ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

Τίτλος εργασίας: *ΑΣΦΑΛΗΣ ΤΡΑΠΕΖΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ ΜΕ ΤΗΝ ΜΕΘΟΔΟ ΚΡΥΦΟΥ ΚΛΕΙΔΙΟΥ DES*

Πτυχιακή εργασία των

Φαφαλιός Παύλος

Παρσάνος Θεοφάνης

Μαυρογιαννάκη Ευαγγελία

Επιβλέπων: **κα Αντωνοπούλου Ήρα**

Καθηγήτρια

Πάτρα 2008

“ το πιο ασφαλές πληροφοριακό σύστημα
είναι εκείνο κατά το οποίο
οι υπολογιστές είναι εκτός λειτουργίας
δηλαδή σβησμένοι”

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΡΥΠΤΟΓΡΑΦΙΑ

Σχήμα κρυπτογράφησης DES

ΚΕΦΑΛΑΙΟ 8^{ο} :DES

ΚΕΦΑΛΑΙΟ 9^{ο} : Άλλα κρυπτογραφικά σχήματα

ΚΕΦΑΛΑΙΟ10^{ο} : Ελληνική τραπεζική εμπειρία

Εισαγωγή

Αναμφισβήτητα ζούμε σε μία εποχή όπου οι πληροφορίες έχουν αρχίσει να γίνονται όλο και πιο σημαντικές για τις επιχειρήσεις. Τάση, μάλιστα, που φαίνεται πώς θα συνεχιστεί για μία μακρά ακόμη περίοδο. Γι' αυτό το λόγο, κάθε σύγχρονη επιχείρηση πρέπει να γνωρίζει ποιες πληροφορίες της είναι πολύτιμες, πώς μπορεί να τις διαχειριστεί και να τις προστατεύσει.

Θεμελιώδη ρόλο, δηλαδή, για την παρουσία και τη λειτουργία κάθε εταιρίας σε ένα δικτυωμένο περιβάλλον παίζει η ασφάλεια των πληροφοριών της. Και αυτό γιατί όλες οι εταιρίες πια χρησιμοποιούν πληροφορίες σε ψηφιακή μορφή για να διεκπεραιώνουν τις καθημερινές τους λειτουργίες. Έτσι, έχουν αποθηκευμένα δεδομένα για τους πελάτες τους, τα προϊόντα τους, τα οικονομικά τους αποτελέσματα, το προσωπικό τους κλπ, τα οποία σε καμία περίπτωση δεν πρέπει να γίνουν προσβάσιμα από τους ανταγωνιστές ή τρίτους, να καταστραφούν ή ακόμη και να μην είναι διαθέσιμα ακαριαία. Η απώλεια δεδομένων, όπως τα παραπάνω, μπορεί να οδηγήσει σε απώλεια πελατών ή και αξιοπιστίας της επιχείρησης, προκαλώντας προβλήματα λειτουργίας και σημαντικές επιπτώσεις στην κερδοφορία.

Η ανάπτυξη του διαδικτύου, το ηλεκτρονικό εμπόριο και οι συναλλαγές μέσω ανοιχτών δικτύων κάνουν επιτακτική την ανάγκη ασφάλειας στις συναλλαγές. Ο χρήστης που συναλλάσσεται ηλεκτρονικά απαιτεί τα δεδομένα (π.χ. ένα μήνυμα ή ένα κείμενο) που στέλνει να μην μπορούν να αποκαλυφθούν ή να διατεθούν σε μη εξουσιοδοτημένα για αυτό άτομα (*εμπιστευτικότητα*). Τα δεδομένα, δεν θα πρέπει να είναι δυνατόν να αλλοιωθούν κατά την μετάδοσή τους. Ο παραλήπτης θα πρέπει να τα λάβει όπως ακριβώς ο αποστολέας τα έστειλε και να είναι σίγουρος ότι τα δεδομένα που λαμβάνει είναι αυτά που ο αποστολέας έχει στείλει (*ακεραιότητα*).

Επιπλέον, σε μία τέτοια συναλλαγή, είναι απαραίτητο ο παραλήπτης να είναι σίγουρος για την ταυτότητα του αποστολέα (*αυθεντικότητα*). Δηλαδή, να γνωρίζει με σιγουριά ότι το μήνυμα που λαμβάνει και φαίνεται να το υπογράφει ο κ. Χ, είναι όντως από τον κ. Χ και όχι από κάποιον που παριστάνει τον κ. Χ. Τέλος, συμμετέχοντας σε μία ηλεκτρονική συναλλαγή (π.χ. ηλεκτρονικό εμπόριο) θα πρέπει

να μην είναι δυνατόν τα εμπλεκόμενα μέρη να αρνηθούν εκ των υστέρων την συμμετοχή τους στη συναλλαγή αυτή (*μη αποποίηση ευθύνης*).

Οι παραπάνω ιδιότητες, (εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα, μη αποποίηση) στον ηλεκτρονικό κόσμο, αποτελούν αντικείμενο της επιστήμης που ασχολείται με την ασφάλεια των πληροφοριών. Διάφοροι μηχανισμοί, τεχνικές και τεχνολογίες έχουν αναπτυχθεί αποσκοπώντας να διασφαλίσουν τις ιδιότητες αυτές σε μία ηλεκτρονική συναλλαγή.

Σκοπός της παρούσας εργασίας

Σκοπό της παρούσας εργασίας αποτέλεσε η διερεύνηση των δυνατοτήτων αποτελεσματικότερης διαχείρισης της γνώσης που σχετίζεται με την ασφάλεια. Στο πλαίσιο πραγματοποίησης της εργασίας επιχειρείται η παρουσίαση με όσο το δυνατόν πιο απλό τρόπο της ασφάλειας στις τραπεζικές συναλλαγές. Επίσης γίνεται μια παρουσίαση των γνωστότερων κρυφών κλειδιών που υπάρχουν δίνοντας μεγαλύτερο βάρος στη μέθοδο του κρυφού κλειδιού (πρότυπο DES). Στη παρούσα μελέτη προσπαθήσαμε να περιορίσουμε τις τεχνικές αναφορές στο βαθμό που αυτές είναι απαραίτητες για την κατανόηση του θέματος.

Αντικείμενο της διπλωματικής

Τι είναι κίνδυνος; Κίνδυνος είναι *η πιθανότητα εμφάνισης μίας απειλής*, και όπως γίνεται κατανοητό ο κίνδυνος ως ένα σημείο δεν μπορεί να αποφευχθεί. Για αυτό κάθε εταιρεία θα πρέπει να αποδέχεται κάποιο βαθμό κινδύνου κατά τη λειτουργία της, ο οποίος και θα πρέπει να είναι όσο πιο μικρός γίνεται.

Αν λοιπόν για κάθε εταιρία είναι τόσο σημαντική η μείωση του κινδύνου και έχει τόση σημασία η ασφάλεια των δεδομένων της, είναι εύκολο να κατανοήσουμε πόσο παραπάνω ευαίσθητη είναι μία τράπεζα στο ζήτημα της ασφάλειας τον Πληροφοριακών Συστημάτων. Αρκεί να φανταστούμε τι επιπτώσεις θα υπήρχαν αν μέρος των τραπεζικών συναλλαγών του κοινού γινόταν λανθασμένα ή ακόμα ποιος θα ήταν ο αντίκτυπος ενδοιασμών και φόβων του κοινού σχετικά με την ακεραιότητα

των πληροφοριακών συστημάτων της τράπεζας και του ενδεχομένου παραβίασης τους από τρίτους, και αμέσως καταλαβαίνουμε γιατί η ασφάλεια των Πληροφοριακών Συστημάτων στις τράπεζες αποκτά βαρύνουσα σημασία.

Αντικείμενο της παρούσας εργασίας είναι να εξετάσουμε το θεωρητικό πλαίσιο της ασφάλειας των Πληροφοριακών Συστημάτων, μέσα από μία συστηματική παρουσίαση της σύγχρονης ελληνικής και ξένης βιβλιογραφίας και αρθογραφίας. Ευελπιστούμε ότι μέσα από την παρούσα διπλωματική εργασία ο αναγνώστης θα αντιληφθεί την ασφάλεια και τη διαχείριση ευαίσθητων δεδομένων από το τραπεζικών χώρο με τη μέθοδο κρυφών κλειδιών.

Σε όλη την εργασία έγινε προσπάθεια να αποφευχθούν όσο το δυνατόν γίνεται τα πολύ τεχνικά ζητήματα και να μείνει η τεχνική ανάλυση σε πιο εισαγωγικά επίπεδα, ώστε να είναι κατανοητή. Ελπίζουμε πως η παρούσα προσπάθεια θα φανεί χρήσιμη στον αναγνώστη ο οποίος επιθυμεί να κατανοήσει το σημαντικό ζήτημα της ασφάλειας των πληροφοριακών συστημάτων στις τραπεζικές συναλλαγές.

Τα συμπεράσματα που προκύπτουν από την εκπόνηση της διπλωματικής είναι χρήσιμα για μια περεταίρω έρευνα για τα κρυπτογραφικά κλειδιά όπως εξελίσσονται και μεταλλάσσονται, με τη πάροδο του χρόνου και την εξέλιξη της τεχνολογίας και των πληροφοριακών συστημάτων .

Οργάνωση της μελέτης

Η παρούσα εργασία αναφέρεται σε εκείνη τη θεματική ενότητα της Κρυπτογράφησης. Συγκεκριμένα διαπραγματεύεται το ζήτημα της : «Ασφάλειας των τραπεζικών συναλλαγών και τη μέθοδο κρυφού κλειδιού (πρότυπο DES)». Η εν λόγω μελέτη αποτελείται από τρία μέρη για τα οποία πραγματοποιείται μια σύντομη-συνοπτική αναφορά στην συνέχεια.

Το πρώτο μέρος αποτελείται από τρία κεφάλαια, όπου περιγράφεται το εννοιολογικό πλαίσιο το σχετικό με τις γνωστικές περιοχές των τραπεζικών συναλλαγών, του πληροφοριακού συστήματος και της ασφάλειας. Στο τρίτο μέρος επιδιώκοντας να γίνουν οι παραπάνω εννοιολογικές αναφορές (τραπεζικές

συναλλαγές, πληροφορικό σύστημα, ασφάλεια) περισσότερο κατανοητές, παραθέτουμε ένα σύγχρονο παράδειγμα, το e-banking, όπου και οι τρεις έννοιες περιπλέκονται λειτουργώντας με άριστο τρόπο.

Στο δεύτερο μέρος που αποτελείται από τα κεφάλαια 4, 5, 6 και 7 περιέχεται ο κύριος όγκος της συμβολής της εργασίας. Στο κεφάλαιο 4 γίνεται μια αναλυτική περιγραφή της ορολογίας κρυπτογραφία και του περιεχομένου της (συμμετρική και ασύμμετρη κρυπτογραφία). Στη συνέχεια κρίθηκε αναγκαία και η παρουσίαση της εννοιολογικής σημασίας της αποκρυπτογράφησης. Στο κεφάλαιο 5 παρουσιάζεται η κρυπτογραφία μέσα από το πρίσμα της προστασίας των πληροφοριών (μονόδρομες συναρτήσεις, κρυπτανάλυση) καθώς και εφαρμογές της. Στο κεφάλαιο 6 περιγράφεται αναλυτικά ένα από τα χαρακτηριστικότερα παραδείγματα της σύγχρονης κρυπτογραφίας, η ψηφιακή υπογραφή. Τέλος στο κεφάλαιο 7 γίνεται μια σύντομη αναφορά στο νομικό πλαίσιο της κρυπτογραφίας σε Ελλάδα και εξωτερικό.

Το τρίτος μέρος της μελέτης, σχετίζεται με το σχήμα κρυπτογράφησης DES. Παραθέτουμε αναλυτικά την έννοια του κλειδιού, τον τρόπο λειτουργίας του και οτιδήποτε συνθέτει μια ολοκληρωμένη εικόνα του πρότυπου κλειδιού DES. Φυσικά στο επόμενο κεφάλαιο, κεφάλαιο 9, δεν παραλείψαμε να αναφερθούμε και σε άλλα κρυπτογραφικά σχήματα. Τέλος στο κεφάλαιο 10 παραθέτουμε την ελληνική τραπεζική εμπειρία, μέσα από την παρουσίαση των πληροφοριακών συστημάτων και των συστημάτων ασφαλείας δυο μεγάλων τραπεζών που δραστηριοποιούνται στον ελλαδικό τραπεζικό χώρο : της Εθνικής τράπεζας και της Eurobank. Οι πληροφορίες που παρουσιάζονται αντλήθηκαν από το δικτυακό τόπο της κάθε τράπεζας.

Ευχαριστίες

Η παρούσα εργασία, αποτελεί διατριβή που πραγματοποιήθηκε το ακαδημαϊκό έτος 2007-2008, στα πλαίσια του Προπτυχιακού Προγράμματος Σπουδών στο τμήμα Διοίκησης Επιχειρήσεων, υπό την εποπτεία και αρωγή της: Καθηγήτριας κας Αντωνοπούλου Ήρας.

Στο σημείο αυτό θα θέλαμε να ευχαριστήσουμε όλους όσους συνέβαλαν στην διεκπεραίωση αυτής της Διπλωματικής Εργασίας που σηματοδοτεί το πέρας των προπτυχιακών σπουδών στο Τεχνολογικό Εκπαιδευτικό Ίδρυμα Πάτρας. Ευχαριστίες οφείλουμε πρωταρχικά στην καθηγήτρια μας κα Αντωνοπούλου Ήρα για την πρόθυμη και αμέριστη βοήθειά της κατά την συγγραφή της διπλωματικής εργασίας. Η βοήθεια της ήταν καταλυτική διαδραματίζοντας σημαίνοντα ρόλο, μια και πέραν του ιδιαιτέρως συμβουλευτικού της έργου, επιτάχυνε την άντληση των όποιων πρόσθετων πληροφορικών δεδομένων.

Τέλος, ευχαριστούμε από τα βάθη της καρδιάς μας τα μέλη της οικογένειάς μας και τα αγαπημένα μας πρόσωπα για την αγάπη και την εμπιστοσύνη τους καθώς και για το γεγονός ότι μας στήριξαν και μας ενθάρρυναν καθ’ όλη τη διάρκεια των σπουδών μας.

1. Τραπεζικό Σύστημα

ΚΕΦΑΛΑΙΟ 1^{ο} : Τραπεζικές συναλλαγές

1.1. Εισαγωγή στο τραπεζικό σύστημα

Τράπεζα ονομάζεται μια επιχείρηση, η οποία ασχολείται με χρηματικές και πιστωτικές συναλλαγές. Ανάλογα με το είδος της μπορεί να δέχεται καταθέσεις, να χορηγεί δάνεια, να φυλάσσει και να διαχειρίζεται αξιόγραφα, να αναλαμβάνει την πληρωμή για λογαριασμό του πελάτη. Η κερδοφορία της τράπεζας βασίζεται στην λεγόμενη "ψαλίδα", δηλαδή τη διαφορά ανάμεσα στο επιτόκιο δανεισμού και στο επιτόκιο καταθέσεων. Έτσι αν για παράδειγμα μία τράπεζα χορηγεί ένα δάνειο με επιτόκιο 9% και δέχεται κατάθεση με ετήσιο επιτόκιο 2% η διαφορά αυτή (7%) αποτελεί την ψαλίδα που οδηγεί στα κέρδη της τράπεζας. Βέβαια οι τράπεζες αποκομίζουν και από αλλού χρήματα όπως από προμήθειες ή από συμμετοχές και επενδύσεις. Ωστόσο η κύρια λειτουργία της έγκειται στον δανεισμό (χορηγήσεις και καταθέσεις).

Υπάρχουν διάφορα είδη τραπεζών :

Οι κεντρικές τράπεζες ελέγχουν συνήθως τη νομισματική πολιτική και μπορούν να είναι ο δανειστής της τελευταίας λύσης σε περίπτωση κρίσης. Χρεώνονται συχνά με τον έλεγχο του διάθεσης χρήματος, συμπεριλαμβανομένης της έκδοσης νομίσματος. Παραδείγματα κεντρικών τραπεζών είναι η Τράπεζα της Ελλάδος και η Ευρωπαϊκή Κεντρική Τράπεζα.

Εμπορική τράπεζα, είναι ο όρος που χρησιμοποιείται για μια κανονική τράπεζα για να τη διακρίνει από μια τράπεζα επενδύσεων. Μιας και αυτές οι δύο δεν είναι πλέον υποχρεωτικό να λειτουργούν κάτω από χωριστή ιδιοκτησία, ορισμένοι χρησιμοποιούν τον όρο "εμπορική τράπεζα" για να αναφερθούν σε μια τράπεζα ή ένα τμήμα τράπεζας που ασχολείται κυρίως με εταιρίες ή μεγάλες επιχειρήσεις.

Τράπεζες κοινοτικής ανάπτυξης είναι οι τράπεζες που παρέχουν οικονομικές υπηρεσίες και πίστωση σε μη ανεπτυγμένες αγορές ή πληθυσμούς.

Οι επενδυτικές δίνουν εγγυητικές επιστολές για πώληση μετοχών και χρεογράφων και συμβουλεύουν για τις συγχωνεύσεις.

Τα ταχυδρομικά ταμιευτήρια είναι ταμιευτήρια που συνδέονται με τα εθνικά ταχυδρομικά συστήματα. Η Ιαπωνία και η Γερμανία είναι παραδείγματα των χωρών με τα προεξέχοντα ταχυδρομικά ταμιευτήρια.

Το Private Banking ασχολείται με λογαριασμούς μεγάλων πελατών με μεγάλη οικονομική επιφάνεια

Το Corporate Banking έχει ως αντικείμενο τα τραπεζικά προϊόντα που αφορούν κυρίως επιχειρήσεις και εταιρίες.

Οι συνεταιριστικές τράπεζες αποτελούν πρωτοβουλίες τοπικού κυρίως χαρακτήρα με σκοπό την ενίσχυση π.χ. των τοπικών παραγωγών γεωργικών προϊόντων.

Όποια μορφή όμως και αν έχει η τράπεζα για την εύρυθμη διεξαγωγή των τραπεζικών της εργασιών απαιτείται η ύπαρξη καλού πληροφοριακού συστήματος. Η λειτουργία των συστημάτων πληροφορικής στοχεύει, αφενός στην αποτελεσματική υποστήριξη της επιχειρησιακής στρατηγικής των πιστωτικών ιδρυμάτων, αφετέρου στην ασφαλή διακίνηση, επεξεργασία και αποθήκευση των κρισίμων επιχειρησιακών πληροφοριών.

Παράλληλα, η αυξημένη ανάγκη χρήσης συστημάτων πληροφορικής από τα πιστωτικά ιδρύματα, σε συνδυασμό με την τυχόν ανάθεση κρισίμων έργων πληροφορικής σε τρίτους, ενισχύει συγκεκριμένες κατηγορίες κινδύνων με σημαντικότερη αυτή του λειτουργικού κινδύνου. Οι κίνδυνοι αυτοί πρέπει να προσδιορίζονται, να εντοπίζονται έγκαιρα και να αντιμετωπίζονται αποτελεσματικά. Στο πλαίσιο της αποτελεσματικής διαχείρισης των κινδύνων που απορρέουν από τη λειτουργία των Συστημάτων Πληροφορικής, τα πιστωτικά ιδρύματα υλοποιούν το πλαίσιο αρχών ασφαλούς και αποτελεσματικής λειτουργίας των συστημάτων πληροφορικής όπως αναφέρεται στους κανονισμούς περί ίδρυσης και λειτουργίας των τραπεζών.

1.2. Η τεχνολογία στην υπηρεσία των τραπεζικών εργασιών

Τα οφέλη της εφαρμογής τεχνολογιών πληροφορικής και επικοινωνίας στον τραπεζικό τομέα, δεν περνούν απαρατήρητα. Αύξηση παραγωγικότητας και ποιότητας των παρεχόμενων υπηρεσιών, βελτιστοποίηση των επιχειρηματικών εργασιών και αύξηση της ανταγωνιστικότητας είναι τα σπουδαιότερα, σ' έναν τομέα που διαρκώς αλλάζει προς το καλύτερο.

Οι επιδράσεις των νέων τεχνολογιών στο τραπεζικό χώρο είναι τόσο σαρωτικές, που τοποθετούν τις τράπεζες σε τροχιά μετασχηματισμού και επαναπροσδιορισμού μοντέλων που διατηρούνταν απαράλλαχτα για δεκαετίες. Η ανάδυση εναλλακτικών δικτύων (εκτός γκισέ), η προσφορά προϊόντων για κάθε τμήμα της αγοράς, η μείωση του χρόνου εξυπηρέτησης με ταυτόχρονη αύξηση της ποιότητας, η δραστική μείωση των λειτουργικών εξόδων, η προσθήκη αξίας στη σχέση πελάτη - τράπεζας και η βαθύτερη επίγνωση πελατειακών προφίλ και αναγκών αποτελούν χειροπιαστές εξελίξεις που δεν θα είχαν συμβεί χωρίς την εφαρμογή των καινοτομικών, από κάθε άποψη, τεχνολογικών λύσεων που είναι σήμερα διαθέσιμες.

Μέσα από αυτές τις διεργασίες, ο πελάτης τίθεται στο επίκεντρο των τραπεζικών εργασιών («πελατοκεντρική προσέγγιση»), κάτι που οδηγεί στην ενδυνάμωση της σχέσης του με την τράπεζα και την αύξηση του βαθμού πιστότητάς του (loyalty), σε μία σχέση αμοιβαίου οφέλους που τροφοδοτείται αμφίδρομα: Η τράπεζα αποκτά καλύτερη επίγνωση του πελάτη, πιθανολογεί βάσιμα τι έχει ανάγκη και του το προσφέρει, ενώ από τον τρόπο ανταπόκρισης του πελάτη - σε συνάρτηση ασφαλώς και με άλλα στοιχεία - η τράπεζα καταστρώνει την πελατειακή στρατηγική της.

Οι τεχνολογίες αυτές καλύπτουν ένα ευρύ φάσμα υλικών υποδομών (υπολογιστών, μηχανημάτων, συσκευών) και λογισμικών εφαρμογών που θα μπορούσαν να διακριθούν σε δύο μεγάλες κατηγορίες. Σε αυτές με τις οποίες ο πελάτης έρχεται σε άμεση επαφή (π.χ. ΑΤΜ) και σ' εκείνες που λειτουργούν υποστηρικτικά ή πάνω στις οποίες βασίζονται οι υπηρεσίες και τα προϊόντα που προσφέρονται από την τράπεζα στους πελάτες της λιανικής (π.χ. διαχείριση

αιτήματος δανείου). Μερικά από τα πιο σημαντικά σχετικά εργαλεία που προσφέρει σήμερα η τεχνολογία, είναι τα παρακάτω.

1.2.1. Για την τράπεζα

Ο θεμέλιος λίθος της ψηφιακής υποδομής μιας τράπεζας είναι το ολοκληρωμένο πληροφοριακό της σύστημα. Τέτοια συστήματα διαχειρίζονται τις back - office και front - office εργασίες του ιδρύματος, από τις συναλλαγές στα καταστήματα, μέχρι εκείνες στο internet και τα άλλα εναλλακτικά δίκτυα, σε πραγματικό χρόνο, επί εικοσιτετραώρου βάσης και υποστηρίζοντας συναλλαγές σε διαφορετικά νομίσματα. Συνήθως τα συστήματα αυτά απαρτίζονται από υποσυστήματα (υπομονάδες) που επιτελούν συγκεκριμένες τραπεζικές λειτουργίες. Για παράδειγμα, διαχείριση πελατών, προϊόντων, καταθέσεις, εισπράξεις - πληρωμές, πάγιες εντολές, χορηγήσεις, χρεόγραφα, αξιόγραφα, διοικητική πληροφόρηση και πολλά άλλα. Ένα σύγχρονο, αξιόπιστο σύστημα του είδους διευκολύνει τη δημιουργία νέων προϊόντων και μπορεί να υποστηρίξει τη γρήγορη διάθεσή τους στην αγορά.

Παράλληλα, παρέχει λογιστική και χρηματοοικονομική ανάλυση και πληροφόρηση σε όλα τα επίπεδα μάνατζμεντ του οργανισμού. Βασικό συστατικό ενός επιτυχημένου ολοκληρωμένου συστήματος είναι το πελατοκεντρικό βάθος εστίασης. Κατά πόσο δηλαδή μπορεί το σύστημα να βοηθήσει στη διακράτηση των υπαρχόντων πελατών και στην προσέλκυση καινούριων, δημιουργώντας ευκαιρίες για την προώθηση νέων προϊόντων, την «απόσπαση» περισσότερων χρημάτων από το πορτοφόλι του πελάτη και την ανάπτυξη υπηρεσιών για συγκεκριμένες κατηγορίες πελατών. Πλάι στο κεντρικό πληροφορικό σύστημα υπάρχουν διάφορες κάθετες λύσεις, που εξυπηρετούν εξειδικευμένες τραπεζικές και πελατειακές ανάγκες, όπως λόγου χάρη οι λύσεις για το private banking, που μεταξύ άλλων αναλαμβάνουν τη διαμόρφωση του κατάλληλου προϊόντος για κάθε - εξ’ ορισμού ιδιαίτερο - προφίλ πελάτη.

1.2.2. Για τον πελάτη

Πέραν αυτών, η σύγχρονη τραπεζική απαιτεί την ύπαρξη κέντρου κλήσεων (call center), για την εξυπηρέτηση των πελατών της μέσω τηλεφώνου. Τα τραπεζικά call centers αναλαμβάνουν την τηλεφωνική εξυπηρέτηση των πελατών για ένα μεγάλο εύρος θεμάτων, από την υποδοχή των εισερχόμενων κλήσεων, μέχρι την προώθηση προϊόντων (δανείων, καρτών κ.λπ.). Σ' ένα τραπεζικό κέντρο κλήσεων, οι εφαρμογές λογισμικού που στηρίζουν τη λειτουργία του αποτελούν το πιο σημαντικό, ίσως, συστατικό του. Στα call centers συναντιούνται εφαρμογές όπως ACD (σύστημα κατανομής και διανομής των εισερχόμενων κλήσεων), predictive dialing (χρησιμοποιείται για τις εξερχόμενες κλήσεις αυτοματοποιώντας μια σειρά διαδικασιών, όπως η κλήση των αριθμών), IVR (προσφέρει στον πελάτη τη δυνατότητα λήψης πληροφοριών χωρίς ανθρώπινη παρέμβαση, μέσω ηχογραφημένων μηνυμάτων και την πληκτρολόγηση αριθμών), ενώ μεταξύ συσκευών και λογισμικού παρεμβάλλονται τα συστήματα CTI (Computer Telephony Integration), που λειτουργούν ως ο συνδετικός κρίκος ανάμεσα στις πολλές και διαφορετικές υποδομές και εφαρμογές ενός call center. Στα συστήματα CTI περιλαμβάνονται λύσεις λογισμικού που φέρνουν σε επαφή διαφορετικά τεχνολογικά πρωτόκολλα, και συσκευές που χρησιμεύουν ως γέφυρες επικοινωνίας μεταξύ του τηλεφωνικού κέντρου (τη συσκευή), των τηλεφώνων, των υπολογιστών κ.λπ.

Στο ίδιο πλαίσιο (τηλεφωνικής εξυπηρέτησης) εντάσσονται και οι λύσεις αναγνώρισης φωνής μέσω φωνητικής πύλης, γνωστότερες με τον όρο «voice portals», που την τελευταία διετία «χτυπούν» όλο και πιο συχνά την πόρτα των εγχώριων τραπεζών. Το voice portal συνιστά σύστημα αυτόματης τηλεφωνικής επικοινωνίας, κατά την οποία ο πελάτης εξυπηρετείται χωρίς τη μεσολάβηση τηλεφωνητή, αλλά από το ίδιο το σύστημα, συνομιλώντας μαζί του και μάλιστα, χωρίς να πληκτρολογεί αριθμούς. Η τηλεφωνική πύλη αξιοποιεί σύνθετες τεχνολογίες αναγνώρισης φωνής, που συνδυάζονται με ηχογραφημένα μηνύματα και τεχνολογίες σύνθεσης φωνής ή μετατροπής της φωνής σε κείμενο και το αντίστροφο. Έτσι ελαττώνεται κατά πολύ ο χρόνος εξυπηρέτησης, με ταυτόχρονη αύξηση της ικανοποίησης του πελάτη, ενώ και η τράπεζα δεν χρειάζεται να διατηρεί πολυάριθμο

call center, αποφεύγοντας μια σειρά σημαντικών δαπανών. Τόσο τα call centers όσο και τα voice portals ολοκληρώνονται ως συστήματα εξυπηρέτησης και πελατειακής διαχείρισης, με κάποιο σύστημα CRM (Customer Relationship Management), που αναλαμβάνει τη συλλογή, ανάλυση και διαχείριση των δεδομένων που προέρχονται από την επικοινωνία με τους πελάτες. Η χρήση του συστήματος CRM δεν περιορίζεται στο call center ή στο voice portal.

Ένα τυπικό τέτοιο σύστημα, που μπορεί ν' ανταποκριθεί στις ανάγκες του τραπεζικού τομέα, υποστηρίζει συνολικά τη διαχείριση των ενεργειών που αφορούν τις σχέσεις της εταιρείας με τους πελάτες της, την αυτοματοποίηση των ενεργειών μάρκετινγκ και πωλήσεων, την εξυπηρέτηση των αιτημάτων των πελατών - από την αρχική καταγραφή και επεξεργασία μέχρι την επίλυση -, τη διαχείριση των ενεργειών που σχετίζονται με τη διαδικασία είσπραξης οφειλών /απαιτήσεων και τη διαχείριση όλων των συναφών νομικών ενεργειών - τα λεγόμενα «collections» -, καθώς και την προώθηση στην αγορά νέων ή υπαρχόντων προϊόντων, μέσω τηλεφώνου ή ηλεκτρονικού ταχυδρομείου.

Ιδιαίτερα σημαντικά για τον τομέα της τραπεζικής είναι μία σειρά άλλων συστημάτων, που συνδυάζουν εξειδικευμένες φυσικές και τεχνολογικές υποδομές με λογισμικό, για την εξυπηρέτηση των πελατών. Τα μηχανήματα ATM, για τη self - service εξυπηρέτηση πλήθους τραπεζικών εργασιών και την αποσυμφόρηση των γκισέ, τα συστήματα προτεραιότητας (για τη διαχείριση της «ουράς») και τα συστήματα POS (Point of Sales) με σταθερά ή φορητά τερματικά και εφαρμογές λογισμικού για την ολοκλήρωση και επεξεργασία των συναλλαγών με πιστωτικές ή χρεωστικές κάρτες, είναι τα πιο διαδεδομένα από αυτά. Στο σημείο αυτό αξίζει να σημειωθεί ότι τα νέας γενιάς ATM αυξάνουν την γκάμα των προσφερόμενων υπηρεσιών, όπως π.χ. με τη δυνατότητα που διαθέτουν να καταμετρούν τα χρήματα της κατάθεσης, χωρίς τη μεσολάβηση υπαλλήλου.

Με τη πάροδο του χρόνου, έδαφος κερδίζει στην Ελλάδα το web banking, η πραγματοποίηση, δηλαδή, τραπεζικών συναλλαγών μέσω του internet. Ένας υπολογιστής, μία σύνδεση με το internet και ένας web browser (λ.χ. Internet Explorer) αρκούν για την πραγματοποίηση πληθώρας συναλλαγών με την τράπεζα, χωρίς να επισκεφτεί ο πελάτης το κατάστημα (μεταφορά χρημάτων, εντολή

πληρωμής κ.λπ.), με όλα τα ωφέλιμα συμπαρομαρτούντα τόσο για τον επιχειρηματικό όσο και για τον απλό πελάτη. Το επόμενο στάδιο, σύμφωνα με όλες τις ενδείξεις, αναμένεται να είναι το mobile banking, η εκτέλεση δηλαδή συναλλαγών μέσω του κινητού τηλεφώνου. Όπως ίσως είναι προφανές, πίσω από την εφαρμογή αυτού του νέου τρόπου ηλεκτρονικών συναλλαγών βρίσκεται πλειάδα εφαρμογών λογισμικού, για την ασφάλεια και τη λειτουργικότητα των συναλλαγών.

Τέλος, αν και άγνωστες στο ευρύ κοινό, οι σχετικά νέες εφαρμογές process management καλύπτουν την αυτοματοποιημένη διαχείριση τραπεζικών διαδικασιών, εξομαλύνοντας μια σειρά συνηθισμένων προβλημάτων στο τραπεζικό χώρο. Για παράδειγμα, η απώλεια πιστωτικών καρτών ή η αλλαγή διεύθυνσης του πελάτη, χωρίς την ύπαρξη κάποιας τέτοιας εφαρμογής μπορεί να προβληματίσει ιδιαίτερα την τράπεζα και ν' απαιτηθεί αρκετός χρόνος για να ολοκληρωθεί η σχετική ενημέρωση. Με κάποια εφαρμογή του είδους αυτό γίνεται αυτόματα και μέσα σ' ελάχιστα δευτερόλεπτα, κάτι που προφανώς λειτουργεί προς όφελος και του πελάτη και της τράπεζας και της λιανικής τραπεζικής.

Εκτός από τα παραπάνω, υπάρχουν και αρκετές άλλες λύσεις και συστήματα που βρίσκουν εφαρμογή στα χρηματοπιστωτικά ιδρύματα και σχετίζονται άμεσα ή έμμεσα με τους πελάτες - επενδυτές, προσφέροντας στις τράπεζες όλα τα απαραίτητα στοιχεία για να προβούν στις ενδεδειγμένες κινήσεις. Όπως είχε πει κάποτε και ο πρόεδρος της Citibank στη δεκαετία του '70, Walter Wriston, ***οι πληροφορίες για τα χρήματα αξίζουν περισσότερο από τα ίδια τα χρήματα*** και οι συγκεκριμένες τεχνολογίες κινούνται προς αυτήν την κατεύθυνση.

ΚΕΦΑΛΑΙΟ 2^{ο}:Ασφάλεια τραπεζικών πληροφοριακών συστημάτων

2.1. Πληροφοριακό Σύστημα (Π.Σ.)

Πληροφοριακό σύστημα σημαίνει ότι ένας αριθμός αλληλεπιδρώντων στοιχείων έχουν οργανικά συναρμολογηθεί σε μια ολότητα, έτσι ώστε να εκτελέσουν μια ορισμένη λειτουργία. Τα στοιχεία αυτά είναι:

α) Ο άνθρωπος, αφού τα Π.Σ. δημιουργούνται από αυτόν και λειτουργούν με τη βοήθειά του, έτσι ώστε να υπηρετήσουν πάλι αυτόν.

β) Η πληροφορία, ένα αγαθό με πολύ μεγάλη ζήτηση.

γ) Η πληροφορική, η επιστήμη/τεχνολογία που σκοπό έχει την επεξεργασία της πληροφορίας.

Με άλλα λόγια το Πληροφοριακό Σύστημα είναι μια συλλογή από το μηχανικό/υλικό μέρος, το λογισμικό, τα μέσα αποθήκευσης, τα δεδομένα και τους ανθρώπους που ένας οργανισμός χρησιμοποιεί για να πετύχει τα λειτουργικά βήματα που θέλει. Εξαιτίας του ρόλου που παίζει το Π.Σ. σε μια επιχείρηση και όχι μόνο, είναι φυσικό να απαιτεί ασφάλεια και προστασία. Συνεπώς τα Π.Σ. θα πρέπει να προστατεύονται από κάθε μορφή απειλής, χωρίς όμως η προστασία αυτή να παρεμποδίζει τη ροή των πληροφοριών.

2.2. Ασφάλεια

Ο όρος ασφάλεια πληροφοριακών συστημάτων δίνει έμφαση στην προστασία των συστατικών στοιχείων ενός πληροφοριακού συστήματος αλλά και του ίδιου του πληροφοριακού συστήματος στην ολότητα του.

«Ασφάλεια πληροφοριακού συστήματος είναι *το οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία του πληροφοριακού συστήματος αλλά και το σύστημα*

ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή». Η ασφάλεια του πληροφοριακού συστήματος συνδέεται άμεσα τόσο με τις τεχνικές, τις διαδικασίες και τα διοικητικά μέσα όσο και με ηθικό-κοινωνικές αντιλήψεις, αρχές και παραδοχές. Είναι βέβαια προφανές ότι η προφύλαξη δεν θα πρέπει να παρεμποδίζει την απρόσκοπτη λειτουργία του συστήματος και την ελεύθερη διακίνηση των πληροφοριών, έτσι ώστε να μην θέτονται αδικαιολόγητοι φραγμοί στην ανάπτυξη της τεχνολογίας της πληροφορίας.

Η ασφάλεια πληροφοριών αναφέρεται αποκλειστικά στην προστασία των πληροφοριών και είναι στενότερη έννοια από αυτή της ασφάλειας πληροφοριακού συστήματος, αφού η πληροφορία εμπεριέχεται σε ένα πληροφοριακό σύστημα. Βέβαια η ασφάλεια τούτη δεν μπορεί να αγνοήσει το πληροφοριακό σύστημα, στα πλαίσια του οποίου παράγεται και χρησιμοποιείται η πληροφορία. Αντίθετα, κάθε αναλυτική εργασία, η οποία αποσκοπεί στην ανάπτυξη και διαχείριση της ασφάλειας των πληροφοριών, θα πρέπει να στηρίζεται στην κατανόηση των σχετικών πληροφοριακών συστημάτων. Συνεπώς, όταν αναφερόμαστε στην ασφάλεια ενός πληροφοριακού συστήματος η προστασία όλων των υλικών που μετέχουν σε αυτό έχει ιδιαίτερη σημασία, ενώ όταν αναφερόμαστε στην ασφάλεια πληροφοριών, η ασφάλεια του υλικού μας ενδιαφέρει μόνο στο βαθμό που σχετίζεται με την προστασία πληροφοριών.

2.3. Ιδιότητες της Ασφάλειας

Οι πληροφορίες είναι ένα πλεονέκτημα, που όπως όλα τα άλλα σημαντικά επιχειρησιακά προτερήματα, έχει και αυτό τη δική του αξία σε μια εταιρική μονάδα και πρέπει συνεπώς να προστατευθεί κατάλληλα. Η «ασφάλεια πληροφοριών» στόχο έχει να προστατεύει τις πληροφορίες από ένα ευρύ φάσμα απειλών, προκειμένου να εξασφαλιστεί η επιχειρησιακή συνοχή, να ελαχιστοποιηθεί η επιχειρησιακή ζημία και να μεγιστοποιηθεί η επιστροφή στις επενδύσεις και στις επιχειρησιακές ευκαιρίες. Οι πληροφορίες μπορούν να υπάρξουν με πολλές μορφές. Μπορεί λοιπόν να τυπωθούν, να γραφτούν σε χαρτί, να αποθηκευτούν ηλεκτρονικά, ή ακόμα και να διαβιβαστούν

με την χρησιμοποίηση ηλεκτρονικών μέσων. Οποιαδήποτε μορφή και να λαμβάνουν οι πληροφορίες, πρέπει πάντοτε να προστατεύονται.

Η ασφάλεια των πληροφοριών αναφέρεται στην προστασία της πληροφορίας στην ολότητα των σχετικών με την ασφάλεια ιδιοτήτων. Ως θεμελιώδεις ιδιότητες ασφάλειας θεωρούνται η ακεραιότητα, η εμπιστευτικότητα και η διαθεσιμότητα οι οποίες ορίζονται ως εξής :

Ακεραιότητα πληροφοριών : Είναι η ιδιότητα των δεδομένων να υφίστανται σε προκαθορισμένο φυσικό μέσο ή χώρο και να είναι ακριβή. Δηλαδή η μη—εξουσιοδοτημένη τροποποίηση της πληροφορίας θα πρέπει να αποτρέπεται, ενώ κάθε αλλαγή του περιεχομένου των δεδομένων να είναι αποτέλεσμα εξουσιοδοτημένης και ελεγχόμενης ενέργειας.

Εμπιστευτικότητα πληροφοριών : Η ιδιότητα των δεδομένων να καθίστανται αναγνώσιμα μόνο από τα εξουσιοδοτημένα λογικά υποκείμενα, όπως φυσικές οντότητες και διεργασίες λογισμικού.

Διαθεσιμότητα πληροφοριών : Η αποτροπή της προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας σε κάθε εξουσιοδοτημένο λογικό υποκείμενο του συστήματος.

Μυστικότητα : Περιλαμβάνει το δικαίωμα των ατόμων να διατηρούν ορισμένες πληροφορίες για τους εαυτούς τους, δίχως την παραμικρή πιθανότητα αποκάλυψης τους και χωρίς το φόβο μη εξουσιοδοτημένης προσπέλασης τους.

Σε αρκετές ερευνητικές εργασίες υποστηρίζεται πως οι παραπάνω τέσσερις ιδιότητες δεν επαρκούν για να οριστεί η ασφάλεια πληροφοριών. Πρόσθετες ιδιότητες που συναντώνται είναι αυτή της αυθεντικότητας, της εγκυρότητας, της μοναδικότητας και άλλες πολλές.

Στο σημείο αυτό θα πρέπει να σημειώσουμε πως η ύπαρξη διαφορετικών θεωρήσεων για της ιδιότητες ασφάλειας δεν είναι κάτι παράδοξο, διότι στον επιστημονικό τομέα της πληροφορικής, η ασφάλεια έχει μεταφερθεί ως μία αφηρημένη έννοια η οποία επιδέχεται ποικίλες ερμηνείες. Η ασφάλεια πληροφοριών επιτυγχάνεται με την εφαρμογή ενός κατάλληλου συνόλου ελέγχων, το οποίο θα μπορούσε να είναι ένα σύνολο από πρακτικές, διαδικασίες, οργανωτικές δομές και διάφορες λειτουργίες λογισμικού. Αυτοί οι έλεγχοι πρέπει να υπάρχουν για να

εξασφαλίσουν ότι οι συγκεκριμένοι στόχοι ασφάλειας της οργάνωσης επιτυγχάνονται.

2.4. Ανάλυση κινδύνων της ασφάλειας τραπεζικών πληροφοριακών συστημάτων

Τα Πληροφοριακά Συστήματα στις μέρες μας χρησιμοποιούνται όλο και περισσότερο και γίνονται όλο και πιο κρίσιμα για την επιτυχή λειτουργία της σύγχρονης επιχείρησης, και ειδικότερα των Τραπεζών. Άρα γίνεται εύκολα κατανοητό, πώς πρέπει να προστατεύονται ευρέως από κάθε πιθανό κίνδυνο που τα απειλεί. Στην εποχή μας, υπάρχουν πολλοί κίνδυνοι που απειλούν τα Πληροφοριακά Συστήματα και είναι και πολύ διαδεδομένοι. Σύμφωνα με έρευνες :

§ το 68% των ερωτηθέντων δηλώνει πώς έχει υποστεί ένα τουλάχιστον ρήγμα ασφαλείας μέσα σε ένα χρόνο, ενώ

§ ποσοστό 47% των ερωτηθέντων στις ΗΠΑ είχε υποστεί οικονομικές ζημιές ύψους μέχρι $100.000 εξαιτίας ιών.

Παρατηρούμε λοιπόν πως οι κίνδυνοι που απειλούν τα Πληροφοριακά Συστήματα δεν είναι θεωρητικοί, αλλά απολύτως απτοί και σημαντικοί για κάθε επιχείρηση. Η έννοια του κινδύνου συνδέεται με οτιδήποτε μπορεί να προκαλέσει ζημιά σε κάποια από τις ιδιότητες ενός Πληροφοριακού Συστήματος. Ο Κίνδυνος στα Πληροφοριακά Συστήματα αποτελείται από δύο επιμέρους έννοιες:

- Την Παραβίαση, που αποτελεί μία γενικότερη έννοια, σύμφωνα με την οποία κάποιος τρίτος καταφέρνει να εισχωρήσει σε ένα Πληροφοριακό Σύστημα και
- το Ρήγμα Ασφαλείας, το οποίο προϋποθέτει την Παραβίαση. Ως Ρήγμα Ασφαλείας εννοούμε την μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες ή και την αλλοίωση ή διαγραφή τους.

Υπάρχει επίσης και η έννοια της Απειλής, η οποία μπορεί να οδηγήσει σε Παραβίαση. Οι απειλές είναι είτε εξωτερικές (πχ ιός), είτε εσωτερικές (πχ δυσαρεστημένος υπάλληλος). Επίσης μπορεί να είναι σκόπιμες ή τυχαίες (πχ σεισμός).

Οι απαιτήσεις ασφάλειας προσδιορίζονται από μια συστηματική αξιολόγηση των κινδύνων. Οι δαπάνες για τους ελέγχους πρέπει να εξισορροπούνται ενάντια στην επιχειρησιακή ζημιά που είναι πιθανόν να προκύψει από τις αποτυχίες εξασφάλισης ασφάλειας. Οι τεχνικές αξιολόγησης του κινδύνου μπορούν να εφαρμοστούν είτε σε όλη την τράπεζα, είτε στα επιμέρους συστήματα πληροφοριών, στα συγκεκριμένα τμήματα συστημάτων ή στις υπηρεσίες και γενικότερα όπου αυτό είναι εφαρμόσιμο, ρεαλιστικό και χρήσιμο. Η αξιολόγηση του κινδύνου είναι η συστηματική εκτίμηση δυο παραγόντων :

α) της επιχειρησιακής ζημιάς που είναι πιθανό να προκύψει από μια αποτυχία ασφάλειας και

β)της πιθανότητας μιας αποτυχίας που ελλοχεύει λαμβάνοντας υπόψη τις επικρατούσες απειλές και αδυναμίες.

Τα αποτελέσματα αυτής της αξιολόγησης θα βοηθήσουν ώστε να καθορίσουν την κατάλληλη διοικητική δράση, τις προτεραιότητες για τη διαχείριση των κινδύνων ασφάλειας πληροφοριών και για την εφαρμογή των ελέγχων που επιλέγονται για να προστατεύσουν την τράπεζα από αυτούς τους κινδύνους. Η διαδικασία αυτή είναι φρόνιμο να γίνεται σε διαφορετικά χρονικά επίπεδα.

Είναι σημαντικό όταν διεξάγονται οι περιοδικές διαδικασίες επανεξέτασης των κινδύνων ασφάλειας και των εφαρμοσμένων ελέγχων :

α) να λαμβάνονται υπόψη οι αλλαγές στις επιχειρησιακές απαιτήσεις και οι προτεραιότητες

β) να εξετάζονται οι νέες απειλές

γ) να επιβεβαιώνεται ότι οι έλεγχοι παραμένουν αποτελεσματικοί και κατάλληλοι.

Ένα πληροφοριακό σύστημα το οποίο διαχειρίζεται ευπαθή δεδομένα, όπως η τράπεζα, και βασίζεται επιπλέον στην αξιοποίηση των δυνατοτήτων του διαδικτύου εκτίθεται σε μία σειρά σημαντικών απειλών, οι οποίες απαιτείται να αντιμετωπιστούν αποτελεσματικά. Ως απειλή ορίζεται « *μια πιθανή ενέργεια ή ένα γεγονός που μπορεί να προκαλέσει την απώλεια ενός ή περισσότερων χαρακτηριστικών ασφάλειας ενός πληροφοριακού συστήματος*». Οι απειλές αυτές δεν προέρχονται μόνο από κακόβουλες ενέργειες που προκαλούνται από τρίτους με στόχο την κατοχή ή την απαξίωση πολύτιμων δεδομένων. Είναι πιθανό να δημιουργηθούν από το εσωτερικό

του συστήματος εξαιτίας σχεδιαστικών λαθών και αδυναμιών. Οι κυριότερες από αυτές περιγράφονται συνοπτικά παρακάτω :

=> Παρακολούθηση γραμμών επικοινωνίας : Παρακολουθώντας τις επικοινωνιακές γραμμές μπορεί κανείς να αποκτήσει μη εξουσιοδοτημένη προσπέλαση σε μετακινούμενα δεδομένα, με πιθανό αποτέλεσμα να παραβιαστεί η ιδιωτικότητά τους

=> Ανάλυση κυκλοφορίας : Για δεδομένες διευθύνσεις πηγής και προορισμού η παρακολούθηση των διακινούμενων δεδομένων μπορεί να οδηγήσει σε ανάπτυξη υποδείγματος κυκλοφορίας. Η στατιστική και μόνο ανάλυση της επικοινωνίας, χωρίς απαραίτητα να γίνεται ανάγνωση των ίδιων των δεδομένων, μπορεί να καταλήξει σε χρήσιμα συμπεράσματα για κάποιον τρίτο

=> Αποτυχία ή καταστροφή υλικού : Σημαντική απειλή στη διαθεσιμότητα ενός υπολογιστικού συστήματος αποτελεί η ενδεχόμενη καταστροφή του χρησιμοποιούμενου υλικού, είτε από κακόβουλη ενέργεια, είτε από αστοχία (υλικού) είτε από φυσική αιτία.

=> Πλαστογράφηση διευθύνσεων δικτύου : Καταργείται η ιδιότητα της μονό-σήμανσης αντιστοίχισης των διευθύνσεων δικτύου σε μια συγκεκριμένη θέση, με αποτέλεσμα τα διακινούμενα δεδομένα να χάνουν την ιδιότητα της αυθεντικότητας προέλευσης .

=> Υποκλοπή συνθηματικών : Ένα συνθηματικό μπορεί να διαρρεύσει σε έναν δυνητικό εισβολέα είτε από αμέλεια του χρήστη του συστήματος είτε μετά από παρακολούθηση των διακινούμενων πακέτων είτε με τη χρήση της μεθόδου ωμής δοκιμής.

=> Αξιοποίηση καταπακτών : Οι καταπακτές είναι γνωστές ή άγνωστες αδυναμίες των υπηρεσιών του συστήματος που επιτρέπουν την υπέρβαση των μηχανισμών ασφάλειας για την προσπέλαση στους πόρους του συστήματος. Η ύπαρξη των αδυναμιών αυτών γίνεται γνωστή στους εισβολείς έπειτα από δοκιμαστική ανίχνευση που πραγματοποιούν σε όλες τις θύρες επικοινωνίας τους συστήματος

=> Μη εξουσιοδοτημένη τροποποίηση : Η κακόβουλη τροποποίηση των δεδομένων ενός συστήματος έπεται της παρακολούθησης των γραμμών επικοινωνίας ή της παρείσφρησης στο σύστημα έπειτα από υποκλοπή συνθηματικού ή αξιοποίηση καταπακτών .

=> Άρνηση παροχής υπηρεσίας : Σε αυτήν την περίπτωση ο εισβολέας επιχειρεί να επηρεάσει αρνητικά τη διαθεσιμότητα μιας υπηρεσίας, αφού έχει παρεισφρήσει στο σύστημα που την παρέχει. Το ίδιο μπορεί να συμβεί όταν ο εισβολέας καταφέρει να εγκαταστήσει λογισμικό που καταναλώνει ανεξέλεγκτα όλους τους διαθέσιμους πόρους του συστήματος ή του δικτύου, με αποτέλεσμα οι υπόλοιπες υπηρεσίες να παραμείνουν ουσιαστικά ανενεργές.

=> Κατανεμημένη επίθεση άρνησης παροχής υπηρεσίας : Η λογική είναι η ίδια με την άρνηση παροχής υπηρεσίας, με τη διαφορά ότι ο εισβολέας έχει εγκαταστήσει το κακόβουλο λογισμικό σε δεκάδες συστήματα αφού έχει παρεισφρήσει σε αυτά και τα χρησιμοποιεί ως μεσάζοντες. Τα συστήματα αυτά με τη σειρά τους επιτίθενται συντονισμένα προς τον τελικό στόχο με δραματικές συνέπειες στους πόρους τους συστήματος αυτού, αλλά και στο δίκτυο που οδηγεί προς αυτό.

=> Κατάχρηση πόρων : Με μια εξουσιοδοτημένη οντότητα είναι πιθανό να υποκλέψει πόρους ενός συστήματος, όπως κύκλους του επεξεργαστή, εύρος ζώνης δικτύου, χωρητικότητα δίσκων, είτε για να εξυπηρετηθούν διεργασίες του εισβολέα είτε για να προκληθεί άρνηση παροχής υπηρεσίας

=> Διάψευση εκτέλεσης ενέργειας : Μία οντότητα μπορεί να αρνηθεί ότι δημιούργησε και απέστειλε ένα μήνυμα ή ότι τροποποίησε κάποια δεδομένα, εφόσον δεν υπάρχουν επαρκή αποδεικτικά στοιχεία. Ομοίως ο παραλήπτης του μηνύματος μπορεί να διαψεύσει την παραλαβή του και την ανάγνωση του περιεχομένου του.

=> Εσωτερικοί κίνδυνοι : Είναι πιθανό μέλη του απασχολούμενου προσωπικού σε μία επιχείρηση να υποκλέψουν χρήσιμες πληροφορίες για παράνομη χρήση. Παράλληλα η έλλειψη ασφάλειας στη φυσική πρόσβαση στο υλικό του συστήματος δημιουργεί επιπλέον κινδύνους.

=> Πλαστοπροσωπία : Στο επίπεδο εφαρμογής είναι πιθανό η προέλευση ενός μηνύματος να φαίνεται διαφορετική (αλλά πραγματική).

=> Ιο μορφικό λογισμικό : Πρόκειται για κακόβουλο λογισμικό που εκτελείται ή φορτώνεται δυναμικά στο σύστημα και προκαλεί ποικίλα σημαντικά προβλήματα. Συνήθως βρίσκεται ενσωματωμένο σε εκτελέσιμο κώδικα ή αυτόνομο σε μορφή

δέσμης εντολών. Φροντίζει να προσκολλάται σε άλλα εκτελέσιμα αρχεία ή να διαδίδεται μέσω δικτυακών εφαρμογών, έτσι ώστε να επηρεάζει όσο το δυνατόν περισσότερα συστήματα.

=> Καταχρηστικά μηνύματα : Αφορά κυρίως τις υπηρεσίες μηνυμάτων όπως τα νέα και η ηλεκτρονική αλληλογραφία. Πρόκειται για μηνύματα διαφημιστικού και πολλές φορές προσβλητικού περιεχομένου που αποστέλλονται μαζικά σε μεγάλο αριθμό χρηστών, χωρίς να υπάρχει υπαρκτή διεύθυνση αποστολέα και από εξυπηρετητές που έχουν εκτεθεί στους εισβολείς έτσι ώστε να μην είναι ανιχνεύσιμη η προέλευση τους ούτε σε επίπεδο εφαρμογής ούτε σε επίπεδο δικτύου.

Η εμπειρία έχει δείξει ότι για την επιτυχή εφαρμογή της ασφάλειας πληροφοριών μέσα σε μια τράπεζα είναι συχνά απαραίτητοι η εμφάνιση των ακόλουθων παραγόντων:

α) εφαρμογή μιας πολιτικής ασφάλειας και ανάπτυξη δραστηριοτήτων που απεικονίζουν τους εκάστοτε τραπεζικούς στόχους

β) προσέγγιση στην εφαρμογή της ασφάλειας, ώστε να είναι σύμφωνη με την τραπεζική φιλοσοφία, κουλτούρα

γ) μια καλή κατανόηση των απαιτήσεων ασφάλειας, της αξιολόγησης του κινδύνου και της διαχείρισης ρίσκου (κινδύνου)

δ) αποτελεσματικό μάρκετινγκ της ασφάλειας σε όλους τους διευθυντές και τους υφιστάμενους αυτών

ε) διανομή της καθοδήγησης σχετικά με την πολιτική ασφάλειας πληροφοριών και των προτύπων σε όλους τους υπαλλήλους και τους αναδόχους

ζ) παροχή κατάλληλων μέσων, κινήτρων, κατάρτισης και εκπαίδευσης

η) καθιέρωση ενός περιεκτικού και παράλληλα ισορροπημένου συστήματος μέτρησης, που θα χρησιμοποιείται για να αξιολογήσει την απόδοση, στις προτάσεις διαχείρισης και ανατροφοδότησης της ασφάλειας πληροφοριών, αναφορικά πάντοτε με τη προσπάθεια για συνεχή επίτευξη βελτίωσης.

2.5. Διαδικασίες ελέγχου ασφάλειας (προσπέλαση και ταυτοποίηση)

Το ζήτημα της μη εξουσιοδοτημένης πρόσβασης σε διαβαθμισμένες πληροφορίες της τράπεζας λύνεται κυρίως με τη χρήση μεθόδων ταυτοποίησης. Έτσι, λοιπόν, δημιουργείται ένα σύστημα διαβάθμισης των δεδομένων αλλά και της χρήσης των εφαρμογών, το οποίο κατηγοριοποιεί τόσο τα δεδομένα όσο και τις εφαρμογές σύμφωνα με το βαθμό σπουδαιότητας και ευαισθησίας τους, ώστε να προστατεύονται ανάλογα. Όσο πιο ψηλά στην ιεραρχία είναι κάθε στέλεχος, τόσο μεγαλύτερα δικαιώματα πρόσβαση έχει. Αυτή η διαβάθμιση επιτυγχάνεται με την ύπαρξη χρηστών και κωδικών, των οποίων γίνεται χρήση για να υπάρχει πρόσβαση στα διάφορα προγράμματα και εφαρμογές. Οι κωδικοί εσωτερικού χρήστη αποτελούν και την πρώτη δικλίδα ασφαλείας και γι' αυτό είναι σημαντικό για την τράπεζα να χρησιμοποιούνται σωστά και η διαχείριση τους να είναι προσεκτική και αξιόπιστη.

Δηλαδή, ο έλεγχος προσπέλασης, περιλαμβάνει συγκεκριμένους μηχανισμούς που έχουν ως σκοπό να προστατεύσουν από μη εξουσιοδοτημένη πρόσβαση τα δεδομένα εκείνα που έχουν οριστεί ως σημαντικά για τη λειτουργία της τράπεζας ή την ασφάλεια του συστήματος. Ανάλογα με τη θέση του ο χρήστης μπορεί να έχει διαφορετική άδεια προσπέλασης:

- είτε προς Παρατήρηση, όπου μπορεί μόνο να αναγνώσει τα δεδομένα,
- είτε προς Αλλαγή, οπού μπορεί και να τα τροποποιήσει και αυτό γιατί το γεγονός πώς ένας χρήστης έχει την εξουσιοδότηση να συνδεθεί στο σύστημα δε σημαίνει ότι πρέπει να έχει και τη δυνατότητα να κάνει ότι θέλει σε αυτό.

Σε κάθε τραπεζικό πληροφορικό σύστημα, τα δεδομένα χαρακτηρίζονται από ένα βαθμό εμπιστευτικότητας, όπως και οι χρήστες έχουν ένα αντίστοιχο βαθμό εμπιστευτικότητας. Έτσι υπάρχει μια ισότιμη σχέση εμπιστοσύνης και εμπιστευτικότητας, σύμφωνα με την οποία κάθε χρήστης μπορεί να έχει πρόσβαση μόνο σε ίσου ή μικρότερου επιπέδου εμπιστευτικότητας πληροφορίες.

Γενικά η αρχή που ισχύει στο ζήτημα της προσπέλασης δεδομένων είναι κάθε φορά να έχει τέτοιο δικαίωμα ο μικρότερος δυνατός αριθμός χρηστών, γιατί όσο μικρότερο είναι αυτός, τόσο λιγότερες είναι οι πιθανότητες να διαχυθεί η πληροφορία. Έτσι τελικά επιδιώκεται κάθε χρήστης να έχει πρόσβαση μόνο σε όσα δεδομένα χρειάζεται για την καθημερινή του εργασία και όχι σε παραπάνω.

Πρακτικά η κυριότερη διαδικασία ελέγχου προσπέλασης που υιοθετείται είναι αυτή της ταυτοποίησης του χρήστη και μπορεί να γίνεται με τέσσερις διαφορετικούς τρόπους :

- Γνώση συνθηματικού
- Κατοχή έξυπνης κάρτας
- Βιομετρική τεχνολογία (δακτυλικά αποτυπώματα, ίριδα ματιού κλπ)
- Τοποθεσία χρήστη (πχ διεύθυνση IP).

Συνήθως για τις τραπεζικές εφαρμογές επιλέγεται η πρώτη λύση, ως υλοποιήσιμη και εφαρμόσιμη αν και ανάλογα με το ζητούμενο επίπεδο ασφάλειας μπορεί να συνδυάζεται και με άλλες μεθόδους. Επίσης η χρήση συνθηματικών ως μεθόδου ταυτοποίησης είναι μικρού κόστους καθώς δεν απαιτείται επιπρόσθετος εξοπλισμός, ενώ όπως έχει δείξει η εμπειρία παρέχει και ικανοποιητικό βαθμό ασφάλειας.

Η ακριβής διαδικασία με τη χρήση κωδικού (password) έχει ως εξής: Αρχικά ο χρήστης εισάγει το όνομα χρήστη (user name), το οποίο είναι και μοναδικό στο σύστημα, και τον κωδικό του. Μετά την εισαγωγή των στοιχείων το σύστημα τα επαληθεύει με τα στοιχεία που έχει ήδη καταχωρημένα και εάν συμπίπτουν, ο χρήστης μπορεί να εργαστεί με την εφαρμογή.

Η εισαγωγή συνθηματικού αποτελεί την πρώτη δικλίδα ασφαλείας, για αυτό και αποτελεί ένα σημαντικό ζήτημα. Άλλωστε πάντα η πρώτη απόπειρα παραβίασης ενός Πληροφοριακού Συστήματος ξεκινάει με την προσπάθεια προσπέρασης του συνθηματικού είτε μαντεύοντας το είτε υποκλέπτοντας το. Η επίθεση μπορεί είτε να γίνεται σειριακά, δοκιμάζοντας όλους τους πιθανούς συνδυασμούς χαρακτήρων, είτε πιο συστηματικά, με τη χρήση λεξικού και στοιχείων του χρήστη (πχ ημερομηνία γέννησης, όνομα κλπ). Επίσης και οι ίδιοι οι χρήστες των Πληροφοριακών Συστημάτων πολλές φορές ενθαρρύνουν τους

επίδοξους εισβολείς αναγράφοντας τους κωδικούς τους σε εμφανή σημεία, ή χρησιμοποιώντας προφανή -για κάποιον που τους γνωρίζει- συνθηματικά.
Οι υπεύθυνοι για την ασφάλεια των πληροφοριακών συστημάτων μπορούν να ενισχύσουν την ασφάλεια που προσφέρουν τα συνθηματικά με κάποια μετρά, όπως :

- Μήκος και Μορφή κωδικού : ο κωδικός πρέπει να έχει ένα μεγάλο σχετικά μήκος, ώστε να μην είναι εύκολο να βρεθεί με λίγους συνδυασμούς από τον επίδοξο εισβολέα. Επίσης μπορούν να χρησιμοποιούνται εκτός από τα γράμματα και οι αριθμοί ή ειδικοί χαρακτήρες αυξάνοντας γεωμετρικά το πλήθος των πιθανών συνδυασμών.
- Συχνές αλλαγές του κωδικού.
- Συστάσεις προς τους χρήστες, ώστε να αποφεύγουν τη χρήση εύκολων συνθηματικών αλλά και να τα φυλάσσουν ασφαλώς.

Σε περίπτωση που αντί για τη χρήση κωδικών προτιμηθεί η διαδικασία ταυτοποίησης με τη χρήση «έξυπνης» κάρτας η διαδικασία αλλάζει. Ο χρήστης για την είσοδό του στο σύστημα, πρέπει να έχει μαζί του την κάρτα την οποία τοποθετεί σε ειδικό μηχάνημα, και να γνωρίζει τον Προσωπικό Κωδικό Αναγνώρισης (PIN), διαδικασία δηλαδή που μας θυμίζει την αντίστοιχη με αυτή που πραγματοποιούμε στα τραπεζικά ATM. Το PIN που εισάγει ο χρήστης συγκρίνεται με αυτό που περιέχει η κάρτα. Η επαλήθευση αυτή δε γίνεται από το μηχάνημα αλλά πραγματοποιείται εσωτερικά στην κάρτα, προσφέροντας μεγαλύτερη ασφάλεια. Οι έξυπνες κάρτες πια διαθέτουν επεξεργαστή ο οποίος προσφέρει υψηλά επίπεδα ασφάλειας και υποστηρίζει την ανανέωση ή επανεγγραφή των δεδομένων που περιέχει η κάρτα. Αν και οι κάρτες έχουν υψηλότερο κόστος από τη χρήση συνθηματικών, εντούτοις προσφέρουν μία επιπλέον δικλίδα ασφάλειας, αφού ο επίδοξος εισβολέας πρέπει να έχει στην κατοχή του και την κάρτα για να επιχειρήσει να μπει στο σύστημα.

Τέλος τα βιομετρικά συστήματα αποτελούν ότι πιο σύγχρονο και ασφαλές στο θέμα της ταυτοποίησης στοιχείων. Βασίζονται στα φυσικά χαρακτηριστικά του χρήστη για την είσοδο του (login) στο σύστημα και συνήθως χρησιμοποιούνται τα

δακτυλικά αποτυπώματα, η ίριδα του ματιού ή η χροιά της φωνής. Κύριο πλεονέκτημα τους η μεγάλη ασφάλεια που προσφέρουν (καθώς βασίζονται στη μοναδικότητα του κάθε ανθρώπου), αν και το κόστος δημιουργίας τους είναι ακόμη αρκετά υψηλό. Επίσης δεν είναι πάντα ακριβή και ενέχουν ένα επίπεδο σφάλματος.

Πρέπει όμως, σχετικά με τα βιομετρικά συστήματα, να σημειωθεί και η διστακτικότητα των χρηστών απέναντι τους. Αυτό συμβαίνει γιατί αισθάνονται ότι παρακολουθούνται από το Πληροφοριακό Σύστημα και πώς καταγράφονται οι κινήσεις τους, ενώ είναι πολλοί και αυτοί που διστάζουν να δώσουν κάποιο προσωπικό τους γνώρισμα για καταγραφή στη βάση δεδομένων του Πληροφοριακού Συστήματος.

Για όλους αυτούς τους λόγους θα λέγαμε, πώς είναι μάλλον σπάνιο να χρησιμοποιεί κάποια τράπεζα βιομετρικά συστήματα ή ακόμη και κάρτες για την ταυτοποίηση των χρηστών της. Η χρήση συνθηματικών, αποτελεί μία δοκιμασμένη σε βάθος χρόνου διαδικασία, η οποία τις περισσότερες φορές είναι αρκετή για τη διαβάθμιση των χρηστών και την προστασία των δεδομένων.

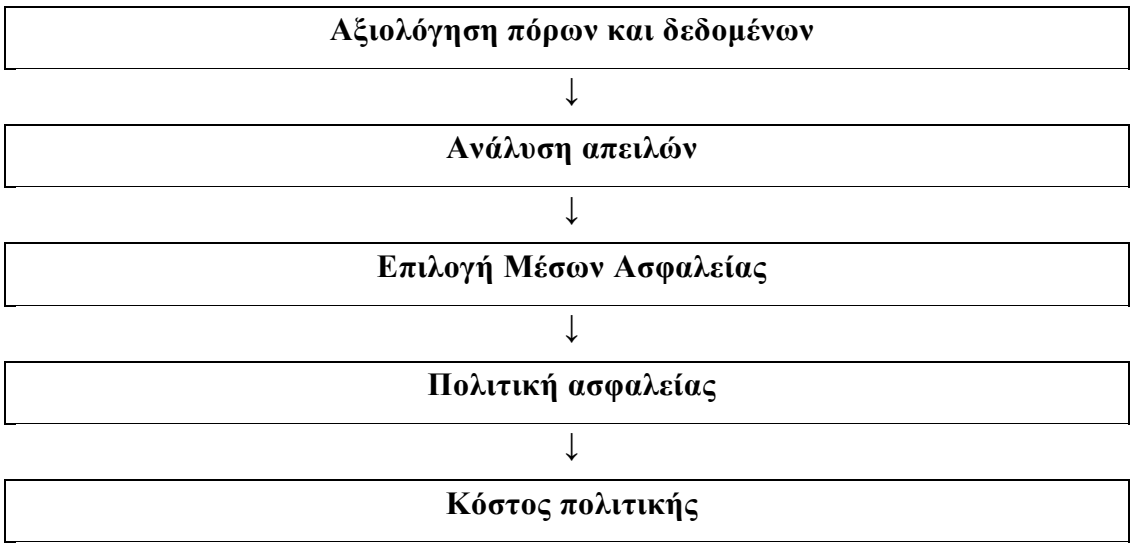
2.6. Σχέση κόστους και ωφέλειας

Η ασφάλεια των Πληροφοριακών Συστημάτων κάθε τράπεζας μπορεί να αποτελεί πρώτη μέριμνα, ώστε η ίδια και οι πελάτες της να γνωρίζω πως δεν κινδυνεύουν οι λογαριασμοί και τα δεδομένα τους, δεν παύει όμως να απορροφά πολλούς πόρους και να έχει σημαντικό κόστος. Έτσι τα μέτρα ασφαλείας που παίρνει κάθε εταιρεία και δε θα πρέπει να είναι χωρίς λόγο αυστηρά ώστε να περιορίζουν και να δυσκολεύουν τις καθημερινές της λειτουργίες και θα πρέπει να μην ξεπερνούν τον περιορισμένο χρηματικό προϋπολογισμό που μπορεί αυτή να αφιερώσει στην ασφάλεια Πληροφοριακών Συστημάτων.

Η εφαρμογή μίας διαδικασίας ανάλυσης κινδύνου (risk analysis), δίνει απαντήσεις σε ερωτήματα σχετικά με τη σχέση κόστους και ασφάλειας. Την διαδικασία ανάλυσης κινδύνου πραγματοποιούν πολλές εταιρίες, σε συνδυασμό

με τη σύγκριση του κόστους των Πληροφοριακών Συστημάτων. Ως ανάλυση κινδύνου ορίζουμε τη διαδικασία με την οποία «ελαχιστοποιείται ο κίνδυνος με την εφαρμογή μέτρων ασφαλείας ανάλογα με τις σχετικές απειλές, αδυναμίες, και αξία των πόρων περιλαμβάνει, την επιρροή που έχουν στην επιχείρηση και την επίδραση που θα επιφέρει η απώλεια ή η μη εξουσιοδοτημένη τροποποίηση δεδομένων».

Στην συνέχεια απεικονίζεται μια διαδικασία με την οποία μπορεί να βρεθεί η σωστή αναλογία ασφάλειας – κόστους.

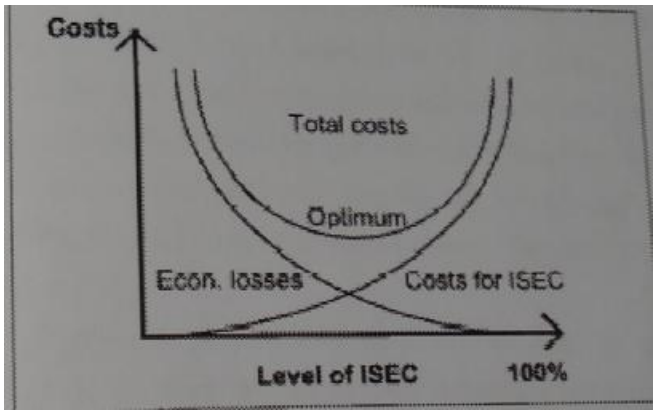


Σχήμα 1 : Η διαδικασία ανάλυσης για την ισορροπία ασφάλειας και κόστους

Το συνολικό κόστος της πολιτικής ασφάλειας, δηλαδή, θα πρέπει να είναι άμεση συνάρτηση της αξίας των πόρων και της πιθανότητας να εκδηλωθεί κάποια απειλή. Και πάλι όμως είναι δύσκολο να απαντηθεί το εάν το κόστος της πολιτικής ασφάλειας έχει τελικά μια ικανοποιητική απόδοση. Όπως αναφέρει και ο Andersen θα ήταν πολύ καλό εάν θα μπορούσε με μια διαδικασία (όπως η παραπάνω) να έβγαινε ένα μέγεθος που θα αντιπροσώπευε την επικινδυνότητα όπως π.χ. «υπάρχει πιθανότητα 83,2% να υποστούμε μια απώλεια αξιών «ΠΑΣ 1» μέσα στον επόμενο χρόνο.» Κάτι τέτοιο όμως δεν μπορεί να γίνει στα

Πληροφοριακά Συστήματα γιατί δεν υπάρχουν τέτοιες απολύτως μετρήσιμες πληροφορίες.

Ωστόσο σύμφωνα με κάποιους συγγραφείς θα μπορούσε να κατασκευαστεί ένα σχήμα όπως το παρακάτω, ώστε να βρεθεί ένα σημείο ισορροπίας ανάμεσα στις οικονομικές ζημιές εξαιτίας κενών ασφαλείας και του κόστους ασφαλείας Πληροφοριακού Συστήματος. Από το σχήμα συνάγεται το συμπέρασμα ότι όσο υψηλότερο είναι το κόστος για την ασφάλεια των Πληροφοριακών Συστημάτων τόσο μικρότερες είναι οι ζημιές εξαιτίας κενών. Από την άλλη πλευρά όμως το κόστος αυξάνεται, όσο αυξάνεται η ασφάλεια. Συνεπώς για κάθε εταιρεία το κόστος ισορροπίας θα είναι διαφορετικό, εξαιτίας της διαφορετικής ανάγκης για ασφάλεια.



Σχήμα 2 : Κόστος, οικονομικές ζημιές και κόστος ασφάλειας ΠΣ

Το παραπάνω σχήμα δεν θέλει να υπονοήσει ότι μπορούμε να βρούμε ένα συγκεκριμένο και μετρήσιμο σημείο ασφαλείας π.χ. 62% ως άριστο, αλλά μόνο ότι κάθε συγκεκριμένο μέτρο ασφαλείας βελτιώνει το επίπεδο όσο οδηγούμαστε και πιο δεξιά στο σχεδιάγραμμα.

Καταλήγοντας λοιπόν θα λέγαμε ότι το δόγμα «ασφάλεια για την ασφάλεια» απορρίπτεται πλήρως και ότι όπως πάντα η μέση οδός είναι η καλύτερη, ώστε να καταλήξουμε σε μια πολιτική ασφαλείας η οποία και τελικά θα επιτυγχάνει το σκοπό της και δεν θα καταναλώνει άσκοπα μεγάλο μέρος χρηματικών πόρων.

2.7. Παράγοντες επιτυχίας των πολιτικών ασφαλείας

Για να πετύχει τους στόχους της μια πολιτική ασφαλείας θα πρέπει να συντρέχουν κάποιο λόγοι κατά την εφαρμογή της. Οι σημαντικότεροι παράγοντες που μπορούν να οδηγήσουν μια πολιτική ασφαλείας στην επιτυχία είναι οι εξής :

α)*Υποστήριξη από την ανώτερη διοίκηση:* Είναι σημαντικό η διοίκηση της εταιρείας να εμπλακεί ενεργά και όσο το δυνατόν νωρίτερα στη διαδικασία διαμόρφωσης της πολιτικής ασφαλείας και να υποστηρίζει ενεργά και με εμφανές τρόπο όλες τις διαδικασίες για την εφαρμογή της πολιτικής. Έτσι εξασφαλίζεται ότι αποδίδεται η αρμόζουσα σημασία στην ασφάλεια ΠΣ μέσα στην εταιρεία, ενώ και οι ενέργειες που αφορούν σε μέτρα θα έχουν την υποστήριξη της διοίκησης ώστε να γίνονται αποδεκτές από τους χρήστες. Επίσης με αυτό τον τρόπο εξασφαλίζονται οι απαραίτητοι πόροι για την υλοποίηση της πολιτικής.

β) *Ευθυγράμμιση με τους επιχειρησιακούς στόχους*. Οι στόχοι και οι δράσεις που περιλαμβάνονται στην πολιτική ασφαλείας θα πρέπει να αντικατοπτρίζουν και τους γενικότερους στόχους του οργανισμού. Η κατανόηση των επιχειρηματικών στόχων κάθε εταιρείας έχει μεγάλη σημασία για τη δημιουργία μιας αποτελεσματικής πολιτικής ασφαλείας. Σε καμία περίπτωση δε θα πρέπει η πολιτική ασφαλείας να είναι πολύ αυστηρή και περιοριστική ώστε να εμποδίζει τους χρήστες στις καθημερινές τους εργασίες. Η διαμόρφωση της πολιτικής ασφαλείας πρέπει να έχει ως γνώμονα την ωφέλεια του οργανισμού.

γ) *Συμβατότητα με την υπάρχουσα κουλτούρα*. Η προσέγγιση που υιοθετεί η πολιτική ασφαλείας και τα μέτρα προστασίας που προδιαγράφει θα πρέπει να είναι συνεπή μεταξύ τους και να είναι συμβατά με την οργανωσιακή κουλτούρα της εταιρείας, ώστε να γίνουν εύκολα αποδεκτά από το σύνολο των μελών της επιχείρησης.

δ) Ενημέρωση και ευαισθητοποίηση των χρηστών. Το σύνολο των μελών του οργανισμού, διοικητικά στελέχη και υπάλληλοι, θα πρέπει να γνωρίζουν τις απειλές για τα Πληροφοριακά Συστήματα και τις επιπτώσεις που μπορεί να έχουν

όπως και να συμμερίζονται τη σημασία της ασφάλειας των Πληροφοριακών Συστημάτων.

ε) Εκπαίδευση και κατάρτιση. Οι χρήστες των Πληροφοριακών Συστημάτων θα πρέπει να λάβουν και αντίστοιχη εκπαίδευση στη σωστή εφαρμογή της πολιτικής ασφαλείας και των μέτρων προστασίας, όπως για παράδειγμα η σωστή διαχείριση των συνθηματικών τους, η αποφυγή χρήσης παράνομου λογισμικού και ο εντοπισμός περιστατικών παραβίασης της ασφάλειας.

στ) Αξιολόγηση της πολιτικής. Η πολιτική ασφαλείας θα πρέπει ανά τακτά χρονικά διαστήματα να επαναξιολογείται και να εκτιμώνται τα δυνατά και αδύνατα σημεία της, ώστε να μπορεί να τροποποιείται επιτυχώς και παράλληλα να ακολουθεί και τις προόδους της τεχνολογίας.

ζ) Σταδιακή εφαρμογή. Η εφαρμογή μιας νέας πολιτικής ασφαλείας συνεπάγεται πολλές αλλαγές στο τρόπο λειτουργίας των Πληροφοριακών Συστημάτων και για αυτό, θα πρέπει να γίνεται σταδιακή εφαρμογή της, ώστε να παρέχεται ο απαιτούμενος χρόνος στους χρήστες των Πληροφοριακών Συστημάτων να εξοικειωθούν με τους νέους ρόλους τους.

ΚΕΦΑΛΑΙΟ 3^{ο}: Παράδειγμα τυπικών τραπεζικών εφαρμογών

3.1. E- banking

Στην εποχή μας, την εποχή του Internet και της πληροφορίας, το ηλεκτρονικό εμπόριο και οι ηλεκτρονικές συναλλαγές έχουν ένα σημαντικά αυξανόμενο ρόλο. Όλο και περισσότερα άτομα εμπιστεύονται το Internet για να αγοράσουν προϊόντα και υπηρεσίες, εκμεταλλευόμενα τη δυναμική του Διαδικτύου, την άμεση συγκρισιμότητα τιμών και προϊόντων που προσφέρει, την άνεση του να κάνουν αγορές από τον χώρο τους κλπ. Παράλληλα με το ηλεκτρονικό εμπόριο, αναπτύσσεται και η ηλεκτρονική τραπεζική (e-banking) καθώς όλο και περισσότερες συναλλαγές πραγματοποιούνται ηλεκτρονικά. Επίσης οι τράπεζες προσφέρουν και πολλές επιπλέον δυνατότητες e-banking όπως πληρωμή λογαριασμών, μεταφορά ποσών κλπ.

Μοναδικό εμπόδιο στην ανάπτυξη του e-banking (αλλά και του ηλεκτρονικού εμπορίου γενικότερα) αποτελεί το ζήτημα της ασφάλειας των συναλλαγών που γίνονται μέσω αυτού, κάτι που όλοι γνωρίζουμε και από προσωπική πείρα. Οι φόβοι για την ασφάλεια των συναλλαγών είναι ένας από τους κύριους λόγους που αποτρέπει τους χρήστες από το να μην πραγματοποιούν ηλεκτρονικές συναλλαγές, σύμφωνα με έρευνες που έχουν διεξαχθεί. Σύμφωνα με τις τελευταίες, το 70% των καταναλωτών είχαν ανησυχία για κατάχρηση της πιστωτικής κάρτας τους και των προσωπικών δεδομένων τους όταν πραγματοποιούσαν on – line συναλλαγές.

Επιπλέον - σύμφωνα με την ίδια έρευνα - το 70% των ανθρώπων που συμμετείχαν σε αυτήν δήλωσαν, πώς αν αυτοί οι φόβοι τους αντιμετωπίζονταν κατά κάποιο ποσοστό επιτυχώς ή εξαφανίζονταν τελείως, θα έκαναν στο εξής αγορές ή άλλες ηλεκτρονικές συναλλαγές. Αλλά και χωρίς το ζήτημα των ηλεκτρονικών συναλλαγών το Διαδίκτυο φαίνεται από μόνο του ότι δημιουργεί προβληματισμό σχετικά με την ασφάλεια χρήσης του. Κάτι τέτοιο προκύπτει και

από την ιεράρχηση των προβλημάτων που πιστεύουν οι χρήστες ότι υπάρχουν στο Internet και παρατίθενται παρακάτω κατά σειρά ιεράρχησης :

- Ιδιωτικότητα
- Ασφάλεια
- Προστασία των παιδιών
- Ασφάλεια των e – mail
- Παραποίηση ταυτότητας και λογοκρισία

Με βάση όλα τα παράπονο κατανοούμε πως οι χρήστες του Internet δεν αισθάνονται ακόμα την απαραίτητη άνεση και σιγουριά για να πραγματοποιούν μεγάλο όγκο των συναλλαγών τους ηλεκτρονικά. Κατά συνέπεια οι τράπεζες πρέπει να δίνουν μεγάλο βάρος στην ασφάλεια κατά τις διαδικασίες και λειτουργίες του e-banking τόσο για να αντιμετωπίζουν τους πραγματικούς κινδύνους που υπάρχουν, όσο όμως και για να καθησυχάζουν το χρήστη.

3.2. Τεχνολογία e-banking

Όλα αυτά τα συμπεράσματα δε θα πρέπει να ερμηνευτούν ως απαισιόδοξα ή αρνητικά για την εξέλιξη του e-banking και των ηλεκτρονικών συναλλαγών. Αντιθέτως, οι ηλεκτρονικές συναλλαγές παρ' όλους τους προβληματισμούς που εξηγήσαμε ότι υπάρχουν αυξάνονται ραγδαία. Για παράδειγμα, από μία έρευνα σε 400 επιχειρήσεις στις ΗΠΑ προέκυψε ότι μέσα στο 2000 σχεδόν διπλασιάστηκε ο αριθμός των επισκεπτών στις ιστοσελίδες τους, σε ώρες αιχμής, από 6300 σε 12000. Αντίστοιχα, ο αριθμός των συναλλαγών ανά ημέρα μέσω των ιστοσελίδων αυξήθηκε από 2000 σε 23000.

Από όλα τα παραπάνω κατανοούμε ότι το e-banking θέτει ορισμένες προκλήσεις για τις τράπεζες αναφορικά με την απόδοση των συστημάτων, τον αριθμό των επισκεπτών και την ασφάλεια των συναλλαγών. Άρα η δημιουργία της υποδομής για e-banking πρέπει να γίνεται με σωστό σχεδιασμό και με κάποια συγκεκριμένα χαρακτηριστικά, χωρίς να δίνεται έμφαση μόνο στην τεχνική πλευρά του.

Σύμφωνα με τους συγγραφείς του βιβλίου «Ηλεκτρονικό Επιχειρείν: Προγραμματισμός και Σχεδίαση», τα χαρακτηριστικά και οι απαιτήσεις που πρέπει να ικανοποιεί ένα σύστημα Ηλεκτρονικού Επιχειρείν είναι τα ακόλουθα.

Εύκολη και γρήγορη επεκτασιμότητα. Το χαρακτηριστικό αυτό επιτρέπει στο δικτυακό τόπο να ανταποκρίνεται γρήγορα στις αλλαγές που προκύπτουν στο πολυτάραχο επιχειρηματικό περιβάλλον του Ηλεκτρονικού Επιχειρείν. Σύμφωνα με αρκετούς υπευθύνους πληροφοριακών συστημάτων, ο αριθμός των αναβαθμίσεων που χρειάζεται ένα σύστημα Ηλεκτρονικού Επιχειρείν είναι από 10 έως 20 σε ένα εξάμηνο.

Ασφάλεια. Η αμφισβήτηση της ασφάλειας των συναλλαγών, αποτελεί το κυριότερο εμπόδιο στην ακόμα μεγαλύτερη ανάπτυξη του Ηλεκτρονικού Επιχειρείν. Επομένως γίνεται φανερό ότι μία ψηφιακή εταιρεία πρέπει να σχεδιάσει το δικτυακό της τόπο ώστε να προσφέρει τη μέγιστη ασφάλεια στους πελάτες της.

Αξιοπιστία. Οι υπεύθυνοι των πληροφοριακών συστημάτων που υποστηρίζουν εφαρμογές Ηλεκτρονικού Επιχειρείν προσπαθούν να επιτύχουν τη μεγαλύτερη δυνατή διαθεσιμότητα των εφαρμογών, ώστε να μπορεί το ψηφιακό κατάστημα να λειτουργεί 24 ώρες την ημέρα, επτά ημέρες την εβδομάδα, με εγγυημένη την υψηλή ποιότητα των υπηρεσιών του. Σε αυτό το σημείο η αρχιτεκτονική του υπολογιστικού συστήματος παίζει τον πρώτο και κύριο ρόλο στην αδιάκοπη λειτουργία του δικτυακού τόπου, καθώς ο αναποτελεσματικός σχεδιασμός ενός συστήματος συνεπάγεται την αύξηση του χρόνου που το σύστημα είναι εκτός λειτουργίας.

Μεταφερσιμότητα. Οι εφαρμογές του ψηφιακού καταστήματος πρέπει να διαθέτουν τη δυνατότητα να εκτελούνται κάτω από διαφορετικά λειτουργικά συστήματα και browsers που διαθέτουν οι χρήστες του διαδικτύου.

Ευχρηστία. Ένα σύστημα το οποίο υποστηρίζει εφαρμογές Ηλεκτρονικού Επιχειρείν μπορεί να μεγαλώσει τόσο πολύ για να είναι σε θέση να ικανοποιήσει την αυξημένη ζήτηση σε σύντομο χρονικό διάστημα, με

αποτέλεσμα να μετατραπεί σε έναν πολύπλοκο μηχανισμό του οποίου η διάχυση να είναι πολυέξοδη και αδύνατη.

Παρατηρούμε δηλαδή, ότι η τεχνολογική υποδομή που χρειάζεται ένα σύστημα e-banking θα πρέπει να ικανοποιεί όλες τις παραμέτρους για τη σωστή λειτουργία του και παράλληλα να είναι ασφαλές, εννοώντας την ασφάλεια, τόσο από την πλευρά της μη παραβίασης του συστήματος από τρίτους, όσο και από την πλευρά της αδιάλειπτης λειτουργίας του. Για αυτούς τους λόγους, χρησιμοποιείται στο e-banking μία συγκεκριμένη αρχιτεκτονική σχεδίασης, γνωστή ως μοντέλο client/server, σύμφωνα με την όποια ο πελάτης (client) επικοινωνεί με τον εξυπηρετητή (server) μέσω Διαδικτύου με τη χρήση ενός απλού web browser. Ο web browser εμφανίζει σελίδες γραμμένες σε HTML ή σε κάποια δυναμική γλώσσα προγραμματισμού (όπως η ASP ή η PHP), οι οποίες είναι κωδικοποιημένες με τη χρήση του πρωτοκόλλου https.

Η μεγάλη αύξηση όμως των χρηστών του Διαδικτύου που κάνουν χρήση των δυνατοτήτων του e-banking αλλά και η ανάγκη για συνεχή και απρόσκοπτη λειτουργία οδήγησαν τις τράπεζες στη χρησιμοποίηση περισσοτέρων από έναν server. Αν και σχετικά ακριβή λύση είναι η μόνη που επιτρέπει επιτυχή διαμερισμό της κίνησης ώστε να εξυπηρετούνται όλοι οι χρήστες και εγγύηση του ότι το σύστημα θα είναι σχεδόν πάντα διαθέσιμο. Ωστόσο απλά η προσθήκη περισσοτέρων εξυπηρετητών δεν δίνει από μόνη της λύση στο πρόβλημα, χωρίς τη χρήση κάποιας συσκευής η οποία θα διαμοιράζει τους χρήστες ανάμεσα στους διάφορους server. Αυτή η συσκευή, που είναι γνωστή ως δρομολογητής (router), επιτυγχάνει με αυτό τον τρόπο να βελτιώσει σημαντικά στην αποδοτικότητα του συστήματος e-banking.

Ο δρομολογητής κάθε φορά που κάποιος χρήστης χρησιμοποιεί την πλατφόρμα e-banking της τράπεζας, ανταποκρίνεται διανέμοντας τα πακέτα δεδομένων σε όποιον εξυπηρετητή είναι διαθέσιμος εκείνη τη στιγμή. Διαμοιράζει, δηλαδή, ομαλά τον όγκο εργασίας ανάμεσα στους server, έτσι ώστε να μην επιβαρύνεται κάποιος πολύ, ενώ παρακάμπτει και όσους server είναι εκείνη τη στιγμή εκτός λειτουργίας λόγω προβλήματος. Η διανομή των πακέτων δεδομένων γίνεται αυτόματα από τον δρομολογητή με βάση τη δυνατότητα που έχει εκείνη τη στιγμή κάθε εξυπηρετητής. Όταν ο router διαπιστώσει πώς κάποιος από τους εξυπηρετητές δεν

λειτουργεί εκείνη τη στιγμή για κάποιο λόγο, τον διαγράφει προσωρινά από τον πίνακα δρομολογίων που έχει, ώστε, μέχρι αυτός να επανέλθει, να μην του στέλνει καθόλου δεδομένα.

Με την χρήση αυτού του εξοπλισμού και αυτής της τεχνολογίας ο τραπεζικός οργανισμός είναι σίγουρος πως είναι διασφαλισμένος έναντι των τεχνικών προβλημάτων των server και πως απολαμβάνει τη μέγιστη δυνατή λειτουργία του συστήματος.

Προσπαθώντας να περιγράψουμε μια διαδικασία θα τονίζαμε ότι στο πρώτο στάδιο βρίσκεται ο πελάτης (client), ο οποίος μέσω του Διαδικτύου, επικοινωνεί με την e-banking εφαρμογή της τράπεζας. Η «αίτηση» για δεδομένα του πελάτη φθάνει στον router (δεύτερο στάδιο), ο οποίος δρομολογεί τα δεδομένα στον web server που μπορεί να ανταποκριθεί εκείνη τη στιγμή. Ο web server περιέχει τις ιστοσελίδες της τράπεζας και στέλνει στον πελάτη τα δεδομένα μέσω του πρωτοκόλλου http. Ταυτόχρονα ο application server (τρίτο στάδιο) περιέχει την εφαρμογή του e-banking και εκτελεί τις λειτουργίες που ζητάει ο χρήστης (πχ μεταφορά υπολοίπου κλπ). Όλα τα ευαίσθητα δεδομένα του πελάτη (οικονομικά στοιχεία κλπ) βρίσκονται στις κεντρικές βάσεις δεδομένων της τράπεζας (τέταρτο στάδιο). Οι application servers επικοινωνούν με τις βάσεις δεδομένων για να εμφανίσουν στον χρήστη τις λεπτομέρειες του λογαριασμού του. Οι βάσεις δεδομένων περιέχουν όλα τα στοιχεία των πελατών της τράπεζας μαζί με όλα τα οικονομικά ποσά γι' αυτό προστατεύονται επιπλέον με κωδικούς και άλλα μέσα.

2. Κρυπτογραφία

ΚΕΦΑΛΑΙΟ 4^{ο} : Κρυπτογραφία και αλγόριθμοι

4.1. Ορολογία Κρυπτογραφίας

Εκτός από την ασφάλεια νοούμενη ως αποτροπή διακοπής της λειτουργία του συστήματος e-banking, υπάρχει και η ασφάλεια ως αποτροπή της μη εξουσιοδοτημένης πρόσβασης κάποιου στην εφαρμογή. Αυτή ακριβώς η πλευρά της ασφάλειας, αποτελεί το σημαντικότερο εμπόδιο στη συνείδηση των πολιτών για την ανάπτυξη του ηλεκτρονικού εμπορίου.

Για αυτό ακριβώς το λόγο έχουν αναπτυχθεί αρχές κρυπτογράφησης, των δεδομένων που διακινούνται ηλεκτρονικά, ώστε να διασφαλίζεται πώς μόνο ο πελάτης (client) και ο εξυπηρετητής (server) θα μπορούν να έχουν πρόσβαση σε αυτά. Η κρυπτογραφία, η οποία αποτελεί κλάδο των μαθηματικών, έχει μεγάλη και εντυπωσιακή ιστορία που φτάνει χιλιάδες χρόνια πίσω ενώ πια ουσιαστικά αποτελεί ξεχωριστή επιστήμη. Οι επιστήμονες που ασχολούνται με την κρυπτογραφία ονομάζονται κρυπτογράφοι. Οι εφαρμογές είναι πολλές και ποικίλες:

• Ασφαλείς δικτυακές επικοινωνίες
• Ασφαλής αποθήκευση αρχείων
• Ασφαλές ηλεκτρονικό ταχυδρομείο
• Ασφαλές ηλεκτρονικό εμπόριο

Η κρυπτογραφία είναι απαραίτητο εργαλείο, αλλά δεν είναι πανάκεια. Ασφαλείς αλγόριθμοι και πρωτόκολλα υπάρχουν, αλλά η εφαρμογή τους απαιτεί σημαντική πείρα. Αρκετοί τομείς της ασφάλειας που αφορούν την διάδραση με ανθρώπους (διαχείριση κλειδιών, ασφάλεια κατά την διαλογή ανθρώπου-μηχανής, έλεγχος πρόσβασης) πολλές φορές είναι υπερβολικά δύσκολο να αναλυθούν. Επιπλέον οι αρχές που διέπουν άμεσα σχετιζόμενα πεδία, όπως η κρυπτογραφία

δημόσιου κλειδιού, η ασφάλεια λογισμικού, η ασφάλεια υπολογιστών, η ασφάλεια δικτύων και ο σχεδιασμός απαραβίαστου υλικού πολλές φορές αγνοούνται.

4.2. Ορολογία αλγόριθμοι και κλειδιά

Ένας *κρυπτογραφικός αλγόριθμος*, ή απλά κώδικας είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για κρυπτογράφηση και αποκρυπτογράφηση (γενικά υπάρχουν δύο συσχετιζόμενες συναρτήσεις: μία για κρυπτογράφηση και μία για αποκρυπτογράφηση).

Αν η ασφάλεια που προσφέρει ένας αλγόριθμος βασίζεται στην απόκρυψη του μηχανισμού λειτουργίας του, τότε μιλάμε για περιορισμένο αλγόριθμο. Τέτοιου είδους αλγόριθμοι έχουν ιστορικό ενδιαφέρον, αλλά είναι τραγικά ανεπαρκείς για τα σημερινά δεδομένα. Καταρχήν, δεν μπορούν να χρησιμοποιηθούν από μεγάλες ομάδες ανθρώπων ή από ομάδες που δεν έχουν σταθερά μέλη, επειδή αν κάποιος εγκαταλείψει την ομάδα ή αν το μυστικό διαρρεύσει, ο αλγόριθμος θα πρέπει να αλλάξει.

Ακόμα σημαντικότερο είναι ότι οι περιορισμένοι αλγόριθμοι δεν επιτρέπουν έλεγχο ποιότητας ή προτυποποίηση. Η κάθε ομάδα θα πρέπει να έχει τον δικό της αλγόριθμο, που επιπλέον θα πρέπει να έχει η ίδια κατασκευάσει. Χωρίς καλό κρυπτογράφο, η ομάδα θα είναι αφημένη στο έλεος της μοίρας. Παρά τα σημαντικά αυτά μειονεκτήματα, οι περιορισμένοι αλγόριθμοι είναι εξαιρετικά δημοφιλείς σε εφαρμογές μικρής ασφάλειας.

Το πρόβλημα της γνωστοποίησης του αλγόριθμου έχει λυθεί από την σύγχρονη κρυπτογραφία με το κλειδί. Το *κλειδί* παίρνει τιμή από ένα πεδίο ορισμού, που γενικά διαφέρει από αλγόριθμο σε αλγόριθμο. Τόσο κατά την κρυπτογράφηση όσο και κατά την αποκρυπτογράφηση χρησιμοποιούνται κλειδιά. Τα κλειδιά αυτά μπορεί να είναι ίδια ή διαφορετικά.

Στους αλγόριθμους που χρησιμοποιούν διαφορετικά κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση, όλη η ασφάλεια έγκειται στο κλειδί και όχι στον ίδιο τον αλγόριθμο. Μόνο η γνώση του κλειδιού επιτρέπει ανάκτηση του

αρχικού κειμένου. Αυτό σημαίνει ότι ο αλγόριθμος μπορεί να δημοσιευτεί και να αναλυθεί, όπως επίσης και ότι μπορεί να χρησιμοποιηθεί σε προϊόντα μαζικής παραγωγής. Ένας αλγόριθμος μαζί με όλα τα δυνατά κείμενα, κρυπτογραφήματα και κλειδιά λέγεται κρυπτοσύστημα.

4.3. Εισαγωγή στην κρυπτογραφία

Ας θεωρήσουμε ότι κάποιος αποστολέας επιθυμεί να στείλει ένα μήνυμα σε κάποιον παραλήπτη και επιπλέον ότι θέλει να εξασφαλίσει πως κανείς τρίτος δεν θα μπορεί να το διαβάσει. Το μήνυμα το ονομάζουμε καθαρό κείμενο ή αρχικό κείμενο ή απλά κείμενο (cleartext ή plaintext). Η διαδικασία μεταλλαγής του μηνύματος, κατά τρόπο που να αποκρύπτει το περιεχόμενο του, ονομάζεται κρυπτογράφηση (encryption ή enciphering). Ένα κρυπτογραφημένο κείμενο ονομάζεται κρυπτογράφημα (ciphertext).

Τα συστήματα κρυπτογράφησης λειτουργούν ως εξής:

- Αρχικά εισάγεται το λεγόμενο απλό κείμενο, το οποίο είναι το αρχικό κείμενο που θέλουνε να κρυπτογραφηθεί
- Στη συνέχεια χρησιμοποιείται ο κρυπτογραφικός αλγόριθμος, ο οποίος μέσω μαθηματικών συναρτήσεων μετατρέπει το απλό κείμενο σε κρυπτογραφημένο.
- Για την κρυπτογράφηση του κειμένου χρησιμοποιείται ένα κλειδί, το οποίο ουσιαστικά είναι μία παράμετρος του κρυπτογραφικού αλγόριθμου. Μόνο ο κάτοχος του κλειδιού μπορεί να αποκρυπτογραφήσει ένα κείμενο.
- Τέλος καταλήγουμε στο κρυπτογραφημένο κείμενο, που είναι το αρχικό κείμενο τροποποιημένο με βάση το κλειδί και τον αλγόριθμο.

Παρατηρούμε λοιπόν ότι κάποιος που δεν έχει στην κατοχή του το κλειδί κρυπτογράφησης, δε θα μπορεί να διαβάσει το αρχικό μήνυμα. Θα μπορούσε όμως με αλλεπάλληλες και συνεχείς δοκιμές να προσπαθεί να βρει το κλειδί, μέχρις ότου να αποκρυπτογραφήσει το αρχικό κείμενο. Ο βαθμός ευκολίας ανακάλυψης του κλειδιού κρυπτογράφησης, εξαρτάται από το μήκος χαρακτήρων, καθώς, όπως

εύκολα κατανοούμε, από όσο πιο πολλούς χαρακτήρες αποτελείται, τόσο αυξάνουν γεωμετρικά οι πιθανοί συνδυασμοί του και τόσο πιο δύσκολο να γίνεται να δοκιμαστούν όλοι σειριακά. Σήμερα το μήκος κλειδιού που χρησιμοποιείται από τις τράπεζες για την κρυπτογράφηση των δεδομένων τους είναι 128 bit που θεωρείται υπεραρκετό για την ασφάλεια των δεδομένων.

Μία επιτυχημένη τεχνολογία κρυπτογράφησης που χρησιμοποιείται από όλες τις τράπεζες είναι το Secure Sockets Layer ή αλλιώς SSL, το οποίο αρχικά είχε αναπτυχθεί από την εταιρεία Netscape και η πρώτη του έκδοση κυκλοφόρησε το 1994. Σήμερα βρισκόμαστε στην τρίτη έκδοση του πρωτοκόλλου SSL, που έχει καθιερωθεί σαν το σημαντικότερο πρωτόκολλο επικοινωνίας για ασφαλείς συναλλαγές, ξεπερνώντας πολλές άλλες προσπάθειες (πχ το πρωτόκολλο PCT της Microsoft).

Το SSL λειτουργεί με τον τρόπο που περιγράφηκε προηγουμένως, κρυπτογραφώντας τα δεδομένα πριν την αποστολή του και αποκρυπτογραφώντας τα όταν παραληφθούν. Η χρήση του SSL είναι εμφανής στον πελάτη κατά τις ασφαλείς συνδέσεις, από τη χρήση του πρωτοκόλλου https (αντί του κανονικού http) και από την εμφάνιση στον browser ενός εικονιδίου που χαρακτηρίζει τη σύνδεση ως ασφαλή.

Το πρωτόκολλο SSL παρέχει συνολικά τις εξής λειτουργίες :

> Κρυπτογράφηση δεδομένων
> Πιστοποίηση εξυπηρετητή
> Ακεραιότητα μηνυμάτων
> Προαιρετική πιστοποίηση πελάτη

Για να αυξηθεί ακόμη περισσότερο το αίσθημα ασφάλειας στο χρήστη υπάρχουν και κάποιοι εμπορικοί οργανισμοί που λειτουργούν ως αρχές πιστοποίησης του επιπέδου ασφάλειας των ηλεκτρονικών συναλλαγών. Οι οργανισμοί αυτοί χορηγούν σε κάθε ηλεκτρονικό κατάστημα ένα πιστοποιητικό μέσω του οποίου βεβαιώνουν την αυθεντικότητα και το επίπεδο ασφαλείας του καταστήματος.

Αν θέλαμε να δώσουμε έναν πιο αυστηρό ορισμό στην έννοια της πιστοποίησης θα λέγαμε ότι, πιστοποίηση είναι η διαδικασία μέσω της οποίας ένας οργανισμός ή διαδικασία δοκιμάζεται, αξιολογείται και βαθμολογείται σε μνα

προσπάθεια να καθοριστεί εάν συμμορφώνεται ή όχι με κάποιο συγκεκριμένο πρότυπο λειτουργίας.

Οι οργανισμοί πιστοποίησης δημιουργούν αυτοπεποίθηση και εμπιστοσύνη στο χρήστη σχετικά με τις ηλεκτρονικές συναλλαγές. Η «ηλεκτρονική σφραγίδα» που παρέχει ο οργανισμός πιστοποίησης τοποθετείται στην ηλεκτρονική σελίδα της πιστοποιημένης εταιρείας παρέχοντας πληροφόρηση στον πελάτη για το επίπεδο ασφάλειας, το είδος κλπ. Έτσι λοιπόν ο χρήστης μπορεί να είναι σίγουρος ότι η τράπεζα με την οποία συναλλάσσεται ηλεκτρονικά, κάνει χρήση συγκεκριμένων αρχών ασφαλείας και κρυπτογράφησης, απαλλάσσοντας τον από το άγχος του να πρέπει να μάθει από εμπειρίες τρίτων, αν η συγκεκριμένη τράπεζα είναι ασφαλής, εάν άλλοι είχαν αντιμετωπίσει προβλήματα κλπ.

4.4. Ιστορική αναδρομή

Η μετάβαση από τον προφορικό λόγο στο γραπτό ήταν σίγουρα ένα μεγάλο βήμα για τον ανθρώπινο πολιτισμό. Ήδη όμως στα χρόνια του αρχαίου Ελληνικού πολιτισμού υπήρχε επίγνωση και των αρνητικών συνεπειών που επέφερε η καταγραφή κάθε είδους πληροφορίας. Η αρνητική αυτή συνέπεια της γραφής ήταν ότι μπορούσε το γραπτό να πέσει σε χέρια που δεν έπρεπε. Άρα λοιπόν ή δεν έπρεπε να γράφονται πληροφορίες ζωτικής σημασίας ή έπρεπε να βρεθεί τρόπος προστασίας των γραπτών αυτών πληροφοριών ώστε να μπορούν να διαβαστούν μόνο από αυτούς που έπρεπε.

Η λέξη κρυπτογραφία είναι σύνθετη. Το πρώτο συνθετικό της είναι το κρυπτο και το δεύτερο συνθετικό είναι το γράφω. Άρα λοιπόν κρυπτογραφία σημαίνει κρύβω αυτά που γράφω. Η κρυπτογραφία λοιπόν είναι η επιστήμη ή η τέχνη της απόκρυψης του γραπτού λόγου από ανεπιθύμητους αναγνώστες. Η κρυπτογραφία είχε αρχικά την μορφή τέχνης που τα μυστικά της γνώριζαν λίγοι και εκλεκτοί. Η ιστορία της κρυπτογραφίας ξεκινά περίπου το 4000 π.Χ. στην αρχαία Αίγυπτο περνά στην αρχαία Ελλάδα που έχουμε αναφορές της στο ιστορικό Πολύβιο και συνεχίζεται στον Ιούλιο Καίσαρα που ήταν από τους πρώτους που την χρησιμοποίησαν ευρύτατα για

στρατιωτικούς σκοπούς. Έτσι όλα τα μηνύματα του Καίσαρα προς τους στρατηγούς των λεγεώνων του ήταν κρυπτογραφημένα ώστε ο εκάστοτε εχθρός να μην είναι σε θέση να γνωρίζει τα σχέδια του, ακόμη και αν ο αγγελιοφόρος έπεφτε στα χέρια του εχθρού. Ο τρόπος κρυπτογράφησης ήταν απλός. Αν ήθελε για παράδειγμα να μεταφέρει την εντολή ΕΠΙΘΕΣΗ έστελνε την λέξη ΗΣΛΚΗΥΙ πού προέκυπτε αν κάθε γράμμα της αρχικής λέξης το αντικαθιστούσε με το μεθεπόμενο γράμμα στο αλφάβητο. Ο παραλήπτης στρατηγός δεν είχε παρά να αντικαταστήσει κάθε γράμμα του μηνύματος με το προ-προηγούμενο γράμμα της αλφαβήτου.

Όπου : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Αντικατάσταση με: DEFGHIJKLMNOPQRSTUVWXYZABC

Από την στιγμή που η κρυπτογραφία άρχισε να χρησιμοποιείται για στρατιωτικούς σκοπούς και για απόκρυψη ζωτικής σημασίας πληροφοριών, έπαψε να είναι απόκρυφη τέχνη και έτυχε της μελέτης τόσο αυτών που ήθελαν να αποκρύψουν τα μυστικά τους όσο και από αυτούς που ήθελαν να βρουν τρόπο να αποκαλύψουν τα μυστικά των αντιπάλων τους. Έτσι η κρυπτογραφία πέρασε στο πεδίο της επιστήμης. Κρυπτογράφοι και κρυπταναλυτές επιδόθηκαν σε έναν ανελέητο συναγωνισμό. Κάθε πρόοδος της κρυπτογραφίας συνοδευόταν από μια αντίστοιχη πρόοδο της κρυπτανάλυσης.

Στον 20ό αιώνα τα παραδείγματα εκτεταμένης χρήσης κρυπτογραφικών τεχνικών είναι πολλά. Την περίοδο της ποτοαπαγόρευσης στην Αμερική (δεκαετία του 20-30) το νεοσύστατο τότε σώμα FBI χρησιμοποίησε τεχνικές κρυπτογραφίας για να αποκρύπτει από τη μαφία τους τόπους παράδοσης μεγάλων φορτίων ποτών. Δεν θα ήταν υπερβολή να πούμε ότι η έκβαση του δευτέρου Παγκοσμίου Πολέμου κρίθηκε υπέρ των συμμάχων εξ' αιτίας της ικανότητας τους να αποκρυπτογραφούν τα γερμανικά μηνύματα και της ανικανότητας των Γερμανών να πράξουν κάτι ανάλογο με τα συμμαχικά μηνύματα. Είναι γνωστή άλλωστε η ιστορία της μηχανής ENIGMA, που χρησιμοποίησαν οι Γερμανοί για να κρυπτογραφούν τα μηνύματα

τους προς τις αγέλες των υποβρυχίων τους, τον κωδικό της οποίας κατάφεραν να σπάσουν οι Άγγλοι.

Από την δεκαετία του 60 και μετά η κρυπτογραφία γνώρισε μεγάλη ανάπτυξη λόγω της ραγδαίας ανάπτυξης των υπολογιστών αλλά και των τηλεπικοινωνιών. Έτσι λοιπόν υπήρξε η ανάγκη για προστασία δεδομένων σε ψηφιακή μορφή. Αρχίζοντας με την εργασία του Feistel στην IBM στις αρχές της δεκαετίας του '70 και καταλήγοντας το 1977 με την υιοθέτηση σαν Αμερικανικού ομοσπονδιακού προτύπου για την επεξεργασία των πληροφοριών την κρυπτογράφηση των μη-διαβαθμισμένων πληροφοριών, DES, το πρότυπο κρυπτογράφησης στοιχείων, είναι ο πιο γνωστός κρυπτογραφικός μηχανισμός της ιστορίας. Παραμένει μέχρι σήμερα το τυποποιημένο μέσο για την ασφάλεια του ηλεκτρονικού εμπορίου σε πολλά οικονομικά ιδρύματα σε όλο τον κόσμο.

Η πιο εντυπωσιακή ανάπτυξη στην ιστορία της κρυπτογραφίας ήρθε το 1976 όταν ο Diffie και ο Hellman δημοσίευσαν το “New directions in cryptography”. Αυτή η επιστημονική δημοσίευση εισήγαγε την επαναστατική έννοια τής κρυπτογραφίας δημοσίου κλειδιού και παρείχε επίσης μια νέα και έξυπνη μέθοδο για ανταλλαγή κλειδιού, η ασφάλεια του οποίου βασίζεται στην αμεταβλητότητα του προβλήματος διακριτού λογαρίθμου. Παρόλο που οι συγγραφείς δεν έκαναν πρακτική εφαρμογή του σχήματος που πρότειναν, η αρχή είχε γίνει και το θέμα έτυχε μεγάλου ενδιαφέροντος από την κρυπτογραφική κοινότητα.

Το 1978 οι Rivest, Shamir και Adleman ανακάλυψαν την πρώτη πρακτική εφαρμογή του προταθέντος σχήματος. Ήταν το λεγόμενο σχήμα RSA και βασιζόταν σε ένα άλλο δύσκολο μαθηματικό πρόβλημα, αυτό της δυσκολίας παραγοντοποίησης μεγάλων ακεραίων. Όπως ήταν φυσικό οι κρυπταναλυτές σήκωσαν τα μανίκια και άρχισαν να ψάχνουν πιο αποτελεσματικούς τρόπους παραγοντοποίησης. Παρά τις μεγάλες προόδους τους κυρίως την δεκαετία του 80 το RSA παρέμεινε ακόμα ασφαλές! Μια από τις σημαντικότερες προσφορές της κρυπτογραφίας δημοσίου κλειδιού αποτελεί και η ψηφιακή υπογραφή.

4.5. Κρυπτογράφηση και αποκρυπτογράφηση

Σε νομικό και κοινωνικό επίπεδο, τίθεται ζήτημα προστασίας του απορρήτου σε όλες τις εκδοχές δικτυακής συναλλαγής (email, εμπορικές συναλλαγές, τραπεζικό και ιατρικό απόρρητο) και γενικότερα ζήτημα προστασίας προσωπικών δεδομένων του κάθε χρήστη του Internet. Η ανάγκη για εμπιστευτικότητα στις ηλεκτρονικές συναλλαγές ικανοποιείται με την κρυπτογράφηση.

Η κρυπτογράφηση έρχεται να εξασφαλίσει το απόρρητο των προσωπικών πληροφοριών. Πρόκειται για μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Το αρχικό μήνυμα ονομάζεται απλό κείμενο (plaintext), ενώ το ακατάληπτο μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται κρυπτογράφημα (ciphertext). Η μέθοδος που χρησιμοποιείται για να «καλυφθεί» το απλό κείμενο ονομάζεται κρυπτογράφηση (encryprion). Η μέθοδος που ακολουθείται για να επανέλθει το κρυπτογραφημένο κείμενο στην αρχική του μορφή ονομάζεται αποκρυπτογράφηση (decryption). [Εικόνα 1]

Εικόνα 1: Κρυπτογράφηση και αποκρυπτογράφηση

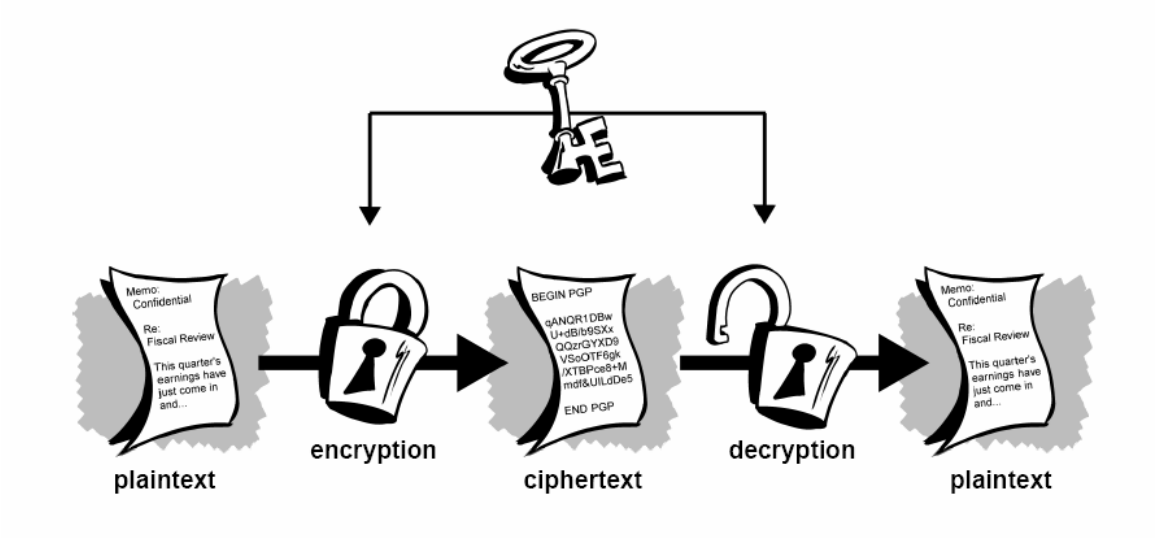
Ο αποστολέας, χρησιμοποιώντας συγκεκριμένη μαθηματική συνάρτηση, μετατρέπει το αρχικό κείμενο σε μορφή μη κατανοητή για οποιονδήποτε τρίτο (κρυπτογραφημένο κείμενο). Ο παραλήπτης, έχοντας γνώση του τρόπου

κρυπτογράφησης, αποκρυπτογραφεί το κείμενο στην αρχική του μορφή. Το μήνυμα παραμένει εμπιστευτικό, ωσότου αποκρυπτογραφηθεί.

Αποκρυπτογράφηση είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή αντίστροφου αλγορίθμου. Η κρυπτογραφημένη επικοινωνία είναι αποτελεσματική, όταν μόνο τα άτομα που συμμετέχουν σε αυτήν μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος. Η κρυπτογραφία δεν πρέπει να συγχέεται με την κρυπτανάλυση, που ορίζεται ως η επιστήμη για την ανάλυση και αποκωδικοποίηση κωδικοποιημένων πληροφοριών χωρίς τη χρήση του αντίστροφου αλγορίθμου κρυπτογράφησης.

Οι διάφορες μέθοδοι κρυπτογράφησης βασίζονται στη χρήση ενός "κλειδιού", ενός μαθηματικού δηλαδή κώδικα - αλγόριθμου (ή cipher), ο οποίος διασφαλίζει το μη "αναγνώσιμο" από τρίτους, και χρησιμοποιείται στην κρυπτογράφηση και την αποκρυπτογράφηση. Κάθε αλγόριθμος παίρνει την ονομασία του από τον αριθμό που μεταλλάσσεται και πρέπει να βρεθεί με μια σειρά μαθηματικών πράξεων. Όσο αυξάνεται ο βαθμός πολυπλοκότητας του αλγορίθμου, τόσο μειώνεται η πιθανότητα να τον προσπελάσει κάποιος.

Αρχικά το κλειδί κρυπτογράφησης ήταν το ίδιο με το κλειδί αποκρυπτογράφησης, δηλαδή αποστολέας και παραλήπτης χρησιμοποιούσαν το ίδιο συμμετρικό κρυπτογραφικό σύστημα. [Εικόνα 2]



Εικόνα 2: Συμμετρικό κρυπτογραφικό σύστημα

Το σύστημα αυτό χρησιμοποιήθηκε κυρίως σε κλειστά συστήματα και εφαρμόστηκε τη δεκαετία του '80 για τη μεταφορά τραπεζικών δεδομένων. Αργότερα η εξέλιξη οδήγησε στη χρησιμοποίηση δύο κλειδιών, ενός ιδιωτικού και ενός δημοσίου (ασύμμετρο κρυπτογραφικό σύστημα). Το ιδιωτικό κλειδί (private key) χρησιμοποιείται για το σφράγισμα του ηλεκτρονικού μηνύματος και είναι απόρρητο, ενώ το δημόσιο κλειδί (public key) αντιστοιχεί στο πρώτο, χρησιμοποιείται για την αποσφράγιση του μηνύματος και δεν είναι απόρρητο.

Συνεπώς, το πρώτο κλειδί το γνωρίζει μόνο ο αποστολέας και μόνο με αυτό μπορεί κανείς να επέμβει στο κείμενο, ενώ το δεύτερο το γνωστοποιεί σε κάθε συναλλασσόμενο του για να μπορεί να αποκρυπτογραφεί/ διαβάζει τα μηνύματα του πρώτου.

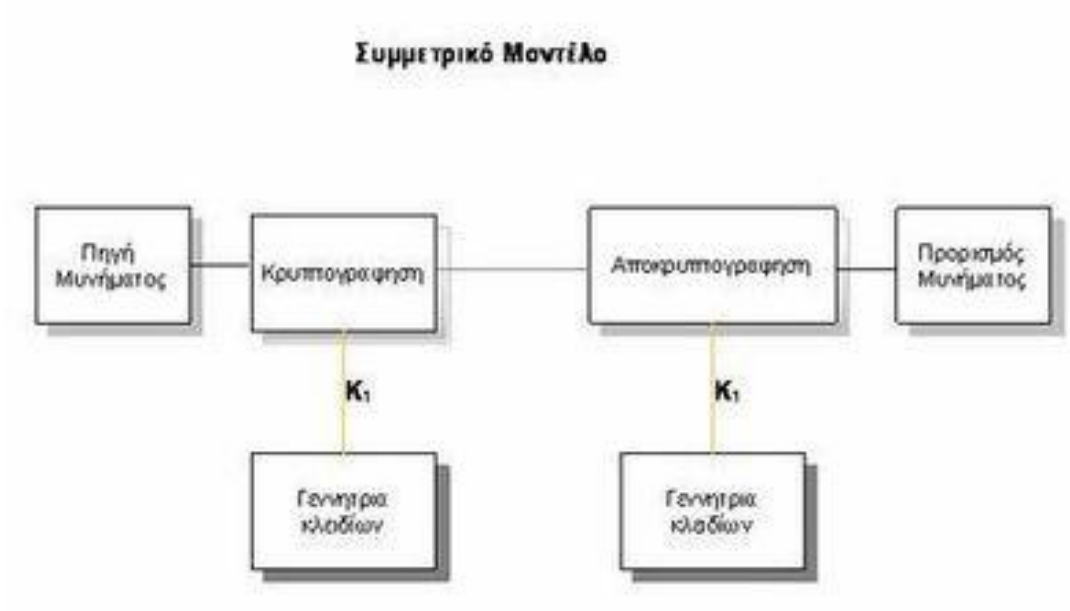
4.6. Συμμετρική κρυπτογραφία

Στη συμμετρική κρυπτογραφία [Εικόνα 2], αποκαλούμενη και ως κρυπτογράφηση μυστικού κλειδιού (secret-key), ένα κλειδί χρησιμοποιείται και για την κρυπτογράφηση και για την αποκρυπτογράφηση. Από τις πιο γνωστές μεθόδους συμμετρικής κρυπτογράφησης είναι ο αλγόριθμος DES (Data Encryption Standard), που υιοθετήθηκε ευρέως από την Αμερικάνικη κυβέρνηση και το σύστημα Kerberos του γνωστού Πανεπιστημίου MIT.

Στη συμμετρική κρυπτογραφία ο αποστολέας και ο παραλήπτης του μηνύματος χρησιμοποιούν το ίδιο (κοινό) κλειδί. Ο αποστολέας κρυπτογραφεί το μήνυμα με βάση αυτό το κλειδί και ο παραλήπτης το αποκρυπτογραφεί με βάση το ίδιο κλειδί. Αν τα δύο επικοινωνούντα μέρη βρίσκονται σε διαφορετικές τοποθεσίες, τότε θα πρέπει με κάποιον τρόπο να ανταλλάξουν το κοινό κλειδί που θα πρέπει να χρησιμοποιήσουν. Αυτό ενέχει τον κίνδυνο να υποκλαπεί το κλειδί από κάποιον τρίτο που παρακολουθεί τις γραμμές επικοινωνίας ή και να διαρρεύσει από το ένα από τα δύο μέρη. Στην κρυπτογραφία αυτού του τύπου, που αποκαλείται συμμετρική κρυπτογράφηση, θα πρέπει όλα τα κλειδιά που χρησιμοποιούνται να παραμένουν

κρυφά, κάτι που είναι εξαιρετικά δύσκολο στα ανοικτά δίκτυα με πολλούς χρήστες, όπως είναι το Internet.

Η συμμετρική κρυπτογραφία ήταν ο μόνος διαθέσιμος τρόπος για τη μετάδοση μυστικών πληροφοριών, δυστυχώς όμως δεν μπορούσαν να τη χρησιμοποιήσουν όλοι εξαιτίας του κόστους ασφαλών καναλιών και της διανομής κλειδιών. Αυτοί που μπορούσαν να το αντέξουν οικονομικά ήταν οι κυβερνήσεις και οι μεγάλες τράπεζες (ή άτομα με μυστικά δαχτυλίδια αποκωδικοποιητών).



Σχήμα 3 : Μοντέλο Συμμετρικού Κρυπτοσυστήματος

Τα στάδια της επικοινωνίας ενός συμμετρικού κρυπτοσυστήματος είναι τα ακόλουθα:

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

5. Η Βασιλική λαμβάνει την κρυπτοσυμβολοσειρά και στην συνέχεια με το ίδιο κλειδί την αποκρυπτογραφεί και η έξοδος που παράγεται είναι το μήνυμα.

Από το παραπάνω παράδειγμα αντιλαμβανόμαστε πως η ασφάλεια αυτών των αλγορίθμων βασίζεται στην μυστικότητα του κλειδιού. Τα συμμετρικά κρυπτοσυστήματα προϋποθέτουν την ανταλλαγή του κλειδιού μέσα από ένα ασφαλές κανάλι επικοινωνίας ή μέσα από την φυσική παρουσία των προσώπων. Αυτό το χαρακτηριστικό καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων. Η κρυπτογράφηση με δημόσιο κλειδί αποτελεί τη τεχνολογική επανάσταση που παρέχει ισχυρό σύστημα κρυπτογραφίας στις ενήλικες μάζες.

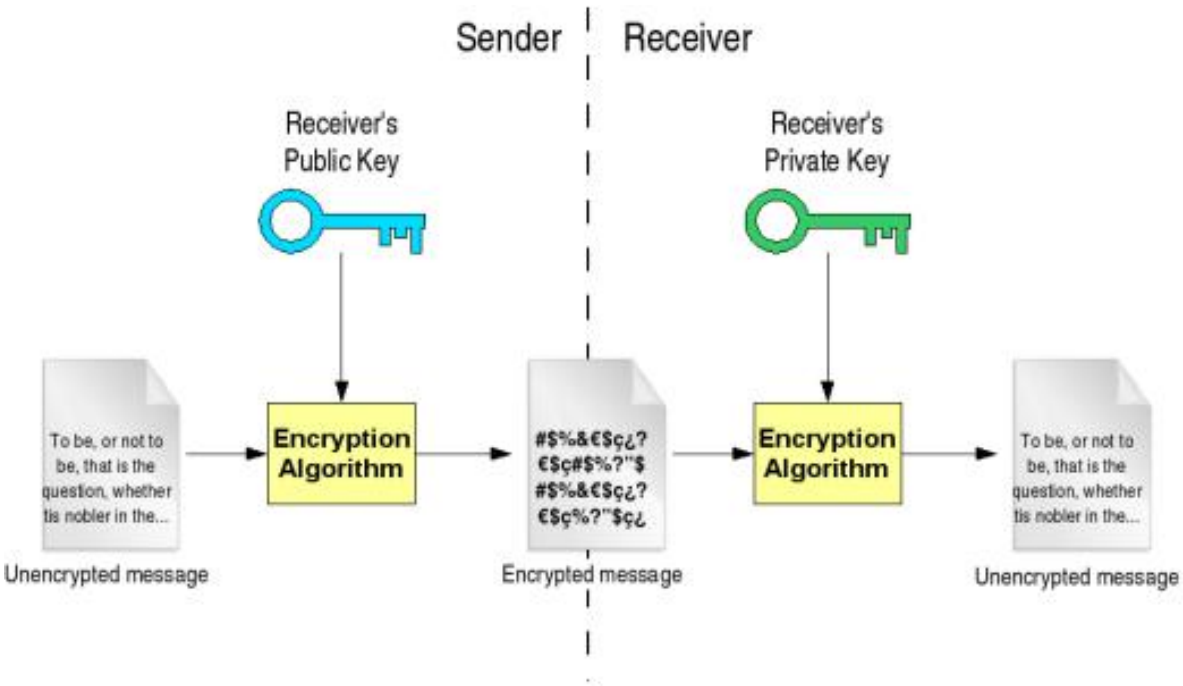
4.7. Ασύμμετρη κρυπτογραφία

Τα προβλήματα της βασικής διανομής λύνονται από την κρυπτογραφία δημόσιου κλειδιού, έννοια που δημιουργήθηκε από τους Whitfield Diffie και Martin Hellman το 1975. Η κρυπτογραφία δημόσιου κλειδιού είναι ένα ασύμμετρο σχέδιο που χρησιμοποιεί ένα ζευγάρι των κλειδιών για κρυπτογράφηση: ένα δημόσιο κλειδί, το οποίο κρυπτογραφεί τα στοιχεία, και ένα αντίστοιχο ιδιωτικό κλειδί (μυστικό κλειδί) για την αποκρυπτογράφηση. Το δημόσιο κλειδί δημοσιεύεται στον κόσμο ενώ το ιδιωτικό κλειδί φυλάσσεται μυστικό. Ο κάθε ένας με ένα αντίγραφο του δημόσιου κλειδιού μπορεί να κρυπτογραφήσει πληροφορίες, τις οποίες μπορεί να διαβάσει μόνο ο κάτοχος του ιδιωτικού κλειδιού. Είναι υπολογιστικά απραγματοποίητο να συναχθεί το ιδιωτικό κλειδί από το δημόσιο κλειδί. Ο κάθε ένας που έχει ένα δημόσιο κλειδί μπορεί να κρυπτογραφήσει τις πληροφορίες αλλά δεν μπορεί να σε αποκρυπτογραφήσει. Μόνο το πρόσωπο που έχει το αντίστοιχο ιδιωτικό κλειδί μπορεί να αποκρυπτογραφήσει πληροφορίες.

Η τεχνολογία της ασύμμετρης κρυπτογραφίας, βάσει συγκεκριμένων ‘μαθηματικών αλγορίθμων’ (π.χ. RSA, DSA, κ.ά.), παράγει τυχαία ζεύγη κρυπτογραφικών ‘κλειδιών’ (ψηφιακά δεδομένα) τα οποία χαρακτηρίζονται από δύο σημαντικές ιδιότητες:

Ø το καθένα κλειδί κρυπτογραφεί ψηφιακά δεδομένα τα οποία μπορούν να αποκρυπτογραφηθούν μόνο από το άλλο (συμπληρωματικό του) κλειδί, *και*

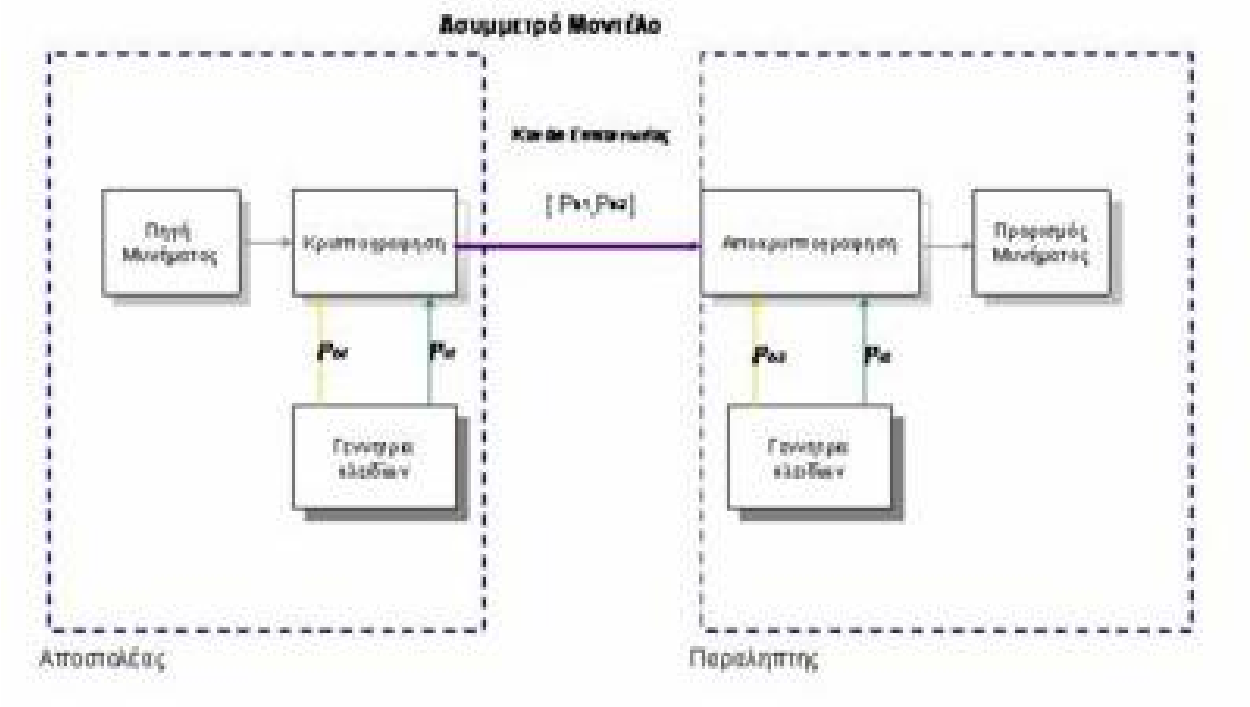
Ø δεν είναι δυνατό, με τις παρούσες δυνατότητες της τεχνολογίας, να συμπεράνει κανείς ή να αναδημιουργήσει το ένα κλειδί όταν γνωρίζει το άλλο.



Εικόνα 3: Ασύμμετρη κρυπτογραφία

Το αρχικό όφελος του συστήματος κρυπτογραφίας με δημόσιο κλειδί είναι ότι επιτρέπει στους ανθρώπους που δεν έχουν καμία προϋπάρχουσα ρύθμιση ασφάλειας να ανταλλάξουν μηνύματα με ασφάλεια. Έτσι τα μηνύματα που αποστέλλονται δεν είναι δυνατό να τροποποιηθούν κατά τη διάρκεια της μετάδοσής τους, καθώς η οποιαδήποτε αλλοίωσή τους τα καθιστά μη δυνάμενα να αποκρυπτογραφηθούν, κάτι που θα γίνει αμέσως αντιληπτό από τον παραλήπτη.

Ουσιαστικά, το ασύμμετρο κρυπτοσύστημα ή κρυπτοσύστημα δημοσίου κλειδιού δημιουργήθηκε για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα.



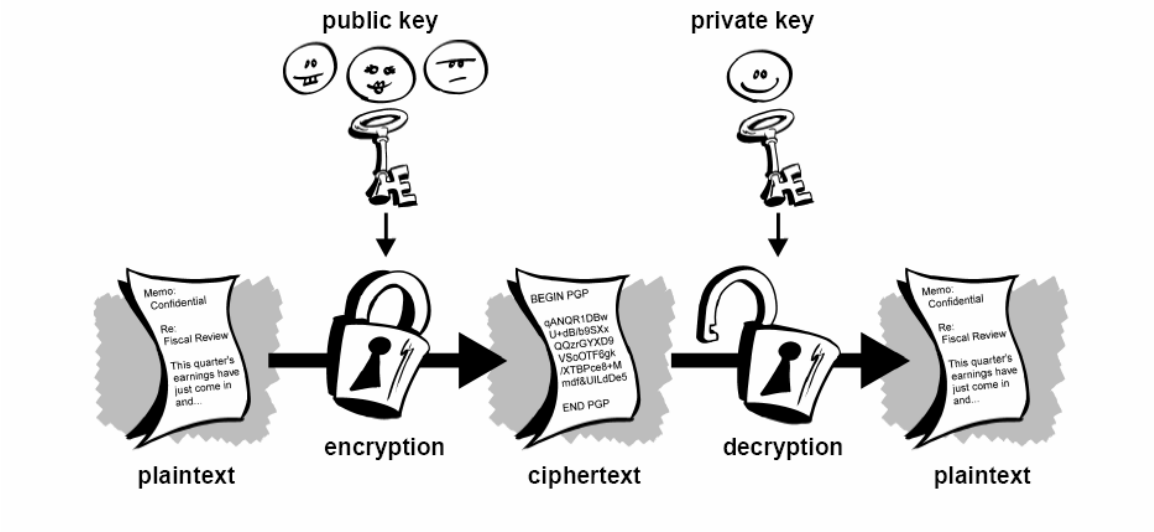
Σχήμα 4 : Μοντέλο Ασύμμετρου Κρυπτοσυστήματος

Τα στάδια της επικοινωνίας του ασύμμετρου κρυπτοσυστήματος είναι τα ακόλουθα:

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

Μερικά παραδείγματα των συστημάτων κρυπτογράφησης με δημόσιο κλειδί είναι το Elgamal (που ονομάστηκε από τον εφευρέτη του Taher Elgamal), το RSA (που ονομάστηκε από τους εφευρέτες του, Ron Rivest, Adi Shamir και Leonard

Adleman), το Diffie-Hellman (ονομασμένο από εφευρέτες του) και το DSA (Digital Signature Algorithm) που εφευρέθηκε από το David Kravitz.



Εικόνα 4: Κρυπτογράφηση δημόσιου κλειδιού

ΚΕΦΑΛΑΙΟ 5^{ο} : Η κρυπτογραφία στη προστασία των πληροφοριών

5.1. Μονόδρομες συναρτήσεις

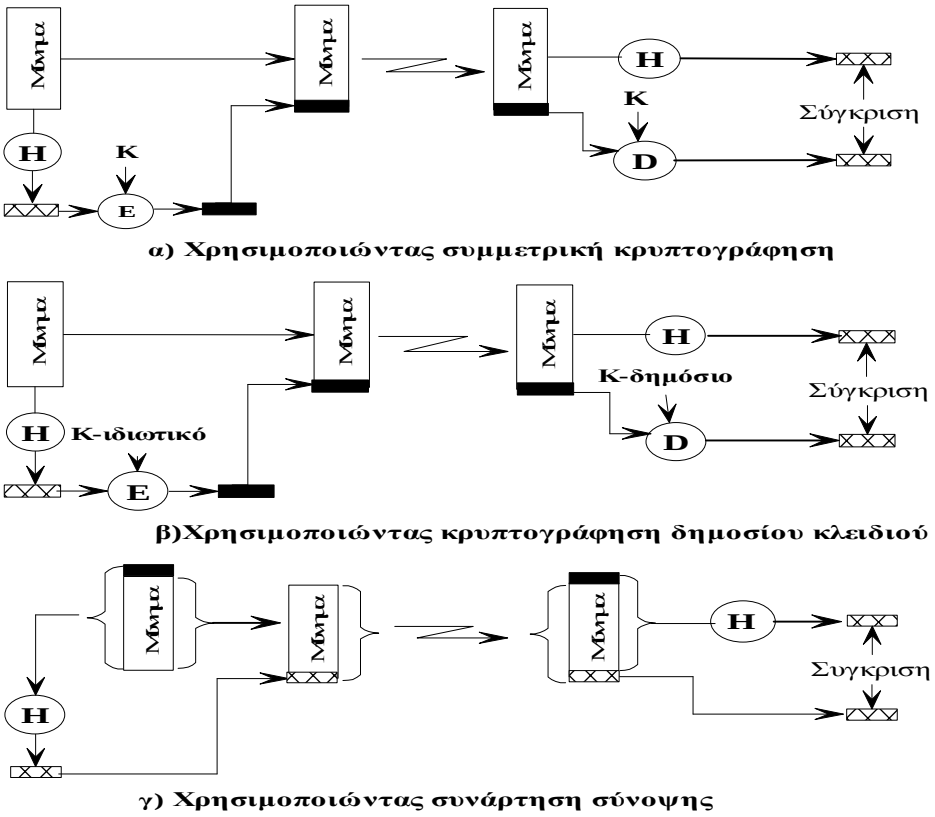
Μία παραλλαγή του κώδικα αυθεντικοποίησης μηνυμάτων, που έχει ιδιαίτερη σημασία στις σύγχρονες κρυπτογραφικές εφαρμογές, αποτελεί η αξιοποίηση μονόδρομης συνάρτησης σύνοψης (one-way hash function). Η σύγχρονη επιστήμη της κρυπτογραφίας μάς εφοδιάζει με εργαλεία για το χτίσιμο μεθόδων που, επαναλαμβανόμενες, παράγουν αριθμούς οι οποίοι δεν είναι προβλέψιμοι εκτός αν δαπανηθεί εξαιρετικά τεράστιος χρόνος με χρήση των ταχύτερων υπολογιστών που υπάρχουν σήμερα και θα υπάρξουν στο εγγύς μέλλον. Μια σχηματική απεικόνιση των συναρτήσεων αυτών δίνεται ακολούθως.

Αν και δεν αποτελούν από μόνες τους πρωτόκολλα, οι συναρτήσεις αυτές είναι από τα θεμελιώδη στοιχεία των περισσότερων πρωτοκόλλων. Οι μονόδρομες συναρτήσεις είναι εύκολες να υπολογιστούν, άλλα σημαντικά δυσκολότερο να αντιστραφούν. Δηλαδή, δοθέντος του x είναι εύκολο να υπολογίσουμε το f(x), αλλά δοθέντος του f(x) είναι δύσκολο να υπολογίσουμε το x. Στην περίσταση αυτή, το «δύσκολο» ορίζεται κάπως έτσι: θα χρειάζονταν εκατομμύρια χρόνια για να υπολογίσουμε το x από το f(x), ακόμη κι αν χρησιμοποιούντο όλοι οι υπολογιστές του κόσμου.

Το σπάσιμο ενός πιάτου είναι καλό παράδειγμα μονόδρομης συνάρτησης. Είναι εύκολο να σπάσουμε ένα πιάτο σε χιλιάδες μικρά κομμάτια. Αντίθετα, είναι μάλλον δύσκολο να συγκολλήσουμε τα κομμάτια για να φτιάξουμε το αρχικό πιάτο.

Η ιδέα ακούγεται καλή, αλλά είναι παραπλανητική. Μιλώντας από καθαρά μαθηματική σκοπιά, δεν έχουμε αποδείξει ότι τέτοιες συναρτήσεις υπάρχουν, ούτε έχουμε ενδείξεις ότι μπορούν να κατασκευαστούν. Οπωσδήποτε δεν κάνουν για κρυπτογραφία. Κανείς δεν θα μπορούσε να αποκρυπτογραφήσει ένα μήνυμα κρυπτογραφημένο με μονόδρομη συνάρτηση. Δεν χρησιμεύουν ούτε και στη

κρυπτογραφία δημόσιου κλειδιού. Μία, πάντως, εφαρμογή που μπορούν να έχουν είναι στην πιστοποίηση ενός χρήστη σε ένα σύστημα.



Σχήμα 5 : Μονόδρομες συναρτήσεις

5.2. Κρυπτανάλυση

Η λέξη κρυπτολογία αποτελείται από την ελληνική λέξη "κρυπτός" και την λέξη "λόγος" και χωρίζεται σε δύο κλάδους: την Κρυπτογραφία και την Κρυπτανάλυση. Η 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. Με άλλα λόγια θα λέγαμε ότι είναι η διαδικασία της προσπάθειας

αποκάλυψης του αρχικού κειμένου ή του κλειδιού από μη εξουσιοδοτημένες οντότητες – δυνητικούς επιτιθέμενους.

Η επιτυχής κρυπτανάλυση μπορεί να ανακτήσει το κείμενο ή το κλειδί. Μπορεί επίσης να εντοπίσει αδυναμίες στο κρυπτοσύστημα οι οποίες τελικά θα οδηγήσουν στα παραπάνω αποτελέσματα.

Μια απόπειρα κρυπτανάλυσης ονομάζεται προσβολή ή επίθεση. Πρώτος ο Ολλανδός A. Kerckhoffs τον 19^{ο} αιώνα διατύπωσε την θεμελιώδη υπόθεση ότι η ασφάλεια του αλγόριθμου πρέπει να βασίζεται αποκλειστικά στο κλειδί. Υπέθεσε επίσης ότι ένας κρυπταναλυτής μπορεί να έχει πλήρη πρόσβαση στις λεπτομέρειες του αλγόριθμου. Αν και στην πραγματικότητα αυτό δεν συμβαίνει πάντα, είναι παρόλα αυτά μια χρήσιμη υπόθεση. Αν κάποιος δεν μπορεί να αναλύσει έναν αλγόριθμο, ακόμη κι αν γνωρίζει το πώς δουλεύει, τότε σίγουρα δεν θα μπορεί να τον αναλύσει χωρίς την γνώση αυτή.

Στη συνέχεια παραθέτουμε σε πίνακα διάφορους τύπους επίθεσης κρυπτανάλυσης.

Τύπος Επίθεσης	**Στοιχεία γνωστά στον κρυπταναλυτή**
Επίθεση κρυπτογραφήματος (ciphertext – only attack)	• Αλγόριθμος κρυπτογράφησης • Κρυπτογράφημα
Επίθεση γνωστού αρχικού κειμένου (known – plaintext attack)	• Αλγόριθμος κρυπτογράφησης • Κρυπτογράφημα • Ένα ή περισσότερα ζεύγη (αρχικού κειμένου, κρυπτογραφήματος) παρανόμενα από το μυστικό κλειδί
Επίθεση επιλεγμένου αρχικού κειμένου (chosen – plaintext attack)	• Αλγόριθμος κρυπτογράφησης • Κρυπτογράφημα • Αρχικό κείμενο επιλεγμένο από τον κρυπταναλυτή, σε συνδυασμό με το αντίστοιχο κρυπτογράφημα που παράγεται με το μυστικό κλειδί
Επίθεση επιλεγμένου κρυπτογραφήματος (chosen – ciphertext attack)	• Αλγόριθμος κρυπτογράφησης • Κρυπτογράφημα • Επιλεγμένο από τον κρυπταναλυτή κρυπτογράφημα, μαζί με το αντίστοιχο αποκρυπτογραφημένο αρχικό κείμενο που παράχθηκε με το μυστικό κλειδί
Επίθεση επιλεγμένου κειμένου (chosen – text attack)	• Αλγόριθμος κρυπτογράφησης • Κρυπτογράφημα • Επιλεγμένο από τον κρυπταναλυτή μήνυμα αρχικού κειμένου, μαζί με το αντίστοιχο κρυπτογράφημα που παράχθηκε με το μυστικό κλειδί • Επιλεγμένο από τον κρυπταναλυτή κρυπτογράφημα, μαζί με το αντίστοιχο αποκρυπτογραφημένο αρχικό κείμενο που παράχθηκε με το μυστικό κλειδί

Σχήμα 6 : Τύποι επίθεσης κρυπτανάλυσης

Υπάρχουν τέσσερις γενικοί τύποι κρυπτανάλυσης, που όλοι έχουν ως δεδομένη την υπόθεση του Kerckhoffs:

1. Προσβολή βάσει κρυπτογραφήματος : Ο κρυπταναλυτής γνωρίζει ορισμένα κρυπτογραφήματα, τα οποία έχουν δημιουργηθεί με τον ίδιο αλγόριθμο κρυπτογράφησης. Ο στόχος είναι να ανακτηθεί το αρχικό κείμενο από όσο το δυνατόν περισσότερα μηνύματα ή ακόμη καλύτερα να βρεθεί το κλειδί ή τα κλειδιά που χρησιμοποιήθηκαν για την κρυπτογράφηση, με σκοπό την περαιτέρω αποκρυπτογράφηση και άλλων κρυπτογραφημάτων που προέκυψαν από το ίδιο κλειδί.

2. Προσβολή γνωστού κειμένου : Ο κρυπταναλυτής έχει πρόσβαση όχι μόνο σε κάποια κρυπτογραφήματα, αλλά και στα κείμενα στα οποία αντιστοιχούν. Ο σκοπός του είναι να βρει το κλειδί ή τα κλειδιά κρυπτογράφησης των κειμένων, ή έναν αλγόριθμο αποκρυπτογράφησης περαιτέρω κρυπτογραφημάτων που δημιουργήθηκαν από το ίδιο κλειδί.

3. Προσβολή επιλεγμένου κειμένου : Ο κρυπταναλυτής όχι μόνο έχει πρόσβαση σε ορισμένα κρυπτογραφήματα και στα αντίστοιχα κείμενα, αλλά επιπλέον μπορεί και διαλέγει το κείμενο που κρυπτογραφείται. Αυτή η περίπτωση είναι πιο πλεονεκτική από την προηγούμενη, επειδή ο κρυπτογράφος μπορεί να διαλέξει για κρυπτογράφηση συγκεκριμένα κομμάτια κειμένου, τέτοια που να φανερώνουν περισσότερες πληροφορίες για το κλειδί. Σκοπός είναι να βρει το κλειδί ή τα κλειδιά κρυπτογράφησης ή έναν αλγόριθμο αποκωδικοποίησης περαιτέρω μηνυμάτων κωδικοποιημένων με το ίδιο κλειδί.

4. Προσβολή προσαρμόσιμου επιλεγμένου κειμένου : Η επίθεση αυτή αποτελεί ειδική περίπτωση της προσβολής με επιλεγμένο κείμενο. Όχι μόνο μπορεί ο κρυπταναλυτής να διαλέξει το κείμενο που θα κρυπτογραφηθεί, αλλά μπορεί και να τροποποιήσει την επιλογή του, βασισμένος στα αποτελέσματα της προηγούμενης κρυπτογράφησης.

Υπάρχουν τρεις, τουλάχιστον, ακόμα τύποι κρυπταναλυτικής επίθεσης.

5. Προσβολή επιλεγμένου κρυπτογραφήματος : Ο κρυπταναλυτής μπορεί να διαλέξει διαφορετικά κρυπτογραφήματα για αποκρυπτογράφηση και να έχει πρόσβαση στο

αποκρυπτογραφημένο κείμενο. Θα μπορούσε, για παράδειγμα, να έχει στην κατοχή του ένα απαραβίαστο κουτί αυτόματης αποκρυπτογράφησης. Σκοπός του είναι να βρει το κλειδί.

Αυτή η επίθεση είναι κατά κύριο λόγο εφαρμόσιμη σε αλγόριθμους δημόσιου κλειδιού. Μερικές φορές είναι αποτελεσματική και σε συμμετρικούς αλγόριθμους.

6. Προσβολή επιλεγμένου κλειδιού : Κατά την προσβολή αυτή δεν σημαίνει ότι ο αναλυτής μπορεί να διαλέξει το κλειδί, αλλά ότι έχει κάποια γνώση σχετικά με τον συσχετισμό ανάμεσα στα διαφορετικά κλειδιά.

Οι προσβολές γνωστού κειμένου και επιλεγμένου κειμένου είναι πιο συχνές απ' ότι θα φανταζόταν κάποιος. Μερικές φορές είναι δυνατόν ο κρυπταναλυτής να αποκτήσει το αρχικό κείμενο ενός κρυπτογραφήματος ή να δωροδοκήσει κάποιον ώστε να κρυπτογραφήσει ένα επιλεγμένο κείμενο. Άλλοτε πάλι ούτε αυτό είναι απαραίτητο. Για παράδειγμα, αν ένας πρέσβης λάβει ένα μήνυμα, τότε κατά πάσα πιθανότητα θα το στείλει στη χώρα του κρυπτογραφημένο.

Ο κρυπταναλυτής μπορεί να βοηθηθεί κι από ορισμένα σταθερά χαρακτηριστικά κάποιου είδους κειμένου. Για παράδειγμα, ο κρυπτογραφημένος πηγαίος κώδικας ενός προγράμματος είναι ευάλωτος καθώς περιέχει δεδομένες λέξεις: define, struct, else, return. Το ίδιο και ο εκτελέσιμος κώδικας: περιέχει κλίσεις συναρτήσεων, δομές επανάληψης κοκ. Γενικά, για να θεωρηθεί ένας κώδικας ανθεκτικός στην κρυπτανάλυση πρέπει να έχει μελετηθεί από πολλούς κρυπτολόγους.

5.3. Εφαρμογές κρυπτογραφίας

Η εξέλιξη της χρησιμοποίησης της κρυπτογραφίας ολοένα αυξάνεται, καθιστώντας πλέον αξιόπιστη την μεταφορά της πληροφορίας για διάφορους λειτουργικούς σκοπούς. Έτσι στις μέρες μπορούμε να συναντήσουμε τη κρυπτογραφία σε :

1. Ασφάλεια συναλλαγών σε τράπεζες δίκτυα - ATM
2. Κινητή τηλεφωνία (ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM)

3. Σταθερή τηλεφωνία (cryptophones)
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. Word 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 6^{ο} : Ψηφιακές υπογραφές

6.1. Έννοια ψηφιακής υπογραφής

Ως ηλεκτρονική υπογραφή, νοείται κάθε "κλειδωμένη" σύντμηση ηλεκτρονικού κειμένου, η οποία παρέχει εγγύηση της αυθεντικότητας και της μη αλλοίωσής του. Έχει επιβεβαιωτική λειτουργία (ο παραλήπτης είναι βέβαιος ότι το μήνυμα που παραλαμβάνει ανήκει στον αποστολέα χωρίς αλλοιώσεις) και εμπιστευτική λειτουργία (μόνο ο παραλήπτης μπορεί να διαβάσει το μήνυμα).

Το ελληνικό Δίκαιο με ειδική πρόβλεψη (Ν. 2672/1999) προτείνει τον όρο "ψηφιακή υπογραφή" αντί για "ηλεκτρονική", και δίνει τον ορισμό της: "Η ψηφιακής μορφής υπογραφή σε δεδομένα ή λογικά συνεχιζόμενη με αυτά, που χρησιμοποιείται από τον υπογράφοντα ως ένδειξη υπογραφής του περιεχομένου των δεδομένων αυτών, εφόσον η εν λόγω υπογραφή α) συνδέεται μονοσήμαντα με τον υπογράφοντα, β) ταυτοποιεί τον υπογράφοντα, γ) δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον έλεγχό του και δ) συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο ώστε να μπορεί να αποκαλυφθεί οποιαδήποτε αλλοίωση των εν λόγω δεδομένων". Παρά τον ορισμό αυτό, ο εν λόγω νόμος δεν εξομοιώνει νομικά τη ψηφιακή υπογραφή με την ιδιόχειρη, κενό το οποίο ήρθε να καλύψει το Προεδρικό Διάταγμα 150/2001.

Ένα σημαντικό όφελος της ασύμμετρης κρυπτογραφίας δημοσίου κλειδιού είναι ότι παρέχει μια μέθοδο για τις ηλεκτρονικές υπογραφές. Οι ηλεκτρονικές υπογραφές αφήνουν τον παραλήπτη των πληροφοριών να ελέγξει την αυθεντικότητα προέλευσης των πληροφοριών και επίσης πιστοποιούν ότι τις πληροφορίες δεν άλλαξαν κατά τη μεταφορά τους. Κατά συνέπεια, οι ηλεκτρονικές υπογραφές δημόσιου κλειδιού παρέχουν την ακεραιότητα και την επικύρωση των στοιχείων. Μια ηλεκτρονική υπογραφή παρέχει επίσης non-repudiation, που σημαίνει ότι αποτρέπει τον αποστολέα από τον ισχυρισμό ότι δεν έστειλε πραγματικά τις πληροφορίες.

Αυτά τα χαρακτηριστικά γνωρίσματα είναι κάθε κομμάτι τόσο θεμελιώδες στη κρυπτογραφία όσο η μυστικότητα. Μια ηλεκτρονική υπογραφή εξυπηρετεί τον

ίδιο σκοπό με μια χειρόγραφη υπογραφή. Εντούτοις, μια χειρόγραφη υπογραφή είναι εύκολο να πλαστογραφηθεί. Μια ηλεκτρονική υπογραφή είναι ανώτερη από μια χειρόγραφη υπογραφή δεδομένου ότι είναι σχεδόν αδύνατο να πλαστογραφήθει, συν το βεβαιώνει στο περιεχόμενο των πληροφοριών καθώς επίσης και στην ταυτότητα του υπογράφοντος.

Στην ηλεκτρονική υπογραφή ακολουθείται το σύστημα της ασύμμετρης κρυπτογράφησης (δημόσιο κλειδί). Μια ηλεκτρονική υπογραφή (digital signature) αποτελείται από ένα ζεύγος (συνδυασμό) κλειδιών, δηλ. από ένα δημόσιο κλειδί (public key), το οποίο μπορεί να αποκτήσει ο οποιοσδήποτε, και από ένα ιδιωτικό κλειδί (private key), το οποίο είναι αυστηρά προσωπικό για τον κάτοχό του και δεν πρέπει να κοινοποιηθεί σε κανέναν άλλον.

Ακόμα κι αν γνωρίζει κάποιος το ένα κλειδί, είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Τα κλειδιά αυτά λειτουργούν πάντα σε ζεύγος και το ένα κλειδί μπορεί να αποκρυπτογραφήσει ό,τι έχει κρυπτογραφηθεί με το άλλο κλειδί και αντίστροφα και επίσης είναι πρακτικά αδύνατη η δημιουργία του ενός κλειδιού όταν γνωρίζουμε το άλλο κλειδί του ζεύγους.

Πρέπει να σημειωθεί ότι κατά την ‘δημιουργία’ μιας ‘ψηφιακής υπογραφής’ δεν κρυπτογραφούνται τα ‘προς υπογραφήν’ δεδομένα, αλλά μία μικρή μαθηματική ‘σύνοψή’ (‘digest’) τους, η οποία παράγεται από την χρήση ‘μονόδρομων αλγορίθμων κατακερματισμού δεδομένων’. Αυτή η ‘σύνοψη’ των δεδομένων, κρυπτογραφείται με το ιδιωτικό κλειδί του υπογράφοντα και επισυνάπτεται (πιθανώς μαζί και με άλλες χρήσιμες σχετικές πληροφορίες, π.χ. χρησιμοποιούμενοι αλγόριθμοι, εφαρμοζόμενη ‘πολιτική υπογραφής’, κ.ά.), στα αρχικά δεδομένα, αποτελώντας την ‘προηγμένη ηλεκτρονική υπογραφή’ τους.

Η διαφοροποίηση από την κρυπτογράφηση έγκειται στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.

Για παράδειγμα, ένα μήνυμα ή και ένα αρχείο που έχει κρυπτογραφηθεί με το δημόσιο κλειδί ενός κατόχου, μπορεί να αποκρυπτογραφηθεί μόνο με το αντίστοιχο ιδιωτικό κλειδί του ίδιου κατόχου, πράγμα που σημαίνει ότι μόνο ο κάτοχος ενός

δημόσιου κλειδιού μπορεί να διαβάσει τα μηνύματα που έχουν κρυπτογραφηθεί με το κλειδί αυτό καθώς μόνο αυτός γνωρίζει το αντίστοιχο ιδιωτικό κλειδί. Η διαδικασία αυτή εξασφαλίζει ότι το μήνυμα ή το αρχείο δεν μπορεί να παρακολουθείται ή και να αλλοιώνεται από κάποιον τρίτο που δεν κατέχει το αντίστοιχο ιδιωτικό κλειδί του δημοσίου κλειδιού με το οποίο κρυπτογραφήθηκε το μήνυμα ή το αρχείο. Στην περίπτωση αυτή λέμε ότι το μήνυμα είναι κρυπτογραφημένο.

Κατά την αντίστροφη διαδικασία της 'επαλήθευσης' μιας ηλεκτρονικής υπογραφής, εφαρμόζεται στα υπό εξέταση δεδομένα ο ίδιος 'αλγόριθμος 'κατακερματισμού' που χρησιμοποιήθηκε κατά την 'υπογραφή' τους. Έτσι, η νέα 'σύνοψη' που παράγεται, συγκρίνεται με την αντίστοιχη 'σύνοψη' που προέρχεται από την αποκρυπτογράφηση της 'προηγμένης ηλεκτρονικής υπογραφής' με το υποδεικνυόμενο δημόσιο κλειδί του υπογράφοντα εάν ταυτίζονται οι δύο συνόψεις τότε η υπογραφή 'επαληθεύεται' και επιβεβαιώνεται ότι:

1. τα δεδομένα υπογράφηκαν από τον κάτοχο του σχετικού ιδιωτικού κλειδιού
2. τα αρχικά δεδομένα δεν έχουν αλλοιωθεί. Παρόλα αυτά διατηρείται ακέραια η ανάγκη - ιδίως σε ανοικτές εφαρμογές με πολλαπλούς ή ακόμη και άγνωστους αποδέκτες - για την ύπαρξη μιας 'Έμπιστης Τρίτης Οντότητας' που ονομάζεται 'Πάροχος Υπηρεσιών Πιστοποίησης' (ΠΥΠ) η οποία, επιπλέον, πιστοποιεί προς οποιοδήποτε τρίτο αποδέκτη μιας ψηφιακής υπογραφής
3. την καταγραφή (registration) της ταυτότητας του κατόχου του ιδιωτικού κλειδιού που αντιστοιχεί στο συγκεκριμένο δημόσιο κλειδί και
4. τη πραγματική κατοχή του σχετικού ιδιωτικού κλειδιού από τον πιστοποιούμενο.

Η παραπάνω πιστοποίηση (προς χρήση από τους αποδέκτες της ηλεκτρονικής υπογραφής) γίνεται με την έκδοση 'ψηφιακών πιστοποιητικών' τα οποία περιέχουν το δημόσιο κλειδί και τα στοιχεία ταυτοποίησης του κατόχου του πιστοποιητικού, και τα οποία υπογράφονται ψηφιακά από τον 'εκδότη' τους. Η υποδομή με την οποία ένας Πάροχος Υπηρεσιών Πιστοποίησης εκδίδει, υπογράφει, δημοσιεύει και υποστηρίζει 'τυποποιημένες ηλεκτρονικές βεβαιώσεις' (πιστοποιητικά) για τα κρυπτογραφικά κλειδιά των συνδρομητών του (υποκειμένων πιστοποίησης) ονομάζεται 'Υποδομή Δημοσίου Κλειδιού',

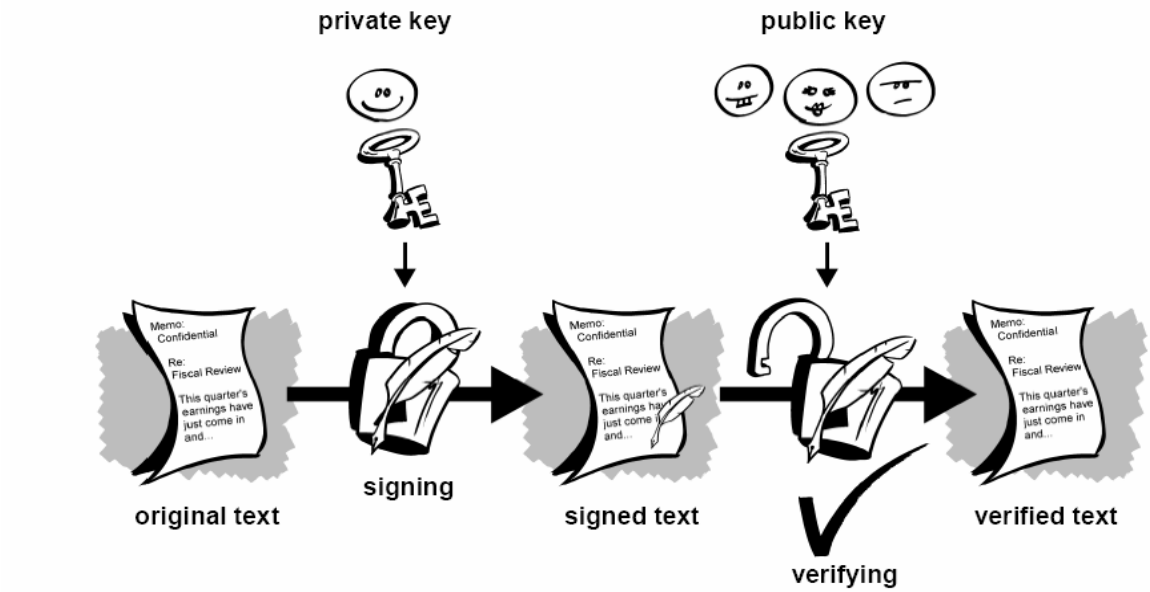
Επειδή τα ‘πιστοποιητικά δημοσίων κλειδιών’ που εκδίδει ένας Πάροχος Υπηρεσιών Πιστοποίησης προς τις ενδιαφερόμενους τελικούς χρήστες ή τελικές ‘οντότητες’, είναι και αυτά μια μορφή ‘ηλεκτρονικών εγγράφων’, επιβάλλεται να φέρουν και αυτά την ‘ψηφιακή υπογραφή’ του εκδότη τους. Αυτό προϋποθέτει ότι και ο ίδιος ο Εκδότης-ΠΥΠ διαθέτει το δικό του ζεύγος κρυπτογραφικών κλειδιών υπογραφής, το οποίο πρέπει εξίσου να υποστηρίζεται από σχετικό πιστοποιητικό δημοσίου κλειδιού -που κι αυτό, με την σειρά του, πρέπει να είναι υπογεγραμμένο ψηφιακά. Η σχηματιζόμενη αλληλουχία (αλυσίδα) πιστοποιητικών τερματίζεται με ένα τελικό και αξιόπιστα δημοσιευμένο ‘αυτοϋπογραφόμενο πιστοποιητικό’ που εκδίδεται από τον ‘Θεμελιώδη Εκδότη Πιστοποιητικών’ του Πάροχου Υπηρεσιών Πιστοποίησης.

Άλλη ευρείας χρήσης εναλλακτική τεχνολογία ‘προηγμένης ηλεκτρονικής υπογραφής’ βασίζεται στα ‘αυτό-υπογραφόμενα’ πιστοποιητικά που εκδίδονται από το ίδιο τον (τελικό) χρήστη-κάτοχο ζεύγους κρυπτογραφικών κλειδιών, ο οποίος λειτουργεί και ως αποδέκτης αντίστοιχων πιστοποιητικών. Τα πιστοποιητικά αυτά δημοσιεύονται από τον εκδότη τους σε έναν ή περισσότερους δημόσιους ‘εξυπηρετητές κλειδιών’ (key servers) όπου αξιολογούνται και υπογράφονται και από άλλους χρήστες, οι οποίοι, μέσω διαπροσωπικής επικοινωνίας τους με το υποκείμενο-κάτοχό τους, αλληλο-επιβεβαιώνουν και πιστοποιούν την συγκεκριμένη συσχέτιση. Αυτή η μέθοδος πιστοποίησης, η οποία είναι ήδη πολύ διαδεδομένη διεθνώς -ιδίως σε κλειστές ομάδες προγραμματιστών Η/Υ και γενικότερα σε κοινότητες με κοινές δραστηριότητες, π.χ. σωματεία, σύλλογοι κ.λπ.- αποκαλείται ‘Pretty Good Privacy’ (PGP) και βασίζεται στην δημιουργία ενός (αποκεντρωμένου) ‘δικτύου εμπιστοσύνης’ που αναπτύσσεται με την μεταβίβαση της εμπιστοσύνης μεταξύ των χρηστών της.

Οι Αρχές Πιστοποίησης (CA – Certification Authorities) αναλαμβάνουν να εκδώσουν τα πιστοποιητικά (certificates) με τα οποία μπορεί να πιστοποιηθεί (εξακριβωθεί) η ταυτότητα ενός προσώπου αλλά και ενός δικτυακού τόπου. Τα πιστοποιητικά δικτυακών τόπων περιέχουν πληροφορίες που πιστοποιούν ότι μια συγκεκριμένη ιστοσελίδα είναι γνήσια και ασφαλής. Δύο από τα πιο γνωστά πρωτόκολλα ασφαλείας ιστοσελίδων είναι το SSL (Secure Sockets Layer), που

δημιουργήθηκε από την εταιρεία Netscape, και το SET (Secure Electronic Transactions), που αναπτύχθηκε από κοινού από τις εταιρείες Visa και MasterCard.

Οι πιο γνωστοί φυλλομετρητές υποστηρίζουν το πρωτόκολλο SSL και την κρυπτογράφησή του και ενημερώνουν τον χρήστη ότι βρίσκεται σε ασφαλή τοποθεσία και μπορεί συνεπώς να στέλνει πληροφορίες ακίνδυνα. Με το πρωτόκολλο αυτό οι πληροφορίες ανταλλάσσονται κωδικοποιημένες (κρυπτογραφημένες) και γίνεται ακόμη και έλεγχος της αυθεντικότητας (γνησιότητας) της ιστοσελίδας.



Εικόνα 5: Ηλεκτρονική υπογραφή

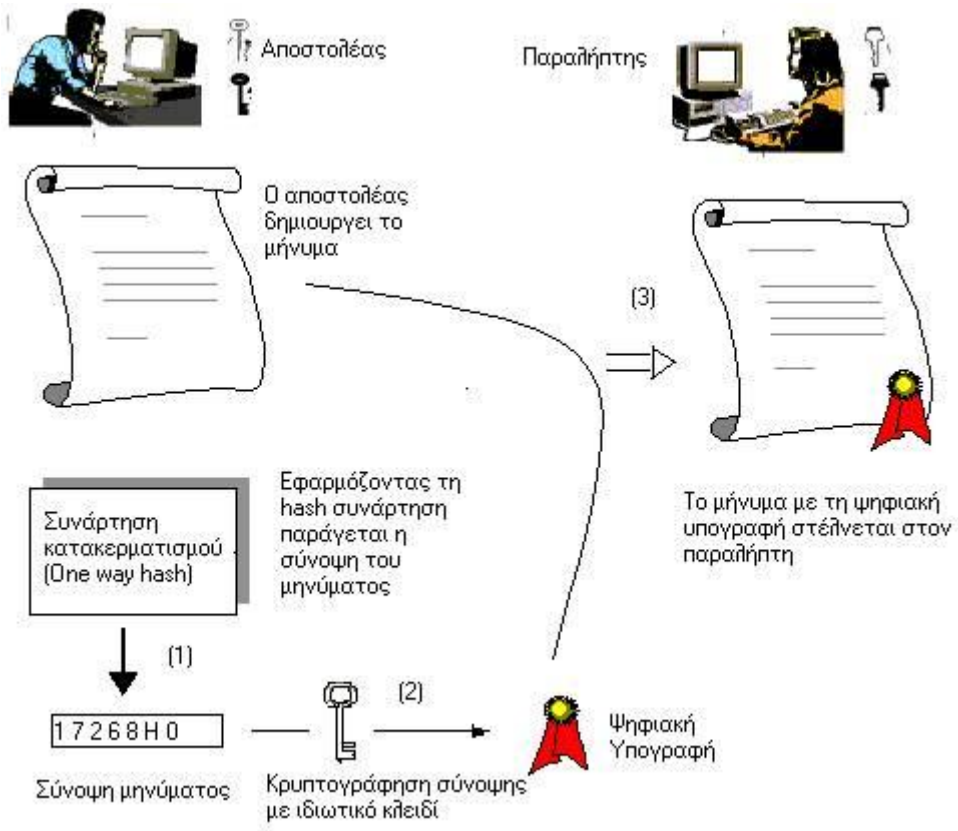
6.2. Δημιουργία ψηφιακής υπογραφής

Η χρήση της ηλεκτρονικής υπογραφής περιλαμβάνει δύο στάδια:

1) τη δημιουργία/ μετάδοση και

2) την επαλήθευσή της.

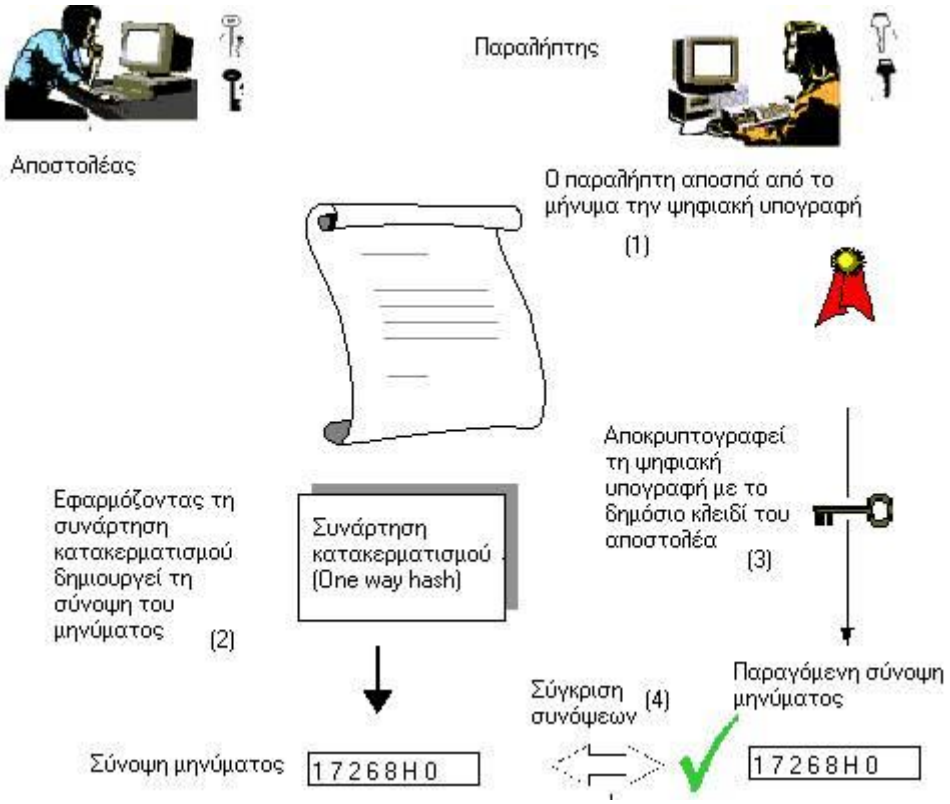
Παρακάτω περιγράφονται οι ενέργειες του αποστολέα και του παραλήπτη, ώστε να γίνει κατανοητός ο μηχανισμός της δημιουργίας και επαλήθευσης της ψηφιακής υπογραφής:



Εικόνα 6: Δημιουργία ηλεκτρονικής υπογραφής

Αποστολέας

1. Δημιουργεί τη σύνοψη του μηνύματος που θέλει να στείλει χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού (one way hash). Ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί θα είναι μία συγκεκριμένου μήκους σειρά ψηφίων.
2. Με το ιδιωτικό του κλειδί κρυπτογραφεί τη σύνοψη. Αυτό που παράγεται είναι η ψηφιακή υπογραφή. Η υπογραφή είναι ουσιαστικά μία σειρά ψηφίων συγκεκριμένου πλήθους.
3. Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου (σημειώνεται ότι ο αποστολέας αν επιθυμεί μπορεί να κρυπτογραφήσει το μήνυμά του με το δημόσιο κλειδί του παραλήπτη).



Εικόνα 7 :Επαλήθευση ηλεκτρονικής υπογραφής

Παραλήπτης

1. Ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή (κρυπτογραφημένη -με το ιδιωτικό κλειδί του αποστολέα- σύνοψη).

2. Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος.

3. Στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος (ψηφιακή υπογραφή).

4. Συγκρίνονται οι δύο συνόψεις και, αν βρεθούν ίδιες, το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από τη σύνοψη που έχει κρυπτογραφηθεί.

6.3. Εξοπλισμός δημιουργίας & επαλήθευσης ηλεκτρονικών υπογραφών

Για την δημιουργία μιας ψηφιακής υπογραφής πάνω σε συγκεκριμένα ηλεκτρονικά δεδομένα, θα πρέπει κάποιος, - εκτός από τα απαραίτητα κρυπτογραφικά κλειδιά και το αντίστοιχο έγκυρο πιστοποιητικό-, να διαθέτει και μια ολοκληρωμένη 'διάταξη δημιουργίας υπογραφής' η οποία να απαρτίζεται από κατάλληλη σύνθεση υλικού (hardware) και λογισμικού (software). Στην διάταξη αυτή περιλαμβάνονται ο 'φορέας' των κρυπτογραφικών κλειδιών (π.χ. σκληρός δίσκος υπολογιστή, έξυπνη κάρτα, USB token, κ.λπ.), ο τυχόν απαραίτητος 'αναγνώστης του φορέα' αυτού (π.χ. αναγνώστης έξυπνης κάρτας, θύρα USB, κ.λπ.), το 'τερματικό επικοινωνίας' του χρήστη (π.χ. PC, pda, smart phone,κ.λπ.), τα 'λειτουργικά συστήματα' και οι 'οδηγοί' (drivers) των συσκευών αυτών, καθώς και το 'λογισμικό επικοινωνίας' (interface) του χρήστη που χρησιμοποιείται για τη δημιουργία της ηλεκτρονικής υπογραφής.

Η έως σήμερα προτυποποίηση για την εξειδίκευση των απαιτήσεων για 'ασφαλείς διατάξεις δημιουργίας υπογραφής' έχει δώσει ιδιαίτερη έμφαση στην ασφάλεια των 'συσκευών δημιουργίας κρυπτογραφικών κλειδιών' καθώς και των 'τελικών φορέων' τους, που συνήθως είναι μια 'έξυπνη κάρτα' (smart card) ή άλλη αντίστοιχη συσκευή (π.χ. USB Token).

Αντίστοιχα, για την επαλήθευση (verification) των ψηφιακών υπογραφών και τον έλεγχο της εγκυρότητας των σχετικών πιστοποιητικών, απαιτείται μια ανάλογη διάταξη, η οποία, εκτός του 'τερματικού επικοινωνίας' του χρήστη και του κατάλληλου 'λογισμικού', θα πρέπει, επιπλέον, να διαθέτει και την δυνατότητα πρόσβασης –είτε με 'on line' σύνδεση, είτε και με συχνές 'off-line' ενημερώσεις- σε επικυροποιημένες πληροφορίες εγκυρότητας ή/ και ανάκλησης πιστοποιητικών τις οποίες δημοσιεύει ο εκάστοτε εκδότης (ΠΥΠ) τους.

6.4. Εφαρμογές ψηφιακών υπογραφών

Σε διεθνές επίπεδο, η χρήση των ηλεκτρονικών υπογραφών και των ηλεκτρονικών πιστοποιητικών ήδη πλαισιώνει και παρέχει υψηλότερα επίπεδα ασφάλειας σε συναλλαγές διαφόρων τύπων όπως:

- Τυποποιημένες εφαρμογές ηλεκτρονικών συναλλαγών, όπως η ηλεκτρονική ανταλλαγή δεδομένων (Electronic Data Interchange -EDI)
- Ηλεκτρονικά τιμολόγια που συντάσσονται σε μορφή άλλη από EDI
- Ηλεκτρονικές δημόσιες προμήθειες
- Ηλεκτρονική ψηφοφορία
- Συστήματα ηλεκτρονικών πληρωμών (π.χ. πιστωτικές κάρτες EuroPay, MasterCard & VISA μέσω του κοινού πρωτοκόλλου τους 'EMV')
- Ηλεκτρονικά 'διαβατήρια' και ηλεκτρονικές 'ταυτότητες' (γενικής ή ειδικής χρήσης –π.χ. 'ναυτικές διεθνείς ταυτότητες') που συνήθως φέρουν ενσωματωμένα και κάποια 'βιομετρικά στοιχεία' (φωτογραφία, δακτυλικά αποτυπώματα, κ.λ.π.) του κατόχου τους
- Υπηρεσίες ασφαλούς ηλεκτρονικού ταχυδρομείου (S/MIME)
- Συστήματα 'υπογραφής αυθεντικότητας' διακινούμενου λογισμικού (π.χ. Microsoft Authenticode)
- Κλειστές υποδομές 'PKI' για εφαρμογές ασφαλείας μεγάλων οργανισμών (π.χ. NATO)
- Πιστοποίηση της ταυτότητας 'εξυπηρετητών διαδικτύου' (web servers), κ.ά. Στην Ευρωπαϊκή Ένωση, εκτός από πλήθος άτυπων εφαρμογών στις τηλεπικοινωνίες, τραπεζικές εφαρμογές, εμπόριο κλπ, έχουν θεσμοθετηθεί και βρίσκονται ήδη σε λειτουργία 'τυπικές εφαρμογές' των e-υπογραφών, οι προϋποθέσεις των οποίων πηγάζουν από το νόμο.
- Τα 'ηλεκτρονικά δελτία ταυτότητας' σε χώρες όπως το Βέλγιο, Φινλανδία, Ιταλία, Εσθονία και αλλού, τα οποία χρησιμοποιούν την τεχνολογία PKI σε συνδυασμό με 'έξυπνες κάρτες', αποτελούν ένα παράδειγμα τέτοιων τυπικών εφαρμογών.

- Ένας άλλος τομέας εφαρμογής ηλεκτρονικών υπογραφών στην ΕΕ είναι τα 'ηλεκτρονικά τιμολόγια', τα οποία σύμφωνα και με την Ευρωπαϊκή Οδηγία 01/115/ΕΚ, εφόσον φέρουν ηλεκτρονική υπογραφή μπορούν να γίνονται αποδεκτά από τις αρμόδιες αρχές των κρατών μελών.
- Άλλη εφαρμογή αποτελούν οι 'ηλεκτρονικές δημόσιες προμήθειες' στο πλαίσιο των σχετικών σχεδίων Οδηγιών της ΕΕ. Επίσης, θεσμικά όργανα της Ευρωπαϊκής Ένωσης, όπως η 'Υπηρεσία Επίσημων Δημοσιεύσεων', σχεδιάζουν την χρήση των ηλεκτρονικών υπογραφών για τα έγγραφα που εκδίδουν σε ηλεκτρονική μορφή (π.χ. την Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, τα περιεχόμενα των νομικών βάσεων δεδομένων CELEX, EUR-Lex & OEIL, τη δημοσίευση προκηρύξεων, κ.λπ.).

Στην Ελλάδα, μια από τις πρώτες εφαρμογές νομικά έγκυρης ηλεκτρονικής υπογραφής επίσημων εγγράφων, η οποία λειτουργεί ήδη από το 2002, είναι το σύστημα ασφαλούς ηλεκτρονικής επικοινωνίας του Χρηματιστηρίου Αθηνών (ΧΑ) με τις εισηγμένες σ' αυτό εταιρίες. Το σύστημα αυτό ονομάζεται "ΕΡΜΗΣ" (ή 'H.E.R.M.E.S.' -Hellenic Exchanges Remote MEssaging Services) και βασίζεται στις ηλεκτρονικές υπογραφές εξουσιοδοτημένων φυσικών προσώπων ('εκπροσώπων' των εισηγμένων), στα οποία παρέχονται δύο διαφορετικά ζεύγη κλειδιών και πιστοποιητικών (ένα για την ταυτοποίησή τους στο σύστημα και ένα για την 'αναγνωρισμένη ηλεκτρονική υπογραφή' τους στις υποβαλλόμενες ηλεκτρονικά δηλώσεις τους) εναποθετημένα σε μια προσωποποιημένη 'έξυπνη κάρτα'.

Παράλληλα, η υποστήριξη και η χρήση ηλεκτρονικών υπογραφών και πιστοποιητικών προβλέπεται στις προδιαγραφές των περισσότερων έργων που προκηρύχθηκαν ή προκηρύσσονται στα πλαίσια του προγράμματος για την 'Κοινωνία της Πληροφορίας' και των σχετικών 'Επιχειρησιακών Προγραμμάτων' των φορέων του ευρύτερου Δημόσιου Τομέα. Χαρακτηριστικά παραδείγματα αποτελούν:

- τα έργα ψηφιοποίησης του Ποινικού Μητρώου του Υπουργείου Δικαιοσύνης,
- οι σχεδιαζόμενες εφαρμογές για την ηλεκτρονική κατάθεση Εμπορικών Σημάτων καθώς και

- το σύστημα ηλεκτρονικών Δημόσιων Προκηρύξεων & Προμηθειών στο Υπουργείο Ανάπτυξης (Γ.Γ. Εμπορίου),
- τα σχέδια για ηλεκτρονικές υπογραφές των ηλεκτρονικών Φύλλων της Εφημερίδας της Κυβερνήσεως (ΦΕΚ) του Εθνικού Τυπογραφείου, η πλήρης ηλεκτρονική λειτουργία των ΚΕΠ (e-ΚΕΠ), κ.ά.

ΚΕΦΑΛΑΙΟ 7° : Νομικό πλαίσιο

7.1. Εξωτερικό

Στην άλλη άκρη του Ατλαντικού το ζήτημα των ηλεκτρονικών υπογραφών και κατ΄ επέκταση το ζήτημα της ασφάλειας από τη χρήση κρυπτογραφικών κλειδιών απασχόλησε το νομοθέτη ήδη από το 1996 όταν σε πολιτειακό επίπεδο θεσπίστηκε η Utah Digital Signature Act στην ομώνυμη πολιτεία. Ακολούθησαν πολλές άλλες πολιτείες που κάλυψαν νομοθετικά το ίδιο ζήτημα με διαφορετικό τρόπο και με μια ευρεία ποικιλία διατάξεων σε σημείο που μέχρι πριν ένα χρόνο περίπου «μεταξύ έστω και δύο πολιτειών να μην υπάρχει τίποτα το κοινό» πάνω στο ζήτημα των ηλεκτρονικών υπογραφών. Ωστόσο την 30 Ιουνίου του 2000 ο Bill Clinton υπέγραψε την " Electronic Signatures in Global and National Commerce Act" ή αλλιώς Esign, η οποία πλέον σε ομοσπονδιακό επίπεδο προέβη στις αναγκαίες ρυθμίσεις. Μάλιστα ο νόμος αυτός – όπως και στην περίπτωση της Οδηγίας 99/93 της Ε.Ε. δίνει τη δυνατότητα στις Πολιτείες να επιλέξουν τη συγκεκριμένη τεχνολογία εφαρμογής των ηλεκτρονικών υπογραφών, ενώ ως υπογραφή μπορεί να αποτελέσει όχι μόνο ένας κωδικός κρυπτογραφημένος αλλά και οποιοδήποτε αρχείο εικόνας, ήχου κτλ. Μάλιστα η Esign καθιστά ισχυρές τις ηλεκτρονικές υπογραφές στα συμβόλαια και σε άλλα δεδομένα που πριν ένα χρόνο η ηλεκτρονική τους φύση τα καθιστούσε ανίσχυρα. Έτσι σχεδόν το σύνολο των συμβάσεων που απαιτούσε off line απαραιτήτως την ιδιόχειρη υπογραφή είναι δυνατό να συναφθεί πλέον και ηλεκτρονικά.

Η Ευρωπαϊκή Ένωση, με την Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 'Σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές (EEL 13/19.1.2000) ακολούθησε μία μικτή προσέγγιση δύο επιπέδων (two-tier approach), η οποία συνδυάζει και τις δύο παραπάνω κατευθύνσεις.

Έτσι, η Ευρωπαϊκή Οδηγία αναγνωρίζει γενικά ως 'ηλεκτρονικές υπογραφές' -οι οποίες μπορούν να χρησιμοποιηθούν ως 'αποδεικτικά στοιχεία' σε νομικές

διαδικασίες (ά. 5§2 της Οδηγίας)-, όλα τα: «δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε, ή λογικά συσχετιζόμενα με, άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας» (ά. 2§1 της Οδηγίας). Ο ορισμός αυτός καλύπτει κάθε ηλεκτρονική μέθοδο απόδειξης της προέλευσης των δεδομένων, από τις πιο 'απλές' (π.χ. απλή αναγραφή του ονόματος του συντάξαντα στο τέλος μιας ηλεκτρονικής επιστολής, αυτόματη σύναψη της ηλεκτρονικής διεύθυνσης αποστολής σε ένα e-mail ή του αριθμού του τηλεφώνου αποστολής σε ένα SMS μήνυμα, κλπ), ως την πιο 'σύνθετες' (π.χ. προηγμένες μέθοδοι κρυπτογράφησης δεδομένων, χρήση βιομετρικών στοιχείων, κλπ), ανεξάρτητα, δηλαδή, από τον βαθμό τεχνικής ασφάλειας που παρέχουν.

7.2. Ελλάδα

Στην Ελλάδα, η πρώτη νομοθετική πρόβλεψη για 'ψηφιακές υπογραφές' και κατ΄επέκταση της ασφάλειας από τη χρήση κρυπτογραφικών κλειδιών γίνεται ήδη από το άρθρο 14 του ν. 2672/98 όπου παρέχεται μια αρχική, αλλά περιορισμένη αναγνώρισή τους σε διαδικασίες του δημόσιου τομέα.

Ακολούθησε το π.δ. 150/2001 (ΦΕΚ Α'/125 25-6-2001) το οποίο εναρμόνισε το εθνικό μας δίκαιο με την παραπάνω Οδηγία και καθόρισε την 'Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων' (ΕΕΤΤ) ως αρμόδια αρχή για την εποπτεία των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης ηλεκτρονικής υπογραφής, καθώς και για την λειτουργία μηχανισμών 'Εθελοντικής Διαπίστευσης' των ΠΥΠ και 'Διαπίστωσης' της συμμόρφωσης των 'προϊόντων ηλεκτρονικής υπογραφής'.

Τον Οκτώβριο του 2002, εκδόθηκε το π.δ. 342/02 το οποίο προσδιορίζει περαιτέρω κάποιους όρους για τη διακίνηση ψηφιακά υπογεγραμμένων 'μηνυμάτων ηλεκτρονικού ταχυδρομείου' στις επικοινωνίες του δημόσιου τομέα.

Τέλος, στο πλαίσιο άσκησης των σχετικών αρμοδιοτήτων της, η ΕΕΤΤ έχει εκδώσει έναν γενικό 'Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής', καθώς και τρεις Κανονισμούς σχετικά με την 'Εθελοντική

Διαπίστευση' των ΠΥΠ, την 'Διαπίστωση' (της συμμόρφωσης με τις απαιτήσεις της Οδηγίας) βασικών 'προϊόντων ηλεκτρονικής υπογραφής και τον ορισμό των 'Φορέων' που θα προβαίνουν σε σχετικούς ελέγχους και διαπιστεύσεις για λογαριασμό της ΕΕΤΤ. [248/71 (ΦΕΚ 603/Β'/16-5-2002)].

Με μια σειρά Αποφάσεών της μέσα στο 2003 [ΦΕΚ Β΄ Αρ. φύλλου 1730, Υ.Α. 295/2003] η ΕΕΤΤ δημιούργησε το θεσμικό πλαίσιο α) για τον ορισμό και τη λειτουργία των εντεταλμένων φορέων για την Εθελοντική Διαπίστευση (των παρόχων υπηρεσιών πιστοποίησης) και τον έλεγχο των προϊόντων (ασφαλών διατάξεων δημιουργίας υπογραφής και ασφαλών κρυπτογραφικών μονάδων) και β) για την Εθελοντική Διαπίστευση των παρόχων υπηρεσιών πιστοποίησης

Σύμφωνα με το άρθρο 2 του Προεδρικού Διατάγματος 150/2001, με τον όρο "ηλεκτρονική ή ψηφιακή υπογραφή" εννοούμε δεδομένα σε ηλεκτρονική μορφή, τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας.

Η ηλεκτρονική υπογραφή ή ψηφιακή υπογραφή πρέπει να πληροί και τους ακόλουθους όρους:

α) Να συνδέεται μονοσήμαντα με τον υπογράφοντα.

β) Να είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος.

γ) Να δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο.

δ) Να συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο ώστε να μπορεί να εντοπισθεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων.

3 Σχήμα κρυπτογράφησης DES

ΚΕΦΑΛΑΙΟ 8^{ο} : DES

8.1. Κρυπτογραφία κλειδιού

Όπως φαίνεται μέσα από την μελέτη που έχει προηγηθεί στην παρούσα εργασία για τη κρυπτογραφία και τα βασικά κρυπτογραφικά σχήματα, εύκολα συμπεραίνουμε πως η κρυπτογραφία δεν αποτελεί παρά μια συνεχής προσπάθεια εύρεσης όλο και πιο «μπερδεμένων» μετασχηματισμών ενός μηνύματος, έτσι ώστε η αντιστροφή του μετασχηματισμού να είναι δύσκολη χωρίς τη γνώση ενός «κλειδιού». Μέσα από την πράξη έχει διαπιστωθεί πως πάρα πολλοί από αυτούς αποτυγχάνουν. Το γεγονός αυτό οφείλεται στην αδυναμία που συνήθως ανακαλύπτεται μετά τη δημοσιοποίηση του. Ως αδυναμία φυσικά νοείται είτε η αποκάλυψη μηνύματος χωρίς τη χρήση του κλειδιού είτε η εύκολη ανάκτηση του κλειδιού και, συνεπώς, η ανάκτηση του μηνύματος.

Ως κοινό σημείο όλων των μεθόδων των κρυπτογραφικών κλειδιών όπως διαφαίνεται από την προηγούμενη μελέτη ήταν με τη χρήση ενός κλειδιού η εφαρμογή ενός μετασχηματισμού αντικατάστασης χαρακτήρων από κάποιους άλλους ή η *αναδιάταξη των χαρα*κτήρων στο αρχικό μήνυμα, χωρίς απαραίτητα να τους έχουμε αντικαταστήσει από άλλους χαρακτήρες. Σε κάθε περίπτωση το αποτέλεσμα είναι ένα ακατανόητο κείμενο το οποίο επανέρχεται στην αρχική του μορφή με τη χρήση ενός κλειδιού. Εννοείται πως το κλειδί αυτό πρέπει να μοιράζεται, να βρίσκεται στην κατοχή και να το κρατούν μυστικό μόνο τα μέρη που επικοινωνούν.

Μια καλή διαδικασία απόκρυψης ενός μηνύματος διέπεται από δυο ιδιότητες αυτές της «σύγχυσης» και της «διάχυσης», οι οποίες θα πρέπει να συνυπάρχουν.

♣ Η ιδιότητα της *σύγχυσης* αναφέρεται στη δημιουργία εμποδίων οποιαδήποτε στατιστικής πληροφορίας σχετική με το αρχικό μήνυμα κατά τη μεταφορά της στο

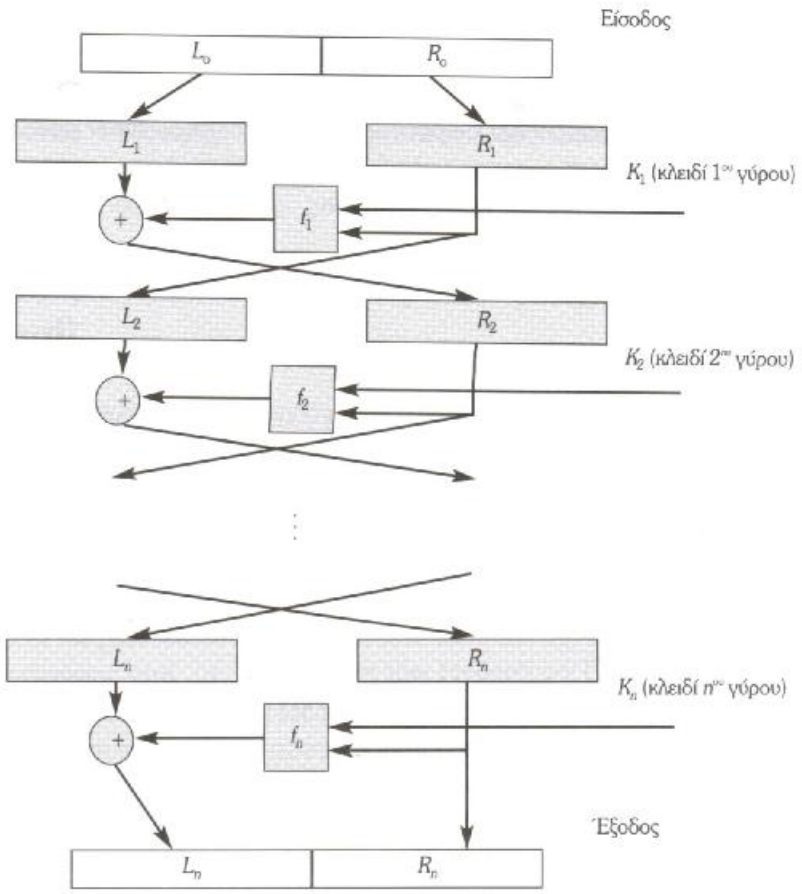
κωδικοποιημένο μήνυμα. Η ιδιότητα αυτή επιβάλλεται με μορφή αντικατάστασης των τιμών ομάδων από bits της εισόδου.

♣ Η ιδιότητα της *διάχυσης* αναφέρεται στην κάθε αλλαγή σε κάποιο μέρος της εισόδου οι οποίες να επηρεάζουν θέσεις στο κωδικοποιημένο μήνυμα που βρίσκονται αρκετά μακριά από τη θέση που έγινε η αλλαγή. Η ιδιότητα αυτή επιβάλλεται με μορφή μετάθεσης κάποιων από τα bits.

Δυστυχώς τόσο οι αντικαταστάσεις όσο και οι μεταθέσεις δεν είναι επαρκείς κατά την εφαρμογή τους τοπικά σε περιορισμένο αριθμό θέσεων στο αρχικό μήνυμα. Εξαιτίας του τελευταίου, προέκυψε η ιδέα της εφαρμογής πολλών μετασχηματισμών στη σειρά στο αρχικό μήνυμα. Με τον τρόπο αυτό το τελικό αποτέλεσμα θα αποτελεί μία αρκετά *ανακατωμένη* (από τις μεταθέσεις) και *αλλαγμένη* (από τις αντικαταστάσεις) έκδοση του αρχικού μηνύματος.

Με βάση τα παραπάνω δημιουργήθηκε ο ορισμός των *δικτύων αντικατάστασης και μετάθεσης ή* SPN (Substitution Permutation Networks). Τα δίκτυα αντικατάστασης και μετάθεσης θέλοντας φυσικά να επιτύχουν ολικό μετασχηματισμό του αρχικού μηνύματος συνδυάζουν διαδοχικά μετασχηματισμούς αντικαταστάσεων και μεταθέσεων, με τη βοήθεια κάποιου κλειδιού.

Σχηματικά μπορούμε να απεικονίσουμε και τη γενική δομή μιας μεγάλης κλάσης κρυπταλγόριθμων διαμοιραζόμενου κλειδιού, τη γνωστή ως δομή Feistel, που ορίστηκε το 1973. Οι κρυπταλγόριθμοι που ακολουθούν τη δομή Feistel έχουν μία κανονική, επαναληπτική δομή που τους κάνει ιδιαίτερα εύκολους στην υλοποίηση σε λογισμικό καθώς και σε ολοκληρωμένα κυκλώματα.



Σχήμα 7 : Δομή Feistel

Σύμφωνα με το παραπάνω σχήμα, οι κρυπταλγόριθμοι κατά την είσοδο τους (που είναι ένα bock από N bits) εφαρμόζουν έναν αριθμό *η*, γενικά, μετασχηματισμών f_i. Κάθε μετασχηματισμός εφαρμόζεται στο δεξί μισό της εισόδου, όπως έχει μετασχηματιστεί στον προηγούμενο (i-1) γύρο, με τη συμμετοχή του κλειδιού του γύρου i το οποίο λαμβάνεται συνήθως από το αρχικό κλειδί. Η πράξη που εκτελείται στον μικρό κύκλο στο σχήμα είναι η πράξη του «Αποκλειστικού Ή» ή XOR (Exclusive Or) μεταξύ των αντίστοιχων bits δύο δυαδικών αριθμών, όπου το XOR δύο bits είναι ίσο με Ο όταν τα bits είναι ίδια, ενώ είναι ίσο με 1 όταν είναι διαφορετικά.

Αντιλαμβανόμαστε λοιπόν πως την ουσία ενός Feistel κρυπταλγόριθμου συνθέτουν οι μετασχηματισμοί f_i. Βέβαια η σχεδίαση τους αποτελεί μια εξαιρετικά

απαιτητική εργασία με σημαντική επίδραση στην ασφάλεια του όλου σχήματος. Αυτό που τελικά γίνεται στη πραγματικότητα είναι η χρήση σε όλους τους γύρους του ίδιου μετασχηματισμού f_i βέβαια με τη χρήση διαφορετικού κλειδιού σε κάθε γύρο

Σχεδόν το σύνολο των συμβατικών αλγορίθμων κρυπτογραφίας τμημάτων δεδομένων, περιλαμβάνουν μία δομή που περιγράφηκε πρώτα από τον H. Feistel. Θα λέγαμε πως το πιο γνωστό παράδειγμα κρυπταλγόριθμου με δομή Feistel δεν είναι άλλο από το περίφημο κρυπταλγόριθμο DES (Data Encryption Standard). Το DES αποτέλεσε ορόσημο στην επιστήμη της κρυπτογραφίας καθώς και τη βάση πειραμάτων και διερευνήσεων κατά κύριο λόγο στα σχήματα κρυπτογράφησης κρυφού κλειδιού, δημιουργώντας έτσι σημαντικά οφέλη για την ανάπτυξη της κρυπτογραφίας και της κρυπτανάλυσης.

8.2. Κρυφό κλειδί DES

Το Πρότυπο Κρυπτογράφησης Δεδομένων DES (Data Encryption Standard) προέκυψε από την επίσημη υποβολή της IBM το 1974 στην πρόσκληση του Εθνικού Οργανισμού Προτύπων των Ηνωμένων Πολιτειών. Το 1977 υιοθετήθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology – NIST), USA, ως Federal Information Processing Standard 46 – FIPS PUB 46. Ο αλγόριθμος που έχει υλοποιηθεί στο σύστημα DES αναφέρεται ως Data Encryption Algorithm – DEA. Το DES προέκυψε σαν μια προσπάθεια να αναπτυχθούν ασφαλείς ηλεκτρονικές εγκαταστάσεις επικοινωνίας για επιχειρήσεις όπως τράπεζες και άλλες μεγάλες οικονομικές οργανώσεις. Ο DES ήταν ο πρώτος δημόσια προσιτός αλγόριθμος κρυπτογράφησης. Η απελευθέρωση της προδιαγραφής της υποκίνησε μια έκρηξη δημόσιου και ακαδημαϊκού ενδιαφέροντος για τα συστήματα κρυπτογραφίας.

Σε μία επικοινωνία σύμφωνα με τα πρότυπα του κρυφού κλειδιού DES οι συμμετέχοντες έχουν συμφωνήσει από πριν σε ένα κλειδί. Το κλειδί αυτό χρησιμοποιείται τόσο για την κρυπτογράφηση του μηνύματος από τον αποστολέα

όσο και για την αποκρυπτογράφηση του από τον παραλήπτη. Για το λόγο αυτό το σχήμα DES είναι ένα σχήμα κρυπτογράφησης διαμοιραζόμενου κλειδιού.

Το πρότυπο DES υλοποιεί μία μέθοδο κρυπτογράφησης κρυφού κλειδιού αποτελώντας στο χώρο των τραπεζικών συναλλαγών, ένα από τα πιο γνωστά μέσα κρυπτογράφησης. Η αποτελεσματικότητα της μεθόδου ήταν τέτοια που για τρεις δεκαετίες είχε υιοθετηθεί επίσημα ως μέθοδος κρυπτογράφησης και ως πρότυπο απόκρυψης δεδομένων από την κυβέρνηση των Ηνωμένων Πολιτειών αλλά και από πολλά κράτη και διεθνείς οργανισμούς. Ωστόσο κατά την περίοδο των τριών δεκαετιών το πρότυπο DES αποτέλεσε αντικείμενο μεγάλης έρευνας αλλά και διαμάχης. Οι πολέμιοί του πίστευαν ότι ο μετασχηματισμός f του DES έκρυβε μια «πίσω πόρτα» που επέτρεπε στην κυβέρνηση των ΗΠΑ να ανακτά εύκολα το κλειδί κρυπτογράφησης. Το DES, όπως ήταν φυσικό, δυστυχώς δεν μπόρεσε να αντισταθεί στη ταχεία ανάπτυξη των υπολογιστικών συστημάτων, τα οποία μπορούν να εξερευνούν γρήγορα το μεγάλο χώρο δυνατών κλειδιών του DES.

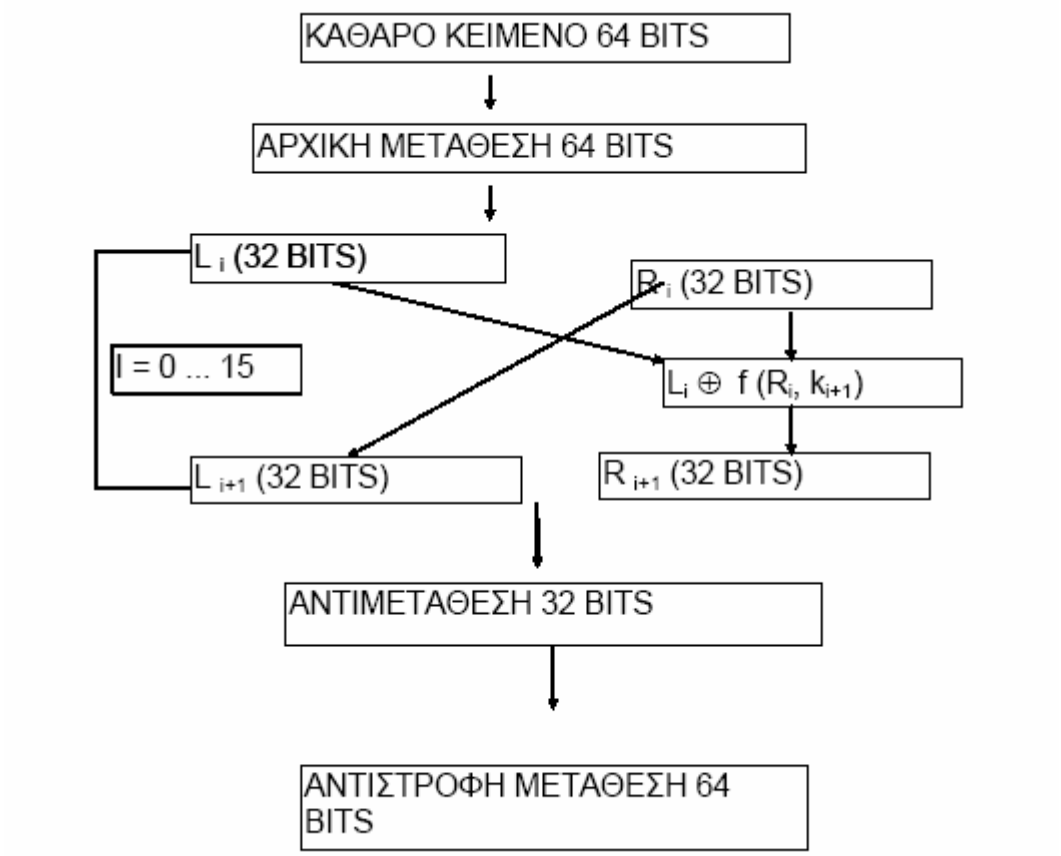
8.3. Περιγραφή του DES

Ο DES είναι ένας αλγόριθμος μπλοκ ο οποίος κρυπτογραφεί τα δεδομένα σε μπλοκ των 64 bit. Κάθε μπλοκ 64 bit αρχικού κειμένου δίνει ένα μπλοκ 64 bit κρυπτογραφήματος. Ο DES είναι ένας συμμετρικός αλγόριθμος. Ο ίδιος αλγόριθμος και το ίδιο κλειδί χρησιμοποιούνται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση.

Το κλειδί έχει μήκος 56 bit. Στην πραγματικότητα είναι 64 bit, αλλά κάθε όγδοο bit χρησιμοποιείται για έλεγχο ισοτιμίας και αγνοείται. Το bit ισοτιμίας είναι το χαμηλής τάξης bit κάθε byte.

Στη βάση του ο DES εφαρμόζει έναν συνδυασμό των δύο βασικότερων τεχνικών στην κρυπτογραφία, την σύγχυση και την διάχυση (confusion και diffusion). Τη σύγχυση την πετυχαίνει με αντικατάσταση και τη διάχυση με μετάθεση (substitution και permutation). Και οι δύο τεχνικές εφαρμόζονται στο κείμενο, με τρόπο εξαρτώμενο από το κλειδί. Αυτό είναι γνωστό σαν γύρος (round).

Ο DES αποτελείται από 16 γύρους. Ο αλγόριθμος χρησιμοποιεί βασικές αριθμητικές και λογικές πράξεις. Η σχηματική λειτουργία του κρυφού κλειδιού DES παρουσιάζεται στο ακόλουθο σχήμα.



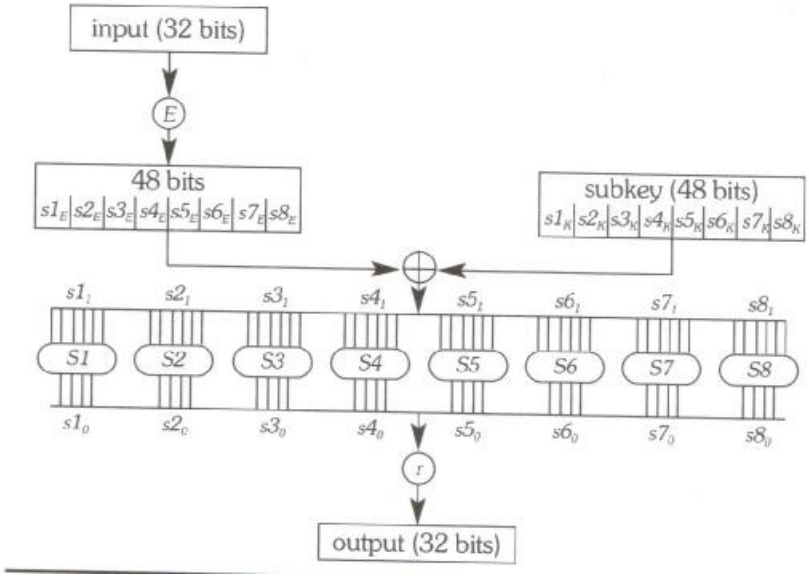
Σχήμα 8 : Σχηματική λειτουργία του DES

Πιο αναλυτικά, ο αλγόριθμος που υλοποιεί το σχήμα DES ανήκει στην κατηγορία κρυπταλγόριθμων blocks, κωδικοποιώντας blocks των 64 bits κάθε φορά. Συγκεκριμένα η λειτουργία του έχει ως εξής :

* *ως είσοδο* αρχικά δέχεται ένα block των 64 bits (π.χ. 8 χαρακτήρες ASCII) καθώς και ένα κλειδί 56 bits (ουσιαστικά το κλειδί είναι 64 bits, αλλά τα 8 από αυτά δεν χρησιμοποιούνται στη διαδικασία κρυπτογράφησης) και

* *ως έξοδο* δίνει ένα block 64 bits που είναι η κωδικοποίηση του αρχικού block. Στο block εισόδου εφαρμόζεται αρχικά μία αντιμετάθεση των bits (δηλαδή τα bits αλλάζουν μεταξύ τους θέσεις) και αυτό που προκύπτει ως αποτέλεσμα χωρίζεται σε

δύο τμήματα των 32 bits, το *αριστερό* και το *δεξί*. Στη συνέχεια εκτελούνται 16 επαναλήψεις του μετασχηματισμού f όπως φαίνεται στο παρακάτω σχήμα.



Σχήμα 9 : οι επαναλήψεις του f στο σχήμα DES

Αναλυτικότερα ο μετασχηματισμός αυτός παρατηρούμε ότι έχει δυο εισόδους:

* μία είσοδο των 32 bits (δηλ. το δεξί μισό της εξόδου των 64 bits της προηγούμενης επανάληψης) και

* μία είσοδο των 48 bits η οποία και αποτελείται από κατάλληλα επιλεγμένα (για την *τρέχουσα* επανάληψη) bits του αρχικού κλειδιού των 56 bits.

Η είσοδος των 32 bits υπόκειται σε μία αντιμετάθεση των bits με επανάληψη μερικών από αυτών με αποτέλεσμα να αυξηθεί το μήκος της λέξης των 32 bits σε 48. Στη συνέχεια, αυτά τα 48 bits συνδυάζονται με τα 48 bits του κλειδιού της τρέχουσας επανάληψης με την πράξη "XOR" (Exclusive Or) που συμβολίζεται με το πρόσημο «+» μέσα στο κύκλο [στο παραπάνω σχήμα, αυτή η αντιμετάθεση συμβολίζεται με το γράμμα Ε μέσα στον κύκλο, από το αρχικό γράμμα της λέξης expansion (επαύξηση)].

Στο σχήμα παρατηρούμε και τους συμβολισμούς S1 μέχρι S8 οι οποίοι παρουσιάζουν τους πίνακες Αντικατάστασης (Substitution Boxes). Κάθε πίνακας έχει :

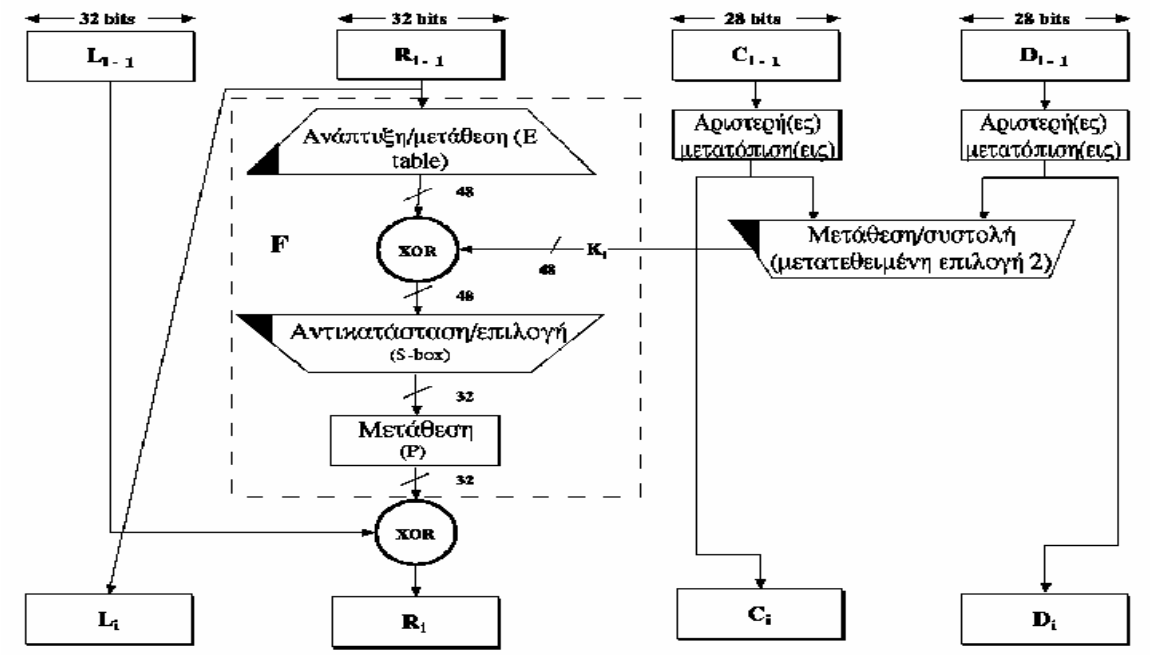
* ως είσοδο 6 από τα 48 bits (τα οποία είναι αποτέλεσμα της πράξης "XOR") και * ως έξοδο δίνει 4 bits.

Ουσιαστικά δηλαδή οι πίνακες αντικατάστασης (Substitution Boxes) αποτελούν ένα κανόνα ο οποίος αντικαθιστά 6 bits από την είσοδο με 4 άλλα bits. Το τελευταίο στάδιο του μετασχηματισμού f είναι η εφαρμογή μίας αντιμετάθεσης, που στο σχήμα συμβολίζεται με το γράμμα r μέσα στον κύκλο. Ως παρεπόμενο είναι η δημιουργία μίας λέξης των 32 bits, η οποία συνδυάζεται με το αριστερό μέρος της εισόδου στο μετασχηματισμό και το αποτέλεσμα γίνεται το καινούριο δεξί μέρος των 32 bits το οποίο δίδεται ως είσοδος στο μετασχηματισμό f της επόμενης επανάληψης. Αντιλαμβανόμαστε λοιπόν πως το προηγούμενο δεξί μέρος, το οποίο αποτελούσε την είσοδο στο μετασχηματισμό f της τρέχουσας επανάληψης, καθίσταται το αριστερό μέρος στην επόμενη επανάληψη.

Αφού ολοκληρωθούν και οι 16 επαναλήψεις του προαναφερθέντος μετασχηματισμού, η τελική λέξη των 64 bits υπόκειται σε αντιμετάθεση των δυαδικών του ψηφίων. Η τελευταία αυτή αντιμετάθεση ουσιαστικά αποκαθιστά τη σειρά των ψηφίων του αρχικού μηνύματος την οποία κατάστρεψε η αρχική αντιμετάθεση.

Στη συνέχεια παραθέτουμε δυο σχηματικές απεικονίσεις του αλγόριθμου κρυπτογράφησης DES χρήσιμες για την πληρέστερη κατανόηση του κρυφού κλειδιού.

Σχήμα 10 : Γενική περιγραφή του αλγορίθμου κρυπτογράφησης DES



Σχήμα 11 : Ένας κύκλος του αλγορίθμου DES

8.4. Τρόποι λειτουργίας του DES

Ο τρόπος λειτουργίας ενός αλγορίθμου καθορίζει πώς τα μπλοκ του αρχικού κειμένου κρυπτογραφούνται σε μπλοκ κρυπτογραφήματος, και αντίστροφα. Ένας κρυπτογραφικός τρόπος λειτουργίας συνήθως συνδυάζει τον βασικό αλγόριθμο, κάποια μορφή ανακύκλωσης (feedback) και μερικές απλές λειτουργίες. Οι λειτουργίες είναι απλές, γιατί δεν έχουν στόχο την ενίσχυση της ασφάλειας. Ακόμη πιο σημαντικό είναι ο τρόπος λειτουργίας να μην αναιρεί την ασφάλεια που προσφέρει ο αλγόριθμος.

Υπάρχουν και άλλα που πρέπει να ληφθούν υπ' όψιν κατά τον σχεδιασμό ενός τρόπου λειτουργίας θα πρέπει να:

- αποκρύπτονται τυχόν αναγνωρίσιμα χαρακτηριστικά του κειμένου,
- να καθίστανται τυχαία τα δεδομένα εισόδου του αλγορίθμου,
- να καθίσταται δύσκολη η μεταβολή του αρχικού κειμένου με εισαγωγή λαθών στο κρυπτογράφημα,

- και να καθίσταται δυνατή η κρυπτογράφηση περισσότερων του ενός μηνυμάτων με το ίδιο κλειδί.

Η αποδοτικότητα είναι ένα ακόμα μέλημα. Ο τρόπος λειτουργίας δεν θα πρέπει να μειώνει σημαντικά την απόδοση του αλγορίθμου. Σε μερικές περιπτώσεις είναι σημαντικό το κρυπτογράφημα να έχει ίδιο μέγεθος με το αρχικό κείμενο.

Ένα τρίτο μέλημα είναι η ανοχή σε λάθη. Σε μερικές εφαρμογές είναι σημαντικό να μπορεί η διαδικασία αποκρυπτογράφησης να αντιμετωπίζει τυχόν λάθη στα bit του κρυπτογραφήματος, που μπορεί να περιλαμβάνουν bit με αλλαγμένη τιμή, bit που έχουν προστεθεί ή bit που έχουν χαθεί.

8.5. Κρυπταναλύοντας το πρότυπο DES

Όπως σε όλα τα κρυπτογραφικά σχέδια έτσι και για το πρότυπο DES υπήρχαν διαμάχες σε σχέση με την ασφάλεια του προτύπου. Ο φόβος εστιαζόταν στο κατά πόσο η σχεδίαση του έκρυβε κάποια παγίδα η οποία θα επέτρεπε σε αυτόν που γνώριζε την ύπαρξη της να εντοπίζει με ευκολία το κλειδί.

Βασική αδυναμία στον αλγόριθμο από αρκετούς ερευνητές θεωρήθηκε η επιλογή κλειδιού μήκους μόνο 56 bits κάνοντας έτσι το πρότυπο DES ευάλωτο σε επιθέσεις «ωμής βίας». Με το όρο επιθέσεις «ωμής βίας» αναφερόμαστε στη συνεχή δοκιμή κάθε πιθανού κλειδιού ως προς το αν η κρυπτογράφηση έχει γίνει με αυτό το κλειδί ή όχι.

Η επίθεση ωμής βίας αποτελεί την πρωταρχική ανησυχία κατά τη σχεδίαση ενός κρυπταλγόριθμου. Για το λόγο αυτό βασική επιδίωξη αποτελεί ο εφοδιασμός του κρυπταλγόριθμου με ένα αρκετά μεγάλο χώρο δυνατών κλειδιών. Η επίθεση ωμής βίας μπορεί να υλοποιηθεί όταν έχουμε ένα αρχικό μήνυμα μαζί με την κωδικοποίηση του υπό ένα κρυπταλγόριθμο με ένα άγνωστο κλειδί και δοκιμάζουμε όλα τα πιθανά κλειδιά μέχρι η αποκωδικοποίηση να δώσει το αρχικό μήνυμα. Ωστόσο δεν αποτελεί ικανή συνθήκη αποφυγής επίθεσης ωμής βίας η ύπαρξη μεγάλου χώρου κλειδιών. Δεν θα πρέπει να παραβλέπουμε επίσης το γεγονός ότι υπάρχουν και άλλες, πιο έξυπνες επιθέσεις οι οποίες εκμεταλλεύονται δομικές

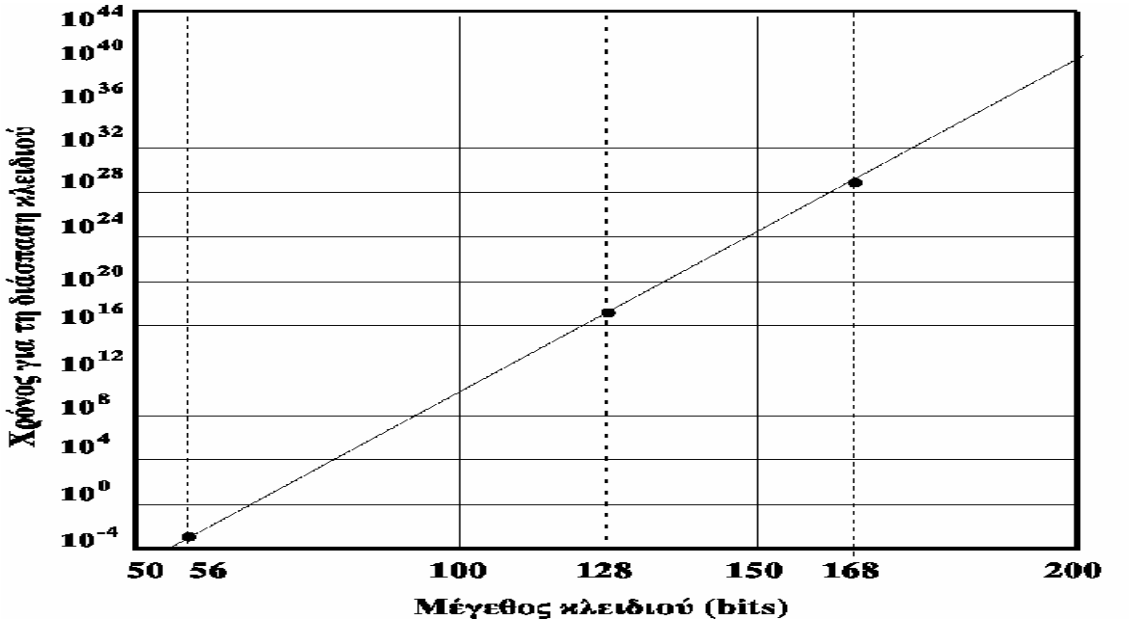
αδυναμίες του κρυπταλγόριθμου, παρακάμπτοντας έτσι την εξέταση όλου του χώρου δυνατών κλειδιών. Για τις αδυναμίες ενός κρυπταλγορίθμου μπορούν να μιλήσουν, από διαφορετική σκοπιά, δύο κατηγορίες ανθρώπων:

* *οι σχεδιαστές του κρυπταλγόριθμου* οι οποίοι προσπαθούν να αποδείξουν ότι τα τρέχοντα τεχνολογικά και οικονομικά δεδομένα καθιστούν ανέφικτη τη συστηματική διερεύνηση του δυνατού χώρου κλειδιών,

* και *οι κρυπταναλυτές*, οι οποίοι πρέπει να εκμεταλλευτούν τα τεχνολογικά και οικονομικά δεδομένα με τον καλύτερο τρόπο.

Μήκος κλειδιού (bits)	Αριθμός των πιθανών κλειδιών	Απαιτούμενος χρόνος για κρυπτανάλυση με ρυθμό δοκιμών 1 αποκρυπτογράφηση/μs	Απαιτούμενος χρόνος για κρυπτανάλυση με ρυθμό δοκιμών 10^6 αποκρυπτογραφήσεις /μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 λεπτά	2.15 ms
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 χρόνια	10 ώρες
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4 × 1024 χρόνια	5.4×10^{18} χρόνια
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9 × 1036 χρόνια	5.9×10^{30} χρόνια

Πίνακας 1 : Μέσος χρόνος που απαιτείται για εξαντλητική αναζήτηση κλειδιών



Σχήμα 12 : Χρόνος που απαιτείται για τη διάσπαση ενός κώδικα (υποθέτοντας 106 αποκρυπτογραφήσεις/μs)

Ας εξετάσουμε όμως το σχήμα DES με αριθμούς, οι οποίοι εκφράζουν τις πραγματικές του διαστάσεις. Το σχήμα DES επιτρέπει κλειδιά μήκους 56 bits. Αυτό σημαίνει ότι ο χώρος των δυνατών κλειδιών περιέχει 2^{56} = 72.057.594.037.927.936 κλειδιά!

<u>Υπόθεση 1η</u>

Έστω ότι :

* ένας υπολογιστής μπορεί να εκτελέσει τον αλγόριθμο κρυπτογράφησης DES σε διάστημα 2 χιλιοστά του δευτερολέπτου και

* για να βρεθεί το κλειδί πρέπει να ελεγχθούν τα μισά κλειδιά ($2^{56}/2 = 2^{55}$).

Με βάση τα δεδομένα αυτά θα χρειαστούν περισσότερα από 2.000 χρόνια για να βρεθεί το σωστό κλειδί.

Συμπεραίνουμε λοιπόν ότι πρόκειται για ένα ασφαλές κλειδί.

Υπόθεση 2η

Έστω ότι

* στο άμεσο μέλλον η τεχνολογία επιτυγχάνει την κατασκευή υπολογιστών με τη διπλάσια ταχύτητα.

Τότε το σωστό κλειδί θα βρισκόταν σε 1.000 χρόνια ή σε 500 χρόνια εάν διπλασιαζόταν η ταχύτητα (αν και η ταχύτητα του υλικού επεξεργασίας είναι δύσκολο να διπλασιαστεί). Να επισημάνουμε επίσης ότι η φύση της ύλης και οι περιορισμοί της μικροηλεκτρονικής απαγορεύουν την απεριόριστη αύξηση της ταχύτητας υλικού.

Συμπεραίνουμε λοιπόν ότι γενικά η αύξηση της ταχύτητας των μικροεπεξεργαστών δεν αποτελεί μεγάλη απειλή για ένα κρυπτοσύστημα όπως είναι το DES.

Υπόθεση 3η

Έστω ότι :

* έχουμε δύο επεξεργαστές και
* ο καθένας ερευνά το μισό χώρο των πιθανών κλειδιών.

Τότε θα απαιτούνταν 250 χρόνια ή 125 χρόνια εάν βάλουμε τέσσερις επεξεργαστές ή 3 μόλις μήνες εάν έχουμε 2.048 επεξεργαστές (καθόλου κοστοβόρο ακόμη και για μία μικρή εταιρία)!

Συμπεραίνουμε λοιπόν ότι ***ο κίνδυνος πηγάζει από τη συνεργασία πάρα πολλών «μικρών» επεξεργαστικών στοιχείων ικανών να εκτελούν απλώς και μόνο μερικές βασικές λογικές πράξεις.***

Η 4η υπόθεση ονομάζεται μαζικός παραλληλισμός και πρώτο-παρουσιάστηκε από τον Mike Wiener.

8.6. Η επίθεση ωμής βίας του Wiener με μαζικά παράλληλους υπολογισμούς

Το 1993 ο Mike Wiener κατόρθωσε να ανακαλύψει ένα DES κλειδί μέσα σε *3,5* ώρες απλά και μόνο με μία ολοκληρωμένη σχεδίαση ενός μαζικά παράλληλου υπολογιστή, λογικού κόστους. Όπως ήταν αναμενόμενο η αξιοπιστία του πρότυπου DES είχε αρχίσει να κλονίζεται. Τέτοιου είδους συστήματα όπως αυτό του Wiener αποτελούν πραγματικό κίνδυνο για μήκη κλειδιών τα οποία πριν από λίγα χρόνια θεωρούνταν ασφαλή χωρίς αντίστοιχα να έχουν απαγορευτικό κόστος κατασκευής.

Πρόκειται για μια τεχνολογία ολοκληρωμένων κυκλωμάτων υψηλής ολοκλήρωσης και μίας οικονομικά υλοποιήσιμης σχεδίασης η οποία οδηγεί σε ένα μαζικά παράλληλο υπολογιστικό σύστημα ικανού να ανακαλύψει ένα κλειδί 56 bits μέσα σε λίγες μόνο ώρες. Συγκεκριμένα η σχεδίαση του Wiener περιλαμβάνει 57.600 ειδικά επεξεργαστικά ολοκληρωμένα κυκλώματα που το καθένα αναζητά το σωστό κλειδί μέσα σε ένα υποσύνολο του χώρου πιθανών κλειδιών που του έχει ανατεθεί. Το καθένα από αυτά τα ολοκληρωμένα κυκλώματα χρησιμοποιεί 16 στάδια σωληνώσεως εντολών.

Παραστατικά θα μπορούσαμε να το απεικονίσουμε σαν μία γραμμή παραγωγής αυτοκινήτων, όπου την ίδια στιγμή σε κάποιο σημείο κάποιος βάζει μία πόρτα, σε κάποιο σημείο κάποιος άλλος βάζει τη μηχανή, ενώ πιο πέρα κάποιος βάζει το τιμόνι. Έτσι ταυτόχρονα επιτυγχάνεται να εκτελούνται διαφορετικές λειτουργίες (Βίδωμα πόρτας κ.λπ.) σε διαφορετικά δεδομένα (αυτοκίνητα).

Να υπενθυμίσουμε ότι το κάθε στάδιο σωληνώσεως τελειώνει τη λειτουργία του σε 1 nanosecond (1 δισεκατομμυριοστό του δευτερολέπτου) με ταχύτητα επεξεργασίας του ολοκληρωμένου τα 50MHz, ενώ όταν και τα 16 στάδια είναι ενεργά τότε η εξέταση ενός κλειδιού απαιτεί χρόνο 20 nanosecond. Αντιλαμβάνεται κανείς το πόσο ανασφαλές είναι το πρότυπο DES αν και μόνο αν αναλογιστούμε τα τεχνολογικά δεδομένα της εποχής μας.

Στη σχεδίαση του Wiener :

* *η ταχύτητα* εξέτασης κλειδιών του ολοκληρωμένου κυκλώματος που περίγραψε ανέρχεται στα 50.000.000 κλειδιά το δευτερόλεπτο,

* *το κόστος* της όλης σχεδίασης φτάνει το 1.000.000 δολάρια ΗΠΑ (σύμφωνα με τα οικονομικά δεδομένα του 1993).

Το ποσό μπορεί να μοιάζει υπερβολικό όμως δεν θα πρέπει να ξεχνάμε τη χρησιμότητα ενός προτύπου. Αν για παράδειγμα το Υπουργείο Εθνικής Άμυνας επιθυμεί να είναι σε θέση ανά πάσα στιγμή να αποκρυπτογραφεί εχθρικά μηνύματα με κάθε τρόπο το να επενδύσει σε ένα τέτοιο ποσό πραγματικά είναι μηδαμινό για τον προϋπολογισμό του.

Επιπλέον ο Wiener και η ερευνητική του ομάδα κυκλοφόρησαν σε βιβλίο την πλήρη σχεδίαση του υλικού της παράλληλης μηχανής μαζί με τους αντίστοιχους αλγόριθμους. Μάλιστα διατυμπάνισαν περίτρανα πως όποιος ακολουθήσει πιστά τα βήματα που αναφέρονται στο εν λόγω βιβλίο (επενδύοντας και τα σχετικά χρήματα) θα είναι ικανός να δημιουργήσει τη δική του μηχανή σπασίματος DES!

ΚΕΦΑΛΑΙΟ 9^{ο} : Άλλα κρυπτογραφικά σχήματα

9.1. Triple DES

Το TDES ή TDEA ή 3DES προτάθηκε από τον W. Tuchman το 1985 και προτυποποιήθηκε στο ANSI X9.17. Ουσιαστικά πρόκειται για μια παραλλαγή του DES όπου το μήνυμα κρυπτογραφείται και αποκρυπτογραφείται διαδοχικά με διαφορετικά κλειδιά για την ενίσχυση του βασικού αλγόριθμου. Το Triple DES, προσφέρει σημαντικά βελτιωμένη ασφάλεια από την εκτέλεση των βασικών DES αλγόριθμο τρεις φορές στη σειρά. Αυτό έχει ως αποτέλεσμα να καθίσταται η DES κρυπτογράφηση πολύ πιο δύσκολη σε επιθέσεις ωμής βίας.

Το TDES χρησιμοποιεί τρία κλειδιά και τρεις εκτελέσεις του αλγορίθμου DES. Ο αλγόριθμος ακολουθεί τη διαδοχή:

κρυπτογράφηση, αποκρυπτογράφηση, κρυπτογράφηση

(EDE – encryption – decryption - encryption):

C = EK3[DK2[EK1[P]]] όπου:

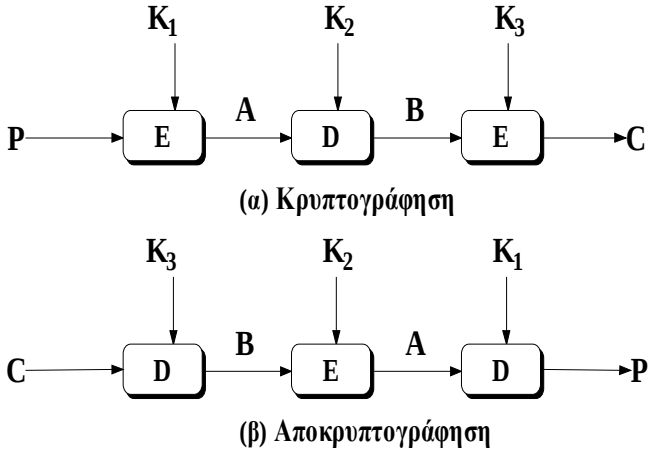
C = κρυπτογράφημα

P = αρχικό κείμενο

EK[X] = κρυπτογράφηση του X με χρήση του κλειδιού K

DK[Y] = αποκρυπτογράφηση του X με χρήση του κλειδιού K

Η αποκρυπτογράφηση ακολουθεί ακριβώς την ίδια διαδικασία με τα κλειδιά σε αντίστροφη χρήση: P = DK1 [EK2 [DK3[C]]]



Σχήμα 13 : Ο αλγόριθμος Triple DES

Το Triple-DES εκτιμάται ότι θα είναι 2 εως 56 φορές πιο δύσκολο να σπάσει από το DES. Το Triple DES μπορεί ακόμη να θεωρηθεί ως ασφαλής αλγόριθμος κρυπτογράφησης. Υπάρχουν τέσσερις διαφορετικοί τρόποι για να επιτευχθεί η κρυπτογράφηση – αποκρυπτογράφησης του Triple-DES :

DES-EEE3 (Encrypt-Encrypt-Encrypt): πραγματοποιούνται τρεις συνεχόμενες κρυπτογραφήσεις με το τρία διαφορετικά κλειδιά.

DES-EDE3 (Encrypt-Decrypt-Encrypt): το μήνυμα διαδοχικά κρυπτογραφείται, αποκρυπτογραφείται και τέλος κρυπτογραφείται με χρήση τριών διαφορετικών κλειδιών.

DES-EEE2: είναι η ίδια με την πρώτη διαδικασία εκτός του ότι απαιτούνται δύο διαφορετικά κλειδιά.

DES-EDE2: είναι η ίδια με την δεύτερη διαδικασία εκτός του ότι απαιτούνται δύο κλειδιά.

Τα επιπλέον κλειδιά δημιουργούνται από το κοινό μυστικό κλειδί με κατάλληλο αλγόριθμο. Από αυτούς τους τρόπους, ο πιο ασφαλής είναι ο DES-EEE3, με την τριπλή κρυπτογράφηση και τα τρία διαφορετικά κλειδιά. Σαν βασικό μειονέκτημα του TDES θα μπορούσαμε να αναφέρουμε ότι ο αλγόριθμος είναι σχετικά αργός σε υλοποιήσεις με χρήση λογισμικού.

9.2. Το σχήμα κρυπτογράφησης RSA

Το σχήμα κρυπτογράφησης RSA αναπτύχθηκε το 1977 από τους Ron Rivest, Adi Shamir και Len Adelman στο MIT. Το σχήμα RSA θεωρείται κορυφαίο αφού είναι η μόνη προσέγγιση που είναι ευρέως αποδεκτή και η μόνη που έχει υλοποιηθεί. Η κρυπτογράφηση περιλαμβάνει σπονδυλωτή αριθμητική. Η ισχύς του αλγορίθμου βασίζεται στη δυσκολία εύρεσης της παραγοντοποίησης των αριθμών στους πρώτους παράγοντές τους.

Συγκεκριμένα, η κρυπτογράφηση και η αποκρυπτογράφηση για ένα κείμενο M και το αντίστοιχο κρυπτογραφημένο C συμβολίζονται ως ακολούθως:

$$C=Me \bmod n$$

$$M=Cd \bmod n=(Me)d \bmod n = Med \bmod n$$

Ο RSA είναι ένας αλγόριθμος όπου το καθαρό κείμενο είναι ακέραιοι μεταξύ του 0 και n-1 για κάποιο n.

Για να είναι ικανοποιητικός ο αλγόριθμος θα πρέπει να ικανοποιούνται οι ακόλουθες απαιτήσεις:

- Είναι δυνατό να βρεθούν τιμές για τα e,d,n, τέτοιες ώστε να ισχύει: Med = M mod n, για κάθε M<n
- Είναι σχετικά εύκολο να υπολογιστούν τα Me και C, για κάθε M<n
- Είναι αδύνατο να προσδιοριστεί το d, δοθέντων των e και n

Παραγωγή κλειδίου

Επέλεξε p, q	p και q κι οι δύο πρώτοι
Υπολόγισε $n = p \times q$	
Υπολόγισε $\phi(n) = (p - 1)(q - 1)$	
Επέλεξε ακέραιο e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Υπολόγισε d	$d = e^{-1} \bmod \phi(n)$
Δημόσιο κλειδί	$KU = \{e, n\}$
Ιδιωτικό κλειδί	$KR = \{d, n\}$

Κρυπτογράφηση

Κρυπτογράφημα:	$M < n$
Αρχικό κείμενο:	$C = M^e \pmod n$

Αποκρυπτογράφηση

Κρυπτογράφημα:	C
Αρχικό κείμενο:	$M = C^d \pmod n$

Σχήμα 14 : Αλγόριθμος RSA

* Έστω ότι πολλαπλασιάζουμε δύο φυσικούς αριθμούς p και q και ζητείται το γινόμενο n. Ας δοκιμάσουμε τώρα το αντίστροφο!

* Έστω ο αριθμός n ο οποίος είναι το γινόμενο δύο άλλων αριθμών (p και q) και ζητείται να βρούμε αυτούς τους αριθμούς (p και q)! Αυτή η πράξη φαίνεται να είναι δυσκολότερη σε σχέση με τη προηγούμενη.

Πράγματι είναι αρκετά πιο εύκολο να πολλαπλασιάσουμε δύο αριθμούς και να βρούμε το γινόμενο τους παρά να βρούμε τους δύο αριθμούς δοθέντος του γινομένου τους. Κατά τη πράξη του πολλαπλασιασμού εφαρμόζουμε επαναληπτικά μερικούς απλούς κανόνες και μετά από ένα μικρό αριθμό βημάτων, που εξαρτάται από το πόσα ψηφία έχουν οι αριθμοί, φθάνουμε στο αποτέλεσμα του. Αντίθετα, κατά τη πράξη εύρεσης του γινομένου φαίνεται ότι πρέπει να ερευνήσουμε ένα μεγάλο πλήθος φυσικών αριθμών και να ανακαλύψουμε το ζεύγος που πολλαπλασιαζόμενο

δίνει το δοσμένο αριθμό. Το πρόβλημα ονομάζεται *πρόβλημα παραγοντοποίησης σε πρώτους αριθμούς*, καθώς οποιοσδήποτε από τους δύο αριθμούς που αναζητάμε έχει την ιδιότητα να είναι πρώτος, δηλαδή να διαιρείται ακριβώς μόνο από τον αριθμό 1 και τον εαυτό του.

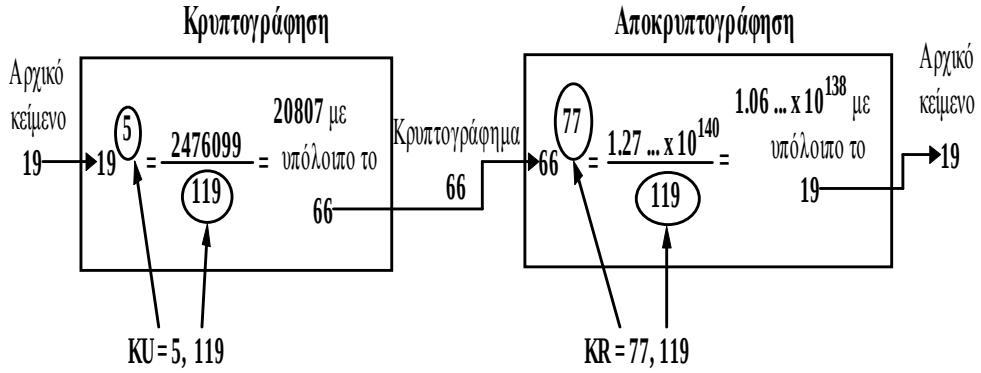
Το πρόβλημα της παραγοντοποίησης αριθμών είναι ένα από μία πολυπληθή ομάδα προβλημάτων τα οποία έχουν την ιδιότητα, ύστερα από δεκαετίες προσπαθειών να μην έχει βρεθεί ακόμη κάποιος γρήγορος τρόπος επίλυσης με υπολογιστή, ενώ θεωρείται μάλλον απίθανο να συμβεί ποτέ κάτι τέτοιο. Το σχήμα RSA που απεικονίσαμε περιγραφικά, στηρίζεται ακριβώς στην ιδιότητα αυτού του προβλήματος.

9.2.1.Παράδειγμα αλγορίθμου RSA

Όλα όσα αναφέραμε σχετικά με τον αλγόριθμο RSA μπορούν να γίνουν περισσότερο κατανοητά με τη βοήθεια ενός απλού παραδείγματος. Έστω τα παρακάτω δεδομένα όπως εμφανίζονται στον ακόλουθο πίνακα :

Επιλογή p,q	p=7, q=17
n=pxq	7 x 17 = 119
φ(n)=(p-1)(q-1)	6 x 16 = 96
gcd(φ(n),e)=1	5
d	77
Δημόσιο Κλειδί	KU (5,119)
Ιδιωτικό Κλειδί	KR (77,119)

Πίνακας 2 : Δεδομένα παραδείγματος RSA



Σχήμα 15 : Παράδειγμα RSA

Έστω ότι κάποιος επιθυμεί να λαμβάνει κωδικοποιημένα μηνύματα από άλλους. Αυτό μπορεί να γίνει απλά επιλέγοντας δύο μεγάλους *πρώτους αριθμούς (*ρ και q) και με κάποιον αλγόριθμο που ανακαλύπτει γρήγορα πρώτους αριθμούς με πολλά ψηφία. Το n είναι το γινόμενο που προκύπτει των ρ και q *:* $\eta = \rho q$.

Στη συνέχεια βρίσκουμε δύο ειδικούς αριθμούς, πρώτα τον ***e*** και μετά τον ***d,*** οι οποίοι σχετίζονται με κάποιον τρόπο με τους ρ και q. Ο αριθμός ***d*** είναι ένας οποιοσδήποτε ακέραιος που είναι συν-πρώτος προς τον (ρ-1)(q-1), δηλαδή ο μεγαλύτερος αριθμός που διαιρεί και τους δύο είναι ο αριθμός 1 και ταυτόχρονα είναι ο *αντίστροφος* του e ως· *προς υπόλοιπα,* είναι δηλαδή τέτοιος ώστε να ισχύει ***ed*** = 1 (mod (ρ-1)(q-1)), το οποίο σημαίνει ότι οι αριθμοί ***d*** και ***e*** είναι τέτοιοι ώστε η διαφορά ***ed-1*** διαιρείται ακριβώς από τον αριθμό (ρ-1)((q-1).

Το δημόσιο κλειδί αποτελείται από το ζεύγος (e,η), ενώ το ιδιωτικό κλειδί αποτελείται από το ζεύγος ***(d,η).***

Παρατηρούμε ότι το ιδιωτικό κλειδί μπορεί εύκολα να μαθευτεί εάν βρεθούν οι πρώτοι παράγοντες του η, οι αριθμοί ρ και ***q*** δηλαδή. Όμως, αυτό είναι υπολογιστικά δύσκολο για μεγάλους αριθμούς η!

9.3. Άλλοι αλγόριθμοι κρυπτογράφησης

Εκτός από το DES, το TRIPLE DES και το RSA (που ήδη περιγράψαμε) πολύ γνωστοί αλγόριθμοι κρυπτογράφησης είναι και οι ακόλουθοι :

9.3.1. DESX

Ο DESX είναι μια άλλη παραλλαγή του DES. Η διαφορά του DES και του DESX είναι ότι η είσοδος στο DESX περνάει από μια X-OR πράξη με ένα επιπλέον κλειδί 64 bits και ομοίως η έξοδος της κρυπτογράφησης. Η αιτία ανάπτυξης του DESX είναι η δραματική αύξηση της αντοχής του DES σε γνωστές επιθέσεις.

9.3.2 IDEA

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

9.3.3. BLOWFISH

Ο Blowfish είναι ένας block cipher που κατασκευάστηκε από τον Schneier. Είναι ένας Feistel cipher με μέγεθος block 64 bits και μεταβλητό μήκος κλειδιού, με μέγιστο μήκος 448 bits. Όλες οι διεργασίες βασίζονται σε X-OR πράξεις και προσθέσεις λέξεων των 32 bits. Από το κλειδί παράγεται πίνακας με subkeys τα

οποία χρησιμοποιούνται σε κάθε γύρο επανάληψης της κρυπτογράφησης. Έχει σχεδιασθεί για 32-bit μηχανές και είναι σημαντικά ταχύτερος από τον DES. Παρ' όλες τις αδυναμίες που έχουν ανακαλυφθεί καθ' όλη την διάρκεια της ύπαρξης του, θεωρείται ακόμα ασφαλής αλγόριθμος.

9.3.4. UNIX CRYPT

Η ρουτίνα κρυπτογράφησης κωδικών του UNIX βασίζεται στον DES. Ο αλγόριθμος DES τροποποιείται χρησιμοποιώντας μια 12-bit τιμή “salt”. Τυπικά αυτή η τιμή σχετίζεται με το χρόνο που ανατέθηκε ο κωδικός πρόσβασης στο χρήστη. Ο τροποποιημένος αλγόριθμος DES εφαρμόζεται με μια είσοδο δεδομένων που αποτελείται από ένα 64-bit μπλοκ μηδενικών. Η έξοδος του αλγορίθμου εν συνεχεία λειτουργεί ως είσοδος σε μία δεύτερη κρυπτογράφηση. Αυτή η διεργασία επαναλαμβάνεται για συνολικά 25 κρυπτογραφήσεις. Η 64-bit έξοδος που προκύπτει μεταφράζεται σε μια ακολουθία 11 χαρακτήρων

9.3.5. KASUMI

Ο αλγόριθμος αυτός χρησιμοποιείται στα UTMs standard και στα νεότερα GSM A5/3 για κρυπτογράφηση φωνής και δεδομένων. Χρησιμοποιεί κλειδί μήκους 128 bits.

ΚΕΦΑΛΑΙΟ 10^{ο} : Ελληνική τραπεζική εμπειρία

Στο κεφάλαιο αυτό γίνεται μια προσπάθεια να περιγράψουμε τις πολιτικές ασφαλείας των πληροφοριακών συστημάτων δύο Τραπεζών ώστε να διαπιστωθεί στη πράξη ο τρόπος με το οποίο χειρίζονται το ζήτημα της ασφάλειας οι ελληνικές τράπεζες. Οι σχετικές με τις τράπεζες πληροφορίες που παραθέτουμε στην συνέχεια αντλήθηκαν από το δικτυακό τόπο της κάθε τράπεζας.

10.1 . Εθνική Τράπεζα της Ελλάδος (ΕΤΕ)

10.1.1. Γενικά στοιχεία

Η Εθνική Τράπεζα της Ελλάδος, με τη μεγαλύτερη και ισχυρότερη παρουσία στον Ελλαδικό χώρο, αλλά και με το δυναμικό προφίλ της στη Νοτιοανατολική Ευρώπη και την Ανατολική Μεσόγειο ηγείται του μεγαλύτερου και ισχυρότερου Ομίλου χρηματοοικονομικών υπηρεσιών στην Ελλάδα. Ιδρύθηκε το 1841 ως εμπορική τράπεζα και μέχρι την ίδρυση της Τράπεζας της Ελλάδος το 1928 είχε το εκδοτικό προνόμιο. Εισήχθη στο Χρηματιστήριο Αξιών Αθηνών από την ίδρυση του το 1880, ενώ από τον Οκτώβριο του 1999, η μετοχή της Εθνικής Τράπεζας διαπραγματεύεται και στο Χρηματιστήριο της Νέας Υόρκης.

Η ΕΤΕ είναι ένα πιστωτικό ίδρυμα που λειτουργεί νόμιμα, υπαγόμενη στην ελληνική και κοινοτική τραπεζική νομοθεσία και ειδικότερα στον Ν.2076/92 όπως ισχύει σήμερα, που ως γνωστόν ενσωμάτωσε στο ελληνικό δίκαιο την δεύτερη τραπεζική οδηγία 89/646/ΕΟΚ του Συμβουλίου των Ευρωπαϊκών Κοινοτήτων.

Ο Όμιλος της ΕΤΕ προσφέρει ευρύ φάσμα χρηματοοικονομικών προϊόντων και υπηρεσιών που ανταποκρίνονται στις συνεχώς μεταβαλλόμενες ανάγκες επιχειρήσεων και ιδιωτών, όπως επενδυτικές εργασίες, χρηματιστηριακές συναλλαγές, ασφάλειες, διαχείριση στοιχείων ενεργητικού - παθητικού, εργασίες χρηματοδοτικής μίσθωσης, διαχείρισης επιχειρηματικών απαιτήσεων.

Με το πληρέστερο δίκτυό της που καλύπτει 604 καταστήματα και 1241 ATMς καλύπτει ολόκληρη τη γεωγραφική έκταση της Ελλάδας. Παράλληλα αναπτύσσει εναλλακτικά δίκτυα πώλησης των προϊόντων της, όπως οι υπηρεσίες Mobile και Internet Banking. Σήμερα και μετά τις πρόσφατες εξαγορές στο χώρο της Βαλκανικής, το Δίκτυο της Τράπεζας στο εξωτερικό περιλαμβάνει 283 μονάδες σε τέσσερις ηπείρους.

Οι λογαριασμοί καταθέσεων που ξεπερνούν τα εννέα εκατομμύρια και οι άνω του εκατομμυρίου λογαριασμοί χορηγήσεων αποτελούν τη σημαντικότερη απόδειξη της εμπιστοσύνης του κοινού της που αποτελεί και τη κινητήρια δύναμη της τράπεζας.

Με επιβεβαιωμένη την ηγετική της θέση στη ελληνική τραπεζική αγορά και με στόχο τη πλήρη κάλυψη των πελατών της καθώς και την αύξηση της κερδοφορίας της, η τράπεζα μεριμνά για το διαρκή εκσυγχρονισμό των διαδικασιών της, επενδύοντας στη νέα τεχνολογία.

10.1.2. Το τμήμα Πληροφοριακών Συστημάτων

Το τμήμα Πληροφοριακών Συστημάτων της Εθνικής Τράπεζας απασχολεί περίπου 450 άτομα και ο διευθυντής Πληροφορικής αναφέρεται στο Γενικό Διευθυντή Οικονομικών και Λειτουργικής Στήριξης.

Η διεύθυνση Πληροφορικής αποτελείται από ξεχωριστές υποδιευθύνσεις, μία από τις οποίες ασχολείται με την Ασφάλεια των Πληροφοριακών Συστημάτων. Η Εθνική Τράπεζα δίνει μεγάλη σημασία στο ζήτημα της αξιοπιστίας και της ασφάλειας των Πληροφοριακών Συστημάτων της και για αυτό το λόγο υπάρχει και ξεχωριστή υποδιεύθυνση για την ασφάλεια. Στα καθήκοντα των εργαζομένων της υποδιεύθυνσης εκτός από τη γενικότερη φροντίδα, τα μετρά προστασίας κτλ περιλαμβάνεται και η συμμετοχή στην ανάπτυξη του νέου λογισμικού. Δηλαδή μετέχουν σε αυτό από κοινού ομάδες με τα τμήματα ανάπτυξης, ώστε εξαρχής να τοποθετούνται συγκεκριμένα πρότυπα ασφαλείας σε όλα τα προγράμματα.

Στα απαραίτητα προσόντα που πρέπει να έχουν οι εργαζόμενοι στην υποδιεύθυνση ασφάλειας περιλαμβάνονται οπωσδήποτε οι σπουδές σε ΑΕΙ με

κατεύθυνση πληροφορικής και κάποιος μεταπτυχιακός τίτλος καθώς και προϋπηρεσία 2-3 ετών. Γενικά οι εργαζόμενοι στην υποδιεύθυνση ασφάλειας μένουν σταθεροί στο τμήμα τους. Γεγονός λογικό, αν σκεφτούμε πώς ο τομέας της ασφάλειας είναι πολύ σημαντικός και πρέπει να υπάρχει εξειδίκευση.

Πέρα από την υποδιεύθυνση για την ασφάλεια των Πληροφοριακών Συστημάτων, στην Εθνική Τράπεζα υπάρχει και ένα ειδικό σώμα Επιθεώρησης Πληροφοριακών Συστημάτων, οι λεγόμενοι ««auditors». Πρόκειται για, περίπου 10 άτομα, τα οποία δρουν κατασταλτικά. Κάθε μέρα εξετάζουν συγκεκριμένα κόμματα των διαδικασιών και του κώδικα για να δουν αν λειτουργούν σωστά. Π.χ στις καταθέσεις γίνονται όλοι οι έλεγχοι που πρέπει; Οι ανατοκισμοί πραγματοποιούνται σωστά, στις σωστές ημερομηνίες;
Σχετικά με το κόστος της πολιτικής ασφαλείας, αυτό αποφασίζετε σε επίπεδο Διεύθυνσης Πληροφορικής. Δηλαδή αφού η ανώτερη διοίκηση κατανείμει τον προϋπολογισμό στις διάφορες διευθύνσεις. Ο διευθυντής του τομέα ζητάει, περίπου το Νοέμβριο ή το Δεκέμβριο κάθε έτους, από τις επιμέρους υποδιευθύνσεις ένα προϋπολογισμό του κόστους τους. Έπειτα αυτός αποφασίζει το ποσοστό του προϋπολογισμού της Διεύθυνσης που θα μοιραστεί σε κάθε υποδιεύθυνση.

10.1.3. Κεντρικό Σύστημα

Κάθε συναλλαγή που κάνει η Εθνική Τράπεζα με τον πελάτη, εγγράφεται σε τέσσερις servers. Το πρώτο mainframe αποτελεί ουσιαστικά το κύριο μηχάνημα το οποίο εκτελεί όλες τις λειτουργίες, ενώ το δεύτερο αντιγράφει σε ζωντανό χρόνο τα δεδομένα του δεύτερου.

Για την αποφυγή κάθε ατυχούς ενδεχομένου και για μεγαλύτερη ασφάλεια βρίσκονται σε άλλο χώρο και περιοχή οι άλλοι δύο εξυπηρετητές. Στην περίπτωση δηλαδή που όλο το κτίριο Μηχανογράφησης της Εθνικής Τράπεζας καταστραφεί ολοσχερώς (πυρκαγιά, σεισμός κλπ) και μαζί του και οι servers, μέσα σε λίγα μόνο λεπτά μπορούν να μπουν σε λειτουργία οι δύο back up servers και να εξυπηρετούν πλήρως τη λειτουργία της τράπεζας.

Το κεντρικό mainframe εξυπηρετεί περίπου 3.500 - 4.000 clients από τα καταστήματα (χωρίς να υπολογίζονται και οι χρήστες του e-banking ή από ATM) νούμερο που μας δείχνει το μέγεθος της κίνησης που υπάρχει καθημερινά. Κατανοούμε, δηλαδή, ότι μιλάμε για εκατομμύρια κινήσεις λογαριασμών καθημερινά, η καταγραφή των οποίων θα πρέπει, να είναι απόλυτα ασφαλής καν εξασφαλισμένη.

Σχετικά με το ζήτημα της ισορροπίας ανάμεσα στο κόστος και την ασφάλεια, οι τράπεζες ναι μεν βρίσκονται στη λογική της μείωσης του κόστους αλλά με τίποτα δε θυσιάζουν την ασφάλεια. Αντιθέτως, συνεχώς επενδύουν σε νέα συστήματα. Η συντήρηση του εξοπλισμού και η πολιτική ασφάλειας κοστίζει λιγότερο από τα κόστη που έχει ένα μόνο κατάστημα με το ανθρώπινο δυναμικό του. Οπότε, εάν θέλει η τράπεζα να μειώσει το κόστος, θα προτιμήσει να εξετάσει πώς μπορεί να γίνει η μείωση αυτή σε επίπεδο υποκαταστήματος, παρά σε επίπεδο Πληροφοριακών Συστημάτων.

10.1.4. Λογισμικό – Αναβαθμίσεις

Η Εθνική Τράπεζα θεωρεί πώς οι απειλές για την ασφάλεια αυξάνονται διαχρονικά και για αυτό κάθε νέο λογισμικό θα πρέπει να δίνει έμφαση σε αυτό το θέμα. Γενικά η Τράπεζα δε βιάζεται να υιοθετήσει νέα συστήματα λογισμικού μόλις κυκλοφορήσουν αυτά, αλλά περιμένει πρώτα να δοκιμαστούν μέσα από την ίδια την αγορά και έπειτα τα επιλέγει. Η Τράπεζα ωστόσο παρακολουθεί τις νέες τεχνολογίες. Κάθε 5 - 6 χρόνια είναι αναγκασμένη εκ των πραγμάτων να προχωρά σε σημαντικές αναβαθμίσεις του λογισμικού της για να μένει στην αγορά.

Η διαδικασία ανάπτυξης των νέων προγραμμάτων είναι κυρίως εσωτερική δηλαδή τα περισσότερα δημιουργούνται από τη διεύθυνση Πληροφορικής. Όλα τα νέα προγράμματα ελέγχονται πριν βγουν σε περιβάλλον «παραγωγής» από το σώμα των auditors. Επίσης, παράλληλα με τη διαδικασία ανάπτυξης, τα προγράμματα λειτουργούν σε test περιβάλλον, όπου δοκιμάζονται από την ομάδα ανάπτυξης. Τέλος πριν κυκλοφορήσουν στα υποκαταστήματα δοκιμάζονται και από μία ομάδα χρηστών.

10.1.5. Υποκαταστήματα

Τα υποκαταστήματα συνδέονται με το κέντρο μηχανογράφησης με μια μισθωμένη γραμμή η οποία παρέχει ταχύτητα και χαμηλό κόστος. Σε περίπτωση που για κάποιο λόγο η γραμμή αυτή παρουσιάσει κάποια δυσλειτουργία, υπάρχει πάντα μια εναλλακτική ίδια γραμμή έτοιμη προς χρήση.

Οι Η/Υ των καταστημάτων είναι απόλυτα προστατευμένοι από τους περισσότερους κινδύνους λογισμικού (όπως ιούς, hackers κλπ). Κάθε υπολογιστής κάνει χρήση του firewall της τράπεζας, ενώ έχει εγκατεστημένο και ειδικό antivirus πρόγραμμα. Όλες οι ανανεώσεις των προγραμμάτων και τα πακέτα ασφάλειας εγκαθίστανται αυτόματα σε κάθε υπολογιστή κεντρικά, από τη διεύθυνση Πληροφορικής.

Τέλος κάθε χρήστη ανάλογα με τη θέση του ανήκει σε διαφορετικό προφίλ χρήστη, έτσι ώστε να έχει πρόσβαση σε διαφορετικές εφαρμογές ανάλογα με την εργασία του. Ο κάθε χρήστης έχει το δικό του username και password και μπορεί να μπει στο σύστημα κάνοντας χρήση μόνο αυτών.

10.1.6. E – banking

Η Εθνική Τράπεζα, υποστηρίζει και λειτουργίες e-banking σε ευρύ φάσμα. Σε αυτές περιλαμβάνονται πληρωμές, διαχείριση λογαριασμών, αναλήψεις, καταθέσεις, εμβάσματα, επενδύσεις κλπ.

Η διαδικασία για να χρησιμοποιήσει ο πελάτης την υπηρεσία e-banking έχει ως εξής: Σε κάποιο από τα υποκαταστήματα της Εθνικής συμπληρώνει μία αίτηση και παραλαμβάνει από το κατάστημα ένα έντυπο που περιλαμβάνει το username και το password του. Η Τράπεζα παρέχει απόλυτη ασφάλεια στο χρήστη. Όπως γράφει χαρακτηριστικά στο δικτυακό της τόπο η ασφάλεια που παρέχει χαρακτηρίζεται από:

1) Τη μυστικότητα και το αναλλοίωτο των δεδομένων. Η Εθνική Τράπεζα, για την ασφαλή λειτουργία του internet banking, χρησιμοποιεί κρυπτογράφηση 128 bit

των διακινουμένων στοιχείων, μέσω του πρωτοκόλλου SSL, το οποίο θεωρείται απαραβίαστο για τις εφαρμογές στο Διαδίκτυο. Το σύστημα αυτό, εκτός της κρυπτογράφησης που πραγματοποιεί, ελέγχει συνεχώς την αυθεντικότητα της επικοινωνίας μεταξύ του PC και του κεντρικού συστήματος. Σε οποιαδήποτε διαταραχή ή παρεμβολή στην επικοινωνία, η συναλλαγή διακόπτεται άμεσα και η επικοινωνία με το κεντρικό σύστημα της Τράπεζας πρέπει να αποκατασταθεί απο την αρχή (αναγνώριση χρήστη, κλπ.).

2) Αυθεντικότητα Χρήστη. Η εφαρμογή internet banking «αναγνωρίζει» τους χρήστες και επιτρέπει, την πρόσβαση τους στο Σύστημα, με τον Κωδικό – UserID και το Μυστικό - Password. Σε περίπτωση εισαγωγής διαδοχών λανθασμένων κωδικών ο χρήστης απενεργοποιείται, ο μυστικός αχρηστεύεται και πρέπει να εκδοθεί νέος μυστικός.

3) Αυθεντικότητα της Τράπεζας. Η Εθνική Τράπεζα έχει προμηθευτεί πιστοποιητικό αυθεντικότητας παρουσίας της στο Διαδίκτυο. Το πιστοποιητικό εμφανίζεται στον χρήστη κάθε φορά που επισκέπτεται την ιστοσελίδα εισόδου του συστήματος και είναι διαθέσιμο, μέσω του κατάλληλου εικονιδίου (κλειδαριά στο κάτω τμήμα της οθόνης), όσο ο χρήστης χρησιμοποιεί την εφαρμογή. Εκτός αυτών, κατά την είσοδο στην ιστοσελίδα με τους κωδικούς, εμφανίζεται και άλλο πιστοποιητικό το οποίο πιστοποιεί ότι τα προγράμματα που μεταφέρονται στο σταθμό του χρήστη είναι τα γνήσια που έχουν εκπονηθεί από την Εθνική Τράπεζα.

Οι πελάτες των Ελληνικών Τραπεζών δεν έχουν πειστεί ακόμη για την ασφάλεια των ηλεκτρονικών συναλλαγών και για αυτό δεν αξιοποιούν ιδιαίτερα τις δυνατότητες του e-banking. Οι τράπεζες από τη μεριά τους προσπαθούν να ενθαρρύνουν το κοινό προς το e-banking γιατί τις συμφέρει λόγω μειωμένου κόστους. Η Εθνική Τράπεζα χρησιμοποιεί διαφημίσεις τόσο στην τηλεόραση και σε άλλα μέσα, όσο μέσα στα καταστήματα της. Επίσης δίνει και οικονομικά οφέλη στους χρήστες του e-banking. Για παράδειγμα, μία συναλλαγή που στο γκισέ χρεώνεται 0,60 € μέσα το e-banking δε χρεώνεται καθόλου.

10.2. Eurobank

10.2.1. Γενικά στοιχεία

Η Τράπεζα Eurobank ιδρύθηκε τα 1990 με αρχική επωνυμία "Ευρωεπενδυτική Τράπεζα". Σήμερα, προσφέρει πλήρες φάσμα τραπεζικών προϊόντων και υπηρεσιών σε ιδιώτες, επιχειρήσεις και θεσμικούς πελάτες. Η Τράπεζα καταλαμβάνει ηγετική θέση στους ταχύτερα αναπτυσσόμενους και πιο προσοδοφόρους τομείς της αγοράς. Επιπλέον, ο Όμιλος κατέχει ηγετική θέση στην επενδυτική τραπεζική, και στα προϊόντα κεφαλαιαγοράς, ενώ διαθέτει ισχυρό συγκριτικό πλεονέκτημα στο χώρο της διαχείρισης περιουσίας ιδιωτών και σημαντική παρουσία στην τραπεζική επιχειρήσεων. Η Τράπεζα επιτυγχάνει τη διάθεση των προϊόντων και των υπηρεσιών της πανελλαδικά διαθέτοντας εγχώριο δίκτυο άνω των 300 καταστημάτων και 700 ATM και με την αξιοποίηση εναλλακτικών δικτύων.

10.2.2. Το τμήμα Πληροφοριακών Συστημάτων

Το τμήμα Πληροφοριακών Συστημάτων της Eurobank αποτελεί ξεχωριστή Διεύθυνση με τίτλο «Διεύθυνση Εργασιών, Τεχνολογίας και Οργάνωσης», η οποία αναφέρεται κατευθείαν στο Διευθύνοντα Σύμβουλο. Η Διεύθυνση Εργασιών, Τεχνολογίας και Οργάνωσης αποτελείται από ξεχωριστές υποδιευθύνσεις και ομάδες, μία ομάδα από τις οποίες ασχολείται αποκλειστικά με την ασφάλεια των Πληροφοριακών Συστημάτων. Η ομάδα αυτή δρα τόσο σε προληπτικό επίπεδο (πχ ποιες θα είναι οι προδιαγραφές των νέων προγραμμάτων, ώστε αυτά να είναι ασφαλή), όσο και σε κατασταλτικό, ελέγχοντας τμήματα των υπαρχόντων εφαρμογών για κενά ασφαλείας.

10.2.3. Κεντρικό Σύστημα

Κάθε συναλλαγή που πραγματοποιείται στη Eurobank εγγράφεται σε δύο κεντρικούς server. Ο ένας εξ αυτών βρίσκεται στο κεντρικό κτίριο της Τράπεζας, ενώ ο άλλος είναι εγκατεστημένος σε άλλη απομακρυσμένη τοποθεσία, για λόγους ασφαλείας. Κάθε συναλλαγή που εγγράφεται στον πρώτο server σε ζωντανό χρόνο εγγράφεται και στο δεύτερο, με χρήση της τεχνικής replication, ώστε και το δεύτερο σύστημα να είναι ενημερωμένο πάντα με όλα τα δεδομένα. Η Eurobank έχει αναπτύξει και disaster scenarios τα οποία προβλέπουν τις ανάλογες αντιδράσεις σε κάθε δυσάρεστο περιστατικό. Επίσης τακτικά γίνονται έλεγχοι, όλου του συστήματος για την ασφάλειά του.

10.2.4. Λογισμικό — Αναβαθμίσεις

Η Eurobank πιστεύει πως διαχρονικά οι απειλές για την ασφάλεια αυξάνονται και πώς παράλληλα και τα νέα προγράμματα γίνονται πιο ασφαλή, αλλά και οι επίδοξοι εισβολείς γίνονται εξυπνότεροι. Αυτό έχει σαν αποτέλεσμα να μη μπορεί να θεωρηθεί ότι με τη χρήση των νέων προγραμμάτων η ασφάλεια γίνεται ευκολότερη υπόθεση. Η Τράπεζα παρακολουθεί τις νέες τεχνολογίες, υποχρεωμένη εκ των πραγμάτων, καθώς οι παλιότερες τεχνολογίες έχουν την τάση να απαξιώνονται γρήγορα.

Τα νέα προγράμματα είτε αναπτύσσονται εσωτερικά, είτε αγοράζονται έτοιμα, ανάλογα με το βαθμό τεχνογνωσίας που απαιτούν και τη σπουδαιότητα τους. Πάντα πριν εγκατασταθούν και ξεκινήσει η χρήση τους δοκιμάζομαι εκτενώς από το τμήμα Πληροφοριακών Συστημάτων και από επιλεγμένους χρήστες.

10.2.5. Υποκαταστήματα

Όσον αφορά την τηλεπικοινωνιακή υποδομή του καταστήματος υπάρχει μια μισθωμένη γραμμή, η οποία συνδέει το υποκατάστημα με το κέντρο μηχανογράφησης. Σε περίπτωση που για κάποιο λόγο η γραμμή αυτή παρουσιάσει κάποια δυσλειτουργία, υπάρχει πάντα ανάλογα και με την περιοχή του

υποκαταστήματος ή ίδια εναλλακτική γραμμή ή απλή τηλεφωνική γραμμή τύπου ISDN έτοιμη προς χρήση.

Οι Η/Υ των καταστημάτων είναι απόλυτα προστατευμένοι από τους περισσότερους κινδύνους (όπως ιούς, hackers κλπ). Κάθε υπολογιστής κάνει χρήση του firewall της τράπεζας, ενώ έχει εγκατεστημένο και ειδικό antivirus πρόγραμμα. Όλες οι ανανεώσεις των προγραμμάτων και τα πακέτα ασφαλείας εγκαθίστανται αυτόματα σε κάθε υπολογιστή κεντρικά, από τη διεύθυνση Πληροφορικής.

10.2.6. E – banking

Η Eurobank προσφέρει ευρύ πεδίο τραπεζικών υπηρεσιών μέσω του e-banking ώστε να εξυπηρετούνται οι πελάτες της. Για να μπορέσει κάποιος να κάνει χρήση του e-banking της Eurobank, δεν έχει παρά να απευθυνθεί σε οποιοδήποτε υποκατάστημα της Τράπεζας και να συμπληρώσει σχετική αίτηση.

Η Τράπεζα παρέχει απόλυτη ασφάλεια στο χρήστη και αποτελεί πρώτη προτεραιότητά της. Σύμφωνα με το δικτυακό της τόπος, μεταξύ άλλων παρέχει :

* Ταυτοποίηση Τράπεζας
* Εισαγωγή Στοιχείων Εισόδου.
* Ταυτοποίηση Χρήστη. Για την ταυτοποίηση των χρηστών e-banking, η Eurobank χρησιμοποιεί έναν προσωπικό κωδικό εισόδου (password) μοναδικό για κάθε χρήστη της υπηρεσίας σε συνδυασμό με τον 16ψήφιο αριθμό μιας οποιασδήποτε κάρτας Eurobank του χρήστη. Ο συνδυασμός αυτών των δύο επιτρέπει στον χρήστη την πρόσβαση στους λογαριασμούς του. Για τη διενέργεια όμως χρηματικών συναλλαγών, η τράπεζα δεν αρκείται σε αυτό το επίπεδο ταυτοποίησης του χρήστη αλλά απαιτεί μια επιπλέον δικλείδα ασφαλείας, την ψηφιακή πιστοποίηση.

Το ψηφιακό πιστοποιητικό αποτελεί το μέσο που παρέχει τη δυνατότητα στο κάτοχό του να υπογράφει ψηφιακά όλες τις ηλεκτρονικές συναλλαγές που εκτελεί μέσα από το e-banking. Το πιστοποιητικό, όταν εγκατασταθεί σε κάποιον υπολογιστή, προσφέρει τη δυνατότητα ταυτοποίησης του χρήστη και επιτρέπει

συναλλαγές και μεταφορές χρημάτων μεταξύ λογαριασμών μόνο από το συγκεκριμένο χρήστη.

* Εξασφάλιση της μεταφοράς δεδομένων. Μια επιπρόσθετη δικλείδα ασφαλείας, με την οποία εξασφαλίζεται το απόρρητο κατά τη μεταφορά των δεδομένων, είναι η κρυπτογράφησή τους. Η Eurobank χρησιμοποιεί το πρωτόκολλο επικοινωνίας SSL μαζί με τη κρυπτογράφηση στα 128bit το οποίο εξασφαλίζει την ασφάλεια των συναλλαγών μέσω διαδικτύου
* Ελεγχόμενη πρόσβαση στα συστήματα της Τράπεζας.
* Αυτόματη αποσύνδεση χρήστη.
* Μπλοκάρισμα κωδικών.

ΕΠΙΛΟΓΟΣ

Στα πλαίσια της παρούσας εργασίας προσπαθήσαμε να διερευνήσουμε τις πολιτικές ασφαλείας των πληροφοριακών συστημάτων, τη κρυπτογραφία που ακολουθούν οι τράπεζες καθώς και το κλειδί DES. Ελπίζουμε να καταφέραμε, χωρίς περιττές τεχνικές λεπτομέρειες, να παρουσιάσαμε με τρόπο αντιληπτό στον αναγνώστη, το ρόλο των πολιτικών ασφαλείας, την αξίας τους, τις κρυπτογραφικές μεθόδους και τον τρόπο λειτουργίας τους.

Συγκεκριμένα έγινε εκτενείς ανάλυση στην έννοια της Κρυπτογραφίας. Η Κρυπτογραφία και η Κρυπτανάλυση ασχολούνται με τη μελέτη, την ανάλυση, την ανάπτυξη και την επαλήθευση κρυπτογραφικών μεθόδων, τεχνικών συστημάτων και πρωτοκόλλων. Οι εφαρμογές της Κρυπτογραφίας αποτελούν το βασικό τεχνολογικό υπόβαθρο σε περιβάλλον δικτύων υπολογιστών για την υλοποίηση μέτρων αντιμετώπισης απειλών (όπως της υποκλοπής δεδομένων, της τροποποίησης δεδομένων, της παράνομης αναπαραγωγής ψηφιακών εγγράφων, της παραβίασης της ιδιωτικότητας κλπ.) στο αναπτυσσόμενο περιβάλλον της Κοινωνίας της Πληροφορίας.

Συμπερασματικά θα μπορούσαμε να πούμε ότι για πολλά χρόνια ακόμη η κρυπτογραφία θα μας παρέχει ασφάλεια σε όλα τα πεδία εφαρμογών. Αυτό που έχει σημασία είναι να υπάρξει εναρμόνιση των νομικών πλαισίων λόγω του προφανούς διεθνούς χαρακτήρα των ηλεκτρονικών συναλλαγών.

Η σωστή ανάπτυξη και η αποδοτική λειτουργία πληροφοριακών συστημάτων είναι μια διαδικασία, που εμπεριέχει αναπόσπαστα τη ταυτόχρονη δόμηση ενός πλαισίου ασφάλειας, το οποίο να εξασφαλίζει τις απαιτήσεις ορθότητας, διαθεσιμότητας και μυστικότητας των περιεχομένων πληροφοριών.

Στο πεδίο της αναφοράς μας στον ελληνικό τραπεζικό χώρο θα λέγαμε ότι οι ελληνικές τράπεζες έχουν κατανοήσει την αξία και την ευαισθησία των δεδομένων τους και ακολουθούν κατά κύριο λόγο συγκροτημένες και αποτελεσματικές πολιτικές ασφαλείας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. *Γκριτζάλης Δημ. « Ασφάλεια Πληροφοριακών συστημάτων», Αθήνα 1989*

2. *Επιστημονική Συλλογή, « Ασφάλεια Πληροφοριακών συστημάτων», Εκδ. Νέων Τεχνολογιών, 2004*

3. *Κουντούζης ευάγγελος, « Ασφάλεια Πληροφοριακών συστημάτων», Εκδ. Μπένου*

4. *« Γεωργόπουλος Ν.Πανταζή Μ, Νικολαράκος Χ, Βαγγελάτος Ι, Ηλεκτρονικό Επιχειρείν : προγραμματισμός και σχεδίαση, Εκδ. Ε. Μπένου, Αθήνα 2001*

5. *Νάστου Ε. Παναγιώτης, Σπυράκης Γ. Παύλος, Σταματίου Κ. Γιάννης, «Σύγχρονη κρυπτογραφία», Εκδ. Ελληνικά Γράμματα, Αθήνα 2003*

6. *Β.Α. Κάτος - Γ.Χ. Στεφανίδης, Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης, ΖΥΓΟΣ, 396, 2003*

7. *Alsaid, Adil- Mitchell J. Chris, 2005, «Dynamic content attacks on digital signatures», Information Management & Computer Security, vol. 13, p. 328-336*

8. *Broderick, Martha A.- Gibson, Virginia R.- Tarasewich, Peter, 2001, «Electronic signatures: they' re legal, now what?»Internet Research, vol. 11, p. 423-434*

9. *Hassler, Vesna-Biely, Helmut, 1999, «Digital signature management», Internet Research, vol. 9, p. 262-271*

10. *Wilson, Stephen, 1999, «Digital signatures and the future of documentation», Information Management & Computer Security, vol. 7, p. 83-87*

11. *Finne Thomas, A conceptual Framework for Information Security, Management, Computers and Security, vol.17, 1998*

12. *Bruce Schneier, Applied Cryptography, 2nd edition, Wiley, 758, 1996 δείγματα του βιβλίου. Το κρυπτόγραμμα του Bruce Schneier στα ελληνικά.*

13. *Simon Singh, Κώδικες και Μυστικά, Τραυλός, 606, 2001,*

ΔΙΑΔΙΚΤΥΟ

1. *www.securityfocus.com/infocus/1775*
2. *www.semper.org/sirene/outsideworld/ecommerce.html*
3. *Autodesk, 2006, «An Introduction to Digital Signatures», http://images.autodesk.com/adsk/files/877487_Extnsns_WP_introdigsig.pdf*
4. *Curry, Ian, 2001, « An Introduction to Cryptography and Digital Signatures» http://www.entrust.com/resources/pdf/cryptointro.pdf*
5. *Cypher Research Laboratories, «A brief history of cryptography» http://www.cypher.com.au/crypto_history.htm*
6. *Fundamental Security Concepts «Public key cryptography», http://gdp.globus.org/gt4-tutorial/multiplehtml/ch09s03.html*
7. *Ius mentis, 2005, «Crash course on cryptography: Digital signatures» http:/www.iusmentis.com/technology/encryption/crashcourse/digitalsignaturs*
8. *Kessler Gary C., 1998, «An overview of Cryptography», http://www.garykessler.net/library/crypto.html#skc*
9. *Magalhaes, Ricky M., 2004, «Digital Signatures», http://www.windowsecurity.com/articles/Digital_Signatures.html*
10. *The Official Website of the State of Utah, Utah Department of Commerce, «Digital Signature Tutorial», http://www.commerce.state.ut.us/digsig/tutorl.htm*
11. *Shaw, Sandy, Computing Services, The University of Edinburgh, JISC Technology Applications Programme (JTAP) — «Overview of Watermarks, Fingerprints, and Digital Signatures» http://www.jisc.ac.uk/uploaded_documents/jtap-034.doc*
12. *Verisign, 2006, «Introduction to Public Key Cryptography» http://www.verisign.com.au/repository/tutorial/cryptography/intro1.shtml*
13. *Wikipedia, The Free Encyclopedia, «Electronic signature»*

http://en.wikipedia.org/wiki/Electronic_signature

14. *Youd, David, 1996, «What is a Digital Signature?» http://www.youdzone.com/signature.html*

15. *Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων «Εισαγωγή στις ηλεκτρονικές υπογραφές» http://www.eett.gr/gr_pages/telec/eSign/IntroEsign.htm*

16. *Ε-επιχειρείν, 2003, «Η ηλεκτρονική υπογραφή στις online συναλλαγές» http://www.eone.gr/4dcgi/_w_articles_technoextrat_2_28/01/2006_83439*

17. *Ε-επιχειρείν, «Η υποδομή δημοσίου κλειδιού και η κρυπτογράφηση στην πράξη», http://www.go-online.gr/ebusiness/specials/article.html?article_id=714*

18. *Ε-επιχειρείν, «Ηλεκτρονική υπογραφή:Το νομικό πλαίσιο στην Ελλάδα», http://www.go-online.gr/ebusiness/specials/article.html?article_id=931*

19. *Κέντρο ΠΛΗ.ΝΕ.Τ Ν. Φλώρινας, «Κρυπτογραφία και ψηφιακή υπογραφή», http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Cryptography-DigitalSignature.html*

20. *Υπουργείο Ανάπτυξης, Ε.Π. Κοινωνία της Πληροφορίας, EBusinessForum,2006, «Ηλεκτρονικές Υπογραφές και Ηλεκτρονικά Πιστοποιητικά Ταυτοποίησης (Τεχνική & Νομική προσέγγιση)», http://www.ebusinessforum.gr/index.php?op=modload&modname=Teams&action=teamsviewnewall&pageid=32*

21. *Χαριστός, Θάνος Ι. , 2002, «Ηλεκτρονική υπογραφή», Lawnet http://www.lawnet.gr/case_study.asp?PageLabel=3&MeletID=98*

22. *Δικτυακός τόπος Εθνικής Τράπεζας,*

23. *Δικτυακός τόπος Eurobank*

ΕΥΡΕΤΗΡΙΟ ΣΧΗΜΑΤΩΝ

ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ

ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ