ΚΡΥΠΤΟΓΡΑΦΙΑ – ΣΤΕΓΑΝΟΓΡΑΦΙΑ

4ο Γενικό Λύκειο Αλίμου

«Μακρυγιάννειο»

Project : Β’ ΛΥΚΕΙΟΥ 2016-2017

Καθηγητής : Ψαρούλης Σπύρος

Ευρετήριο

Εισαγωγή

Η λέξη κρυπτογραφία (αγγλ.: cryptography) προέρχεται από τα συνθετικά «κρυπτός» + «γράφω» και είναι ένα διεπιστημονικό γνωστικό πεδίο που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. Η κρυπτογραφία είναι ο ένας από τους δύο κλάδους της κρυπτολογίας (ο άλλος είναι η κρυπτανάλυση), η οποία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Σήμερα η κρυπτολογία θεωρείται ένα διεπιστημονικό γνωστικό πεδίο, το οποίο μπορεί να μελετηθεί ως όψη των εφαρμοσμένων μαθηματικών, της θεωρητικής πληροφορικής ή της επιστήμης ηλεκτρονικού μηχανικού. Παρεμφερείς κλάδοι είναι, αντιστοίχως, η στεγανογραφία και η στεγανοανάλυση

Κεφάλαιο 1. Κρυπτογραφία

1.1 Στόχοι Κρυπτογραφίας

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.

1.2 Επιθυμητές Ιδιότητες Συστημάτων Κρυπτογραφίας

- Πρέπει να υπάρχουν αποδοτικοί αλγόριθμοι για τις λειτουργίες της κωδικοποίησης και της αποκωδικοποίησης.
- Εύχρηστο σύστημα.
- Η προστασία που παρέχει το σύστημα πρέπει να προϋποθέτει μόνο τη μυστικότητα των κλειδιών, όχι του αλγόριθμου.

1.3 Ανάγκες Κρυπτογραφίας

Η ικανότητα να προστατεύσουμε και να ασφαλίσουμε πληροφορίες είναι αναγκαία για την ανάπτυξη του ηλεκτρονικού εμπορίου, αλλά και ολόκληρου του διαδικτυακού συστήματος. Πολλοί άνθρωποι χρειάζεται να χρησιμοποιούν επικοινωνιακά και πληροφοριακά συστήματα από διαφορετικά μέρη.

Οι τράπεζες σε όλον τον κόσμο χρησιμοποιούν στεγανογραφικές μεθόδους για την επεξεργασία οικονομικών συναλλαγών. Αυτές περιλαμβάνουν μεταφορές τεράστιων ποσοτήτων χρημάτων από μία τράπεζα σε άλλη. Οι τράπεζες επίσης χρησιμοποιούν κρυπτογραφικές μεθόδους για την προστασία του αριθμού ID των πελατών τους.

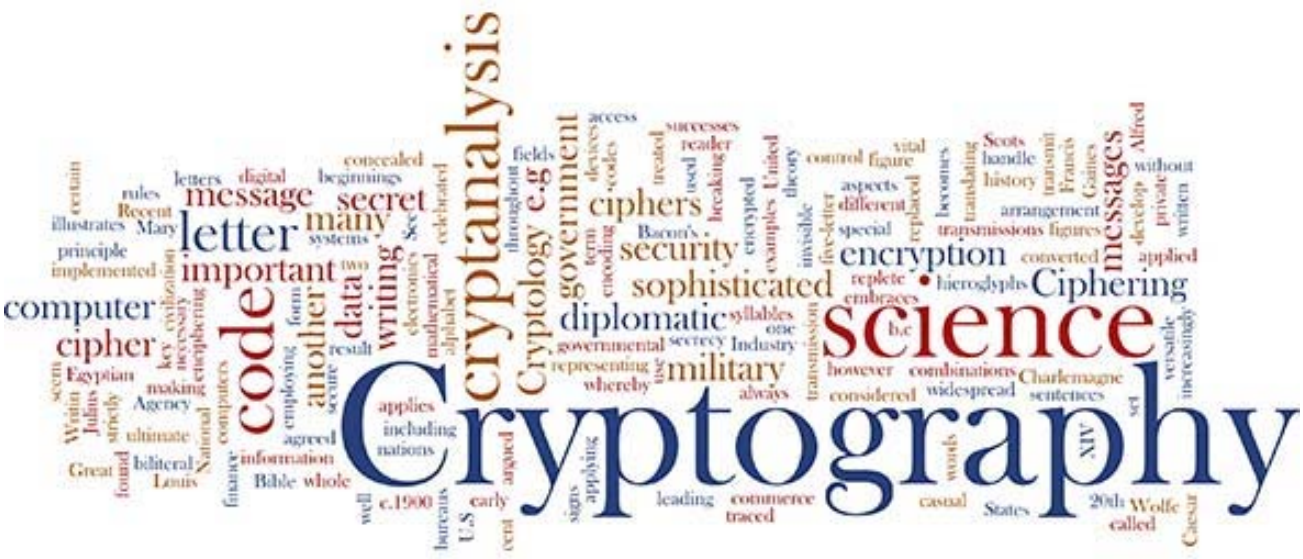
Καθώς η οικονομία απομακρύνεται από τις χρηματικές συναλλαγές και προσεγγίζει το «ψηφιακό χρήμα», οι

πελάτες έχουν ανάγκη την αυθεντικότητα, η οποία παρέχεται από γνήσιες ψηφιακές υπογραφές, ώστε να ελαχιστοποιηθεί η πλαστογραφία και να αυξηθεί η προστασία των διαφόρων συναλλαγών.

Αυτό αποτελεί ένα σημαντικό θέμα, διότι σχετίζεται με τους χρήστες του διαδικτύου. Υπάρχουν πολλές εταιρίες που πουλάνε ποικιλία προϊόντων μέσω του διαδικτύου και αυτές οι συναλλαγές πραγματοποιούνται με την χρήση πιστωτικών καρτών και ασφαλών διαδικτυακών μέσων περιήγησης συμπεριλαμβανομένων και κρυπτογραφικών και πιο συγκεκριμένα στεγανογραφικών μεθόδων. Οι πελάτες που επιδίδονται σε συναλλαγές μέσω του διαδικτύου θα πρέπει να είναι πεπεισμένοι για την ασφαλή αποστολή των πληροφοριών των πιστωτικών καρτών τους και άλλων οικονομικών λεπτομερειών που αποστέλλονται διαμέσου ενός πολυεθνικού περιβάλλοντος.

Κάτι τέτοιο μπορεί να επιτύχει αποκλειστικά με τη χρήση ισχυρών και κρυπτογραφικών μεθόδων.

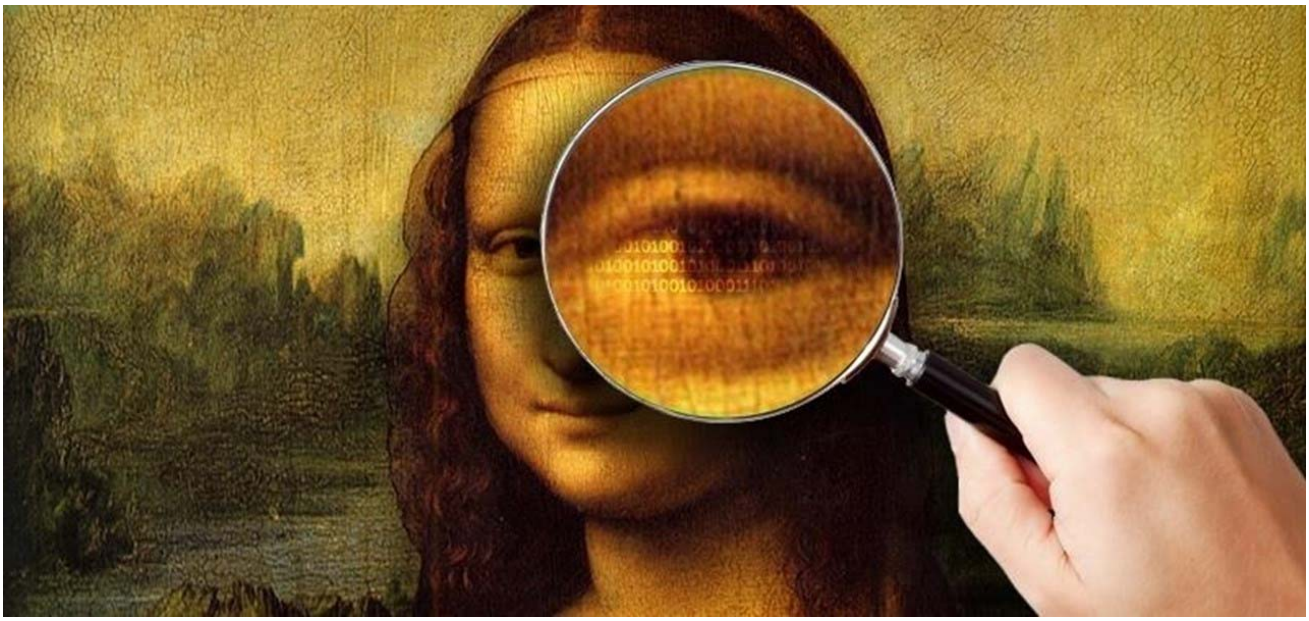
Επιπλέον, οι επιχειρηματικές και εμπορικές εταιρείες με εμπορικά μυστικά χρειάζονται την κρυπτογραφία έναντι υψηλής τεχνολογίας μεθόδων υποκλοπών και βιομηχανικής κατασκοπείας. Ακόμη, επαγγελματίες, όπως δικηγόροι, γιατροί και λογιστές που χρησιμοποιούν εμπιστευτικές πληροφορίες στις δραστηριότητες τους θα έχουν ανάγκη την κρυπτογραφία, εάν το επάγγελμά τους επεκταθεί και στον χώρο του διαδικτύου στο μέλλον. Οι εγκληματίες χρησιμοποιούν την κρυπτογραφία, ώστε να συγκαλύπτουν τις παράνομες δραστηριότητές τους και για να διεξάγουν ανεύρετα εγκλήματα. Πιο σημαντικό αποτελεί το γεγονός της ύπαρξης της αναγκαιότητα της κρυπτογραφίας για την ηλεκτρονική ασφάλεια κυβερνητικών εισχωρήσεων ή επιτηρήσεων στο πλαίσιο του διαδικτύου.



Χαρακτηριστικό παράδειγμα ανάγκης της κρυπτογραφίας και της στεγανογραφίας αποτελεί το εξής γεγονός: μια εφημερίδα που δημοσιεύει τα άρθρα της και στο Διαδίκτυο θα ήθελε αυτά τα άρθρα να είναι ασφαλή από μετατροπές ενός χάκερ που επιθυμεί να εισάγει λανθασμένες πληροφορίες στα κείμενα. Ακριβώς αυτό συνέβη το 1995, όταν άγνωστα άτομα κατάφεραν να εξουδετερώσουν τα μέτρα ασφάλειας της Ελευθεροτυπίας και να εισαγάγουν πρωτοσέλιδο άρθρο για τον πρόωρο θάνατο του Ανδρέα Παπανδρέου, που εκείνη τη στιγμή νοσηλευόταν στο Ωνάσειο.

Κεφάλαιο 2 – Στεγανογραφία

Η στεγανογραφία προέρχεται από της λέξεις στεγανός + γραφή και είναι η διαδικασία κατά την οποία αποκρύπτεται κάποια πληροφορία που πρέπει να αποσταλεί σε κάποιον παραλήπτη μέσα σε ένα μέσο. Ως μέσο εδώ μπορεί να οριστεί οποιοδήποτε υλικό αντικείμενο ή άυλο (π.χ. άυλο αντικείμενο μπορεί να είναι τα αρχεία ενός Ηλεκτρονικού υπολογιστή).



Ο σκοπός της στεγανογραφίας είναι η αποστολή της επιθυμητής πληροφορίας κρυμμένης μέσα στο μέσο, έτσι ώστε να μην γίνει αντιληπτή από ανεπιθύμητα άτομα, άλλα μόνο από τον παραλήπτη που για τον οποίο προορίζεται. Για μεγαλύτερη ασφάλεια, τον τρόπο με τον οποίο έγινε η στεγανογράφηση της πληροφορίας και τον τρόπο με τον οποίο μπορεί να ανακτηθεί πρέπει να τον γνωρίζει μόνο ο αποστολέας και ο παραλήπτης.

Η στεγανογραφία, παρόλο που σήμερα χρησιμοποιείται κατά βάση στους ηλεκτρονικούς υπολογιστές, δεν είναι καινούργια μέθοδος απόκρυψης της πληροφορίας κατά την επικοινωνία. Χαρακτηριστικό παράδειγμα χρήσης της στεγανογραφίας στην αρχαιότητα είναι η αφήγηση ενός ιστορικού γεγονότος από τον Ηρόδοτο: αναφέρεται ότι ο Δημάρατος ήθελε να ειδοποιήσει τη Σπάρτη ότι ο Ξέρξης προτίθετο να εισβάλει στην Ελλάδα. Για να αποφύγει την κλοπή του μηνύματος έγραψε το μήνυμά του σε ξύλινη πινακίδα, αφού έξυσε το κερί που αυτή είχε και την οποία μετά κάλυψε πάλι με κερί. Οι πινακίδες φαίνονταν λευκές και αχρησιμοποίητες και με αυτό το τρόπο πέρασαν κάθε έλεγχο.

Αντίστοιχα η στεγανογραφία σήμερα μπορεί να υλοποιηθεί στους ηλεκτρονικούς υπολογιστές, κρύβοντας για παράδειγμα ένα αρχείο κειμένου μέσα σε μία εικόνα χρησιμοποιώντας το κατάλληλο λογισμικό. Φαινομενικά η εικόνα, μετά από την απόκρυψη του αρχείου κειμένου μέσα σε αυτήν, παραμένει ίδια με την αρχική.

Όσον αφορά τα θέματα ασφάλειας, η στεγανογραφία προσφέρει προστασία της κρυμμένης πληροφορίας για όσο δεν γίνεται αντιληπτή η ύπαρξη της πληροφορίας αυτής. Αν γίνει αντιληπτή η ύπαρξη της κρυμμένης πληροφορίας τότε είναι θέμα χρόνου η ανάκτησή της από ανεπιθύμητα άτομα, αν η πληροφορία δεν είναι κρυπτογραφημένη. Ο κλάδος που ασχολείται με την ανάκτηση των στεγανογραφικά κρυμμένων

πληροφοριών λέγεται στεγανάλυση.

Επίσης πρέπει να ξεκαθαριστεί πως η στεγανογραφία δεν είναι μέθοδος κρυπτογραφίας. Η στεγανογραφία έχει ως σκοπό να αποκρύψει την ύπαρξη της πληροφορίας, σε αντίθεση με την κρυπτογραφία που σκοπεύει στην μετατροπή της πληροφορίας σε μη κατανοητή μορφή, έτσι ώστε ακόμα και αν γίνει αντιληπτή η ύπαρξη της πληροφορίας να μην μπορεί να διαβαστεί από άτομα που δεν είναι κάτοχοι του κλειδιού αποκρυπτογράφησης. Συνεπώς, για την επίτευξη μεγαλύτερης ασφάλειας μπορούμε να συνδυάσουμε τη στεγανογραφία με την κρυπτογράφηση.

Για παράδειγμα, μπορούμε ένα αρχείο κειμένου πρώτα να το κρυπτογραφήσουμε και ύστερα να το κρύψουμε μέσα σε μια εικόνα, πάντοτε με την χρήση του κατάλληλου λογισμικού. Έτσι αν γίνει αντιληπτή η ύπαρξη του κειμένου μέσα στην εικόνα και ανακτηθεί μέσω στεγανάλυσης από ανεπιθύμητα άτομα, δεν θα μπορεί παρ' όλα αυτά να διαβαστεί, λόγω του ότι είναι κρυπτογραφημένο.

Κεφάλαιο 3 – Ιστορική Αναδρομή

3.1. 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.

3.1.1 Η Κρυπτογραφία στην Αρχαιότητα

Εικονογραφική (Ιερογλυφική) γραφή

Κύριος εκπρόσωπος της εικονογραφικής γραφής είναι η από το 4.000 - 3.000 π.Χ. δημιουργημένη γραφή των αρχαίων Αιγυπτίων, η ονομαζόμενη ιερογλυφική, που κάθε σύμβολό της εκφράζει ή έννοια ή λέξη ή συλλαβή ακόμη και ένα μόνο γράμμα. Το πρώτο βήμα στην ανακάλυψη της γραφής πρέπει να δημιουργήθηκε με τη ζωγραφική απεικόνιση των διάφορων αντικειμένων. Έχουν βρεθεί σε ολόκληρο τον κόσμο πάρα πολλά σπήλαια που περιέχουν ωραιότατες τοιχογραφίες, που απεικονίζουν τις συνθήκες ζωής των ανθρώπων αυτών, τα κυνήγια που έκαναν και γενικά μας δίνουν μια εικόνα της πολιτιστικής τους στάθμης. Η εξέλιξη της γραφής αυτής (ιερογλυφικής) διαβάστηκε για πρώτη φορά από το Γάλλο αρχαιολόγο Σαμπολιόν. Η γραφή αυτή λεγόταν ιερογλυφική, γιατί την έγραφαν ιερείς. Πράγματι η ιερογλυφική γραφή είναι φοβερά δύσκολη τόσο απ' την πλευρά της συγγραφής, όσο και απ' την πλευρά της ανάγνωσης. Στην αρχαία Αίγυπτο μόνο οι ιερείς είχαν τη δυνατότητα να τη μελετήσουν και να τη μάθουν, γιατί η γνωριμία με τη γραφή απαιτούσε ασχολία πολλών χρόνων. Εκτός από τους ιερείς υπήρχαν ειδικοί άνθρωποι, κάτι σαν επιστήμονες εκείνης της εποχής, οι ονομαζόμενοι γραφείς.

Στα νεότερα χρόνια η ανάγνωση της ιερογλυφικής γραφής οφείλεται στην ανακάλυψη της τρίγλωσσης επιγραφής της Ροζέτας. Αυτή είναι γραμμένη στα ιερογλυφικά, στη δημοτική αιγυπτιακή γραφή και στην ελληνική. Με το συσχετισμό αυτό των γραφών μεταξύ τους κατόρθωσε ο Σαμπολιόν να τη διαβάσει. Κάθε

συλλαβή της είναι και ένα ιδιαίτερο γραφικό σύμβολο. Αργότερα το σύμβολο έχασε την αρχική σημασία του και σήμαινε το πρώτο γράμμα του.

Γραμμική γραφή Α

Η Γραμμική Α είναι μια μινωική γραφή που ανακαλύφθηκε στην Κρήτη από τον Άρθουρ Έβανς το 1900μ.Χ.. Η γραφή αυτή θεωρείται πρόγονος της Γραμμικής Β, η οποία είναι μυκηναϊκή. Όπως και η Γραμμική Β, έτσι και η Γραμμική Α είναι αποτυπωμένη κυρίως σε πήλινες πινακίδες. Τέτοιες πινακίδες έχουν βρεθεί στην Κνωσό, στη Φαιστό, στην Αγία Τριάδα, στα Χανιά, στις Αρχ άνες κ.α. αλλά και εκτός Κρήτης στη Μήλο, στην Κέα, στα Κύθηρα, στη Θήρα, στη Μίλητο και στην Τροία.

Χρονολογείται πριν την έλευση των Μυκηναίων στην Κρήτη, από το 1800 ως το 1450 π.Χ. περίπου.

Η Γραμμική Α, που φέρει και ο δίσκος της Φαιστού, δεν κατέστη δυνατόν να αποκρυπτογραφηθεί μέχρι σήμερα. Αν αποδειχτεί ότι η Γραμμική Α είναι ελληνική τότε αποδεικνύεται και ότι οι Έλληνες ήταν αυτόχθονες και όχι ετερόχθονες σύμφωνα με την ισχύουσα σήμερα θεωρία για την ινδοευρωπαϊκή τους προέλευση.

Ο Δίσκος της Φαιστού είναι ένα αρχαιολογικό εύρημα από τη Μινωική πόλη της Φαιστού στη νότια Κρήτη και χρονολογείται πιθανώς στον 17ο αιώνα π.Χ.. Αποτελεί ένα από τα γνωστότερα μυστήρια της αρχαιολογίας, αφού ο σκοπός της κατασκευής του και το νόημα των όσων αναγράφονται σε αυτόν παραμένουν άγνωστα. Ο δίσκος ανακαλύφθηκε στις 3 Ιουνίου 1908 από τον Ιταλό αρχαιολόγο Λουΐτζι Περνιέ (Luigi Pernier) και φυλάσσεται σήμερα στο Αρχαιολογικό Μουσείο Ηρακλείου.

Γραμμική Γραφή Β

Η Γραμμική Β είναι η πρώτη γραφή της ελληνικής γλώσσας, μεταγενέστερη μορφή της Γραμμικής Α, και χρησιμοποιήθηκε στη Μυκηναϊκή Περίοδο, από το 17ο ως τον 13ο αι. π.Χ., κυρίως για την τήρηση λογιστικών αρχείων στα ανάκτορα. Ανακαλύφθηκε στις αρχές του εικοστού αιώνα στην Κνωσό από τον Άρθουρ Έβανς, που την ονόμασε έτσι επειδή χρησιμοποιούσε γραμμικούς χαρακτήρες (και όχι εικονιστικούς, όπως η μινωική ιερογλυφική γραφή) χαραγμένους σε πήλινες πινακίδες.

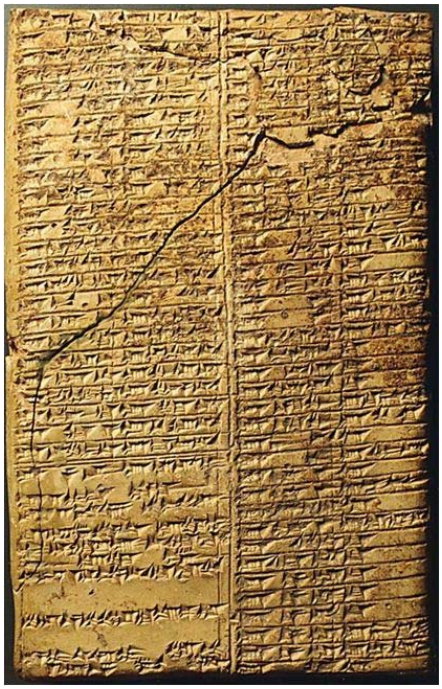
Η Γραμμική Β αρχικά δεν ταυτίστηκε με καμία γλώσσα, θεωρούμενη από τον Έβανς ότι αναπαριστούσε μια ξεχωριστή γλώσσα που ονόμαζε "Μινωϊκή", ενώ ήταν σχεδόν απόλυτα πεπεισμένος ότι ήταν αδύνατο να ήταν ελληνική.

Πολύ αργότερα από την ανακάλυψη των πινακίδων και μετά από πολλές αποτυχημένες προσπάθειες αρχαιολόγων και γλωσσολόγων, αποκρυπτογραφήθηκε το 1952 από το νεαρό αρχιτέκτονα Μάικλ Βέντρις (M. Ventris). Ο Βέντρις ζήτησε τη βοήθεια του κλασικού φιλολόγου Τζων Τσάντγουικ (J. Chadwick) και μαζί δημοσίευσαν ένα ιστορικό άρθρο στο Journal of Hellenic Studies [1]. Εκεί ερμήνευαν με σιγουριά 65 από τα 88 τότε γνωστά σύμβολά της, διατύπωναν τους βασικούς κανόνες ορθογραφίας της και έφερναν στο φως μια αρχαϊκή ελληνική διάλεκτο πέντε αιώνες παλαιότερη από τα Ελληνικά του Ομήρου.

Η Γραμμική Β περιλαμβάνει 89 συλλαβογράμματα, που αναπαριστούν συλλαβές με φωνητική αξία και περί τα 260 ιδεογράμματα (ή λογογράμματα), που αποδίδουν έννοιες όπως άνδρας, γυναίκα, αγελάδα, λάδι, κρασί κλπ. και σύμβολα για την απόδοση αριθμών. Αν και τα κείμενά της είναι στην πλειοψηφία τους λίστες εφοδίων που μπαίνουν, βγαίνουν ή είναι αποθηκευμένα στα ανάκτορα και τηλεγραφικές επιγραφές εμπορευμάτων, η αξία τους ως πρωτογενείς πηγές για την οικονομία, το εμπόριο, τη θρησκεία, την κοινωνική διαστρωμάτωση και τη διοικητική οργάνωση της μυκηναϊκής Ελλάδας είναι τεράστια. Ως σήμερα έχει αποκρυπτογραφηθεί το 87% των κειμένων.

Αρκετές προσπάθειες έχουν γίνει μέχρι σήμερα, για να ερμηνευθούν και τα υπόλοιπα 17 περίπου σύμβολα των οποίων δεν είναι γνωστή η συλλαβική τους αξία.

Σφηνοειδής Γραφή



Η σφηνοειδής γραφή είναι το αρχαιότερο γνωστό σύστημα γραφής στον κόσμο, το οποίο χαρακτηρίζεται από τους χαρακτήρες σε σχήμα σφήνας στις πήλινες πλακέτες που χρησιμοποιούνταν για την γραφή του, με την χρήση ενός αμβλέος καλαμιού ως γραφίδα.

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

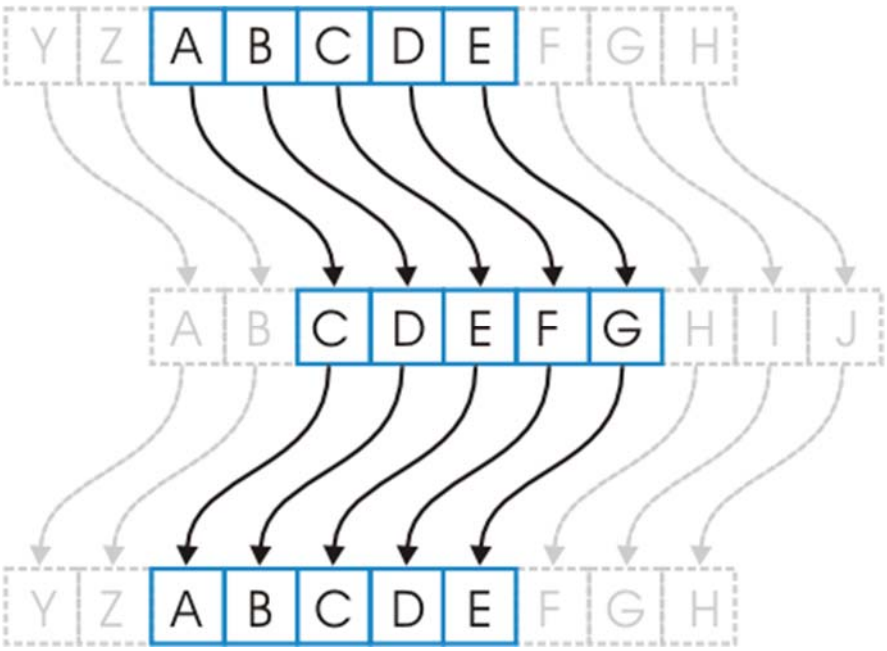
βάση τον Kahn). Επίσης, ως το αρχαιότερο βιβλίο κρυπτοκωδικών στον κόσμο, θεωρείται μία σφηνοειδής επιγραφή στα Σούσα της Περσίας. η οποία περιλαμβάνει τους αριθμούς 1 έως 8 και από το 32 έως το 35, τοποθετημένους τον ένα κάτω από τον άλλο, ενώ απέναντι τους βρίσκονται τα αντίστοιχα για τον καθένα σφηνοειδή σύμβολα.

Σπαρτιάτικη Σκυτάλη

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 αναδιάταξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της σκυτάλης.

Κρυπτοσύστημα αντικατάστασης του 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.



3.1.2. Η Κρυπτογραφία στο Μεσαίωνα

Στη διάρκεια του Μεσαίωνα, η κρυπτολογία ήταν κάτι το απαγορευμένο και αποτελούσε μια μορφή αποκρυφισμού και μαύρης μαγείας, κάτι που συντέλεσε στην καθυστέρηση της ανάπτυξης της. 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. Η κρυπτογραφία, λόγω των στρατιωτικών εξελίξεων, σημείωσε σημαντική ανάπτυξη στους επόμενους αιώνες. Ο Ιταλός Giovanni Batista 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.

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

3.2. 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

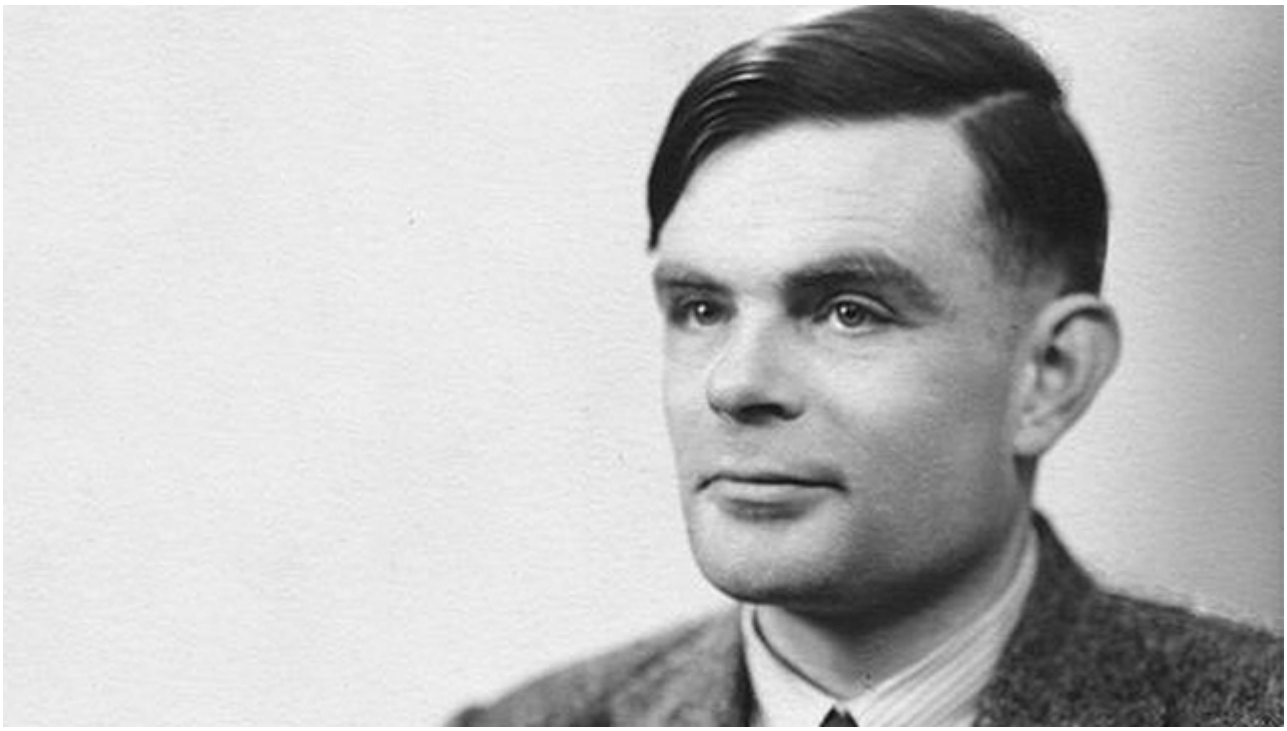
3.2.1. Μηχανή Enigma – Alan Matheson Turing

Μια συσκευή Enigma είναι μια οποιαδήποτε συσκευή από μια οικογένεια συσχετιζόμενων ηλεκτρο μηχανικών rotor συσκευών που χρησιμοποιήθηκαν για την κρυπτογράφηση και αποκρυπτογράφηση μυστικών μηνυμάτων.

Η πρώτη συσκευή Enigma εφευρέθηκε από τον Γερμανό μηχανικό Άρθουρ Σέρμπιους στο τέλος του Πρώτου Παγκοσμίου Πολέμου. Αυτό το μοντέλο και οι παραλλαγές του χρησιμοποιήθηκαν εμπορικά από της αρχές της δεκαετίας του 1920 και υιοθετήθηκαν από στρατιωτικές και κυβερνητικές υπηρεσίες από διάφορες χώρες, πιο αξιοσημείωτα από την Ναζιστική Γερμανία πριν και κατά τη διάρκεια του Δευτέρου Παγκοσμίου Πολέμου.

Αρκετά διαφορετικά μοντέλα συσκευών Enigma παρήχθησαν, αλλά τα Γερμανικά στρατιωτικά μοντέλα,τα Wehrmacht Enigmas, είναι τα πιο πολυσυζητημένα.

Ο Άλαν Μάθισον Τιούρινγκ (Alan Matheson Turing, 23 Ιουνίου, 1912 -7 Ιουνίου, 1954) ήταν Βρετανός μαθηματικός, καθηγητής της λογικής και κρυπτογράφος. Θεωρείται «πατέρας της επιστήμης υπολογιστών», χάρη στην πολύ μεγάλη συνεισφορά του στο γνωστικό πεδίο της θεωρίας υπολογισμού κατά τη δεκαετία του 1930, αλλά και της τεχνητής νοημοσύνης, χάρη στη λεγόμενη δοκιμή Τιούρινγκ την οποία πρότεινε το 1950: έναν τρόπο να διαπιστωθεί πειραματικά αν μία μηχανή έχει αυθεντικές γνωστικές ικανότητες και μπορεί να σκεφτεί.



Το έργο του από τη δεκαετία του '30 προσέδωσε στην ως τότε άτυπη έννοια του αλγορίθμου μία επίσημη, αυστηρή μαθηματική διατύπωση μέσω της λεγόμενης Μηχανής Τιούρινγκ. Ακόμα, ο Τιούρινγκ διατύπωσε από κοινού με τον Αλό νζο Τσερτς την περίφημη εικασία του, ευρέως αποδεκτή, σύμφωνα με την οποία οποιοδήποτε μαθηματικό μοντέλο υπολογισμού είναι είτε ισοδύναμο είτε υποδεέστερο της Καθολικής Μηχανής Τιούρινγκ, επομένως αυτή περιγράφει τον ευρύτερο δυνατό υπολογιστή γενικού σκοπού: είναι θεωρητικά ικανή να υπολογίσει ό,τι είναι δυνατό να υπολογιστεί αλγοριθμικά.

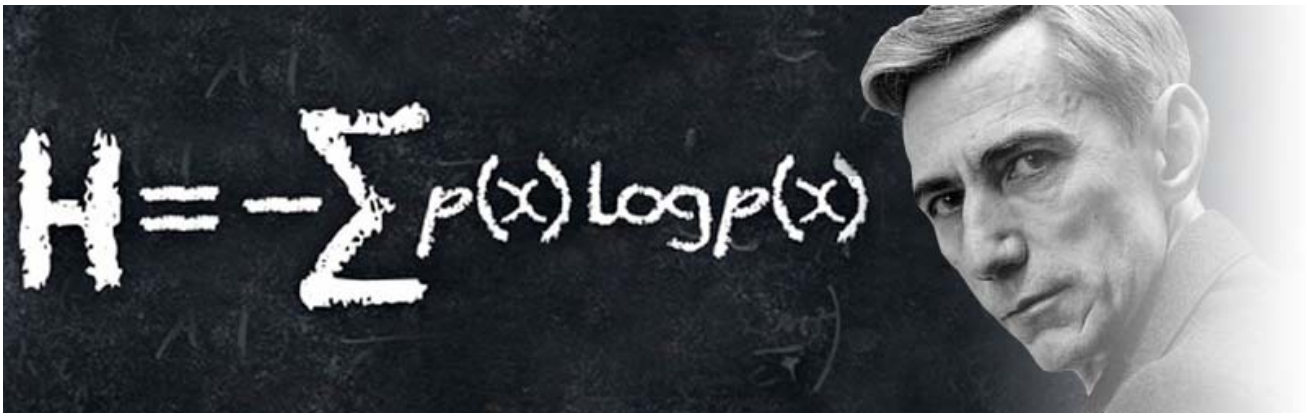
Οι επιστημονικές συνεισφορές του Τιούρινγκ κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου δεν αναγνωρίστηκαν ποτέ δημόσια κατά τη διάρκεια της ζωής του επειδή η εργασία του ήταν απόρρητη. Στο Μπλέτσλεϊ Παρκ (Bletchley Park), κέντρο της Βρετανικής Υπηρεσίας Αντικατασκοπείας, ήταν το κεντρικό πρόσωπο στην αποκρυπτογράφηση των γερμανικών στρατιωτικών κωδικών, όντας ο προϊστάμενος της Ομάδας 8. Η ομάδα αυτή ήταν που επιφορτίστηκε με την αποκωδικοποίηση της γερμανικής κρυπτογραφικής συσκευής Enigma.

Μετά τον Πόλεμο, σχεδίασε έναν από τους πρώτους ηλεκτρονικούς προγραμματίσιμους ψηφιακούς υπολογιστές στο Εθνικό Φυσικό Εργαστήριο, όπως λεγόταν, και κατασκεύασε μια δεύτερη υπολογιστική μηχανή στο Πανεπιστήμιο το υ Μάντσεστερ . Ο Τιούρινγκ αυτοκτόνησε το 1954. Το Βραβείο Τιούρινγκ, η ύψιστη επιστημονική διάκριση στον χώρο της πληροφορικής από το 1966 κι έπειτα, ονομάστηκε έτσι προς τιμήν του.

3.3 Τρίτη Περίοδος Κρυπτογραφίας (1950 μ.Χ. – Σήμερα)

Αυτή η περίοδος χαρακτηρίζεται από την έξαρση της ανάπτυξης στους επιστημονικούς κλάδους των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων. Η εποχή της σύγχρονης κρυπτογραφίας αρχίζει ουσιαστικά με τον Claude Shannon, αναμφισβήτητα 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.



4. Κρυπτογραφία στου Υπολογιστές

Σήμερα, κάθε κρυπτογράφηση δεδομένων βασίζεται σε υπολογιστές. Πολύ απλά, όποιον αλγόριθμο κι αν επινοήσει ο άνθρωπος, όσο περίπλοκος κι αν είναι, είναι υπερβολικά εύκολο να τον σπάσει ένας κατάλληλα προγραμματισμένος υπολογιστής.

Η κρυπτογράφηση δεδομένων μέσω υπολογιστή γενικά ανήκει σε δύο κατηγορίες:

- **Symmetric key encryption** (Συμμετρική Κρυπτογράφηση)
- **Public key ή Asymmetric key encryption** (Κρυπτογράφηση δημοσίου)

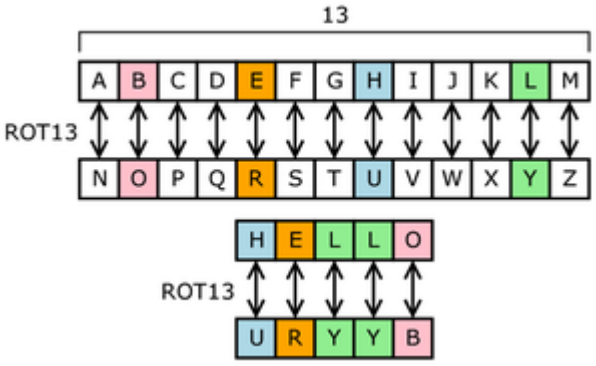
4.1 Σύγχρονα Κρυπτογραφικά Συστήματα

Με την εξέλιξη παλαιότερων μεθόδων κρυπτογραφίας, στις μέρες μας έχουν αναπτυχθεί πολυάριθμα κρυπτογραφικά συστήματα (ή αλγόριθμοι, όπως είναι ευρύτερα γνωστά) για διάφορους λόγους.

4.1.1 Κρυπτογράφηση Υποκατάστασης

Η κρυπτογραφία υποκατάστασης θεωρείται η πιο απλή, επειδή τα γράμματα υποκαθίστανται μεταξύ τους σε όλο το «μήκος» του μηνύματος. Αυτό το είδος κρυπτογράφησης μπορεί να

«σπάσει» εύκολα αναλύοντας απλώς τη συχνότητα των γραμμάτων και τοποθετώντας τα πιο κοινά-χρησιμοποιούμενα γράμματα στις κατάλληλες θέσεις.



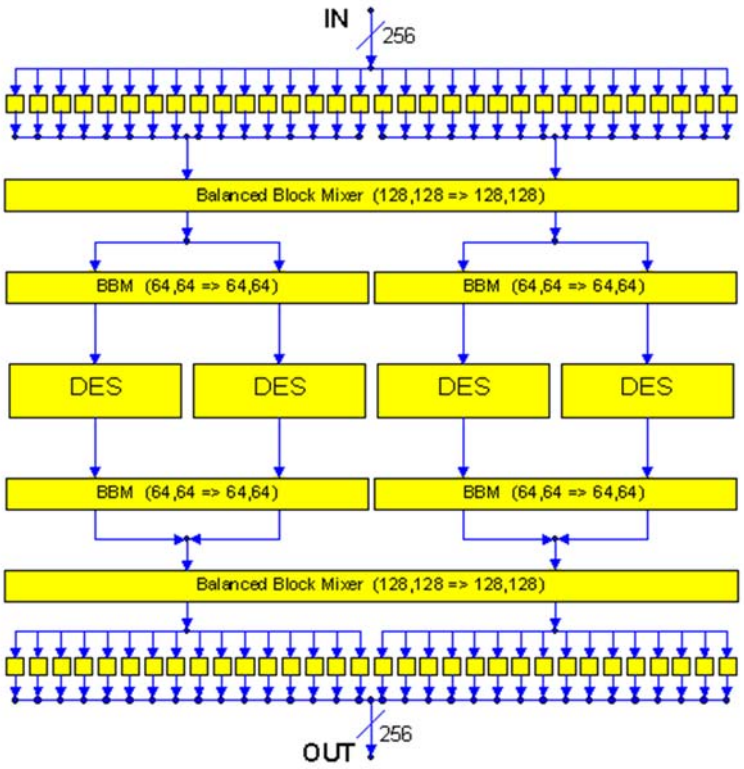
4.1.2 Αμοιβαία Κρυπτογράφηση

Πολλά κρυπτογραφικά συστήματα είναι τύπου αμοιβαίας κρυπτογράφησης και μπορεί να κάνει το σύστημα είτε λιγότερο ασφαλές είτε πιο εύχρηστο. Η αμοιβαία κρυπτογράφηση σημαίνει πως κάποιος θα μπορούσε να εισάγει ένα καθαρό κείμενο στο κρυπτογραφικό σύστημα και να λάβει το κρυπτογραφημένο κείμενο, αλλά και αντίστροφα θα μπορούσε να εισάγει το κρυπτογραφημένο στο ίδιο σύστημα ώστε να λάβει το καθαρό κείμενο. Η χρησιμοποίηση τέτοιου είδους κρυπτογράφησης είναι μια μορφή αυτοκτονίας, καθώς καθιστά το κρυπτογράφημα πιο εύκολο για να «σπάσει». Ωστόσο, εάν η μηχανή Enigma δεν ήταν αμοιβαίας κρυπτογράφησης, θα αυξανόταν σημαντικά ο βαθμός δυσκολίας χρήση του.

4.1.3 Συμμετρική Κρυποτγράφηση

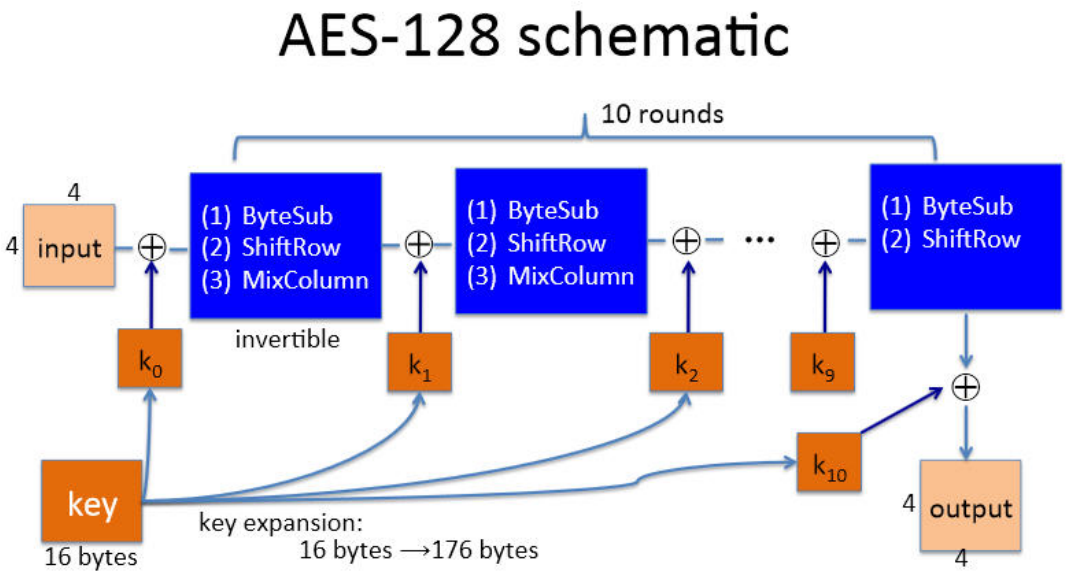
Για πολύ καιρό, η συμμετρική κρυπτογράφηση αποτελούσε το μοναδικό είδος κρυπτογραφίας που ήταν διαθέσιμο. Η συμμετρική κρυπτογραφία χρησιμοποιεί το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Αυτό, ωστόσο, δεν σημαίνει πως η συμμετρική είναι λιγότερο ασφαλής από την ασύμμετρη κρυπτογράφηση, διότι στα περισσότερα κρυπτογραφικά συστήματα η ασφάλιση του κλειδιού είναι πιο σημαντική από την ασφάλιση του ίδιου του κρυπτογραφικού συστήματος.

Ο πρώτος σημαντικός αλγόριθμος για κρυπτογράφηση δεδομένων μέσω υπολογιστή ήταν ο Data Encryption Stantard (**DES**) που αναπτύχθηκε από την IBM στις ΗΠΑ και εγκρίθηκε για χρήση το 1970.



Ο DES χρησιμοποιεί κλειδί μήκους 56-bit, που διαθέτει πάνω από 72 τετράκις εκατομμύρια πιθανούς συνδυασμούς (72.057.594.037.927.936, για την ακρίβεια). Μπορεί να ακούγονται ατέλειωτοι, όμως το 1998 δημιουργήθηκε η συσκευή EFF DES cracker ("Deep Crack"), με ειδικά κατασκευασμένα τσιπάκια, που επέτρεπαν σε έναν υπολογιστή να δοκιμάσει 90 δισεκατομμύρια κλειδιά το δευτερόλεπτο!

Πλέον, ο DES έχει αντικατασταθεί από τον αλγόριθμο Advanced Encryption Standard (AES), που χρησιμοποιεί κλειδιά 128, 192 ή 256-bit. Με την αύξηση των bit, οι πιθανοί συνδυασμοί ανεβαίνουν εκθετικά. Ένα κλειδί 128-bit μπορεί να έχει πάνω από 300.000.000.000.000.000.000.000.000.000.000.000 πιθανούς συνδυασμούς.



Ο μεγαλύτερος υπερυπολογιστής αυτή τη στιγμή στον κόσμο, που μπορεί να εκτελέσει 33,86 petaflop/s (τετράκις εκατομμύρια υπολογισμούς το δευτερόλεπτο) και θα μπορούσε θεωρητικά να σπάσει τον DES σε 2 δευτερόλεπτα, θα χρειαζόταν περίπου 250 δισεκατομμύρια χρόνια για να ελέγξει όλους τους συνδυασμούς του AES-128.

4.1.4 Ασύμμετρη Κρυπτογράφηση

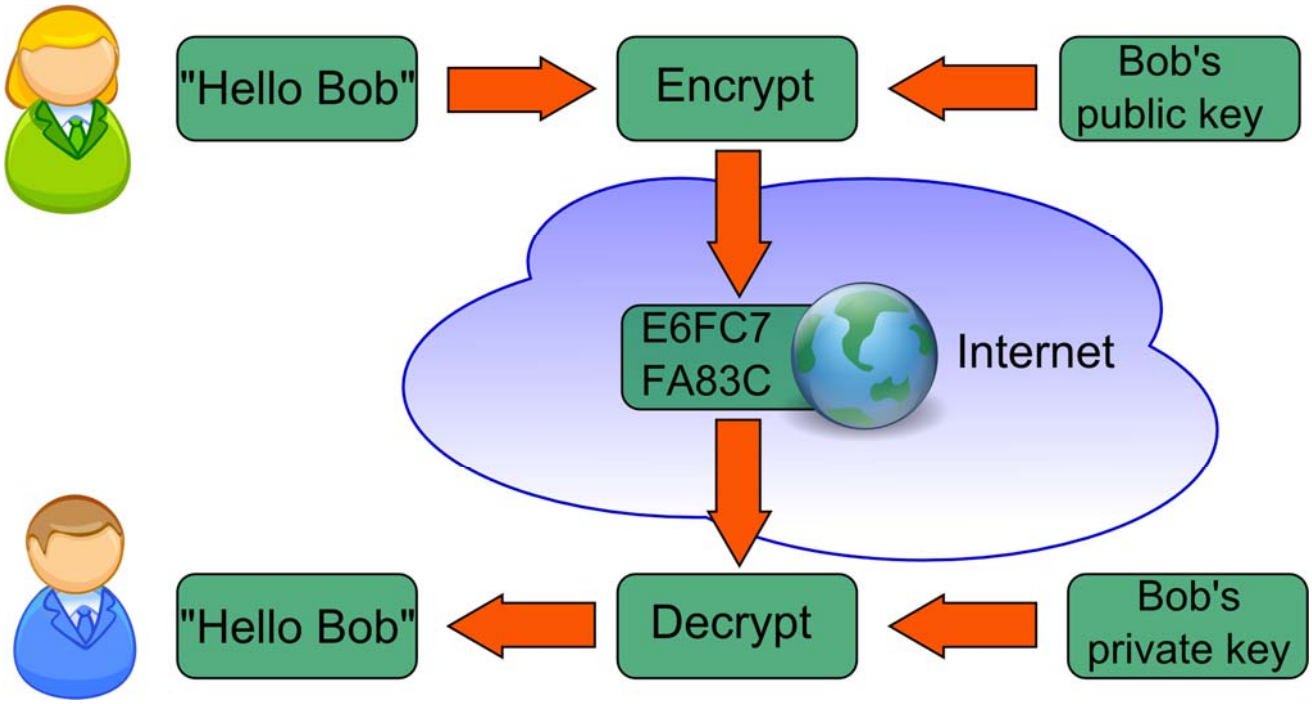
Η κρυπτογράφηση δημοσίου κλειδιού (Public Key Cryptography) ή ασύμμετρου κλειδιού (Asymmetric Cryptography) επινοήθηκε στο τέλος της δεκαετίας του 1970 και παρέχει ένα εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης από την προγενέστερη κρυπτογράφηση συμμετρικού κλειδιού. Η ασύμμετρη κρυπτογράφηση χρησιμοποιεί διαφορετικό κλειδί για την «αποκωδικοποίησή» του και διαφορετικό για την «κωδικοποίησή» του. Με αυτόν τον τρόπο, μόνο ο δέκτης του μηνύματος θα μπορούσε να διαβάσει το περιεχόμενο της κρυπτογράφησης. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της κρυπτογράφησης συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

Ουσιαστικά, σε αυτή τη μέθοδο κρυπτογράφησης υπάρχουν δύο κλειδιά:

Το Public key, είναι δημόσιο και μπορεί να το χρησιμοποιήσει οποιοσδήποτε για την κρυπτογράφηση δεδομένων.

Το Private Key που είναι μυστικό. Συνδέεται μαθηματικά με το Public key και είναι απαραίτητο για την αποκρυπτογράφηση.

Για να γίνει κατανοητός ο τρόπος λειτουργίας αυτής της μεθόδου, θα χρησιμοποιήσουμε ένα παράδειγμα με δύο χρήστες, την Alice και τον Bob. Τα ονόματα Alice και Bob, παρεμπιπτόντως, είναι τα στάνταρ ονόματα που χρησιμοποιούν οι κρυπτογράφοι για παραδείγματα και να δείξουν πώς λειτουργούν οι αλγόριθμοι.



Ο παραλήπτης ενός μηνύματος που χρησιμοποιεί κρυπτογράφηση δημοσίου κλειδιού χρησιμοποιεί δυο κλειδιά με τον ακόλουθο τρόπο:

- Δημοσιοποιεί το δημόσιο κλειδί του π.χ. σε ένα site.
- Οποιοσδήποτε θέλει να στείλει μήνυμα στον κάτοχο του κλειδιού αυτού χρησιμοποιεί το δημόσιο κλειδί για να κάνει την κρυπτογράφηση.
- Το κρυπτογραφημένο κείμενο αποκρυπτογραφείται από τον παραλήπτη που εφαρμόζει τον κατάλληλο αλγόριθμο αποκρυπτογράφησης χρησιμοποιώντας το ιδιωτικό κλειδί.

Με αυτό τον τρόπο δεν χρειάζεται ο παραλήπτης να δημοσιοποιήσει το κλειδί που χρησιμοποιείται για αποκρυπτογράφηση.

4.1.5 Σύγκριση Συμμετρικής – Ασύμμετρης Κρυπτογράφησης

Αξίζει σε αυτό το σημείο να συγκρίνουμε τις δυο μεθόδους κρυπτογράφησης πριν εξετάσουμε μερικές τεχνολογίες δημοσίου κλειδιού.

- Όταν χρησιμοποιούνται αρκετά μεγάλα κλειδιά και οι δυο μέθοδοι είναι ασφαλείς.
- Η κρυπτογραφία δημοσίου κλειδιού είναι ευκολότερο να υλοποιηθεί γιατί δεν χρειάζεται να ανησυχούμε για την μετάδοση κλειδιών μέσω ενός ανασφαλούς δικτύου.
- Η υπολογιστική ισχύς που χρειάζεται για κρυπτογραφία δημοσίου κλειδιού είναι πολύ μεγαλύτερη από αυτή που χρειάζεται για κρυπτογραφία συμμετρικού κλειδιού. Αυτό σημαίνει ότι για μεταφορά μεγάλων ποσοτήτων δεδομένων προτιμούνται συνήθως οι μέθοδοι συμμετρικού κλειδιού.

4.1.6 Τεχνολογίες Ασύμμετρης Κρυπτογράφησης

Υπάρχουν διάφορες τεχνολογίες και υλοποιήσεις της κρυπτογραφίας δημοσίου κλειδιού.

Ορισμένα άλλα δύσκολα υπολογιστικά προβλήματα προτάθηκαν για κρυπτογραφία δημοσίου κλειδιού. Όμως η ανάλυση ενός μεγάλου αριθμού άντεξε στο χρόνο και είναι η ιδέα πίσω από την κρυπτογραφία δημοσίου κλειδιού.

Έξυπνες κάρτες, ιδιωτικά και δημόσια κλειδιά

Ένας από τους πιο ασφαλείς τρόπους για να διασφαλιστεί η προστασία ενός ιδιωτικού κλειδιού είναι να το αποθηκεύσουμε σε μια έξυπνη κάρτα. Αυτές έχουν μέγεθος πιστωτικής κάρτας και περιέχουν και το ιδιωτικό και το δημόσιο κλειδί. Μπορούν να

συνδεθούν σε ένα υπολογιστή και να στείλουν το ιδιωτικό κλειδί στον υπολογιστή ώστε αυτός να εκτελέσει την κρυπτογράφηση. Αυτό σημαίνει ότι το ιδιωτικό κλειδί δεν χρειάζεται ποτέ να αποθηκευθεί στον υπολογιστή και ότι όποιος θέλει να

αποκτήσει το ιδιωτικό κλειδί πρέπει να κλέψει την κάρτα. ακόμη κι έτσι όμως μπορεί να μην είναι δυνατόν να χρησιμοποιήσει το ιδιωτικό κλειδί καθώς οι έξυπνες κάρτες μπορούν να προγραμματιστούν ώστε να ζητάνε ένα κωδικό πριν δώσουν το δημόσιο κλειδί.

Η πρώτη τεχνολογία που θα εξετάσουμε είναι η ανταλλαγή κλειδιού Diffie- Hellman. Αυτή είναι μια τεχνική για την ανταλλαγή ενός συμμετρικού κλειδιού χρησιμοποιώντας δημόσιο κλειδί. Οι δυο πλευρές που συμμετέχουν σε αυτή τη διαδικασία ανταλλάζουν αρχικά πληροφορίες σχετικά με κάποιο συμμετρικό κλειδί χρησιμοποιώντας μεθόδους δημοσίου κλειδιού και στη συνέχεια χρησιμοποιούν το συμφωνηθέν κλειδί για να επικοινωνήσουν.

Το RSA είναι σίγουρα το πιο γνωστό σύστημα κρυπτογράφησης δημοσίου κλειδιού. Αναπτύχθηκε από τρεις καθηγητές στο MIT: τον Ronald Rivest, τον Adi Shamir και τον Leonard Adelman. το RSA μπορεί να χρησιμοποιηθεί για την αποστολή

δεδομένων μέσω μιας μη ασφαλούς γραμμής και μπορεί επίσης να χρησιμοποιηθεί για τη δημιουργία ψηφιακών υπογραφών: σειρών χαρακτήρων δηλαδή που πιστοποιούν ότι ο αποστολέας του μηνύματος είναι αυτός που ισχυρίζεται πως είναι.

Το σύστημα ElGamel sytem είναι ένα σύστημα δημοσίου κλειδιού που βασίζεται στην ανταλλαγή κλειδιου Diffie-Hellman. Μπορεί επίσης να χρησιμοποιηθεί για ψηφιακές υπογραφές.

Το Digital Signature Standard, γνωστό ως DSS, αναπτύχθηκε από της αμερικανική εθνική υπηρεσία ασφάλειας και υιοθετήθηκε ως πρότυπο από την αμερικανική εθνική υπηρεσία τυποποιήσεων. Στην αρχική του μορφή μπορεί να χρησιμοποιηθεί μόνο για ψηφιακές υπογραφές, ωστόσο μπορεί να τροποποιηθεί για κανονική μεταφορά δεδομένων. Η τεχνική αυτή βασίζεται στον αλγόριθμο Digital Signature Algorithm.

4.2 Διαδεδομένοι Μέθοδοι Κρυπογράφησης

4.2.1 SSL

Η SSL δεν είναι μία επαναστατική μέθοδος κρυπτογραφικού συστήματος. Στην πραγματικότητα είναι κυρίως σημαντική στο πλαίσιο του διαδικτύου. Η SSL σημαίνει Secure Sockets Layer (Ασφαλές υποδοχές υποστρώματος) και είναι απολύτως απαραίτητη στο διαδικτυακό εμπόριο.

Η λειτουργία του SSL βρίσκεται μεταξύ του απλού και του περίπλοκου. Βασίζεται σε ένα ασύμμετρο κρυπτογράφημα που διαβεβαιώνει πως ο εν λόγω υπολογιστής του διακομιστή ανήκει στην εταιρεία που ισχυρίζεται ότι είναι, καθώς επίσης και σε ένα συμμετρικό κρυπτογράφημα για να επεξεργάζεται την κρυπτογραφημένη επικοινωνία.

- Ο πελάτης/υπολογιστής σου στέλνει δεδομένα στον εξυπηρετητή. Αυτό περιλαμβάνει την εκδοχή SSL που χρησιμοποιεί ο φυλλομετρητής σου (το χρόνο της συγγραφής, βρισκόμαστε στην εκδοχή 3.0), κάποιες ρυθμίσεις του κρυπτογραφήματος (ποιους αλγόριθμους κατανοεί ο φυλλομετρητής), κάποια τυχαία δεδομένα και διάφορες άλλες πληροφορίες.

- Ο εξυπηρετητής/λήπτης στέλνει στον υπολογιστή σου μια σειρά δεδομένων.

Είναι παρόμοια με εκείνα που είχαν αποσταλεί εξαρχής, αλλά ακόμη περιλαμβάνουν και το Πιστοποιητικό Αυθεντικότητας. Εάν οι άνθρωποι που «τρέχουν» τον εξυπηρετητή αποφασίσουν πως χρειάζονται το πιστοποιητικό του πελάτη/εξυπηρετούμενου, τότε το εξυπηρετητής ζητάει το πιστοποιητικό.

- Στη συνέχεια, ο πελάτης βεβαιώνεται πως το πιστοποιητικό του εξυπηρετητή είναι έγκυρος. Με αυτόν τον τρόπο γίνεται βέβαιο πως ο πελάτης εμπιστεύεται την εταιρεία, η οποία έχει αναφέρει πως ο εξυπηρετητής είναι όντως ό,τι ισχυρίζεται ότι είναι. Εάν αυτό δεν γίνει, ο φυλλομετρητής προειδοποιεί τον χρήστη και εγκαταλείπει κάθε προσπάθεια ασφαλούς επικοινωνίας.

- Αργότερα ο πελάτης δημιουργεί ένα «premaster secret» βασιζόμενο σε ό,τι μηνύματα έχουν αποσταλεί μέχρι εκείνο το σημείο. Μετά κρυπτογραφεί το «premaster secret» με το δημόσιο κλειδί του εξυπηρετητή (ελήφθη με το πιστοποιητικό αυθεντικότητας) και το στέλνει στον εξυπηρετητή. Αν ο εξυπηρετητής χρειάζεται το πιστοποιητικό του πελάτη, το αποθηκεύει και στέλνει με τη σειρά του το δικό του πιστοποιητικό.

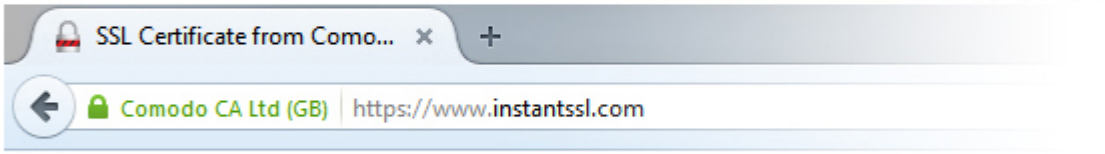
- Αν το παραπάνω βήμα δεν μπορεί να γίνει, ο εξυπηρετητής σταματά τη προσπάθεια ασφαλούς μεταβίβασης πληροφοριών και δεδομένων. Αν, ωστόσο, πραγματοποιηθεί, ο εξυπηρετητής ενεργοποιεί το «master secret» με το «premaster secret» (αφού έχει εφαρμόσει το ιδιωτικό του κλειδί στο premaster). Ο πελάτης εκτελεί την ίδια διαδικασία. Σε αυτό το σημείο, και οι 2 υπολογιστές διαθέτουν το ίδιο «master key».

- Το «master secret» χρησιμοποιείται για να ενεργοποιήσει τα «session keys» Αυτά τα κλειδιά είναι συμμετρικά και χρησιμοποιούνται όχι μόνο για να κρυπτογραφούν και αποκρυπτογραφούν δεδομένα , αλλά και για να επικυρώνουν ότι οι πληροφορίες δεν έχουν τροποποιηθεί κατά τη διάρκεια της μεταβίβασης.

- Τέλος, ο πελάτης στέλνει ένα μήνυμα στον εξυπηρετητή λέγοντας πως όλες οι μελλοντικές μεταβιβάσεις θα χρησιμοποιούν τα session keys.

Google Chrome address bar

Mozilla Firefox address bar



Internet Explorer address bar

Τώρα όλες οι πληροφορίες που στέλνονται μεταξύ του πελάτη και του εξυπηρετητή μπορούν να διαβαστούν μόνο από αυτούς τους δύο. Αριθμοί πιστωτικών καρτών, κωδικοί δεν μπορούν να διαβαστούν από δευτερεύοντα πρόσωπα.

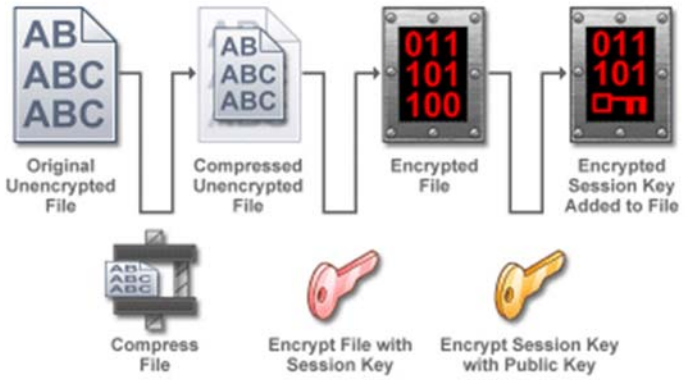
4.2.2 PGP

Η PGP αποτελείται από μια σειρά ασύμμετρων και συμμετρικών αλγορίθμων προκειμένου να κρυπτογραφούνται τα e-mail με ασφάλεια,ανάλογα με το περιεχόμενο του πιστοποιητικού. Αυτό το πιστοποιητικό περιλαμβάνει το δημόσιο κλειδί σου και ο επιλεγμένος συμμετρικός αλγόριθμος. Το λογισμικό αυτό κρυπτογραφεί ακολουθώντας τα επόμενα βήματα:

- Το μήνυμα συμπιέζεται (στεγανογραφία). Αυτό συμβαίνει για προστασία για τυχόν ελαττώματα στον αλγόριθμο κρυπτογράφησης.
- Ένα session key ενεργοποιείται τυχαία, χρησιμοποιώντας πληκτρολογήσεις και κινήσεις του ποντικιού κατά βάσιν.

- Το συμπιεσμένο μήνυμα κρυπτογραφείται χρησιμοποιώντας έναν επιλεγμένο από το χρήστη αλγόριθμο από ένα σύνολο συμμετρικών αλγορίθμων.

- Το session key κρυπτογραφείται χρησιμοποιώντας το δημόσιο κλειδί του χρήστη. Τώρα, μόνο ο χρήστης μπορεί να αποκρυπτογραφήσει το μήνυμα.



Η PGP είναι απλή στη θεωρία. Οι αλγόριθμοι που χρησιμοποιούνται είναι αυτοί που κάνουν αυτό το λογισμικό τόσο δύσκολο να προγραμματιστεί. Η αποκρυπτογράφηση λειτουργεί με την αντίθετη κατεύθυνση, καθώς το session key αποκρυπτογραφείται με το ιδιωτικό κλειδί του χρήστη, το συμπιεσμένο μήνυμα αποκρυπτογραφείται χρησιμοποιώντας τον κατάλληλο αλγόριθμο και στο τέλος η PGP αποσυμπιέζει το μήνυμα.

4.3 Ασφάλεια στο Διαδίκτυο

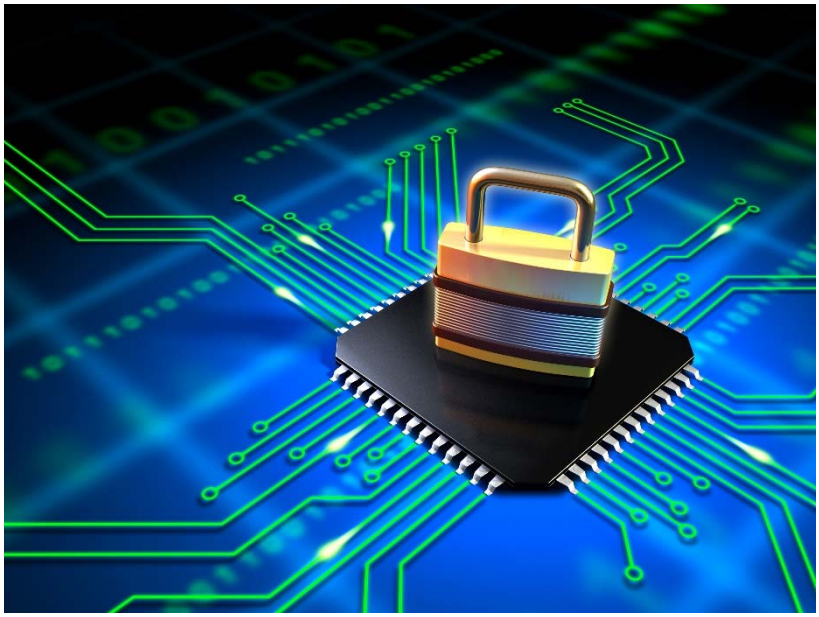
Διαδίκτυο (αγγλ. Internet) είναι παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών, οι οποίοι χρησιμοποιούν καθιερωμένη ομάδα πρωτοκόλλων, η οποία συχνά αποκαλείται "TCP/IP" (αν και αυτή δεν χρησιμοποιείται από όλες τις υπηρεσίες του Διαδικτύου) για να εξυπηρετεί εκατομμύρια χρηστών καθημερινά σε ολόκληρο τον κόσμο. Οι διασυνδεδεμένοι ηλεκτρονικοί υπολογιστές ανά τον κόσμο, οι οποίοι βρίσκονται σε ένα κοινό δίκτυο επικοινωνίας, ανταλλάσσουν μηνύματα (πακέτα) με τη χρήση διαφόρων πρωτοκόλλων (τυποποιημένοι κανόνες επικοινωνίας), τα οποία υλοποιούνται σε επίπεδο υλικού και λογισμικού. Το κοινό αυτό δίκτυο καλείται Διαδίκτυο.

Το διαδίκτυο αποτελεί ένα παγκόσμιο και χαμηλού κόστους μέσο για τη διακίνηση πληροφοριών και την παροχή υπηρεσιών. Διαδεδομένη χρήση του Διαδικτύου σε εφαρμογές που περιλαμβάνουν επικοινωνία ευαίσθητων δεδομένων είναι:

- τραπεζικές συναλλαγές
- ηλεκτρονικό εμπόριο
- ιατρική πληροφορία

Η ασφάλεια της πληροφορίας αποτελεί σημαντικό ζήτημα για την ηλεκτρονική κοινωνία

Οι αδυναμίες που παρουσιάζει το διαδίκτυο στο θέμα της ασφάλειας των διακινούμενων πληροφοριών και της ασφαλούς πρόσβασης σε εφαρμογές, οφείλονται στον σχεδιασμό του πρωτοκόλλου TCP/IP. Οι σχεδιαστές του IP δημιούργησαν ένα απλό και εύκολο στη χρήση πρωτόκολλο, με αποτέλεσμα να μην είναι ασφαλές. Τα ασφαλή συστήματα πρέπει να βασίζονται: στην αυθεντικοποίηση των χρηστών και στην κρυπτογραφία.



4.3.1. Επιθέσεις σε Αλγορίθμους Συμμετρικού Κλειδιού

Υπάρχουν διάφοροι τρόποι με τους οποίους ένας αλγόριθμος συμμετρικού κλειδιού μπορεί να δεχθεί επίθεση. Ο πιο απλός είναι η δοκιμή όλως των δυνατών κλειδιών μέχρι να προκύψει κάποιο κείμενο που φαίνεται να έχει λογικό περιεχόμενο. Αυτό μπορεί να φαίνεται μια όχι και τόσο εύκολη δυνατότητα αλλά αν το μέγεθος του κλειδιού είναι σχετικά μικρό, τότε είναι εφικτό. Ωστόσο όταν χρησιμοποιούνται μεγάλα κλειδιά, για παράδειγμα με 128 bits, αυτή η μέθοδος γίνεται ανέφικτη.

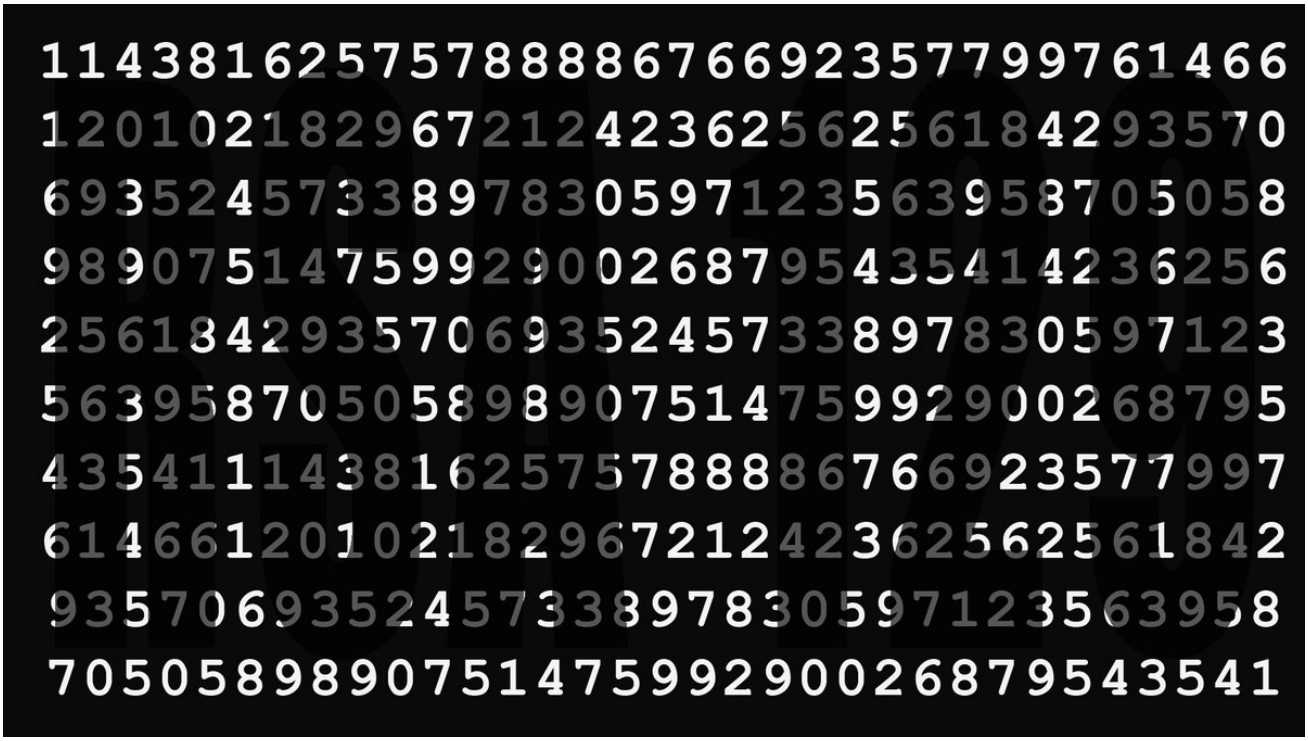
4.3.2 Επιθέσεις σε Συστήματα Δημοσίου Κλειδιού

Υπάρχουν δυο είδη επιθέσεων σε συστήματα δημοσίου κλειδιού. Η πρώτη είναι επίθεση με δεδομένα (factoring attack). Οι γνωστές μέθοδοι κρυπτογραφίας δημοσίου κλειδιού βασίζονται στην τεράστια δυσκολία επίλυσης αντεστραμμένων προβλημάτων. Όποιος μπορεί να αναλύσει μεγάλους αριθμούς μπορεί να σπάσει και ένα σύστημα δημοσίου κλειδιού βασιζόμενος σε ανάλυση. Αυτό δεν είναι απίθανο: μαθηματικοί που δουλεύουν στην περιοχή την θεωρίας αριθμών έχουν μελετήσει προβλήματα ανάλυσης για καιρό και είναι πετυχημένοι με αριθμούς που έχουν συγκεκριμένα χαρακτηριστικά.

Η επίθεση RSA-129

Η πιο διάσημη επίθεση ανάλυσης έγινε στον αριθμό RSA-129 (129 ψηφία). Αυτός ο μεγάλος αριθμός παρουσιάστηκε σε ένα τεύχος του περιοδικού Popular Science το1977. Τελικά αναλύθηκε από μια ομάδα ερευνητών υπό τον Arjen Lenstra.

Η άλλη τεχνική που εφαρμόζεται για το σπάσιμο μιας κρυπτογραφίας δημοσίου κλειδιού είναι να βρεθεί κάποιο μειονέκτημα στον αλγόριθμο που χρησιμοποιείται. Για παράδειγμα, ένα από τα πρώτα προβλήματα που παρουσιάστηκαν είναι το knapsack. Βρέθηκε ότι είναι εύκολο να εξακριβωθεί το ιδιωτικό κλειδί από το δημόσιο κλειδί σε ένα σύστημα με αυτό το πρόβλημα.



Κρυπτογραφία ελλειπτικής καμπύλης.

Μια πολλά υποσχόμενη μορφή κρυπτογραφίας που απειλεί να ξεπεράσει τη χρήση ανάλυσης στα συστήματα δημοσίου κλειδιού είναι η κρυπτογραφία ελλειπτικής καμπύλης. περιλαμβάνει την επίλυση δύσκολων υπολογιστικά προβλημάτων χρησιμοποιώντας μια οικογένεια καμπυλών, γνωστές σαν ελλειπτικές καμπύλες. Πολλά συστήματα δημοσίου κλειδιού χρησιμοποιούν τον RSA. Παρόλα αυτά, Η αυξανόμενη ισχύς των υπολογιστών έφερε και την αύξηση του μήκους των bit, που οδήγησε σε ακόμη μεγαλύτερες υπολογιστικές απαιτήσεις. Η κρυπτογραφία ελλειπτικής καμπύλης είναι το ίδιο ασφαλή με τον RSA. Όμως, απαιτεί μικρότερα μήκη bit και συνεπώς λιγότερους υπολογισμούς.

5. Εφαρμογές Κρυπτογραφίας

Η κρυπτογραφία είναι επιστήμη που με τη βοήθεια των μαθηματικών επιτυγχάνει την κωδικοποίηση και αποκωδικοποίηση δεδομένων. Πρόκειται για ένα σύνολο μαθηματικών τεχνικών που στοχεύουν στην ασφάλεια μετάδοσης της πληροφορίας. Οι ακολουθούμενοι μέθοδοι καθιστούν ευαίσθητα δεδομένα, προσβάσιμα μόνο από – αποκλειστικά για αυτό το σκοπό – εξουσιοδοτημένα άτομα , εξασφαλίζοντας έτσι το απόρρητο της διαδικασίας. Το αρχικό κομμάτι της πληροφορίας ονομάζεται απλό κείμενο (plaintext) ενώ το μήνυμα που προκύπτει από την κρυπτογράφηση του ονομάζεται κρυπτογράφημα (ciphertext). Αποκρυπτογράφηση (decryption) είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή αντίστροφου αλγόριθμου.

Η κρυπτογραφία χρησιμοποιείται σε ένα μεγάλο εύρος εφαρμογών. Η σημαντικότητα της κρυπτογραφίας θα αυξάνεται όσο θα αυξάνεται και ο όγκος των πληροφοριών που θα αποθηκεύονται και θα μεταδίδονται ηλεκτρονικά. Η κρυπτογραφία βρίσκει σήμερα πολλές εφαρμογές στους παρακάτω τομείς:

- Ασφάλεια συναλλαγών σε τράπεζες (Α.Τ.Μ)
- Κινητή τηλεφωνία.
- Σταθερή τηλεφωνία (cryptophones).
- Διασφάλιση εταιρικών πληροφοριών.
- Στρατιωτικά δίκτυα.
- Διπλωματικά δίκτυα.
- Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές).
- Ηλεκτρονική ψηφοφορία.
- Ηλεκτρονική δημοπρασία.
- Ηλεκτρονικό γραμματοκιβώτιο.
- Συστήματα συναγερμών.
- Συστήματα βιομετρικής αναγνώρισης.
- Έξυπνες κάρτες.
- Ιδιωτικά δίκτυα.
- World Wide Wed.
- Δορυφορικές εφαρμογές (δορυφορική τηλεόραση).
- Ασύρματα δίκτυα (bluetooth).
- Συστήματα ιατρικών δεδομένων.
- Τηλεσυνδιάσκεψη.

Μερικές εφαρμογές στις οποίες χρησιμοποιείται η κρυπτογραφία αναλυτικότερα είναι οι ακόλουθες:

Ηλεκτρονικό ταχυδρομείο.

Τα δεδομένα ενός μηνύματος ηλεκτρονικού ταχυδρομείου στέλνονται συνήθως μέσω μη ασφαλών καναλιών επικοινωνίας, όπως το Internet. Η χρήση, αλλά και κατάχρηση, του Internet έχει καταστήσει απαραίτητη την κρυπτογράφηση των μηνυμάτων που αποστέλλονται μέσω της υπηρεσία του ηλεκτρονικού ταχυδρομείου δεδομένου ότι η εξασφάλιση της έχει ως αποτέλεσμα την αποστολή κρίσιμων πληροφοριών.

Ασφαλείς συναλλαγές στο Internet – Ψηφιακές Συναλλαγές (Digital transactions).

Από τη στιγμή που οικονομικές συναλλαγές λαμβάνουν χώρα και μέσω δικτύων (γενικότερα μέσα σε ένα ηλεκτρονικό επιχειρηματικό περιβάλλον), η αυθεντικοποίηση των συναλλαγών είναι ζωτικής σημασίας για την αποφυγή εξαπάτησης κάποιου από τους συναλλασσόμενους. Το πρωτόκολλο SSL αποτελεί το πιο επιτυχημένο πρότυπο κρυπτογραφημένης επικοινωνίας. Έρευνες αποδεικνύουν ότι συνεχώς αυξάνόμενο είναι το ποσοστό των διακτυακών τόπων που προσφέρουν κρυπτογράφηση SSL. Επίσης, σημαντικά έχει αυξηθεί και ο αριθμός των Αρχών Πιστοποίσης (Certification Authorities), οι οποίες προδφέρουν πιστοποιητικά SSL τόσο για servers όσο και για clients. Το SSL χρησιμοποιείται κυρίως για την παροχή ενός ασφαλούς καναλιού επικοινωνίας μεταξύ servers και clients για τη μετάδοση πληροφοριών, όπως passwords, αριθμοί πιστωτικών καρτών.

Εθνική Ασφάλεια

Η κρυπτογραφία έχει διαδραματίσει, και συνεχίζει να διαδραματίζει, καθοριστικό ρόλο σε σημαντικό αριθμό στρατιωτικών υποθέσεων. Οι πρεσβείες των κρατών μεταδίδουν και δέχονται διαρκώς κρίσιμες πληροφορίες των οποίων η εμπιστευτικότητα πρέπει να εξασφαλίζεται.

«Έξυπνες κάρτες» (Smart Cards).

Η κρυπτογραφία χρησιμοποιείται στις έξυπνες κάρτες λόγω της αυξανόμενης χρήσης της ως μηχανισμού λογικής και φυσικής πρόσβασης σε ευαίσθητες πληροφορίες και χώρους.

Πρόσβαση σε ασφαλείς διαδικτυακούς τόπους.

Η αποδοχή της Αρχής Πιστοποίησης συνεπάγεται την προσθήκη ψηφιακών ποστοποιητικών στον browser του χρήστη του Internet. Με βάση τα ιδιαίτερα χαρακτηριστικά του πιστοποιητικού αυτού, ο χρήστης έχει τη δυνατότητα να επισκεφθεί ασφαλείς διαδικτυακούς τόπους και να προσπελάσει δεδομένα χωρίς αυτά να είναι δημοσιευμένα σε κοινή θέα.

Εικονικά Ιδιωτικά Δίκτυα (VPNs).

Οι routers και οι firewalls χρησιμοποιούν κρυπτογραφία για την ασφαλή σύνδεση ενός υπολογιστή με ένα εταιρικό δίκτυο.

Κρυπτογράφηση αρχείων και αποθηκευτικών μέσων.

Τα ιδιωτικά δεδομένα που περιέχονται στο σύστημα αρχείων πρέπει να προστατευθούν από πιθανές επιθέσεις κάποιου αντιπάλου ο οποίος ίσως να αποκτήσει πρόσβαση μέσω δικτύου στον υπολογιστή ή μπορεί να αποκτήσει το ίδιο το φυσικό μέσο (π.χ. το σκληρό δίσκο) στο οποίο βρίσκεται το σύστημα αρχείων. Ο αντίπαλος θα πρέπει να μην μπορεί να διαβάσει τα ιδιωτικά δεδομένα (ή ακόμα καλύτερα δεν θα πρέπει να μπορεί να διαπιστώσει καν την ύπαρξή τους).

BARCODE ή Γραμμωτός Κώδικας

Ο γραμμωτός κώδικας (barcode) πρωτοεμφανίστηκε στα τέλη της δεκαετίας του 1940 και βασίζεται σε αυστηρές προδιαγραφές. Ένα από τα πλέον διαδεδομένα συστήματα είναι το EAN-13. Αποτελείται από 13 ψηφία με τη μορφή ενός συνδυασμού γραμμών και διαστημάτων. Στον κώδικα υπάρχουν ορισμένες γραμμές που είναι μακρύτερες από τις υπόλοιπες. Στην αρχή και το τέλος υπάρχουν οι γραμμές ορίων που επιτρέπουν σε ένα σαρωτή να προσδιορίσει πού αρχίζει και πού τελειώνει ο κώδικας. Οι δύο μεσαίες γραμμές χωρίζουν τον κώδικα σε δύο τμήματα ώστε να είναι εύκολη, αν χρειαστεί, η πληκτρολόγηση των 13 ψηφίων. Παράλληλα, είναι ευχερέστερη η αποκωδικοποίηση των δύο τμημάτων από το σαρωτή χωριστά, ανεξάρτητα από το αν το προϊόν είναι ανεστραμμένο ή όχι. Τα δύο πρώτα ψηφία από τα 13 του γραμμωτού κώδικα είναι ο κωδικός της χώρας όπου είναι καταχωρημένος ο κατασκευαστής, όχι όμως απαραίτητα και της χώρας που κατασκευάστηκε το προϊόν. Η Σουηδία, για παράδειγμα, έχει κωδικό χώρας 73 και η Ελλάδα 52. Τα επόμενα πέντε ψηφία κωδικοποιούν τον παραγωγό ή τον εισαγωγέα ενώ τα επόμενα πέντε είναι ο αριθμός του προϊόντος που προσδιορίζεται από τον παραγωγό για τη διευκόλυνση παρακολούθησης της αποθήκης του και των πωλήσεών του. Το τελευταίο ψηφίο του κώδικα είναι ψηφίο ελέγχου. Ο σαρωτής διαθέτει έναν τύπο που τον εφαρμόζει πάνω στα δώδεκα πρώτα ψηφία επιβεβαιώνοντας έτσι πως το αποτέλεσμα είναι ίδιο με το ψηφίο ελέγχου.

Ψηφιακή Υπογραφή

Η Ψηφιακή Υπογραφή είναι ένα μαθηματικό σύστημα που χρησιμοποιείται για την απόδειξη της γνησιότητας ενός ψηφιακού μηνύματος ή εγγράφου. Μια έγκυρη ψηφιακή υπογραφή δίνει στον παραλήπτη την πιστοποίηση ότι το μήνυμα που δημιουργήθηκε ανήκει στον αποστολέα που το υπέγραψε ψηφιακά και ότι δεν αλλοιώθηκε-παραποιήθηκε κατά την μεταφορά. Οι ψηφιακές υπογραφές χρησιμοποιούν συνδυασμό μιας κρυπτογραφικής συνάρτησης κατατεμαχισμού (hash function) για δημιουργία της σύνοψης (hash) σε συνδυασμό με ασυμμετρική κρυπτογραφία για κρυπτογράφηση/αποκρυπτογράφηση σύνοψης (ο συνδυασμός σύνοψης και κρυπτογράφησης με ασυμμετρική κρυπτογραφία αποδεικνύει την ακεραιότητας του εγγράφου αλλά και την απόδειξη ταυτότητας του αποστολέα).

5.1 Βιομετρικά Συστήματα

Όλα τα κινητά τελευταίας τεχνολογίας είναι εξοπλισμένα με fingerprint scanner (αναγνώστη δακτυλικού αποτυπώματος) που λειτουργούν ως fingerprint_featuredένα επιπλέον μέτρο ασφάλειας. Είναι όμως τόσο ασφαλή όσο οι εταιρείες κινητής τηλεφωνίας λένε ότι είναι;

Ας ξεκινήσουμε με το γεγονός ότι τα fingerprint scanner δεν είναι αλάνθαστα. Ειδικά τα πρώτα κινητά που διαθέτουν αυτήν την τεχνολογία, έχουν πρόβλημα στην ανάγνωση του δακτυλικού αποτυπώματος όταν το δάκτυλο που σκανάρουν είναι βρώμικο, ιδρωμένο ή έχει ουλές. Αυτό γιατί πολλοί αισθητήρες σκανάρουν το δακτυλικό αποτύπωμα σαν φωτογραφία και αυτό έχει ως αποτέλεσμα να μην μπορεί να διακρίνει το πραγματικό δάκτυλο από ψεύτικο. Αυτό είναι και το μεγαλύτερο πρόβλημα στην ασφάλεια των συσκευών. Πολλά από αυτά τα προβλήματα θα λυθούν όταν η υπερηχητική τεχνολογία σκαναρίσματος εμφανιστεί στις συσκευές. Το πρόβλημα ασφαλείας των fingerprint scanners εμφανίστηκε στις αρχές του 2015, όταν πρωτοεμφανίστηκε αυτή η τεχνολογία, και είχε ως αποτέλεσμα χάκερ να καταφέρουν να κλέψουν τις φωτογραφίες με τα δακτυλικά αποτυπώματα του χρήστη, και να ξεκλειδώσουν τα τηλέφωνα.

Επιστήμονες κατάφεραν να αποδείξουν πόσο εύκολα μπορεί να κλαπεί ένα δακτυλικό αποτύπωμα, από μια φωτογραφία υψηλής vkansee-fingerprint-scanner-02ανάλυσης, τραβηγμένη από SLR φωτογραφική fingeprintμηχανή με δυνατό ζουμ, ακόμα και από μια φωτογραφία περιοδικού σε υψηλή ανάλυση μπορεί να κάνει την ίδια δουλειά (με την ίδια μέθοδο μπορεί να υποκλαπεί και η ίριδα του ματιού, για ξεκλείδωμα τηλεφώνων με iris scanner). Όταν έχει μαθευτεί ένας κωδικός ξεκλειδώματος μπορείτε πολύ απλά να τον αλλάξετε χωρίς κανένα πρόβλημα.

Σε αντίθετη περίπτωση, με το δακτυλικό αποτύπωμα δεν μπορείτε να κάνετε κάτι τέτοιο. Αυτός είναι και ο λόγος που δεν πρέπει να εμπιστεύεστε τις διαφημίσεις του marketing για την ασφάλεια του fingerprint scanner.

Αν διαθέτετε συσκευή με αυτή την τεχνολογία, σας παραθέτουμε ορισμένες συμβουλές να ακολουθήσετε για την ασφάλεια της συσκευής σας:

- Μην χρησιμοποιείτε τον αναγνώστη δακτυλικού αποτυπώματος για να ξεκλειδώνετε τραπεζικές εφαρμογές (παρόλο που οι εταιρείες κινητής τηλεφωνίας λένε το αντίθετο). Αν κλαπεί το κινητό σας, το δακτυλικό αποτύπωμά σας βρίσκεται στην επιφάνεια της συσκευής και μπορεί να αντιγραφεί πολύ εύκολα.fingerprintsensor
- Οι περισσότεροι χρησιμοποιούν τον δείκτη ή τον αντίχειρα για το ξεκλείδωμα της συσκευής, όταν αυτά τα δάχτυλα είναι αυτά που χρησιμοποιούνται περισσότερο για την λειτουργεία της, και είναι εύκολο να αντιγραφούν από την οθόνη ή από άλλα μέρη.
- Αν παρόλα αυτά χρησιμοποιείτε fingerprint scanner, θα ήταν πιο φρόνιμο να χρησιμοποιήσετε και άλλη εφαρμογή για επιπλέων ασφάλεια. Όπως για παράδειγμα μια εφαρμογή για εντοπισμό της συσκευής, και για απομακρυσμένο έλεγχο (διαγραφή, κλείσιμο, καθαρισμός προσωπικών δεδομένων).

Σε γενικές γραμμές οι αναγνώστες δακτυλικού αποτυπώματος είναι μια τεχνολογία που χρησιμοποιείται για να κάνουν την ζωή μας πιο εύκολη αλλά μην βασίζεστε απόλυτα σε αυτή. Χρησιμοποιείστε δικλίδες ασφαλείας, όπως είναι κωδικοί πρόσβασης και άλλα μέτρα ασφαλείας.

Με τους σαρωτές δακτυλικού αποτυπώματος να έχουν εισέλθει στον χώρο των smartphones εδώ και καιρό, η Fujitsu πήγε ένα βήμα παραπέρα, ανακοινώνοντας ότι έχει αναπτύξει ένα σύστημα αναγνώρισης της ίριδας του ματιού, το οποίο και ενσωμάτωσε ένα πρωτότυπο smartphone.

Απλά και μόνο κοιτώντας την οθόνη του smartphone, η ίριδα του χρήστη σαρώνεται και το τηλέφωνο ξεκλειδώνει.

Όπως υποστηρίζει η εταιρεία, το εν λόγω σύστημα έχει σαφές πλεονέκτημα έναντι των κωδικών ή των δακτυλικών αποτυπωμάτων, καθώς είναι δύσκολο να πλαστογραφηθεί και βολικό στη χρήση. Η οθόνη ξεκλειδώνεται με το βλέμμα, κάτι που σημαίνει πως τα χέρια του χρήστη είναι ελεύθερα σε κάθε περίπτωση. την ουσία αυτό που έκανε η εταιρεία ήταν να συρρικνώσει και να βελτιώσει την παρούσα τεχνολογία αναγνώρισης ίριδας (η οποία σταματά να αλλάζει μετά την ηλικία των δύο ετών, και είναι μοναδική σε κάθε άνθρωπο), έτσι ώστε να είναι δυνατή η ενσωμάτωσή της σε smartphone. Το σύστημα «διαβάζει» το μάτι με υπέρυθρο LED φως, τραβώντας μια φωτογραφία για να αποθηκεύσει το σχήμα της, που στη συνέχεια χρησιμοποιείται για σύγκριση/ επιβεβαίωση.

Τα δύο βασικά τμήματα του συστήματος είναι μία ειδική, υψηλών επιδόσεων LED, και μία ειδική υπέρυθρη κάμερα, σε συνδυασμό με τεχνολογίες ελέγχου κάμερας και βιομετρικής ταυτοποίησης που αναπτύσσονταν εδώ και χρόνια.

Όσον αφορά στην εμβέλειά του, η απόσταση που απαιτείται είναι η κανονική που κρατά ένας χρήστης όταν χρησιμοποιεί το κινητό του- δηλαδή δεν απαιτείται να πλησιάσει το μάτι στα 10 εκατοστά. Σημειώνεται ότι, βάσει δοκιμών που έχουν γίνει, το υπέρυθρο φως LED είναι ακίνδυνο για τα μάτια.

Βιομετρική τεχνολογια

Η βιομετρική τεχνολογία σήμερα, προσφέρει πολλά περισσότερα από το να χρησιμοποιείται σαν μία τεχνολογία για την καταπολέμηση της εγκληματικότητας. Πλέον αποτελεί μία σύγχρονη υψηλή τεχνολογία όπου μπορεί να εφαρμοστεί σε κάθε είδους πληροφοριακό σύστημα εκμεταλλευόμενη τα φυσιολογικά και συμπεριφοριστικά χαρακτηριστικά του ατόμου με στόχο την προστασία πρόσβασης σε χώρους ευαίσθητων πληροφοριών και δεδομένων.

Με τα τεχνολογικά και οικονομικά εμπόδια να αποτελούν πλέον παρελθόν, η βιομετρική τεχνολογία θα πρέπει να εξεταστεί ενδελεχώς και να γίνει κατανοητό μέχρι πιο βαθμό μπορεί να χρησιμοποιηθεί και να εφαρμοστεί και με ποιον τρόπο. Η ευρύτερη εφαρμογή της στο χώρο της ασφάλειας αποσκοπεί στην εξέλιξη των παραδοσιακών συστημάτων πρόσβασης (access control) τα οποία κατά κανόνα βασίζονται στη χρήση μαγνητικών και RFID (proximity) καρτών των οποίων το τρωτότερο σημείο είναι η υπόθεση πως ο φερόμενος χρήστης της είναι ο νόμιμος και πραγματικός κάτοχος, που όμως δεν είναι απαραίτητα αληθές καθώς μέσω αυτής της τεχνολογίας δεν προσφέρεται καμία δυνατότητα ταυτοποίησης. Η βιομετρική (ψηφιακή) τεχνολογία έρχεται συμπληρωματικά να καλύψει το συγκεκριμένο κενό ασφάλειας προσθέτοντας ευφυείς μονάδες ταυτοποίησης που εστιάζουν στην αναγνώριση της ταυτότητας ενός ατόμου μέσα από χαρακτηριστικά που υποσυνείδητα χρησιμοποιεί και ο ανθρώπινος εγκέφαλος, π.χ. 3Δ χαρακτηριστικά προσώπου και βαδίσματος. Ο μη παρεμβατικός τρόπος συλλογής του βιομετρικού προφίλ των ατόμων δεν αλλάζει τις καθημερινές συνήθειές τους και αποκλείει μόνο ένα πολύ μικρό ποσοστό κοινωνικών ομάδων, ενώ οι εξελιγμένες τεχνικές κρυπτογραφίας και ασφάλειας διασφαλίζουν ότι τα δεδομένα δεν μπορούν να υποκλαπούν και να χρησιμοποιηθούν σε άλλες εφαρμογές.

Αντικείμενο του ερευνητικού έργου Ασφαλείς και Ανακλήσιμες Βιομετρικές Ταυτότητες για Χρήση σε Περιβάλλοντα Διάχυτης Νοημοσύνης, με διακτριτικό τίτλο «ΒΙΟΤΑΥΤΟΤΗΤΑ» είναι η δημιουργία ενός ολοκληρωμένου πλαισίου ασφαλείας που θα υποστηρίζει την αυθεντικοποίηση ατόμων σε ολοκληρωμένες και ασφαλείς υπηρεσίες πληροφοριακών συστημάτων καθώς και σε χώρους υποδομών ασφαλείας, με τη χρήση βιομετρικών προτύπων και προηγμένων τεχνολογιών κρυπτογράφησης και κωδικοποίησης αυτών. Το προτεινόμενο πλαίσιο ασφαλείας θα μπορεί αφενός να ενσωματωθεί σε υπάρχοντα πληροφοριακά συστήματα παλαιότερων γενεών (legacy systems) καθώς και να προσαρμοστεί σε σύγχρονες ηλεκτρονικές υπηρεσίες και πληροφοριακά συστήματα ευρείας κλίμακας, επιτρέποντας έτσι όπου και όταν απαιτείται την

ασφαλέστερη πρόσβαση σε εξουσιοδοτημένες υπηρεσίες ηλεκτρονικής διακυβέρνησης, λήψης αποφάσεων κ.ά.

Οι δράσεις του έργου ΒΙΟΤΑΥΤΟΤΗΤΑ (http://biotaytotita.encodegroup.com/) περιλάμβαναν, μεταξύ άλλων, τη μελέτη και καταγραφή της βιομετρικής αγοράς (κυρίως στην ευρωπαϊκή και ελληνική αγορά), ώστε να δημιουργηθεί μια εκτεταμένη τεχνολογική στάθμιση στις σημαντικότερες βιομετρικές μεθόδους και να αναλυθούν τα τεχνολογικά τους χαρακτηριστικά καθώς και η πρακτική λειτουργικότητα τους. Με αυτήν την μελέτη αποτυπώνονται τα κυριότερα ζητήματα ασφάλειας που καλούνται να αντιμετωπίσουν τα σύγχρονα βιομετρικά συστήματα όπως και αυτό της ΒΙΟΤΑΥΤΟΤΗΤΑΣ. Ο στόχος αυτός μας οδήγησε στη βαθύτερη ανάλυση των κριτηρίων επιλογής εξοπλισμού βιομετρικών συστημάτων ώστε να διατηρηθεί το υψηλό επίπεδο ασφάλειας που έθεσαν οι Έλληνες ερευνητές ώστε το σύστημα να μπορεί να εφαρμοστεί σε όλες τις περιπτώσεις που ζητείται πιστοποιημένη είσοδος του ατόμου (διαβαθμισμένη πρόσβαση σε χώρους), διατηρώντας παράλληλα την απλότητα της καθημερινής χρήσης του.

Μελλοντικές Προκλήσεις - Σύνοψη

Για την τεχνολογική ενίσχυση συστημάτων βασισμένων σε βιομετρικές τεχνολογίες και τη χρήση των βιομετρικών χαρακτηριστικών, η εισαγωγή της μονάδας κρυπτογράφησης εξασφαλίζει όχι μόνο ένα νέο επίπεδο επιπρόσθετης ασφάλειας αλλά παρέχει την εξασφάλιση του ίδιου του ατόμου και των προσωπικών του δεδομένων.

Η επίλυση των ηθικών και νομικών ζητημάτων με την εφαρμογή της μονάδας κρυπτογράφησης των ήδη κατακερματισμένων διανυσμάτων που εξάγονται από τα βιομετρικά δεδομένα (1ος βαθμός ασφάλειας) συμβάλλει στη δημιουργία ενός ασφαλούς βιομετρικού συστήματος ως προς τους συμμετέχοντες και επιτρέπει την εφαρμογή του σε χώρους όπου η διαβαθμισμένη-αυτοματοποιημένη πρόσβαση είναι απαραίτητη αποκλείοντας έτσι την εφαρμογή του για τον έλεγχο και την δημιουργία νέων τύπων βιομετρικής ταυτότητας με σεβασμό προς το άτομο.

Συνοψίζοντας, δεν θα πρέπει να παραληφθεί ότι για τη δημιουργία του συστήματος «ΒΙΟΤΑΥΤΟΤΗΤΑΣ» εφαρμόστηκε το χρυσό τρίπτυχο του CIA Μοντέλου (Confidentiality, Integrity & Authenticity – Εμπιστευτικότητα, Ακεραιότητα, Αυθεντικοποίηση) προσθέτοντας την επιπρόσθετη έννοια της Εξουσιοδότησης-Authorization. Με τον τρόπο αυτό καταφέρνουμε να εφαρμόσουμε το χρυσό τρίπτυχο ασφάλειας για τα πληροφοριακά συστήματα:

1. Κάτι που γνωρίζουμε (PIN)
2. Κάτι που κατέχουμε (smart card)
3. Κάτι μοναδικό που μας χαρακτηρίζει (βιομετρικό χαρακτηριστικό)

Η μελλοντική πρόκληση είναι η περαιτέρω βελτιστοποίηση του συστήματος που θα βασίζεται σε δυναμικά χαρακτηριστικά συμπεριφοράς και όχι φυσιολογίας ώστε να ενισχυθούν οι παρούσες τεχνικές ασφάλειας, όπως αυτή των κωδικών σε έξυπνες κάρτες με τεχνικές βιομετρικού κατακερματισμού, μη θέτοντας σε κίνδυνο τα προσωπικά δεδομένα.

Πηγές

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

http://www.cyber-rights.org/crypto/cryptog.htm

http://www.comsol.gr/dat/04FFDD5A/file.pdf

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

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

http://users.teilam.gr/~klimn/cryptography/Lec1.pdf

http://users.sch.gr/geokasap/site/index.php/component/attachments/download/57

http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas- aris_ptyxiakh/Phtml/steganografia.htm

http://h2g2.com/approved_entry/A1315919