοτυχαία ακολουθία bits (κλειδοροή) που παράγεται από την γεννήτρια κλειδοροής θα πρέπει να έχει αρκετά μεγάλη περίοδο επανάληψης.** Επειδή ουσιαστικά η γεννήτρια κλειδοροής είναι μία μαθηματική συνάρτηση που δέχεται ως είσοδο το μυστικό κλειδί και παράγει στην έξοδο την κλειδοροή, είναι βέβαιο πως η κλειδοροή που θα παραχθεί θα είναι από ένα σημείο και μετά περιοδική. Αυτό σημαίνει πως μετά από κάποιον αριθμό bits της κλειδοροής, αυτή θα επαναλαμβάνεται ξεκινώντας από την αρχή. Αν η περίοδος επανάληψης είναι πολύ μικρή, τότε το γεγονός αυτό καθιστά τον αλγόριθμο κρυπτογράφησης ιδιαίτερα ευάλωτο σε προσπάθειες κρυπτανάλυσης.

- **Η ακολουθία bits της κλειδοροής θα πρέπει να μοιάζει πολύ με τυχαία.** Αυτό σημαίνει ότι η μαθηματική συνάρτηση που χρησιμοποιείται στην γεννήτρια κλειδοροής θα πρέπει να επιλεγεί κατάλληλα ούτως ώστε το αποτέλεσμά της να πλησιάζει όσο το δυνατόν περισσότερο το τυχαίο. Υπάρχουν ειδικές μέθοδοι δοκιμής της καταλληλότητας της γεννήτριας κλειδοροής, οι οποίοι εκπονούν ελέγχους τυχαιότητας (randomness tests) σε αυτήν. Ένας έλεγχος τυχαιότητας είναι για παράδειγμα ο εξής: Για μία κλειδοροή μήκους εκατομμυρίων bits, θα πρέπει ο αριθμός των 1 να ισούται με τον αριθμό των 0. Επίσης θα πρέπει κάθε 0 να ακολουθείται από 1 τόσο συχνά όσο και το αντίστροφο. Σε κάθε περίπτωση όμως η κλειδοροή που θα παραχθεί δεν μπορεί να είναι εντελώς τυχαία, γι' αυτό και ονομάζεται ψευδοτυχαία ακολουθία bits.

- **Η κλειδοροή θα πρέπει να έχει μεγάλη γραμμική ισοδυναμία (linear equivalence).** Οποιαδήποτε ακολουθία δυαδικών ψηφίων μπορεί να παραχθεί με χρήση γραμμικών μεθόδων, για παράδειγμα με υπολογισμό της επόμενης τιμής βάσει των προηγούμενων τιμών της ακολουθίας. Αν στον υπολογισμό αυτό χρησιμοποιείται ένας μικρός σχετικά αριθμός προηγούμενων τιμών, τότε λέμε πως η ακολουθία έχει μικρή γραμμική ισοδυναμία. Αντίθετα εάν στο υπολογισμό χρησιμοποιείται ένας μεγάλος αριθμός προηγούμενων τιμών, τότε η ακολουθία έχει μεγάλη γραμμική ισοδυναμία. Μία κλειδοροή με μεγάλη γραμμική ισοδυναμία εγγυάται μεγαλύτερη ασφάλεια των κρυπτογραφημένων δεδομένων απέναντι σε προσπάθειες κρυπτανάλυσης.

Οι συνθήκες που παρουσιάστηκαν παραπάνω είναι αναγκαίες για να εξασφαλίσουν έναν αξιόπιστο αλγόριθμο ροής, όχι όμως επαρκείς. Γενικά για να είναι ένας κρυπτογραφικός αλγόριθμος ροής αξιόπιστος θα πρέπει να εξασφαλίζει ότι ακόμη και εάν κάποιος αποκτήσει οποιαδήποτε πληροφορία για κάποιο κομμάτι της ακολουθίας κλειδοροής, είναι υπολογιστικά αδύνατο να συνάγει άλλα κομμάτια της ακολουθίας.

Η κρυπτογράφηση με αλγόριθμους ροής είναι σχετικά γρήγορη αφού η κρυπτογράφηση και η αποκρυπτογράφηση είναι σχετικά απλές διαδικασίες, ενώ πλέον έχουν κατασκευαστεί γεννήτριες κλειδοροών που είναι ασφαλείς και λειτουργούν σε αρκετά μεγάλες ταχύτητες. Υπάρχουν ακόμη και συσκευές (hardware) με την μορφή chip που υλοποιούν τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης σε ιδιαίτερα υψηλές ταχύτητες. Τέτοια chip χρησιμοποιούνται κυρίως σε κινητά τηλέφωνα και σε άλλες συσκευές ασύρματης επικοινωνίας.

Τέλος, οι κρυπτογραφικοί αλγόριθμοι ροής έχουν και την εξής πολύ ενδιαφέρουσα ιδιότητα: Δεν πολλαπλασιάζουν τα λάθη μετάδοσης. Αυτό σημαίνει ότι εάν συμβεί κάποιο σφάλμα μετάδοσης της κρυπτογραφημένης πληροφορίας και αλλάξει η τιμή ενός bit, τότε η αποκρυπτογραφημένη ακολουθία θα εμφανίζει σφάλμα σε ένα μόνο bit.

2.1.2 Συμμετρικοί Κρυπταλγόριθμοι Τμήματος (Block Ciphers)

Οι κρυπταλγόριθμοι τμήματος (block ciphers) είναι το κεντρικό εργαλείο στο σχεδιασμό πρωτοκόλλων στη συμμετρική κρυπτογραφία. Πρόκειται για πολύ ισχυρά εργαλεία τα οποία όμως, αν είναι τα μόνα που έχουμε στη διάθεσή μας, όσο καλά και αν χρησιμοποιηθούν δεν παράγουν κάτι ασφαλές.
Σε αυτό το κεφάλαιο θα έρθουμε σε επαφή με κάποιους τυπικούς αλγορίθμους τμήματος καθώς και με τις επιθέσεις εναντίον τους, και θα δούμε εκτενέστερα δύο παραδείγματα, τον DES και τον AES. Ο DES είναι ο παλαιότερος και ο πιο ευρέως χρησιμοποιούμενος αλγόριθμος τμήματος ενώ ο AES έχει αντικαταστήσει τον DES τα τελευταία χρόνια.

Τι είναι ένας αλγόριθμος τμήματος και ο τρόπος λειτουργίας του

Ένας αλγόριθμος τμήματος είναι μια συνάρτηση $E: \{0,1\}^k * \{0,1\}^n \rightarrow \{0,1\}^n$ Αυτός ο συμβολισμός σημαίνει ότι η E παίρνει δύο εισόδους (inputs), η μία είναι ένα k-bit string και η άλλη ένα n-bit string, και επιστρέφει (output) ένα n-bit string. Η πρώτη είσοδος είναι το «κλειδί». Η δεύτερη μπορεί να ονομαστεί «απλό κείμενο» και η έξοδος μπορεί να ονομαστεί «κρυπτοκείμενο». Το μήκος του κλειδιού k και το μήκος του τμήματος (block) n είναι παράμετροι που σχετίζονται με τον block cipher. Ποικίλουν από block cipher σε block cipher όπως βεβαίως κάνει και ο σχεδιασμός του αλγόριθμου.

Για κάθε κλειδί $K \in \{0,1\}^k$ θέτουμε την $E_K : \{0,1\}^n \rightarrow \{0,1\}^n$ να είναι η συνάρτηση που ορίζεται από την $E_K(M) = E(K,M)$. Για κάθε block cipher, και οποιοδήποτε κλειδί K, απαιτείται η συνάρτηση E_K να είναι μια μετάθεση στον $\{0,1\}^n$. Αυτό σημαίνει ότι είναι μια αντιστοιχία 1-1 και επί από το $\{0,1\}^n$ στο $\{0,1\}^n$. Για κάθε $C \in \{0,1\}^n$ υπάρχει ακριβώς ένα $M \in \{0,1\}^n$ έτσι ώστε $E_K(M) = C$. Ως εκ τούτου η E_K έχει αντίστροφη και τη συμβολίζουμε E_K^{-1}. Αυτή η συνάρτηση είναι επίσης από τον $\{0,1\}^n$ στον $\{0,1\}^n$ και φυσικά έχουμε $E_K^{-1}(E_K(M)) = M$ και $E^{-1}(K,C) = E_K^{-1}(C)$. Αυτός είναι ο αντίστροφος κρυπταλγόριθμος τμήματος της E.
Ο E και ο E^{-1} πρέπει να είναι εύκολα υπολογίσιμοι δηλαδή αν δίνονται τα K,M να υπολογίζεται εύκολα το E(K,M) και αν δίνονται τα K,C να υπολογίζεται εύκολα το E^{-1} (K,C). Όταν λέμε να «υπολογίζονται εύκολα» εννοούμε με τη χρήση δημόσια γνωστών και σχετικά αποτελεσματικών προγραμμάτων που διατίθενται για τέτοιες εργασίες.

Σε μια τυπική χρήση, ένα τυχαίο κλειδί επιλέγεται και κρατείται μυστικό μεταξύ δύο χρηστών. Η συνάρτηση E_K χρησιμοποιείται στη συνέχεια από τα δύο μέρη για την επεξεργασία των δεδομένων με κάποιο τρόπο πριν την αποστολή από τον έναν στον άλλον. Τυπικά, θα υποθέσουμε ότι ο αντίπαλος θα είναι σε θέση να αποκτήσει κάποια παραδείγματα εισόδου-εξόδου για την E_K δηλαδή κάποια ζεύγη της μορφής (M,C) όπου $C = E_K(M)$. Όμως συνήθως, ο αντίπαλος δε θα μπορεί να δει το κλειδί. Η ασφάλεια βασίζεται στη μυστικότητα του κλειδιού. Ο αντίπαλος θα προσπαθήσει να υπολογίσει το κλειδί από τα παραδείγματα εισόδου-εξόδου της E_K . Ο αλγόριθμος θα πρέπει να έχει σχεδιαστεί με τέτοιον τρόπο ώστε να κάνει αυτό το κομμάτι υπολογιστικά δύσκολο για τον αντίπαλο.

Συμμετρικοί Κρυπταλγόριθμοι Τμήματος (Block Ciphers) :

- Data Encryption Standard (DES)
- 3-Way
- Blowfish
- CAST
- CMEA
- Triple-DES
- DEAL FEAL
- GOST
- IDEA
- LOKI
- Lucifer
- MacGuffin
- Twofish
- MARS
- MISTY
- MMB
- NewDES
- RC2
- RC5

- RC6 REDOC
- Rijndael
- Safer
- Serpent
- SQUARE
- Skipjack
- Tiny Encryption Algorithm

2.2 DES

Ο DES είναι αρχετυπικός block cipher, δηλαδή, ένας πρωτότυπος κρυπταλγόριθμος συμμετρικού κλειδιού, που λαμβάνει μια σειρά από bits απλού κειμένου (plaintext bits) σταθερού μήκους και την μετατρέπει, μέσω μιας σειράς πολύπλοκων ενεργειών, σε μια άλλη σειρά bits, το κρυπτοκείμενο (cipher text) με το ίδιο μήκος. Στην περίπτωση του DES το μέγεθος του μπλοκ (block size: Η σειρά των bits σταθερού μήκους) είναι 64 bits. Ο DES χρησιμοποιεί, επίσης, ένα κλειδί για να προσαρμόσει την μετατροπή, ώστε η αποκρυπτογράφηση να μπορεί, υποθετικά, να πραγματοποιηθεί μόνο από εκείνους που γνωρίζουν το συγκεκριμένο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση. Το κλειδί φαινομενικά αποτελείται από 64 bits. Ωστόσο, στην πραγματικότητα μόνο 56 από αυτά χρησιμοποιήθηκαν από τον αλγόριθμο. Τα υπόλοιπα 8 bits χρησιμοποιούνται αποκλειστικά για τον έλεγχο της ισοτιμίας (parity) και στη συνέχεια απορρίπτονται (αυτά καλούνται parity bits), εξ ου και αναφέρεται συνήθως ως κλειδί μήκους 56 bits. Όπως οι άλλοι block αλγόριθμοι κρυπτογράφησης, έτσι και ο DES από μόνος του δεν είναι ασφαλής τρόπος κρυπτογράφησης αλλά, αντίθετα, πρέπει να χρησιμοποιηθεί με ειδικό τρόπο λειτουργίας (mode of operation). Ο DES είναι ένας εξαιρετικού σχεδιασμού αλγόριθμος με ισχυρή επιρροή στην κρυπτογραφία και ευρεία χρήση. Για παράδειγμα, κάθε φορά που χρησιμοποιούμε ένα μηχάνημα ανάληψης ATM χρησιμοποιούμε τον DES.

2.2.1 Ιστορικά

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 (National Bureau of Standards) – που τώρα ονομάζεται NIST (National Institute of Standards and Technology) - 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 μια 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 Χορστ Φάιστελ (Horst Feistel). Αυτός ο κρυπταλγόριθμος θα εξελισσόταν τελικά στον DES. Η ομάδα της IBM συνέχισε τον 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.

Ο DES εγκρίθηκε ως ομοσπονδιακό πρότυπο τον Νοέμβριο του 1976 και δημοσιεύθηκε στις 15 Ιανουαρίου του 1977 ως FIPS PUB 46 και η χρήση του ήταν επιτρεπτή σε όλα τα μη απόρρητα δεδομένα. Στη συνέχεια επιβεβαιώθηκε ως πρότυπο το 1983, το 1988 (αναθεωρήθηκε ως FIPS-46-1), το 1993 (ως FIPS-46-2) και πάλι το 1999 (ως FIPS-46-3). Ο τελευταίος ορισμός ήταν ο Triple DES. Στις 26 Μαΐου του 2002 ο DES τελικά εκτοπίστηκε από τον Advanced Encryption Standard (AES) κατόπιν δημόσιου διαγωνισμού. Στις 19 Μαΐου του 2005 ο FIPS 46-3 είχε επισήμως αποσυρθεί, αλλά το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology - NIST) ενέκρινε τον Triple DES στο έτος 2003 για τις ευαίσθητες πληροφορίες της κυβέρνησης. Μια άλλη θεωρητική επίθεση, η γραμμική κρυπτανάλυση, δημοσιεύθηκε το 1994, αλλά ήταν μια επίθεση brute force το 1998 που αναπαράστησε/απέδειξε ότι μπορεί κάποιος θα μπορούσε πρακτικά να επιτεθεί στον DES και τονίστηκε η ανάγκη για αντικατάσταση του αλγόριθμου. Αυτές και άλλες μέθοδοι κρυπτανάλυσης εξετάζονται λεπτομερώς.

Η εισαγωγή του DES θεωρείται ότι ήταν καταλύτης για την ακαδημαϊκή μελέτη της κρυπτογραφίας, ιδιαίτερα των μεθόδων για να "σπάζουν" block κρυπταλγόριθμους, σύμφωνα με αναδρομή στο NIST για τον DES.

Μπορεί να ειπωθεί ότι το "αρχικό άλμα" του DES ξεπέρασε τις στρατιωτικές μελέτες και την ανάπτυξη των αλγορίθμων κρυπτογράφησης. Στην 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 γενεά κρυπταναλυτών έχει αναλύσει εξονυχιστικά τον αλγόριθμο DES προσπαθώντας να τον "σπάσουν". Ανέφεραν πως ο DES έκανε περισσότερα για να γαλβανίσει τον τομέα της κρυπτανάλυσης από οτιδήποτε άλλο γιατί έτσι υπήρχε ένας αλγόριθμος για μελέτη. 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 αλγόριθμους συμμετρικού κλειδιού μετά από σύγκριση.

2.2.2 Κατασκευή Αλγορίθμου

function $DES_K(M)$ //$|K| = 56$ and $|M| = 64$

$(K_1,\ldots,K_{16}) \leftarrow KeySchedule(K)$ //$|K_i| = 48$ for $1 \le i \le 16$

$M \leftarrow IP(M)$

Parse M as $L_0||R_0$ //$|L_0|=|R_0|=32$

for r=1 to 16 **do**

$L_r \leftarrow R_{r-1}$; $R_r \leftarrow f(K_r,R_{r-1}) \oplus L_{r-1}$

$C \leftarrow IP^{-1}(L_{16}||R_{16})$

return C

Σχήμα 2.1 : Ο αλγόριθμος τμήματος DES

Ο αλγόριθμος DES απεικονίζεται παραπάνω. Παίρνει ως είσοδο ένα 56-bit κλειδί K και ένα 64-bit απλό κείμενο M. Ο αλγόριθμος KeySchedule (ο οποίος θα περιγραφεί παρακάτω) παράγει από το 56-bit κλειδί K μια σειρά από 16 υποκλειδιά, ένα για κάθε γύρο που ακολουθεί. Κάθε υποκλειδί έχει 48-bits.

2.2.2.1 Αρχική Μετάθεση (IP)

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

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

Πίνακες 2.2 που περιγράφουν την αρχική μετάθεση IP του DES και το αντίστροφο IP^{-1}.

Η αρχική μετάθεση IP απλά μεταθέτει τα bits του M, όπως περιγράφηκε από τον πίνακα 2.2. Σύμφωνα με τον πίνακα το bit 1 της εξόδου είναι το bit 58 της εισόδου; το bit 2 της εξόδου είναι το bit 50 της εισόδου,..., το bit 64 της εξόδου είναι το bit 7 της εισόδου. Το κλειδί δεν συμπεριλαμβάνεται στη μετάθεση. Η αρχική μετάθεση δε δείχνει να επηρεάζει το κρυπτογραφικό σθένος του αλγορίθμου, και ο σκοπός της παραμένει μυστήριο.

Το απλό κείμενο που έχει υποστεί μετάθεση είναι τώρα η είσοδος σε έναν βρόχο ο οποίος λειτουργεί σε 16 γύρους. Κάθε γύρος λαμβάνει 64-bit input, το οποίο φαίνεται να αποτελείται από ένα 32-bit αριστερό μισό και από ένα 32-bit δεξί μισό, και κάτω από την επιρροή του υποκλειδιού Kr, παράγεται μια έξοδος 64-bit. Η είσοδος στον γύρο r είναι $L_{r-1}||R_{r-1}$ και η έξοδος από τον γύρο r είναι $L_r||R_r$. Κάθε γύρος είναι αυτό που αποκαλούμε «**Feistel round**», το οποίο έχει πάρει το όνομά του από τον Horst Feistel, έναν από τους σχεδιαστές της IBM που σχεδίασε έναν πρόδρομο του DES.

Στο Σχ.2.1 φαίνεται πως υπολογίζεται $L_r||R_r$ ως συνάρτηση των $L_{r-1}||R_{r-1}$ μέσω της f, με την τελευταία να εξαρτάται από το υπο-κλειδί K_r που σχετίζεται με το γύρο r.

Ένας από τους λόγους χρησιμοποιείται η τακτική με τους γύρους είναι ότι είναι αντιστρέψιμη διαδικασία, σημαντικό για να εξασφαλιστεί ότι ο DES_K είναι μια μετάθεση για κάθε κλειδί K, όπως θα έπρεπε για να χαρακτηριστεί ως ένας block cipher. Πράγματι, δεδομένων των $L_r||R_r$ (και K_r) μπορούμε να ανακτήσουμε τα $L_{r-1}||R_{r-1}$ μέσω των $R_{r-1} \leftarrow L_r$ και $L_{r-1} \oplus f(K\text{-}r, L_r) \oplus R_r$. Ακολουθώντας τους 16 γύρους, η

αντίστροφη της μετάθεσης IP, που επίσης απεικονίζεται στον πίνακα 2.2 εφαρμόζεται στην 64-bit έξοδο και το αποτέλεσμα αυτού είναι το κρυπτοκείμενο ως output.

Μια ακολουθία από Feistel rounds είναι ένα σύνηθες υψηλού επιπέδου σχέδιο για έναν block cipher. Για να εμβαθύνουμε χρειάζεται να δούμε πως λειτουργεί η συνάρτηση f.

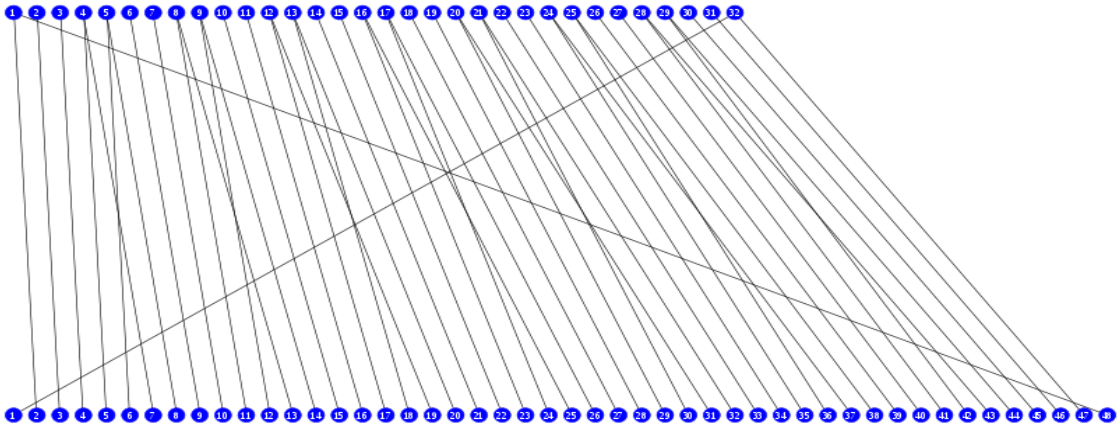
```
Function f(J,R)                                    //|J|=48  and  |R|=32
R←E(R)  ; R←R ⊕ J
Parse R as R1||R2||R3||R4||R5||R6||R7||R8          //|Ri| = 6 for 1≤i≤8
for i=1,...,8 do
        Ri←Si(Ri)                                  //Each S-box returns 4 bits
R ← R1||R2||R3||R4||R5||R6||R7||R8                 //|R| = 32bits
R←P(R)
return R
```

Σχήμα 2.3: Η συνάρτηση f του DES

Όπως φαίνεται στο σχήμα 2.3 λαμβάνει ένα 48-bit υποκλειδί και μία 32-bit είσοδο R για να επιστρέψει μια έξοδο 32-bit. Η 32-bit R αρχικά επεκτείνεται σε 48-bit μέσω της συνάρτησης E που περιγράφεται στον πίνακα 2.4. Αυτό σημαίνει ότι το bit 1 της εξόδου είναι το bit 32 της εισόδου, το bit 2 της εξόδου output είναι το bit 1 της εισόδου input, ..., το bit 48 του output είναι το bit 1 του input.

Να σημειώσουμε ότι η συνάρτηση E είναι αρκετά δομημένη. Στην πραγματικότητα, η ανταλλαγή των 1 και 32 (πάνω αριστερά και κάτω δεξιά) φαίνεται σχεδόν διαδοχική:

Η expansion function E . Το 32-bit block έχει επεκταθεί σε 48



E

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

P

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

Πίνακες 2.4: Πίνακες που περιγράφουν την επέκταση συνάρτησης E and την τελική μετάθεση P του DES f-function.

Στη συνέχεια το υποκλειδί J δέχεται την πράξη XOR με την έξοδο της συνάρτησης E ώστε να προκύψει ένα 48-bit αποτέλεσμα το οποίο συνεχίζει να υποδηλώνεται από την R. Αυτό χωρίζεται σε 8 τμήματα (blocks), μήκους το καθένα 6-bits. Στο block –i εφαρμόζουμε τη συνάρτηση $\mathbf{S}_i$ που ονομάζεται το S-box -i. Κάθε S-box είναι μια συνάρτηση που λαμβάνει 6 bits και επιστρέφει 4 bits.Το αποτέλεσμα είναι ότι το R των 48-bit συμπιέζεται σε 32 bits. Αυτά τα 32 bits μετατίθενται σύμφωνα με τη μετάθεση P όπως περιγράφηκε στον πίνακα 2.4 και το αποτέλεσμα της f function.

2.2.2.2 Τα S-boxes

Κάθε S-box περιγράφεται από έναν πίνακα όπως φαίνεται παρακάτω στους πίνακες 2.5.

S1 :

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

S2 :

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

S3 :

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

S4 :

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

S5 :

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

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

S6 :

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

S7 :

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

S8 :

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

Πίνακες 2.5: Τα S-boxes του DES

Αυτοί οι πίνακες διαβάζονται ως εξής :

Ο Si παίρνει μια είσοδο 6-bit. Γράφεται ως $b_1b_2b_3b_4b_5b_6$. Τα $b_3b_4b_5b_6$ διαβάζονται σαν ένας ακέραιος από 0 έως 15 κατονομάζοντας μια στήλη στον πίνακα που περιγράφει τον Si. Έστω ότι τα b_1b_2 κατονομάζουν τη γραμμή στον πίνακα που περιγράφει τον Si. Παίρνουμε το δεδομένο τη γραμμής b_1b_2, στη στήλη $b_3b_4b_5b_6$ του πίνακα Si κι έχουμε έναν ακέραιο από 0 έως 15. Το Si στην είσοδο $b_1b_2b_3b_4b_5b_6$ είναι ένα αλφαριθμητικό 4-bit που αντιστοιχίζεται στο δεδομένο αυτού του πίνακα.

Τα S-boxes είναι η καρδιά του αλγόριθμου και απαιτήθηκε πολλή προσπάθεια για να σχεδιαστούν έτσι ώστε να υπάρχει ασφάλεια εναντίον διαφόρων επιθέσεων.

2.2.2.3 Key Schedule (Πρόγραμμα Κλειδιού)

```
Algorithm KeySchedule(K)                                    //|K| = 56
K←PC-1(K)
Parse K as C0||D0
for r=1,...,16 do
        if r ∈ {1,2,9,16} then j←1 else j←2
        Cr←leftshiftj(Cr-1) ; Dr←leftshiftj(Dr-1)
        Kr←PC-2(Cr||Dr)
return(K1,...,K16)
```

Σχήμα 2.6 Ο αλγόριθμος Key Schedule του DES. Με το $leftshift_j$ εννοείται η συνάρτηση που περιστρέφει την είσοδο προς τα αριστερά κατά j θέσεις

Σε κάθε γύρο το υπο-κλειδί K_r σχηματίζεται παίρνοντας κάποια 48 bits του K. Ειδικά, μια μετάθεση η οποία καλείται PC-1 εφαρμόζεται πρώτα στο κλειδί των 56-bit με σκοπό να αποδώσει μια μετατεθειμένη εκδοχή αυτού. Αυτό μετά χωρίζεται σε δύο μισά των 28-bits και χαρακτηρίζονται $C_0||D_0$. Ο αλγόριθμος τώρα εκτελεί 16 γύρους. Στον γύρο r, παίρνει ως είσοδο τα $C_{r-1}||D_{r-1}$, υπολογίζει τα $C_r||D_r$, και εφαρμόζει τη συνάρτηση PC-2 η οποία εξάγει 48 bits από την ποσότητα των 56-bit. Αυτό είναι το υπό-κλειδί K_r για τον r γύρο. Ο υπολογισμός των $C_r||D_r$ είναι σχετικά απλός. Για το C_r, τα bits του C_{r-1} περιστρέφονται προς τα αριστερά κατά j θέσεις, και ομοίως για το D_r. Το j είναι είτε 1 είτε 2, ανάλογα το r.

2.2.2.4 Οι συναρτήσεις PC-1 και PC-2

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

PC-2

14	17	11	24	1	5
3	28	15	6	21	10
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

Πίνακες2.7: Πίνακες που περιγράφουν τις συναρτήσεις PC-1 και PC-2 που χρησιμοποιούνται από τον αλγόριθμο DES Key Schedule στο σχήμα 2.6

Ο πρώτος πίνακας διαβάζεται με λίγο περίεργο τρόπο. Περιέχει 56 ακεραίους, όλοι από το 1 έως το 64 εκτός των πολλαπλασίων του 8. Δεδομένου ενός αλφαριθμητικού 56-bit $K = K[1]...K[56]$ ως είσοδο, η αντίστοιχη συνάρτηση επιστρέφει το αλφαριθμητικό των 56-bits $L = L[1]...L[56]$ υπολογιζόμενο με τον εξής τρόπο. Έστω $1 \leq i \leq 56$, και έστω a το i- δεδομένο στον πίνακα. Γράφουμε $a = 8q + r$ όπου $1 \leq r \leq 7$. Έπειτα, $L[i] = K[a - q]$.

Για παράδειγμα ας καθορίσουμε το πρώτο bit, L[1], της εξόδου. Παίρνουμε το πρώτο δεδομένο στον πίνακα , το οποίο είναι το 57. Το διαιρούμε με 8 για να πάρουμε $57 = 8(7) + 1$. Συνεπώς, το L[1] ισούται με $K[57 - 7] = K[50]$, που σημαίνει ότι το πρώτο bit της εξόδου θα είναι το 50ο bit της εισόδου.

Ο δεύτερος πίνακας, ο PC-2 διαβάζεται με το συνηθισμένο τρόπο, λαμβάνοντας μια είσοδο 56-bit για να έχει μια έξοδο 48 bit : το bit 1 της εξόδου είναι το bit 14 της εισόδου; το bit 2 της εξόδου είναι το bit 17 της εισόδου,..., το bit 56 της εξόδου είναι το bit 32 της εισόδου.

2.2.3 Ταχύτητα του DES

Ένας από τους σχεδιαστικούς στόχους του DES ήταν ότι θα είχε γρήγορες υλοποιήσεις σχετικά με την τεχνολογία της εποχής του. Σε λογισμικό, με έναν αρκετά γρήγορο επεξεργαστή, ο DES χρειάζεται περίπου 80 κύκλους ανά byte. Αυτό είναι απογοητευτικά αργό αλλά και αναμενόμενο καθώς ο DES προοριζόταν για hardware και είχε σχεδιαστεί πριν από την εποχή που οι εφαρμογές λογισμικού θεωρήθηκαν εφικτές ή επιθυμητές.

2.2.4 Επιθέσεις ανάκτησης κλειδιού (Κρυπτανάλυση) σε block ciphers

Αναφερόμαστε σε έναν αλγόριθμο τμήματος $E:\{0,1\}^k * \{0,1\}^n \rightarrow \{0,1\}^n$ με μέγεθος κλειδιού k και μέγεθος τμήματος n. Υποθέτουμε ότι ο αντίπαλος (κρυπταναλυτής) γνωρίζει την περιγραφή της E και μπορεί να την υπολογίσει. Πιο ορθά μπορούμε να θεωρούμε την E ως τον DES. Από παλιά, η κρυπτανάλυση των αλγορίθμων τμήματος είναι επικεντρωμένη στην ανάκτηση του κλειδιού κρυπτογράφησης.

Εξαντλητική Αναζήτηση Κλειδιού

Η πιο προφανής στρατηγική επίθεσης είναι η εξαντλητική αναζήτηση κλειδιού. Ο αντίπαλος διατρέχει όλα τα πιθανά κλειδιά $K' \in \{0,1\}^k$ μέχρι να βρει ένα το οποίο να επεξηγεί τα ζεύγη εισόδου-εξόδου. Παρακάτω παρατίθεται η επίθεση με λεπτομέρειες, όπου q = 1, δηλαδή 1 ζεύγος εισόδου-εξόδου. Για i = 1,..., 2^k το T_i υποδεικνύει το i-αλφαριθμητικό που αποτελείται από k-bits :

EKS_E (M_1,C_1)

for i=1,...,2^k **do**

if $E(T_i,M_1) = C_1$ **then return** T_i

Η επίθεση αυτή επιστρέφει πάντα ένα κλειδί σύμφωνο με το δεδομένο παράδειγμα ζεύγους εισόδου-εξόδου (M_1,C_1). Αν είναι ή όχι το ζητούμενο κλειδί εξαρτάται από τον αλγόριθμο τμήματος, και συγκεκριμένα από το μήκος του κλειδιού και το μήκος του τμήματος (block). Η πιθανότητα αυτή η επίθεση να επιστρέψει το σωστό κλειδί αυξάνεται δοκιμάζοντας επίθεση εναντίον περισσότερων ζευγαριών εισόδου-εξόδου :

```
EKS_E ((M_1 ,C_1),..., (M_q ,C_q))
   for i = 1,...,2^k do
      if E(T_i ,M_1) = C_1 then
         if ( E(T_i ,M_2) = C_2  AND ... AND E(T_i ,M_q) = C_q ) then return T_i
```

Μια αρκετά μικρή τιμή του q, δηλαδή κάτι παραπάνω από k=n, είναι αρκετό ώστε αυτή η επίθεση να επιστρέψει το κλειδί «στόχο». Για τον DES, q = 2 είναι αρκετό.

Συνεπώς, κανένας αλγόριθμος τμήματος δεν είναι απόλυτα ασφαλής. Είναι πάντα πιθανό για έναν κρυπταναλυτή να ανακτήσει το κλειδί. Ωστόσο, κάθε καλός αλγόριθμος τμήματος σχεδιάζεται για να κάνει αυτό το έργο υπολογιστικά απαγορευτικό.

Όσον αφορά στο χρόνο που απαιτεί η εξαντλητική αναζήτηση κλειδιού για την ανάκτηση του κλειδιού ενός αλγορίθμου τμήματος, στη χειρότερη περίπτωση, χρειάζεται 2^k υπολογισμούς του αλγορίθμου. Αν όμως ο αντίπαλος είναι τυχερός και το κλειδί βρίσκεται στο πρώτο μισό του χώρου αναζήτησης τότε θα χρειαζόταν μόνο 2^{k-1} υπολογισμούς. Ένας μέσος όρος των υπολογισμών που απαιτούνται είναι :

$$\sum i*Pr[K = T_i] = \sum i/2^k = 1/2^k * \sum i = 1/2^k * 2^k(2^k+1)/2 = (2^k+1)/2 \approx 2^{k-1}$$

Συνεπώς για να γίνει η εξαντλητική μέθοδος αναζήτησης κλειδιού υπολογιστικά απαγορευτική πρέπει το μήκος του κλειδιού k του κρυπταλγόριθμου να είναι αρκετά μεγάλο.

Συγκεκριμένα για τον DES, υπάρχει ένα VLSI chip με το οποίο μπορεί να υπολογιστεί με ρυθμό 1.6 Gbits/sec. Εφόσον ένα αρχικό κείμενο είναι 64 bits, το chip μας επιτρέπει να κάνουμε $(1.6*10^9)/64 = 2.5*10^7$ υπολογισμούς DES ανά δευτερόλεπτο. Για να εκτελέσουμε 2^{55} υπολογισμούς (k = 56) χρειαζόμαστε $2^{55}/(2.5*10^7) \approx 1.44*10^9$ δευτερόλεπτα, δηλαδή περίπου 45.7 χρόνια. Αυτό είναι ξεκάθαρα απαγορευτικό. Με χρήση της ιδιότητας της συμπληρωματικότητας των κλειδιών του DES μπορεί κάποιος να μειώσει αυτόν τον χρόνο σε 22.8 χρόνια που και πάλι θεωρείται απαγορευτικός. Όμως θα ήταν βεβιασμένο να θεωρήσουμε ότι ο DES είναι ασφαλής απέναντι στην επίθεση εξαντλητικής αναζήτησης.

Η επίθεση εξαντλητικής αναζήτησης είναι μια μέθοδος γενική, που χρησιμοποιείται ενάντια όλων των αλγορίθμων τμήματος υπολογίζοντας τον αλγόριθμο και όχι αναλύοντάς τον εκμεταλλευόμενη τις αδυναμίες στη δομή του. Τέτοιες επιθέσεις εναντίον του DES ξεκίνησαν να ανακαλύπτονται το 1990.

- Η Διαφορική Κρυπτανάλυση είναι ικανή να ανακαλύψει το κλειδί του DES χρησιμοποιώντας περίπου 2^{47} παραδείγματα εισόδου-εξόδου ($q = 2^{47}$) σε μια επίθεση με επιλεγμένο αρχικό κείμενο (chosen-plaintext)
- Η Γραμμική Κρυπτανάλυση βελτίωσε την Διαφορική με δύο τρόπους. Μείωσε τα ζεύγη εισόδου-εξόδου που χρειάζονται σε 2^{44} και χρησιμοποιεί μόνο την επίθεση με γνωστό αρχικό κείμενο (known-plaintext)

Παρόλο που αυτές οι επιθέσεις εκμεταλλεύτηκαν τις αδυναμίες στη δομή του DES, πρακτικά τον επηρέασαν πολύ λίγο για δύο λόγους. Πρώτον, διότι κανονικά ήταν αδύνατο για τον αντίπαλο να αποκτήσει 2^{44} παραδείγματα εισόδου-εξόδου και δεύτερον οι απαιτήσεις αποθήκευσης θα ήταν τεράστιες. Μόνο ένα ζεύγος εισόδου-εξόδου, αποτελούμενο από 64-bit απλού κειμένου και 64-bit κρυπτοκειμένου χρειάζεται 16 bytes χώρου αποθήκευσης. Τα 2^{44} αντίστοιχα ζεύγη απαιτούν $16*2^{44} = 2.81*10^{14}$ bits, ή περίπου 281 terabytes χώρο! Η Γραμμική και η Διαφορική Κρυπτανάλυση, παρόλα αυτά, ήταν πολύ καταστροφικές όταν εφαρμόστηκαν σε άλλους αλγορίθμους.

Συνεπώς, η καλύτερη δυνατή επίθεση εναντίον του DES είναι η Εξαντλητική Αναζήτηση Κλειδιού όταν όμως –κάτι που δεν αναφέραμε παραπάνω- εκτελείται παράλληλα. Το 1993 ο Weiner υποστήριξε ότι κανένας δε θα μπορούσε να σχεδιάσει μια μηχανή η οποία να κάνει την Εξαντλητική Αναζήτηση Κλειδιού του DES σε 3.5 ώρες και να κοστίζει 1 εκατομμύριο δολάρια . Η μηχανή του είχε 57,000 chips, κάθε ένα από τα οποία εκτελούσε πολλούς υπολογισμούς DES. Πιο πρόσφατα, ο Electronic Frontier Foundation δημιούργησε μια μηχανή Εξαντλητικής Αναζήτησης Κλειδιού του DES , με κόστος 250.000 δολάρια. Βρίσκει το κλειδί σε 56 ώρες, ή περίπου 2.5 ημέρες κατά μέσο όρο.

2.3 Επαναλαμβανόμενος DES και DESX

Η ανάδειξη των όσων συζητήσαμε παραπάνω για τις μηχανές αναζήτησης κλειδιού οδήγησαν στην άποψη ότι στην πράξη ο DES θεωρείται σπασμένος. Αδυναμία του ήταν το μήκος του κλειδιού του (56), όχι αρκετά δυνατό για να αντισταθεί στην Εξαντλητική Αναζήτηση Κλειδιού. Αναζητήθηκαν οικονομικότεροι τρόποι για την

ενίσχυση του DES, μετατρέποντάς τον, με απλό τρόπο σε ένα κρυπτογράφημα με μεγαλύτερο μήκος κλειδιού. Ένα παράδειγμα παρακάτω είναι η επανάληψη αυτού.

2.3.1 Double-DES

Έστω K_1,K_2 τα κλειδιά των 56-bit του DES και έστω M το αρχικό κείμενο των 64-bit. Τότε $2DES(K_1||K_2,M) = DES(K_2 , DES(K_1 , M))$

Πρόκειται για έναν αλγόριθμο τμήματος 2DES: $\{0,1\}^{112} * \{0,1\}^{64} \rightarrow \{0,1\}^{64}$ τον οποίο αποκαλούμεl Double-DES. Έχει ένα κλειδί 112-bit, το οποίο φαίνεται να αποτελείται από δύο κλειδιά DES 56-bits. Ο αντίστροφος αλγόριθμος για κάθε 64-bit κρυπτοκείμενο C - όπως απαιτεί κάθε αλγόριθμος τμήματος που είναι αντιστρέψιμος- είναι

$2DES^{-1}(K_1||K_2,C) = DES^{-1}(K_1 , DES^{-1}(K_2,C))$

Το μήκος του κλειδιού 112 είναι αρκετά μεγάλο ώστε να υπάρχει μικρός κίνδυνος 2DES να υποκύψει στην Εξαντλητική μέθοδο αναζήτησης κλειδιού, ακόμα κι όταν εκμεταλλεύεται τη δυνατότητα της παράλληλης αναζήτησης. Επίσης, ο 2DES φαίνεται ασφαλής ακόμα και απέναντι στην διαφορική και γραμμική κρυπτανάλυση, αφού η επανάληψη αυξάνει αποτελεσματικά τον αριθμό των γύρων Feistel.

Όμως, παρόλο που ο 2DES έχει μήκος κλειδιού 112, φαίνεται ότι μπορεί να κρυπταναλυθεί χρησιμοποιώντας περίπου 2^{57} DES and DES^{-1} υπολογισμούς με μια επίθεση που λέγεται meet-in-the-middle, ως εξής :

Έστω τα $K_1||K_2$ υποδηλώνουν το κλειδί-στόχο και έστω $C_1 = 2DES(K_1||K_2,M_1)$. Ο επιτιθέμενος, δεδομένων των M_1,C_1, προσπαθεί να βρει τα $K_1||K_2$. Παρατηρούμε ότι

$C_1 = DES(K_2, DES(K_1,M_1)) \Rightarrow DES^{-1}(K_2,C_1) = DES(K_1,M_1)$

Αυτό οδηγεί στην παρακάτω επίθεση. Παρακάτω για $i = 1,\ldots, 2^{56}$ θέτουμε T_i να υποδηλώνει το i-αλφαριθμητικό των 56-bit:

```
MinM_2DES(M_1 , C_1)
    for i = 1,..., 2^56 do L[i] ← DES( T_i , M_1)
    for j = 1,..., 2^56 do R[j] ← DES^-1( T_j , C_1)
    S ← { ( i , j ) : L[i] = R[j] }
Pick some ( l , r) ∈ S and return T_l || T_r
```

Για οποιαδήποτε $(i , j) \in S$ έχουμε

$DES(T_i , M_1) = L[i] = R[j] = DES^{-1}(T_j , C_1)$

Και ως συνέπεια $DES(T_j , DES (T_i , M_1)) = C_1$.

Άρα το κλειδί $T_i || T_j$ είναι σύμφωνο με το ζεύγος εισόδου-εξόδου (M_1 , C_1). Έτσι,

$\{ T_l ||T_r : (l , r) \in S \} = Cons_E((M_1 , C_1))$:

Η επίθεση, εισάγει κάποια ζεύγη (l , r) από το S και δίνει $T_l || T_r$, δηλαδή επιστρέφει κλειδί σύμφωνο με το ζεύγος input-output (M_1 , C_1).

Το σύνολο S είναι πιθανό να είναι κάπως μεγάλο σε μέγεθος, περίπου $2^{56+56}/2^{64} = 2^{48}$, ώστε η επίθεση να μην είναι πιθανό να επιστρέψει το ίδιο το κλειδί. Όμως, χρησιμοποιώντας μερικά ακόμα ζεύγη input-output, είναι εύκολο να περιοριστούν οι επιλογές στο σύνολο S μέχρις ότου παραμείνει μόνο το κλειδί-στόχος. Η επίθεση κάνει $2^{56} + 2^{56} = 2^{57}$ DES ή DES^{-1} υπολογισμούς. Το βήμα που αφορά το σύνολο S μπορεί να υλοποιηθεί σε γραμμικό χρόνο για το μέγεθος των πινάκων που συμμετέχουν. Έτσι, ο χρόνος εκτέλεσης εξαρτάται από τους DES και DES^{-1} υπολογισμούς. Η meet-in-the-middle επίθεση δείχνει ότι ο 2DES είναι αρκετά μακριά από το ιδανικό αλγόριθμου για τον οποίο η καλύτερη επίθεση είναι αυτή της Εξαντλητικής Αναζήτησης Κλειδιού. Ωστόσο, αυτή η επίθεση δεν είναι ιδιαίτερα πρακτική ακόμα και για ειδικά για την εφαρμογή της μηχανήματα. Οι μηχανές θα μπορούσαν να κάνουν τους DES και DES^{-1} υπολογισμούς γρήγορα παράλληλα, αλλά για να σχηματίσει το σύνολο S η επίθεση χρειάζεται να αποθηκεύσει τους πίνακες L και R, κάθε ένας από τους οποίους έχει 2^{56} δεδομένα, και κάθε ένα από αυτά τα δεδομένα αποτελείται από 64 bits. Το ποσό του χώρου αποθήκευσης που απαιτείται είναι $8 * 2^{57} \approx 1.15*10^{18}$ bytes, ή περίπου $1.15 *10^6$ terabytes, που είναι τόσο πολύ που καθιστά την εφαρμογή της επίθεσης μη πρακτική. Υπάρχουν κάποιες τεχνικές που τροποποιούν την επίθεση με σκοπό να μειωθεί το κόστος αποθήκευσης εις βάρος ορισμένου επιπλέον χρόνου, αλλά και πάλι η επίθεση δεν είναι πρακτική. Δεδομένου ότι ένα 112-bit 2DES κλειδί μπορεί να βρεθεί με χρήση 2^{57} DES ή DES^{-1} υπολογισμών, λέγεται μερικές φορές ότι το 57 είναι ένα αποτελεσματικό μήκος κλειδιού για τον 2DES.

2.3.2 Triple-DES

Ο triple-DES κρυπταλγόριθμος έχει τρεις επαναλήψεις του DES ή του DES^{-1}. Η μεταβλητή τριών κλειδιών ορίζεται από

$3DES3(K_1||K_2||K_3,M) = DES(K_3,DES^{-1}(K_2, DES(K_1,M))$

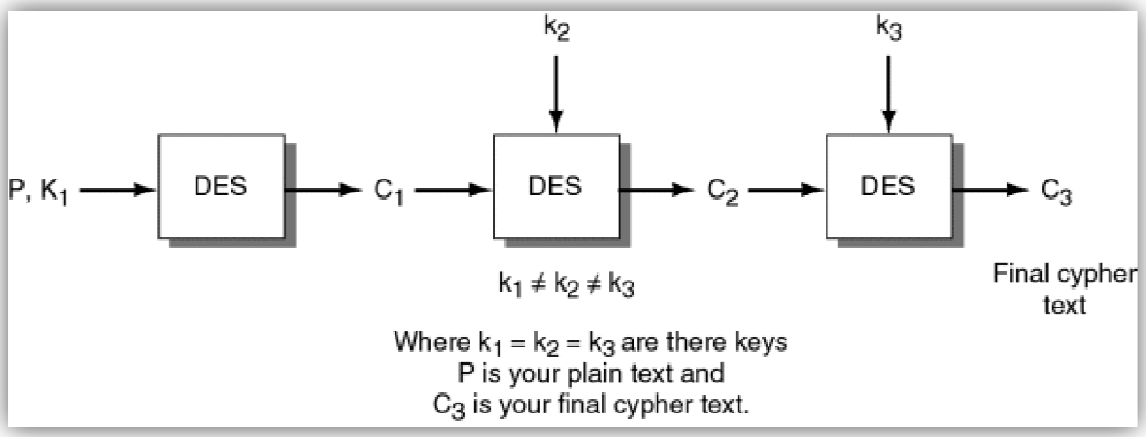
έτσι ώστε 3DES3: $\{0,1\}^{168} * \{0,1\}^{64} \rightarrow \{0,1\}^{64}$

Η μεταβλητή των δύο κλειδιών ορίζεται από

$3DES2(K_1||K_2,M) = DES(K_2,DES^{-1}(K_1, DES(K_2,M))$

έτσι ώστε 3DES2: $\{0,1\}^{112} * \{0,1\}^{64} \rightarrow \{0,1\}^{64}$

Αυτές οι συναρτήσεις είναι αντιστρέψιμες όπως πρέπει για να πληρούν τις προϋποθέσεις ενός αλγορίθμου τμήματος. Ο όρος «triple» αναφέρεται στις τρεις εφαρμογές των DES και DES^{-1}.



Όπως και με τον 2DES, το μήκος του κλειδιού εμφανίζεται αρκετά μεγάλο ώστε να καθιστά την μέθοδο εξαντλητικής αναζήτησης απαγορευτική, και επιπλέον η διαφορική και η γραμμική κρυπτανάλυση δεν είναι ιδιαίτερα αποτελεσματικές διότι οι επαναλήψεις αυξάνουν το πλήθος των γύρων Feistel.

Ο 3DES3 αποτελεί ζήτημα για την επίθεση « meet-in-the-middle» που βρίσκει το κλειδί των 168-bit χρησιμοποιώντας περίπου 2^{112} υπολογισμούς DES και DES^{-1}. Δε φαίνεται να υπάρχει τέτοια επίθεση στον 3DES2 , ωστόσο, το μήκος κλειδιού 112 θεωρείται ένα αποτελεσματικό μήκος κλειδιού.

Ο 2DES, παρόλο που έχει το ίδιο αποτελεσματικό κλειδί με τον 3DES2 και μοιάζει να προσφέρει –αν όχι την ίδια- ικανοποιητική ασφάλεια, δεν είναι το ίδιο δημοφιλής στην πράξη.

2.3.3 DESX

Παρόλο που οι 2DES, 3DES3 και 3DES2 δείχνουν να παρέχουν ικανοποιητική ασφάλεια, είναι αργοί. Ο πρώτος είναι διπλάσια πιο αργός από τον DES και οι άλλοι δύο είναι τρεις φορές πιο αργοί.

Υπάρχει ένας σχεδιασμός που είναι στη βάση του ίδιος με τον DES αλλά με μεγαλύτερου μήκους κλειδί και χωρίς πολύ μεγαλύτερο κόστος. Αυτός είναι ο εξής :

Έστω K είναι το κλειδί DES των 56-bit, και K_1,K_2 αλφαριθμητικά με 64-bits, και M το απλό κείμενο των 64-bit. Τότε

$DESX(K||K_1||K_2,M) = K_2 \oplus DES(K, K_1 \oplus M)$

Πρόκειται για τον αλγόριθμο τμήματος DESX : $\{0,1\}^{184} * \{0,1\}^{64} \rightarrow \{0,1\}^{64}$. Έχει ένα κλειδί 184-bit, το οποίο αποτελείται από ένα κλειδί DES 56-bit μαζί με δύο βοηθητικά κλειδιά που το κάθε ένα είναι 64 bits. Φυσικά είναι αντιστρέψιμος αλγόριθμος , όπως προβλέπεται.

$DESX^{-1}(K||K_1||K_2,C) = K_1 \oplus DES^{-1}(K, K_2 \oplus C)$

Το μήκος του κλειδιού στα 184 είναι αδιαμφισβήτητα αρκετό για να αποκλείσει την επίθεση εξαντλητικής αναζήτησης.

Ο DESX δεν είναι περισσότερο ασφαλής από τον DES ενάντια στη διαφορική και γραμμική κρυπτανάλυση, αλλά όπως ήδη είδαμε αυτές δεν είναι αρκετά πρακτικές επιθέσεις.

Υπάρχει η «meet-in-the-middle» επίθεση στον DESX. Βρίσκει ένα DESX κλειδί 184-bit χρησιμοποιώντας 2^{120} DES και DES^{-1} υπολογισμούς. Άρα το αποτελεσματικό μήκος κλειδιού για τον DESX φαίνεται να είναι το 120. Ο DESX είναι λιγότερο ασφαλής από τον Double ή τον Triple DES διότι τα τελευταία είναι πιο ανθεκτικά από τον DES ενάντια στη διαφορική και τη γραμμική κρυπτανάλυση ενώ ο DESX είναι μόνο όσο καλός είναι ο DES. Παρόλα αυτά αυτό είναι αρκετά καλό, καθώς όπως είδαμε στην πράξη η αδυναμία του DES δεν ήταν αυτές οι επιθέσεις αλλά μάλλον το μικρό μήκος κλειδιού που οδηγεί στην επιτυχή επίθεση εξαντλητικής αναζήτησης. Ο DESX το διορθώνει αυτό και με μικρό κόστος.

Εν ολίγοις, ο DESX είναι δημοφιλής καθώς είναι πολύ οικονομικότερος από τον Double ή τον Triple DES ενώ παρέχει επαρκή ασφάλεια.

ΚΕΦΑΛΑΙΟ 3: ΔΙΠΛΩΜΑΤΑ ΕΥΡΕΣΙΤΕΧΝΙΑΣ (ΠΑΤΕΝΤΕΣ) ΚΑΙ ΠΡΟΤΥΠΑ ΣΕ ΚΡΥΠΤΟΓΡΑΦΙΚΕΣ ΤΕΧΝΙΚΕΣ

3.1 Εισαγωγή

Έχει εκδοθεί ένας τεράστιος αριθμός διπλωμάτων ευρεσιτεχνίας (πατέντες), με ευρεία χρήση και σημασία στον τομέα της κρυπτογραφίας. Εμείς θα επικεντρωθούμε σε ένα υποσύνολο αυτών, δίνοντας έμφαση στις πατέντες βιομηχανικού ενδιαφέροντος, που αφορούν θεμελιώδεις τεχνικές, ειδικούς αλγορίθμους και πρωτόκολλα καθώς και σε αυτές με ιστορική σημασία.

Τα διπλώματα ευρεσιτεχνίας, στην καλύτερη περίπτωση, καθιστούν διαθέσιμες στο κοινό λεπτομέρειες σημαντικών νέων διαδικασιών και αποτελεσματικών τεχνικών με σκοπό την αύξηση της ευαισθητοποίησης και την προώθηση της χρήσης. Από την άλλη πλευρά, μερικές φορές περιορίζουν ή καταπνίγουν τη χρήση αυτών των τεχνικών λόγω των αυστηρών απαιτήσεων αδειοδότησης.

ΛΗΞΗ ΤΩΝ ΔΙΠΛΩΜΑΤΩΝ ΕΥΡΕΣΙΤΕΧΝΙΑΣ

Στις Η.Π.Α., τα διπλώματα ευρεσιτεχνίας ισχύουν για 17 χρόνια από την ημερομηνία έκδοσής τους, ή 20 χρόνια από την ημερομηνία που κατατέθηκε η αίτηση. Για αιτήσεις που κατατέθηκαν πριν από την 8η Ιουνίου του 1995 και δεν είχαν λήξει ως εκείνο το σημείο ισχύει το μεγαλύτερο διάστημα. Ο κανόνας των 20 χρόνων ισχύει για αιτήσεις που κατατέθηκαν πριν από αυτήν την ημερομηνία.

ΠΡΟΤΕΡΑΙΟΤΗΤΑ ΔΕΔΟΜΕΝΩΝ

Σε πολλές χώρες απαιτείται η κατάθεση της πατέντας πριν από οποιαδήποτε δημοσιοποίηση της εφεύρεσης. Στις Η.Π.Α., η κατάθεση πρέπει να γίνει ένα χρόνο πριν την αποκάλυψη. Πολλές χώρες είναι συμβαλλόμενα μέλη σε μια συμφωνία που αναγνωρίζει την προτεραιότητα δεδομένων των διπλωμάτων ευρεσιτεχνίας. Αν μια πατέντα κατατεθεί σε μια από αυτές τις χώρες και εντός ενός χρόνου κατατεθεί σε κάποια άλλη από αυτές τις χώρες, χρησιμοποιείται η πρώτη ημερομηνία προτεραιότητας για τη δεύτερη καταχώρηση.

3.2 Πέντε Βασικά Διπλώματα Ευρεσιτεχνίας

Παρακάτω θα παρουσιάσουμε 5 βασικές πατέντες, συμπεριλαμβανομένου του DES καθώς και κάποιων διπλωμάτων ευρεσιτεχνίας κρυπτογραφίας δημοσίου κλειδιού. Η παρουσίαση θα γίνει με χρονολογική σειρά. Επειδή οι περισσότερες πατέντες έχουν αρχειοθετηθεί στις Η.Π.Α., δίνονται οι αριθμοί Αμερικάνικων πατεντών καθώς και σχετικές λεπτομέρειες.

Εφευρέτες	**Αριθμός Πατέντας**	**Ημερομηνία Έκδοσης**	**Αναφορά**	**ΘΕΜΑ**
Ehrsam et al.	3,962,539	Jun. 08 1976	[363]	DES
Hellman-Diffie-Merkle	4,200,770	Apr. 29 1980	[551]	Diffie-Hellman agreement
Hellman-Merkle	4,218,582	Aug. 19 1980	[553]	public-key systems
Merkle	4,309,569	Jan. 05 1982	[848]	tree authentication
Rivest-Shamir-Adleman	4,405,829	Sep. 20 1983	[1059]	RSA system

3.2.1 DES block cipher

Η πατέντα του Ehrsam et al. (με αριθμό 3,962,539) καλύπτει τον αλγόριθμο που αργότερα έγινε γνωστός ως DES. Καταχωρήθηκε στις 24 Φεβρουαρίου του 1975 και σήμερα έχει λήξει. Η πατέντα ανατέθηκε στην International Business Machines Corporation (IBM). Σε σημείο του πλαισίου σχολιάζονται σύντομα το 1974 οι κρυπτογραφικές πατέντες του Feistel (με αριθμό 3,798,359) και του Smith (3,796,830) οι οποίες είχαν κατατεθεί στις 30 Ιουνίου του 1971 και στις 2 Νοεμβρίου του 1971 αντίστοιχα. Σημειώνεται ότι ενώ η πατέντα του Feistel γνωστοποιεί ένα προϊόν κρυπτογραφίας το οποίο συνδυάζει γραμμικούς και μη γραμμικούς μετασχηματισμούς που εξαρτώνται από το κλειδί, παραλείπει να αποκαλύψει συγκεκριμένες λεπτομέρειες όπως είναι το πώς ακριβώς χρησιμοποιούνται τα bits του κλειδιού, όσον αφορά τη μη γραμμική μετατροπή στα S-boxes, και μια συγκεκριμένη μετάθεση. Επίσης, σχολιάζεται επιπλέον ο κρυπταλγόριθμος στην πατέντα του Smith , χαρακτηρίζοντας ως μειονέκτημα τον εκ φύσεως σειριακό χαρακτήρα του και το γεγονός ότι και αυτός αλλά και αυτός του Feistel έχουν μόνο δύο τύπους κουτιών αντικατάστασης. Έτσι, δημιουργήθηκε προφανής ανάγκη για νέο κρυπταλγόριθμο.
Η πατέντα περιέχει δέκα (10) ισχυρισμούς.

3.2.2 Συμφωνία Κλειδιού Diffie-Hellman

Πρόκειται για την πρώτη πατέντα δημοσίου κλειδιού και εκδόθηκε στις 29 Απριλίου του 1980. Ήταν η Hellman-Diffie-Merkle πατέντα (με αριθμό 4,200,770). Καταχωρήθηκε στις 6 Σεπτεμβρίου του 1977 και ανατέθηκε στο Πανεπιστήμιο του Στάνφορντ (Στάνφορντ, Καλιφόρνια). Γενικά αναφέρεται ως " The *Diffie-Hellman patent"* , καθώς καλύπτει τη συμφωνία κλειδιού Diffie-Hellman.
Υπάρχουν δύο σημαντικά αντικείμενα σε αυτή την πατέντα. Το πρώτο, είναι μια μέθοδος ασφαλούς επικοινωνίας μέσω ενός ανασφαλούς καναλιού χωρίς να έχει μοιραστεί το κλειδί εκ των προτέρων. Αυτό γίνεται με τη συμφωνία κλειδιού Diffie-Hellman. Το δεύτερο αντικείμενο, είναι μια μέθοδος που επιτρέπει την πιστοποίηση μιας ταυτότητας σε ανασφαλή κανάλια. Αυτό μπορεί να γίνει χρησιμοποιώντας μακροπρόθεσμα, αυθεντικά, δημόσια κλειδιά Diffie-Hellman ασφαλισμένα σε ένα δημόσιο ευρετήριο, τα οποία με την εξαγωγή και χρήση των μυστικών κλειδιών Diffie-Hellman που προκύπτουν, να αποδεικνύουν την πιστοποίηση.
Η πατέντα περιέχει οκτώ (8) ισχυρισμούς συμπεριλαμβανομένης και της ιδέας της καθιέρωσης ενός κλειδιού για κάθε κύκλο λειτουργίας μέσω της διανομής δημοσίου κλειδιού. Για παράδειγμα, όπως οι ανταλλαγές μηνυμάτων σε δύο διόδους της συμφωνίας κλειδιού Diffie-Hellman.

3.2.3 Merkle-Hellman Knapsacks και Συστήματα Δημοσίου Κλειδιού

Το δίπλωμα ευρεσιτεχνίας Hellman-Merkle (με αριθμό 4,218,582) κατατέθηκε στις 6 Οκτωβρίου του 1977 και ανατέθηκε στο Board of Trustees του Πανεπιστημίου Leland Stanford Junior (Στάφορντ, Καλιφόρνια). Καλύπτει κρυπτοσυστήματα δημοσίου κλειδιού βασισμένα στο πρόβλημα αθροίσματος υποσυνόλου (subset-sum problem), καθώς επίσης και διάφορους ισχυρισμούς στην κρυπτογράφηση δημοσίου κλειδιού και στις υπογραφές δημοσίου κλειδιού.
Τα αντικείμενα αυτής της εφεύρεσης είναι

- να επιτρέπονται ιδιωτικές συνομιλίες διαμέσου καναλιών τα οποία υπόκεινται σε παρακολούθηση από ωτακουστές
- να επιτρέπεται η πιστοποίηση της ταυτότητας ενός παραλήπτη μέσω της ικανότητας του να χρησιμοποιεί ένα κλειδί που μόνο αυτός θα μπορούσε να υπολογίσει
- να επιτρέπεται η πιστοποίηση της προέλευσης των δεδομένων, χωρίς την απειλή της διαφωνίας (π.χ. μέσω τεχνικών δημοσίου κλειδιού αντί για ένα κοινό μυστικό κλειδί)

Υπάρχουν δεκαεπτά (17) ισχυρισμοί σε αυτήν την πατέντα. Οι ισχυρισμοί 1-6, σε γενικές γραμμές εφαρμόζονται σε συστήματα δημοσίου κλειδιού, και οι ισχυρισμοί 7-17 εστιάζονται περισσότερο στα συστήματα «knapsack». Οι γενικοί ισχυρισμοί απευθύνονται σε πτυχές των μεθόδων που χρησιμοποιούν ζευγάρια δημόσιου-μυστικού κλειδιού για κρυπτογράφηση δημοσίου κλειδιού, για υπογραφές δημοσίου κλειδιού, και για τη χρήση κρυπτογράφησης δημοσίου κλειδιού με σκοπό να παρέχεται πιστοποίηση του παραλήπτη μέσω της μετάδοσης μιας αναπαράστασης του κρυπτογραφημένου μηνύματος πίσω στον αποστολέα.

3.2.4 Δέντρο Πιστοποίησης Μεθόδων παραμέτρων επικύρωσης (Tree authentication method of validating parameters)

Η πατέντα της Merkle του 1982 (με αριθμό 4,309,569) καλύπτει τα δέντρα πιστοποίησης. Καταχωρήθηκε στις 5 Σεπτεμβρίου του 1979, και ανατέθηκε στο Board of Trustees του Πανεπιστημίου του Leland Stanford Junior (Στάνφορντ, Καλιφόρνια). Το κύριο κίνητρο που παρατίθεται ήταν η εξάλειψη των μεγάλων απαιτήσεων χώρου αποθήκευσης που ήταν συνυφασμένες με προηγούμενα συστήματα υπογραφής, παρόλο που η ιδέα είχε ευρύτερη εφαρμογή. Οι βασικές ιδέες είναι η χρήση ενός δυαδικού δέντρου και μιας one-way συνάρτησης κατακερματισμού για να επιτρέψει την πιστοποίηση των τιμών των φύλλων Yi που σχετίζονται με κάθε χρήστη i. Τροποποιήσεις που αναφέρονται περιλαμβάνουν :

- χρήση ενός τριαδικού ή κ-αδικού δέντρου στη θέση του δυαδικού δέντρου
- χρήση του δέντρου όχι μόνο για δημόσιες τιμές one-time υπογραφών, αλλά και για την πιστοποίηση αυθαίρετων τιμών για εναλλακτικούς σκοπούς
- χρήση ενός διακριτού δέντρου πιστοποίησης για κάθε χρήστη i, η ρίζα Ri του οποίου θα αντικαθιστά τα παραπάνω Yi , ως εκ τούτου επιτρέποντας πιστοποίηση όλων των τιμών στο i-δέντρο, και όχι ενός μόνο Yi.

Πρόκειται για την επιτομή της περιεκτικότητας, καθώς αυτή η πατέντα περιέχει ένα μόνο σχήμα και μόλις πάνω από δύο σελίδες κειμένου, συμπεριλαμβανομένων και τεσσάρων (4) ισχυρισμών.

3.2.5 RSA κρυπτογράφηση δημοσίου κλειδιού και συστήματα υπογραφής (signature system)

Το δίπλωμα ευρεσιτεχνίας των Rivest-Shamir-Adleman (με αριθμό 4,405,829) καταχωρήθηκε στις 14 Δεκεμβρίου του 1977, και ανατέθηκε στο Massachusetts Institute of Technology (MIT). Καλύπτει την κρυπτογραφία δημοσίου κλειδιού RSA και τη μέθοδο ψηφιακής υπογραφής. Επίσης, περιλαμβάνονται γενικεύσεις όπως :

- χρήση ενός συντελεστή n ως προϊόν τριών ή περισσότερων πρώτων αριθμών (όχι απαραίτητα διακριτών)
- χρήση ενός δημοσίου κλειδιού κρυπτογράφησης e για την κρυπτογράφηση ενός κειμένου M σε κρυπτοκείμενο C μέσω της αξιολόγησης ενός πολυωνύμου $\Sigma^{t}_{i=0}\ a_i M^e \bmod n$ όπου e και a_i , $0 \leq i \leq t$ είναι ακέραιοι, και
- ανάκτηση του απλού κειμένου M χρησιμοποιώντας συμβατικές τεχνικές εύρεσης ρίζας, επιλέγοντας ποια από όλες τις ρίζες είναι στη σωστή αποκωδικοποιημένη έκδοση

Άλλες παραλλαγές που αναφέρονται περιλαμβάνουν τη χρήση κρυπτογράφησης RSA σε λειτουργία CFB ή σαν μια γεννήτρια ψευδοτυχαίων αριθμών για την παραγωγή κλειδιών υπογράφοντας μια συμπιεσμένη έκδοση του μηνύματος αντί για το ίδιο το μήνυμα και χρησιμοποιώντας κρυπτογραφία RSA για μεταφορά του κλειδιού, το κλειδί με αυτόν τον τρόπο μεταφέρεται για να χρησιμοποιηθεί σε μια άλλη μέθοδο κρυπτογράφησης.

Αυτή η πατέντα έχει τη διάκριση στον τομέα των ισχυρισμών με σαράντα (40) ισχυρισμούς , οι οποίοι καλύπτουν μεγαλύτερο μέρος από την ίδια την πατέντα.

3.3 Δέκα Εξέχοντα Διπλώματα Ευρεσιτεχνίας

Παρακάτω θα αναφερθούν δέκα εξέχοντα διπλώματα ευρεσιτεχνίας των Η.Π.Α.

Εφευρέτες	Αριθμός Πατέντας	Ημερομηνία Έκδοσης	Αναφορά	ΘΕΜΑ
Okamoto et al.	4,625,076	Nov. 25 1986	[952]	ESIGN signatures
Shamir-Fiat	4,748,668	May 31 1988	[1118]	Fiat-Shamir identification
Matyas et al.	4,850,017	Jul. 18 1989	[806]	Control vectors
Shimizu-Miyaguchi	4,850,019	Jul. 18 1989	[1125]	FEAL cipher
Brachtl et al.	4,908,861	Mar. 13 1990	[184]	MDC-2, MDC-4 hashing
Schnorr	4,995,082	Feb. 19 1991	[1095]	Schnorr signatures
Guillou-Quisquater	5,140,634	Aug. 18 1992	[523]	GQ identification
Massey-Lai	5,214,703	May 25 1993	[791]	IDEA cipher
Kravitz	5,231,668	Jul. 27 1993	[711]	DSA signatures
Micali	5,276,737	Jan. 04 1994	[861,862]	“fair” key escrow

3.3.1 ESIGN υπογραφές

Το δίπλωμα ευρεσιτεχνίας των Okamoto, Miyaguchi, Shiraishi, Kawaoka (με αριθμό 4.625.076) καλύπτει το πρωτότυπο ESIGN σύστημα υπογραφών. Το δίπλωμα αυτό κατατέθηκε στις 11 Μαρτίου 1985 και ανατέθηκε στην Nippon Telegraph και την Telephone Corporation (Tokyo), με προτεραιότητα τα δεδομένα που αναφέρονται ως 19 Μαρτίου 1984 (Ιαπωνικό γραφείο διπλωμάτων ευρεσιτεχνίας). Ο στόχος είναι η παροχή ενός ταχύτερου συστήματος υπογραφών από το RSA. Αυτό το δίπλωμα περιέχει εικοσιπέντε (25) ισχυρισμούς.

3.3.2 Ταυτοποίηση Fiat – Shamir και υπογραφές

Η ευρεσιτεχνία των Fiat και Shamir (με αριθμό 4.748.668) κατατέθηκε στις 9 Ιουλίου 1986 και ανατέθηκε στο Yeda Research and Development Co. Ltd. (Israel). Για ταυτοποίηση, οι εφευρέτες προτείνουν έναν τυπικό αριθμό t γύρων, από 1 μέχρι 4 και ως παράμετρο τις επιλογές συμπεριλαμβανομένου του k = 5 (μυστικά), t = 4 για μία στις 2^{-20} πιθανότητα για πλαστογραφία και k = 6, t = 5 για μία στις 2^{-30}. Ένα

εύρος από παραμέτρους k,t για kt = 72 είναι σε μορφή πινάκων για το αντίστοιχο σύστημα υπογραφών, που εμφανίζει αλλαγές μεταξύ αποθήκευσης κλειδιών, μεγέθους υπογραφών και απαιτήσεων πραγματικού χρόνου για την περαίωση των ενεργειών αυτών. Σημειώνεται χαρακτηριστικά ότι σε σχέση με την προηγούμενη ευρεσιτεχνία η συγκεκριμένη είναι σε θέση να διοχετεύει με υπολογισμούς, και να αλλάζει το επίπεδο ασφαλείας εφόσον το κλειδί είναι επιλεγμένο (αλλάζοντας την t). Γενικεύσεις που σημειώθηκαν περιλάμβαναν την αντικατάσταση των τετραγωνικών ριζών με κυβικές ή μεγαλύτερες ρίζες Αυτό το δίπλωμα περιέχει σαράντα δύο (42) ισχυρισμούς.

3.3.3 Διανύσματα ελέγχου για τη διαχείριση κλειδιών

Η ευρεσιτεχνία των Matyas, Meyer και Brachtl (με αριθμό 4.850.017) είναι μία από τις πολλές στον τομέα των διανυσμάτων ελέγχου για τη διαχείριση κλειδιών. Στην περίπτωση αυτή επιτρέπει την αποστολή κόμβου για τον περιορισμό της χρήσης κλειδιών σ' έναν εισερχόμενο κόμβο. Κατατέθηκε στις 29 Μαΐου 1987 και ανατέθηκε στην IBM Corporation. Τα διανύσματα ελέγχου μείωναν την πιθανότητα μίας κακής χρήσης κλειδιού. Διακρίνονται δύο γενικές μέθοδοι. Στην πρώτη, το κλειδί και μια τιμή ελέγχου επικυρώνονται πριν τη χρήση, μέσω της επαλήθευσης ενός ειδικού κωδικού ταυτότητας, το κλειδί για το οποίο είναι μέρος των δεδομένων που επικυρώνονται. Στη δεύτερη μέθοδο το κλειδί και η τιμή ελέγχου δεσμεύονται κρυπτογραφικά κατά τη δημιουργία του κλειδιού, έτσι ώστε η ανάκτηση κλειδιού να απαιτεί προδιαγραφές του σωστού διανύσματος ελέγχου. Σε κάθε μέθοδο, πρόσθετες τεχνικές μπορεί να χρησιμοποιηθούν για να ελέγχεται ποιοί χρήστες μπορούν να χρησιμοποιούν το συγκεκριμένο κλειδί. Το δίπλωμα ευρεσιτεχνίας περιέχει είκοσι δύο (22) ισχυρισμούς.

3.3.4 Κρυπταλγόριθμος τμήματος FEAL

Η ευρεσιτεχνία των Shimizu-Miyaguchi (με αριθμό 4.850.019) κατατέθηκε στις 3 Νοεμβρίου 1986 και ανατέθηκε στην Nippon Telegraph and Telephone Corporation (του Τόκυο) με προτεραιότητα στα στοιχεία που ήταν καταγεγραμμένα από τις 8 Νοεμβρίου 1985 (Ιαπωνικό γραφείο διπλωμάτων ευρεσιτεχνίας). Οι ενσωματώσεις της Feal περιγράφονται με ποικίλους αριθμούς γύρων, συμπεριλαμβανομένων των 4 και 6 γύρων Feal, όπου τώρα πια είναι γνωστό ότι είναι ανασφαλείς καθώς επίσης και αναφορές για μήκη κλειδιών συμπεριλαμβανομένων και των 128bits. Το δίπλωμα ευρεσιτεχνίας περιέχει είκοσι έξι (26) ισχυρισμούς.

3.3.5 MDC-2/MDC-4 συναρτήσεις κατακερματισμού

Το δίπλωμα ευρεσιτεχνίας των Brachtl et al. (με αριθμό 4.908.861) κατατέθηκε στις 28 Αυγούστου 1987 και ανατέθηκε στην IBM Corporation. Η ευρεσιτεχνία αυτή διαπιστώνει ότι η εναλλαγή των εσωτερικών μισών των κλειδιών, κάτι που γίνεται σ' ένα συγκεκριμένο στάδιο και στους δύο αλγορίθμους, απαιτείται πραγματικά για την ασφάλεια του MDC-2 αλλά όχι του MDC-4. Ωστόσο, ο κοινός σχεδιασμός χρησιμοποιήθηκε ώστε να επιτρέψει στο MDC-4 να υλοποιηθεί χρησιμοποιώντας το MDC-2 εις διπλούν. Ένα προκαταρκτικό τμήμα του διπλώματος ευρεσιτεχνίας συζητά εναλλακτικές λύσεις για την εξασφάλιση πιστοποίησης του μηνύματος, καθώς επίσης και εκτιμήσεις της ασφάλειας των νέων συναρτήσεων κατακερματισμού, και αιτιολόγηση για τη διόρθωση ορισμένων bits εντός προδιαγραφών προς αποφυγή επιπτώσεων λόγω αδύναμων DES κλειδιών. Περιέχει εικοσιένα (21) ισχυρισμούς που αφορούν κυρίως την οικοδόμηση 2N-bit συναρτήσεων κατακερματισμού από N-bit κρυπταλγόριθμους τμήματος.

3.3.6 Ταυτοποίηση Schnorr και υπογραφές

Το δίπλωμα ευρεσιτεχνίας του Schnorr (με αριθμό 4.995.082) καλύπτει την ταυτοποίηση Schnorr, συστήματα υπογραφών και βελτιστοποιήσεις αυτών ιδίως πριν την επεξεργασία τους. Κατατέθηκε στις 23 Φεβρουαρίου 1990 χωρίς κανέναν διάδοχο, και με στοιχεία προτεραιότητας στις 24 Φεβρουαρίου 1989 (Ευρωπαϊκό γραφείο διπλωμάτων ευρεσιτεχνίας. Περιέχει έντεκα (11) ισχυρισμούς. Μέρος του 6^{ου} ισχυρισμού καλύπτει μια συγκεκριμένη παραλλαγή της μεθόδου ταυτοποίησης των Fiat-Shamir, με τη χρήση ενός πρώτου συντελεστή βάσης λογαρίθμου p, τέτοιον ώστε ο (p-1) να διαιρείται από έναν πρώτο q κάνοντας χρήση μιας βάσης της τάξης q.

3.3.7 Ταυτοποίηση GQ και υπογραφές

Το δίπλωμα ευρεσιτεχνίας των Guillou και Quisquater (με αριθμό 5,140,634) κατατέθηκε στις 9 του Οκτώβρη του 1991, ως συνέχισης δύο εγκαταλελειμμένων εφαρμογών, η πρώτη εκ των οποίων κατατέθηκε την 7η Σεπτεμβρίου του 1988. Ο αυθεντικός διάδοχος ήταν η αμερικανική εταιρία Philips (Νέα Υόρκη). Οι τεχνικές που αναφέρονται σε αυτήν, επιτρέπουν την πιστοποίηση των πληροφοριών διαπίστευσης, την πιστοποίηση της γνησιότητας των μηνυμάτων, καθώς και την υπογραφή των μηνυμάτων. Το κεντρικό πρωτόκολλο ελέγχου ταυτότητας περιλαμβάνει μια μέθοδο δέσμευσης-πρόκλησης-απάντησης και συνδέεται στενά με

την μηδενικής γνώσης τεχνική εξακρίβωσης των Fiat και Shamir. Ωστόσο, αυτό απαιτεί μόνο μία εκτέλεση του πρωτοκόλλου και μία τιμή της διαπίστευσης, αντί για επανάληψη των εκτελέσεων και πολλαπλές τιμές διαπίστευσης. Τα πλεονεκτήματα σε σχέση με τις προηγούμενες μεθόδους περιλαμβάνουν μικρότερες απαιτήσεις μνήμης, και συνολικά μικρότερη διάρκεια λόγω λιγότερων ανταλλαγών μηνυμάτων. Οι κύριες εφαρμογές είναι εκείνες που αφορούν κάρτες με τσιπ σε τραπεζικές εφαρμογές. Υπάρχουν είκοσι τρεις (23) ισχυρισμοί, συμπεριλαμβανομένων ειδικών ισχυρισμών που αφορούν τη χρήση του καρτών με τσιπ (chipcards).

3.3.8 Κρυπταλγόριθμος Τμήματος IDEA

Το δίπλωμα ευρεσιτεχνίας των Massey και Lai (με αριθμό 5,214,703) καλύπτει το μπλοκ κρυπτογράφησης IDEA, προτάθηκε ως μια ευρωπαϊκή ή διεθνής εναλλακτική στο DES, προσφέροντας μεγαλύτερο μήκος κλειδιού (key bitlength) (και ως εκ τούτου, μεγαλύτερη ασφάλεια). Κατατέθηκε την 16η Μαΐου του 1991, και αποδίδεται στην ASCOM Tech AG (Βέρνη), με στοιχεία προτεραιότητας να δίνονται στις 18 Μαΐου του 1990 από την πρωτότυπη ελβετική ευρεσιτεχνία. Μια βασική έννοια στην κρυπτογράφηση είναι η χρήση τουλάχιστον δύο διαφορετικών τύπων αριθμητικών και λογικών διαδικασιών, με έμφαση στις διαφορετικές λειτουργίες σε διαδοχικές φάσεις. Τρία τέτοια είδη λειτουργίας προτείνονται: πρόσθεση mod 2^m, πολλαπλασιασμός mod $2^m + 1$, και bitwise exclusive-or (XOR). Τα σύμβολα που δηλώνουν τις εργασίες αυτές, είναι συμπληρωμένα με το χέρι στην Ευρωπαϊκή έκδοση του διπλώματος ευρεσιτεχνίας (WO 91/18459, με ημερομηνία 28 Νοεμβρίου του 1991, στα γερμανικά), και απουσιάζουν στο κείμενο της αμερικάνικης ευρεσιτεχνίας, κάνοντας το τελευταίο δύσκολο να διαβαστεί. Υπάρχουν δεκατέσσερα (14) στοιχεία και δέκα (10) σύνθετοι ισχυρισμοί.

3.3.9 Σύστημα υπογραφής DSA

Το δίπλωμα ευρεσιτεχνίας του Kravitz (με αριθμό 5,.231,668), με τίτλο "Digital Signature Algorithm", έχει γίνει ευρέως γνωστό και έχει υιοθετηθεί ως DSA. Κατατέθηκε στις 26 Ιουλίου του 1991, και αποδίδεται στον "Οι Ηνωμένες Πολιτείες της Αμερικής, όπως εκπροσωπείται από τον υπουργό Εμπορίου, Ουάσιγκτον, DC ". Περικλείει μια λεπτομερή συζήτηση των υπογραφών ElGamal και των υπογραφών Schnorr, συμπεριλαμβανομένων των πλεονεκτημάτων τους σε σχέση με την RSA - επιτρέποντας αποτελεσματικότερες online υπογραφές χρησιμοποιώντας offline προεπεξεργασία. Οι υπογραφές Schnorr σημειώθηκαν ως πιο αποτελεσματικές από τις ElGamal για την επικοινωνία και την επαλήθευση της υπογραφής, αν και λείπουν κάποια «επιθυμητά χαρακτηριστικά του ElGamal» και έχοντας το μειονέκτημα ότι η κρυπταναλυτική εμπειρία και εμπιστοσύνη που συνδέονται με το σύστημα ElGamal, δεν μεταφέρονται. Το DSA έχει την αποτελεσματικότητα του μοντέλου Schnorr, παραμένοντας συμβατό με το μοντέλο ElGamal από την πλευρά της ανάλυσης. Στις υποδειγματικές προδιαγραφές του DSA, η συνάρτηση κατακερματισμού που χρησιμοποιήθηκε ήταν MD4. Το δίπλωμα ευρεσιτεχνίας έχει σαράντα τέσσερις (44) ισχυρισμούς.

3.3.10 Fair Κρυπτοσυστήματα και Μεταβίβαση Κλειδιού

Το δίπλωμα ευρεσιτεχνίας του Micali (με αριθμό 5,276,737) και η συνέχιση αυτού (5,315,658), κατατέθηκαν στις 20 Απριλίου του 1992 και 19 Απριλίου του 1993 αντίστοιχα (χωρίς να έχουν καταγραφεί διάδοχοι), και καλύπτουν συστήματα μεταβίβασης κλειδιού που καλούνται «fair κρυπτοσυστήματα». Το θέμα του πρώτου είναι μια μέθοδος που περιλαμβάνει ένα κρυπτοσύστημα δημοσίου κλειδιού, που επιτρέπει την παρακολούθηση συνομιλιών από τρίτους (π.χ. υποκλοπή τηλεφωνικών συνδιαλέξεων από την κυβέρνηση). Ένα πλήθος από μερίδια που δημιουργήθηκαν από ένα ιδιωτικό κλειδί επιλεγμένο από τον χρήστη δίνεται σε ένα σύνολο από «έμπιστους». Με κάποια μέθοδο επαλήθευσης της κρυφής μοιρασιάς, οι «έμπιστοι» μεμονωμένα επιβεβαιώνουν την αυθεντικότητα των μεριδίων τους και το αναφέρουν σε κάποιον υπεύθυνο, ο οποίος εγκρίνει ένα δημόσιο κλειδί λαμβάνοντας τις επιβεβαιώσεις από όλους τους «έμπιστους». Μετά την κατάλληλη εξουσιοδότηση (π.χ. δικαστική απόφαση), οι «έμπιστοι» παράσχουν τα μερίδια τους στον υπεύθυνο για να επιτραπεί η ανακατασκευή ιδιωτικού κλειδιού χρήστη. Υποδειγματικά συστήματα περιλαμβάνουν τη μετατροπή συστημάτων Diffie-Hellman και δημοσίου κλειδιού RSA σε fair κρυπτοσυστήματα. Τροποποιήσεις απαιτούν μόνο k από n «έμπιστοι» να συνεισφέρουν μερίδια με σκοπό την ανάκτηση ιδιωτικού κλειδιού και αποτρέπουν τους «έμπιστους» από το να γνωρίζουν την ταυτότητα ενός χρήστη του οποίου το μερίδιο ζητήθηκε.

Το δίπλωμα ευρεσιτεχνίας περιλαμβάνει δεκαοκτώ (18) ισχυρισμούς, εκ των οποίων οι δεκατέσσερις (14) περιορίζονται σε κρυπτοσυστήματα δημοσίου κλειδιού.

Η συνέχιση αυτού του διπλώματος ευρεσιτεχνίας επιδιώκει περιορισμένο χρόνο κατά τον οποίον θα επιτρέπεται η παρακολούθηση με μεγάλη λεπτομέρεια, και περιλαμβάνει και χρήση απαραβίαστων τσιπ με εσωτερικά ρολόγια. Οι μέθοδοι που καθορίζονται επιτρέπουν στον υπεύθυνο (εφεξής, στην κυβέρνηση) την πρόσβαση σε κλειδιά συνόδου.
Μια άλλη μέθοδος επιτρέπει την επαλήθευση, χωρίς τη χρήση περιεχομένου παρακολούθησης, προερχόμενο από εγκεκριμένες από την κυβέρνηση συσκευές. Αυτό
μπορεί να περιλαμβάνει απαραβίαστα τσιπς σε κάθε συσκευή επικοινωνίας. Αυτές οι συσκευές επιτρέπουν την εξακρίβωση μεταδίδοντας μια περιττή συμβολοσειρά δεδομένων που εξαρτάται από αυτό το κλειδί.
Η συνέχιση του διπλώματος περιλαμβάνει δεκατρείς (13) ισχυρισμούς, με τους δύο πρώτους να περιορίζονται σε συστήματα δημοσίου κλειδιού. Οι ισχυρισμοί 11 και 12 επιδιώκουν μεθόδους για επαλήθευση ότι τα μηνύματα προέρχονται από μια απαραβίαστη συσκευή χρησιμοποιώντας έναν εξουσιοδοτημένο αλγόριθμο κρυπτογράφησης.

3.4 Πρότυπα Κρυπτογράφησης

Τα κρυπτογραφικά πρότυπα εξυπηρετούν δύο σημαντικούς στόχους:
διευκολύνουν την ευρεία χρήση των κρυπτογραφικά ευρέως αποδεκτών τεχνικών και προωθούν τη διαλειτουργικότητα μεταξύ των στοιχείων που αφορούν τους μηχανισμούς ασφαλείας σε διάφορα συστήματα.

Διεθνή πρότυπα - κρυπτογραφικές τεχνικές

Ο Διεθνής Οργανισμός Τυποποίησης (ISO) και η Διεθνής Ηλεκτροτεχνική Επιτροπή (IEC) αναπτύσσουν πρότυπα μεμονωμένα και από κοινού. Κοινά πρότυπα αναπτύχθηκαν στο πλαίσιο της κοινής τεχνικής επιτροπής ISO / IEC JTC 1. Κάθε ISO και ISO / IEC πρότυπο αναθεωρείται κάθε πέντε χρόνια, χρόνος κατά τον οποίο είτε αναθεωρήθηκε ή ανασύρθηκε. Η ISO / IEC υποεπιτροπή που είναι αρμόδια για την τυποποίηση γενικών τεχνικών κρυπτογράφησης είναι η SC 27 (ISO / IEC JTC 1 SC 27). Ο παρακάτω πίνακας περιλαμβάνει κάποια επιλεγμένα ISO και ISO / IEC πρότυπα σχετικά με τις τεχνικές κρυπτογράφησης:

ISO and ISO/IEC πρότυπα για γενικές κρυπτογραφικές τεχνικές

ISO #	ΘΕΜΑ	ΑΝΑΦ.
8372	Τρόποι χρήσης για ένα 64-bits κώδικα	[574]
9796	Υπογραφές με αποκατάσταση μηνύματος (π.χ. RSA)	[596]
9797	Μηχανισμός ακεραιότητας δεδομένων	[597]
9798–1	Οντότητα αυθεντικοποίησης - Εισαγωγή	[598]
9798–2	Οντότητα αυθεντικοποίησης – με χρήση συμμετρικής κρυπτογράφησης	[599]
9798–3	Οντότητα αυθεντικοποίησης – με χρήση τεχνικών δημοσίου κλειδιού	[600]
9798–4	Οντότητα αυθεντικοποίησης – με χρήση one-way λειτουργιών κλειδιού	[601]
9798–5	Οντότητα αυθεντικοποίησης – με χρήση zero knowledge τεχνικών	[602]
9979	Εγγραφή κρυπτογραφικών αλγορίθμων	[603]
10116	Τρόποι χρήσης ενός n-bit κώδικα	[604]
10118–1	Συναρτήσεις κατακερματισμού - Εισαγωγή	[605]
10118–2	Συναρτήσεις κατακερματισμού – με χρήση αλγορίθμων τμήματος	[606]
10118–3	Συναρτήσεις κατακερματισμού –	[607]

	προσαρμοσμένοι αλγόριθμοι	
10118–4	Συναρτήσεις κατακερματισμού – με χρήση δυαδικής αριθμητικής	[608]
11770–1	Διαχείριση Κλειδιών-Εισαγωγή	[616]
11770–2	Διαχείριση Κλειδιών-συμμετρικές τεχνικές	[617]
11770–3	Διαχείριση Κλειδιών-ασύμμετρες τεχνικές	[618]
13888–1	Μη αποκήρυξη - Εισαγωγή	[619]
13888–2	Μη αποκήρυξη – συμμετρικές τεχνικές	[620]
13888–3	Μη αποκήρυξη – ασύμμετρες τεχνικές	[621]
14888–1	Υπογραφές με παράρτημα - Εισαγωγή	[622]
14888–2	Υπογραφές με παράρτημα – μηχανισμοί αναγνώρισης	[623]
14888–3	Υπογραφές με παράρτημα – μηχανισμοί πιστοποίησης	[624]

ΒΙΒΛΙΟΓΡΑΦΙΑ

- ΚΡΥΠΤΟΓΡΑΦΙΑ
  Χ.ΚΟΥΚΟΥΒΙΝΟΣ – Α.ΠΑΠΑΙΩΑΝΝΟΥ
  ΕΚΔΟΣΗ ΕΘΝΙΚΟΥ ΜΕΤΣΟΒΙΟΥ ΠΟΛΥΤΕΧΝΕΙΟΥ, ΑΘΗΝΑ 2007

- ΣΗΜΕΙΩΣΕΙΣ ΣΤΗ ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ ΚΑΙ ΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ
  Ε.ΖΑΧΟΣ, 2007

- "LECTURE NOTES ON CRYPTOGRAPHY"
  S.Goldwasser - M.Bellare, 2008

- "HANDBOOK OF APPLIED CRYPTOGRAPHY"
  MENEZES, P. VAN OORSCHOT, S. VANSTONE
  CRC PRESS, 1996

- "DIFFERENTIAL CRYPTANALYSIS OF DES-LIKE CRYPTOSYSTEMS"
  E.BIHAM, A.SHAMIR

- ΣΗΜΕΙΩΣΕΙΣ ΜΑΘΗΜΑΤΟΣ «ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ»
  Μ.ΜΑΓΚΟΣ PhD

- «ΤΕΧΝΙΚΕΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ ΚΑΙ ΚΡΥΠΤΑΝΑΛΥΣΗΣ»
  Β.Α.ΚΑΤΟΣ – Γ.Χ.ΣΤΕΦΑΝΙΔΗΣ, 2003

- CRYPTOGRAPHY : AN INTRODUCTION
  N.P.SMART
  McGraw HILL,2002

- THE CODE BOOK
  THE SECRET HISTORY OF CODES AND CODE-BREAKING
  SIMON SINGH