Η Ορολογία (Γλωσσάριο) της Κρυπτογραφίας

(AES) Advanced Encryption Standard - Το Advanced Encryption Standard, δηλ. το *Προηγμένο Πρότυπο Κρυπτογράφησης*, θα αποτελεί τον νέο στάνταρτ αλγόριθμο κρυπτογράφησης για χρήση από τις κυβερνητικές υπηρεσίες των ΗΠΑ. Επιλέχθηκε ο αλγόριθμος Rijndael από μια ομάδα υποψηφίων αλγορίθμων. Στοχεύεινα γίνει ο διάδοχος του DES και οι νεώτερες εκδόσεις των PGP και GPG περιλαμβάνουν υποστήριξη για το AES.

Algorithm - Αναφέρεται στον αλγόριθμο κρυπτογράφησης, που είναι μια μαθηματική διαδικασία (μέθοδος) κρυπτογράφησης (κωδικοποίησης) και αποκρυπτογράφησης (αποκωδικοποίησης) μηνυμάτων και κειμένων, τα οποία μετατρέπονται σε μια μη αναγνώσιμη μορφή.

Asymmetric Encryption - Αποδίδεται στα ελληνικά ως *Ασύμμετρη Κρυπτογράφηση* και είναι ένα σύγχρονο σύστημα κρυπτογράφησης, το οποίο με τη χρήση δύο κλειδιών (δημόσιο και ιδιωτικό) επιτυγχάνει σχεδόν απόλυτη προστασία των ευαίσθητων (απόρρητων) πληροφοριών (δεδομένων).

Authentication - Αποδίδεται στα ελληνικά με τον όρο *Ταυτοποίηση* ή *Πιστοποίηση* και είναι η διαδικασία ή μέθοδος επιβεβαίωσης (εξακρίβωσης) με τη χρήση ψηφιακών ταυτοτήτων ή πιστοποιητικών της ταυτότητας

ενός ατόμου ώστε να έχει δικαίωμα για πρόσβαση σε διάφορα συστήματα. Στην ουσία αυτό που ζητάμε να μάθουμε είναι αν το άτομο ή η εταιρεία που ζητάει μια συναλλαγή είναι όντως αυτός ή αυτή που ισχυρίζεται ότι είναι. Ο ίδιος όρος αναφέρεται και στη διαδικασία επαλήθευσης ότι κάποιο αρχείο ή μήνυμα δεν έχει υποστεί κάποια τροποποίηση κατά τη μεταφορά του από τον αποστολέα ως τον παραλήπτη και ότι έχει παραληφθεί ακέραιο.

Authorization - Αποδίδεται στα ελληνικά με τον όρο *Εξουσιοδότηση* και είναι η διαδικασία σύμφωνα με την οποία γίνεται ο απαραίτητος έλεγχος από την τράπεζα του πελάτη (πληρωτή) ως προς το υπόλοιπο του λογαριασμού του, έτσι ώστε να εγκριθεί η εισαγωγή του σ' ένα δίκτυο και να δοθεί η σχετική εντολή πληρωμής στην τράπεζα του αποδέκτη. Το authorization επιτρέπει σ' έναν χρήστη την πρόσβαση σε περιοχές ή στο σύνολο ενός δικτύου βάσει της ταυτότητάς του.

Back Door - Αποδίδεται στα ελληνικά με τον όρο *Πίσω Πόρτα* ή και *Κερκόπορτα* και αναφέρεται σε ορισμένες αδυναμίες των λειτουργικών συστημάτων των υπολογιστών, τις οποίες μπορούν να εκμεταλλευτούν κάποιο επίδοξοι hackers ή crackers και να προκαλέσουν ζημιά ή απλά να καταγράφουν (παρακολουθούν) τις κινήσεις και τις επιλογές μας στο Internet ή και να υποκλέπτουν μυστικούς κωδικούς εν αγνοία μας.

Certification Authority (CA/TTP) - Αποδίδεται στα ελληνικά μ' έναν από τους όρους *Οργανισμός Πιστοποίησης* ή *Έμπιστη Τρίτη Οντότητα* ή και *Πάροχος Υπηρεσιών Πιστοποίησης* και αναφέρεται στους Οργανισμούς ή Εταιρείες που έχουν το δικαίωμα (άδεια) να εκδίδουν ψηφιακές ταυτότητες και να εγγυώνται μ' αυτόν τον τρόπο τη διασφάλιση (απόρρητο) των επικοινωνιών.

Chosen Plain Text Attack - Αποτελεί το επόμενο βήμα από την ***Known Plain Text Attack***, όπου ο κρυπταναλυτής (cryptanalyst) μπορεί να επιλέξει ποιο μήνυμα plain text επιθυμεί να κρυπτογραφήσει και να δει το αποτέλεσμα, σ' αντίθεση από το πάρει απλά ένα παλιό plain text. Αν μπορέσει να ανακτήσει το κλειδί, μπορεί να το χρησιμοποιήσει για να αποκωδικοποιήσει όλα τα δεδομένα που είναι κρυπτογραφημένα κάτω απ' αυτό το κλειδί. Είναι μια πολύ πιο δυνατή μορφή επίθεσης σε σχέση με την known plain text. Τα καλύτερα συστήματα κρυπτογράφησης μπορούν να αντισταθούν σ' αυτή τη μορφή επίθεσης.

Cipher - Όρος που αναφέρεται στην κρυπτογράφηση (κωδικοποίηση) μηνυμάτων. Εϊναι συνώνυμος με τους όρους ***Encryption*** και ***Encode***.

CipherText - Αποδίδεται στα ελληνικά με τον όρο ***Κρυπτογράφημα*** και είναι το κρυπτογραφημένο (κωδικοποιημένο) αρχείο, κείμενο ή μήνυμα που στέλνει ο αποστολέας στον παραλήπτη. Το αρχικό (αυθεντικό), δηλ. το μη κρυπτογραφημένο μήνυμα, αποκαλείται ***PlainText***.

Code - Αποδίδεται στα ελληνικά με τον όρο ***Κώδικας*** και αναφέρεται στη χρήση χαρακτήρων ή λέξεων για την αναπαράσταση άλλων λέξεων ή προτάσεων. Κλασικό παράδειγμα αποτελεί ο Κώδικας Morse, όπου με τον κατάλληλο συνδυασμό από τελείες και πάυλες μπορούμε να παραστήσουμε όλα τα γραμματα και τα ψηφία αλλά και μερικές τυποποιημένες προτάσεις.

Cracker - Χρήστης ο οποίος εισβάλει σε σύστημα στο οποίο δεν έχει νόμιμη πρόσβαση, με σκοπό να παραποιήσει ή ακόμη και να καταστρέψει δεδομένα και πληροφορίες ή και να δημιουργήσει παράνομα αντίγραφα νόμιμων προγραμμάτων.

Cryptography - Αποδίδεται στα ελληνικά με τον όρο ***Κρυπτογραφία*** και είναι η προστασία των ευαίσθητων

(απόρρητων) πληροφοριών (δεδομένων) με την μετατροπή τους από την απλή μορφή κειμένου, που αποκαλείται plain text, σε μια μη αναγνώσιμη μορφή, που αποκαλείται cipher text. Το κρυπτογραφημένο μήνυμα μπορεί να αποκρυπτογραφηθεί (decrypted) μόνο από τον κάτοχο ενός απόρρητου αλγορίθμου (encryption algorithm), που αποκαλείται κλειδί ή κλείδα (key).

Cryptoanalysis - Αποδίδεται στα ελληνικά με τον όρο *Κρυπτανάλυση* και αναφέρεται στην τέχνη της παραβίασης, δηλ. της αποκρυπτογράφησης, των κρυπτοσυστημάτων. Μπορεί να αναφέρεται επίσης και στην εύρεση λαθών ή και ελλείψεων κατά την εφαρμογή ενός αλγορίθμου κρυπτογράφησης.

Cryptology - Αποδίδεται στα ελληνικά με τον όρο *Κρυπτολογία* και αναφέρεται στη μελέτη (έρευνα) της κρυπτογραφίας και της κρυπτανάλυσης.

Cryptosystem - Αποδίδεται στα ελληνικά με τον όρο *Σύστημα Κρύπτο* και αναφέρεται στην όλη διαδικασία χρησιμοποίησης της κρυπτογραφίας, δηλ. στις μεθόδους κρυπτογράφησης και αποκρυπτογράφησης καθώς και στις μεθόδους διαπίστωσης της ταυτότητας του αποστολέα ενός μηνύματος.

Data Enrcyption - Αποδίδεται στα ελληνικά με τον όρο *Κρυπτογράφηση Δεδομένων* και αναφέρεται στη χρήση μαθηματικών εργαλείων για την καθιέρωση της εμπιστοσύνης ανάμεσα στον αποστολέα και τον παραλήπτη (αποδέκτη) ενός μηνύματος. Η κύρια χρήση της κρυπτογραφίας είναι αυτή της κωδικοποίησης της πληροφορίας με τέτοιο τρόπο ώστε η αποκωδικοποίηση της να είναι δυνατή μόνο από τον τελικό αποδέκτη του μηνύματος. Για να γίνει αυτό ο τελικός αποδέκτης του μηνύματος αναγνωρίζεται από ένα ειδικό identifier, ευρύτερα γνωστό ως κλειδί αποκωδικοποίησης. Οι δύο σημαντικότερες μορφές (μέθοδοι) κρυπτογράφησης

δεδομένων είναι η *Συμμετρική Κρυπτογράφηση* και η *Κρυπτογράφηση Δημόσιου Κλειδιού*, στην οποία ο κάθε χρήστης έχει τη δυνατότητα να δημιουργήσει ένα ζεύγος κλειδιών, δηλ. ένα γνωστό ή δημόσιο κλειδί (public key) και ένα κρυφό κλειδί (secret key) ή ιδιωτικό κλειδί (private key). Το δημόσιο κλειδί μπροεί να το δημοσιοποιήσει (κοινοποιήσει) σ' όλον τον κόσμο. Στη συμμετρική κρυπτογραφία, υπάρχει μόνο ένα κλειδί το οποίο χρησιμοποιείται τόσο για την κωδικοποίηση όσο και για αποκωδικοποίηση του μηνύματος, το οποίο κλειδί πρέπει να παραμένει κρυφό σ' όλους εκτός από τον αποστολέα και τον αποδέκτη του μηνύματος, πράγμα βέβαια δύσκολο σήμερα με τις εκπληκτικές δυνατότητες των hackers και των crackers. Η κρυπτογραφία με χρήση δημόσιου κλειδιού χρησιμοποιεί ένα πιο ευέλικτο και πιο ασφαλή σχήμα πιστοποίησης για την αποκωδικοποίηση των δεδομένων και ως εκ τούτου έχει επικρατήσει (με δημοφιλέστερες μορφές δεδομένων το PKI και το PGP).

Decryption - Αποδίδεται στα ελληνικά με τον όρο *Αποκρυπτογράφηση* και είναι η μέθοδος (διαδικασία) επαναφοράς ενός μηνύματος, που έχει κρυπτογραφηθεί σε μη αναγνώσιμη μορφή (cipher text), στην κανονική ή αρχική του του μορφή (plain text). Η αποκρυπτογράφηση μπορεί να γίνει μ' ένα απόρρητο ή μ' ένα δημόσιο (public key) ή και μ' έναν κωδικό πρόσβασης (password).

Data Encryption Standard (DES) - Αποδίδεται στα ελληνικά με τον όρο *Πρότυπο Κρυπτογράφησης Πληροφοριών* και είναι ένας είδος κρυπτογράφησης που δημιουργήθηκε από την κυβέρνηση των ΗΠΑ τη δεκαετία του 1970 ως ο επίσημος αλγόριθμος κρυπτογράφησης σε χρήση στις ΗΠΑ. Αναπτύχθηκε από την IBM υπό την αιγίδα της κυβέρνησης των ΗΠΑ. Αναπτύχθηκαν ανησυχίες ότι ίσως υπάρχουν κρυμμένες παγίδες στη λογική του αλγορίθμου που θα επέτρεπαν στην κυβέρνηση να σπάσει τον κωδικό μιας οποιασδήποτε επικοινωνίας. Το DES χρησιμοποιεί ένα κλειδί των 56 bit για να κάνει μια σειρά

από μη γραμμικούς μετασχηματισμούς σ' έναν μπλοκ δεδομένων των 64 bit. Όμως, σήμερα με την ολοένα αυξανόμενη ταχύτητα του hardware και το χαμηλό του κόστος, είναι εφικτό να κατασκευασθεί ένα μηχάνημα που αν μπορεί να σπάισε ένα κλειδί των 56 bit σε μία μόνο ημέρα. Γι' αυτόν τον λόγο, έχει αναπτυχθεί το τριπλό-DES ή *3DES*, το οποίο χρησιμοποιεί το απλό-DES για να κρυπτογραφήσει τα δεδομένα, μετά τα αποκρυπτογραφεί μ' ένα άλλο κλειδί και κρυπτογραφεί ξανά το αποτέλεσμα μ' ένα άλλο κλειδί. Η κρυπτογράφηση που επιτυγχάνεται μ' αυτόν τον τρόπο είναι ισοδύναμη μ' ένα υποθετικό 112-bit DES.

Digital ID/Certificate - Αποδίδεται στα ελληνικά με τον όρο *Ψηφιακή Ταυτότητα* ή *Ψηφιακή Βεβαίωση* ή και *Ψηφιακό Πιστοποιητικό* και πρόκειται για μια κρυπτογραφημένη ταυτότητα που την εκδίδουν ειδικά εξουσιοδοτημένοι Οργανισμοί Παροχής Υπηρεσιών Πιστοποίησης, με την οποία επιβεβαιώνεται η γνησιότητα των στοιχείων του κατόχου, το ότι αυτός που στέλνει το μήνυμα είναι όντως αυτός που ισχυρίζεται ότι είναι και ότι δεν γίνεται ηλεκτρονική απάτη ή πλαστοπροσωπία. Μπορεί να την χρησιμοποιήσει ο κάτοχός της για να κάνει ασφαλείς ηλεκτρονικές συναλλαγές και επικοινωνία μέσω του Internet. Η ψηφιακή ταυτότητα περιλαμβάνει την ψηφιακή υπογραφή του κατόχου της (digital signature) και το δημόσιο κλειδί του (public key). Το πρότυπο που χρησιμοποιείται κυρίως στα ψηφιακά πιστοποιητικά είναι το X.509.

Digital Signature - Αποδίδεται στα ελληνικά με τον όρο *Ψηφιακή Υπογραφή* και πρόκειται για ειδικό αρχείο το οποίο δημιουργείται από κείμενο που το υπογράφει και το κρυπτογραφεί (κωδικοποιεί) ο κάτοχός του. Ο παραλήπτης του μηνύματος θα πρέπει να κάνει αποκρυπτογράφηση του κειμένου, σύγκριση της ψηφιακής υπογραφής και πιστοποίηση (επιβεβαίωση) της ταυτότητας του αποστολέα του μηνύματος. Με την ψηφιακή υπογραφή μπορεί να γίνει

η ηλεκτρονική πιστοποίηση (επιβεβαίωση) στοιχείων, όπως είναι η ταυτότητα ενός χρήστη, η ικανότητα πληρωμής ή και η γνησιότητα ενός ηλεκτρονικού εγγράφου.

Encryption - Αποδίδεται στα ελληνικά με τον όρο *Κρυπτογράφηση* και είναι η μέθοδος (διαδικασία) μετατροπής κάποιων πληροφοριών (δεδομένων) σε απόρρητο (μη αναγνώσιμο) κώδικα, που είναι γνωστό και ως κρυπτογράφημα (cipher text). Αποτελεί την αποτελεσματικότερη μέθοδο για την επίτευξη της ασφάλειας στις επικοινωνίες. Για την ανάγνωση ενός κρυπτογραφημένου αρχείου είναι απαραίτητη η κατοχή του απόρρητου (ιδιωτικού) κλειδιού ή του κωδικού πρόσβασης, με τα οποία μπορεί να γίνει η αποκρυπτογράφηση των δεδομένων. Τα μη κρυπτογραφημένα δεδομένα ονομάζονται plain text, ενώ τα κρυπτογραφημένα δεδομένα ονομάζονται cipher text. Υπάρχουν δύο είδη κρυπτογράφησης : η *Ασύμμετρη Κρυπτογράφηση*, που είναι γνωστή και ως *Κρυπτογράφηση Δημόσιου Κλειδιού* και η *Συμμετρική Κρυπτογράφηση*.

Encryption Algorithm - Είναι ένας αλγόριθμος (μαθηματική μέθοδος) κρυπτογράφησης δεδομένων, με τη βοήθεια του οποίου μπορούμε να μετατρέψουμε κανονικό κείμενο (πληροφορία) σε μη αναγνώσιμη μορφή (cipher text). Για την επαναφορά των δεδομένων στην αρχική τους μορφή απαιτείται η ύπαρξη ειδικού κλειδιού.

Firewall - Ειδικό Πρόγραμμα (λογισμικό) ή και υλικό (hardware) που έχει τη δυνατότητα να ελέγχει ή και να απαγορεύει την απομακρυσμένη πρόσβαση σ' έναν υπολογιστή ή και να περιορίζει τις διαθέσιμες ιστοσελίδες σ' έναν προσωπικό υπολογιστή ή και σ' ένα δίκτυο υπολογιστών. Το firewall κάνει έλεγχο στα εισερχόμενα και εξερχόμενα δεδομένα από και προς τον υπολογιστή ή το δίκτυο από τη μια μεριά και το Internet από την άλλη.

Hacker - Χρήστης ο οποίος εισβάλει σε σύστημα στο οποίο δεν έχει νόμιμη πρόσβαση, αλλά μόνο για πειραματισμό και ευχάριστη απασχόληση καθώς και για να εντοπίσει και να υποδείξει κενά στα συστήματα ασφαλείας των υπολογιστικών συστημάτων. Διακρίνονται από τους λεγόμενους ***Crackers***, οι οποίοι προκαλούν ζημιές ή κάνουν μη νόμιμες ενέργειες.

Hashing Algorithm - Ειδικός αλγόριθμος κρυπτογράφησης, με τη βοήθεια του οποίου δημιουργείται μια σύνοψη (περίληψη) ενός κειμένου (εγγράφου) σ' έναν αριθμό σταθερού μήκους, π.χ. 128 bits. Από δύο διαφορετικά έγγραφα είναι αστρονομικά αδύνατο να προκύψουν δύο ίδιοι κωδικοί των 128 bits. Η μέθοδος αυτή χρησιμοποιείται για να διαπιστωθεί η ακεραιότητα (integrity) ενός αποσταλέντος μηνύματος και όχι τόσο για την κρυπτογράφηση απόρρητων μηνυμάτων. Η διαδικασία που ακολουθείται είναι η εξής : ο αποστολέας του μηνύματος στέλνει το κανονικό μήνυμα σε απλή (όχι κωδικοποιημένη) μορφή μαζί με τον αριθμό που έχει προκύψει από την κρυπτογράφηση με τον αλγόριθμο hashing. Ο παραλήπτης εφαρμόζει στο ίδιο μήνυμα τον ίδιο αλγόριθμο hashing και συγκρίνει τους δύο αριθμούς των 128 bits που έχουν προκύψει, δηλ. αυτόν που έχει λάβει και αυτόν που έχει δημιουργήσει ο ίδιος και αν προκύψει διαφορά αυτό σημαίνει όυι το μήνυμα έχει αλλοιωθεί στην πορεία και θα πρέπει να ξανασταλεί.

HTTPS (Secure Hypertext Transfer Protocol) - Ασφαλές πρωτόκολλο για την ανταλλαγή κρυπτογραφημένων ιστοσελίδων ανάμεσα στον Web server και τον φυλλομετρητή (browser). Οι δικτυακοί τόποι που υποστηρίζουν το συγκεκριμένο πρωτόκολλο, στο πεδίο διευθύνσεων του φυλλομετρητή εμφανίζεται το https:// αντί του γνωστού http:// και στη γραμμή κατάστασης το σύμβολο μιας κλειδαριάς. Το πρωτόκολλο αυτό παρέχει ασφαλή διαχείριση των προσωπικών δεδομένων των χρηστών και χρησιμοποιείται συνήθως σε online

συναλλαγές ή σε αποστολή στοιχείων πιστωτικής κάρτας κ.ά. Πρόκειται στην ουσία για μια ασφαλή μορφή του γνωστού πρωτοκόλλου μεταφοράς υπερκειμένου HTTP, ώστε να είναι εξασφαλισμένη η ανταλλαγή πληροφοριών ανάμεσα στον φυλλομετρητή και τον Web server.

(IDEA) International Data Encryption Algorithm - Αναπτύχθηκε στην Ελβετία και χρησιμοποιείται στο PGP 2.x ως ο συμμετρικός αλγόριθμος κρυπτογράφησης. Χρησιμοποιεί ένα κλειδί των 128 bit για να κάνει μια σειρά από μη γραμμικούς μαθηματικούς μετασχηματισμούς σ' ένα μπλοκ δεδομένων (data block) των 64 bit.

Key - Αποδίδεται στα ελληνικά με τον όρο *Κλειδί* ή και *Κλείδα* και είναι μια συλλογή από δυαδικά ψηφία που είναι αποθηκευμένα σ' ένα αρχείο που χρησιμοποιείται για την κρυπτογράφηφη ή αποκρυπτογράφηση ενός μηνύματος.

Key Escrow - Σε γενικές γραμμές, η διαδικασία key escrow σημαίνει ότι ένα αντίγραφο του μυστικού κλειδιού που είναι απαραίτητο στην αποκρυπτογράφηση αποθηκεύεται (φυλάσσεται) από κάποιον τρίτο, που μπορεί να είναι ένας συμβολαιογράφος ή μια τράπεζα, και οι οποίοι το κρατούν σε ασφάλεια σε περιπτωση απώλειας του κλειδιού ή θανάτου του κατόχου του. Η χρήση του είναι κοινή και στις επιχειρήσεις, όπως όταν ένας υπάλληλος κατέχει κρυπτογραφημένο υλικό στον υπολογιστή της εταιρείας του και σε περίπτωση που συμβεί κάτι με τον υπάλληλο ή με τον υπολογιστή, η εταιρεία δεν θα μπορέσει να αποκρυπτογραφήσει τα μηνύματα. Γι' αυτόν τον λόγο, ένα αντίγραφο του μυστικού κλειδιού φυλάσσεται από έναν ή περισσότερους προϊσταμένους. Για να υπάρχει η εξασφάλιση ότι ένας προϊστάμενος δνε θα κάνει κατάχρηση της θέσης του, το κλειδί μπορεί να διαχωρισθεί και να μοιρασθεί σε πολλά άτομα, οι οποίοι θα πρέπει να συνεργασθούν για την ανάκτηση του κλειδιού.

Known Plain Text Attack - Είναι μια μέθοδος επίθεσης σ' ένα σύστημα κρυπτογράφησης όπου ο κρυπταναλυτής κατέχει αντίγραφα του plain text και του αντίστοιχου κρυπτογραφημένου κειμένου. Με τα ασθενέστερα συστήματα κρυπτογράφησης, η μέθοδος αυτή μπορεί να βελτιώσει τις πιθανότητες σπασίματος του κωδικού και απόκτησης του plain text των άλλων μηνυμάτων όπου το plain text δεν είναι γνωστό.

Message Digest Algorithm #5 (MD5) - Ο MD5 Message Digest Algorithm είναι ο αλγόριθμος σύνοψης μηνύματος που χρησιμοποιείται στο PGP. Υπολογίζεται ότι η πιθανότητα να έχουν δύο μηνύματα την ίδια σύνοψη είναι μετά από 2^{64} περιπτώσεις και ότι η πιθανότητα να έχει ένα οποιοδήποτε μήνυμα μια δεδομένη σύνοψη μηνύματος είναι είναι μετά από 2^{128} περιπτώσεις. Ο αλγόριθμος MD5 είναι ένας καινούργιος αλγόριθμος αλλά το επίπεδο ασφαλείας που παρέχει είναι αρκετό για την υλοποίηση ψηφιακών υπογαρφών υψηλών απαιτήσεων που βασίζονται στο MD5 και το RSA.

One Time Pad (OTP) - Το one time pad είναι το μόνο σχήμα κρυπτογράφησης (encryption scheme) που μπορεί να αποδειχθεί ότι είναι απολύτως απαραβίαστο. Χρησιμοποιείται πολύ από τους κατασκόπους καθώς δεν απιατεί κάποιον μηχανισμό (hardware) για να υλοποιηθεί και λόγω της απόλυτης ασφάλειας που παρέχει. Αυτός ο αλγόριθμος απαιτεί τη δημιουργία πολλών συνόλων από keys pads, όπου το κάθε pad αποτελείται από έναν αριθμό από τυχαίους χαρακτήρες κλειδιών. Each party involved receives matching sets of pads. Ο κάθε χαρακτήρας κλειδιού στο pad χρησιμοποιείται για να κρυπτογραφήσει έναν μόνο χαρακτήρα plain text και μετά δεν χρησιμοποιείται ποτέ ξανά. Ο λόγος που δεν χρησιμοποιείται ευρέως αυτό το σχήμα κρυπτογράφησης είναι ότι λόγω της πολυπλοκότητάς του δεν είναι κατάλληλο για τα σύγχρονα συστήματα επικοινωνιών που έχουν μεγάλες απαιτήσεις σε ταχύτητα. Ένα από τα

διασημότερα links επικοινωνίας που χρησιμοποιούν αυτό το σχήμα είναι η κόκκινη γραμμή Ουάσινγκτον - Μόσχας.

Passphrase - Αποδίδεται στα ελληνικά με τον όρο *Συνθηματική Λέξη* ή και *Κωδική Φράση* και είναι ουσιαστικά το ίδιο πράγμα με το Password με τη διαφορά ότι είναι πιο περίπλοκο και συνεπώς πιο δύσκολο να εντοπισθεί.

Password - Αποδίδεται στα ελληνικά με τον όρο *Συνθηματικό* ή και *Κωδικός Πρόσβασης* και είναι μια μοναδική και απόρρητη λέξη κλειδί με την οποία σε συνδυασμό με το όνομα χρήστη (username) μπορούμε να αποδείξουμε την ταυτότητά μας όταν εισερχόμαστε σε περιορισμένης πρόσβασης σελίδες ή εφαρμογές ή σε πύλες (portals) ή και αλλού. Αποτελεί καλή τακτική να αλλάζουμε συχνά το password μας και να μην χρησιμοποιούμε κωδικούς που να μπορεί εύκολα να τους μαντέψει κάποιος αλλά περίεργους συνδυασμούς από γράμματα, ψηφία και σύμβολα.

PGP (Pretty Good Privacy) - Αποτελεί ένα από τα πιο δημοφιλή προγράμματα που χρησιμοποιούνται για την κρυπτογράφηση μηνυμάτων και την αποστολή τους μέσω του Internet. Χρησιμοποιεί την κρυπτογράφηση με συνδυασμό δημόσιου και ιδιωτικού κλειδιού (public key - private key). Θεωρείται απόλυτα ασφαλές. Το δημόσιο κλειδί είναι γνωστό σ' όλους και μπορούμε να το κατεβάσουμε (download) από κάποια ιστοσελίδα, ενώ το ιδιωτικό κλειδί είναι αυστηρά προσωπικό για τον κάθε χρήστη. Ό,τι κωδικοποιείται με το ένα κλειδί μπορεί να αποκωδικοποιηθεί με το άλλο και αντίστροφα. Όμως, είναι εξαιρετικά δύσκολη, αν όχι αδύνατη, η εύρεση του ιδιωτικού κλειδιού όταν γνωρίζουμε το δημόσιο κλειδί ενός χρήστη. Όταν ένα μήνυμα κωδικοποιείται με το ιδιωτικό κλειδί ενός χρήστη, μπορεί να αποκωδικοποιηθεί από οποιονδήποτε τρίτο με το γνωστό δημόσιο κλειδί του ίδιου χρήστη, αλλά αυτό αποτελεί μια επιβεβαίωση της

ταυτότητας του χρήστη. Επίσης, η κωδικοποίηση ενός μηνύματος με το δημόσιο κλειδί ενός χρήστη εξασφαλίζει το ότι μόνο ο συγκεκριμένος χρήστης θα μπορέσει να το αποκωδικοποιήσει.

PlainText - Είναι το αυθεντικό (αρχικό) αρχείο, κείμενο ή μήνυμα, το οποίο πρέπει να λάβει κανονικά ο παραλήπτης. Το κρυπτογραφημένο μήνυμα που αποστέλνεται αποκαλείται *CipherText (Κρυπτογράφημα)*.

Private Key - Αποδίδεται στα ελληνικά με τον όρο *Ιδιωτικό Κλειδί* και είναι το μυστικό (κρυφό) κλειδί ενός κρυπτογραφικού συστήματος. Μπορεί να το χρησιμοποιεί ο κάτοχός του για να υπογράφει ηλεκτρονικά τα εξερχόμενα μηνύματά του καθώς και για να αποκρυπτογραφεί τα εισερχόμενα μηνύματά του.

Public Key - Αποδίδεται στα ελληνικά με τον όρο *Δημόσιο Κλειδί* και είναι το κοινό κλειδί ενός κρυπτογραφικού συστήματος. Μπορεί να το χρησιμοποιεί ένας οποιοσδήποτε τρίτος για να κρυπτογραφεί τα εξερχόμενα μηνύματά του προς τον κάτοχο του αντίστοιχου ιδιωτικού κλειδιού καθώς και για να αποκρυπτογραφεί τα εισερχόμενα μηνύματα που έχουν κωδικοποιηθεί με το ιδιωτικό κλειδί του αποστολέα.

Public Key Encryption - Αποδίδεται στα ελληνικά με τον όρο *Κρυπτογράφηση με Δημόσιο Κλειδί* και πρόκειται για ένα σύστημα (τεχνική) κρυπτογράφησης που χρησιμοποιεί έναν συνδυασμό από ένα δημόσιο και ένα ιδιωτικό κλειδί για την κρυπτογράφηση των μηνυμάτων. Με τον τρόπο αυτό αποφεύγουμε την αποστολή του κλειδιού από τον αποστολέα στον παραλήπτη, κάτι που είναι πολύ επικίνδυνο για υποκλοπή. Η τεχνική αυτή κρυπτογράφησης λειτουργεί μ' έναν εμπιστευτικό κωδικό του νόμιμου χρήστη, που είναι το γνωστό ιδιωτικό κλειδί (private key), και μ' έναν δημόσιο κωδικό, που είναι το γνωστό δημόσιο κλειδί (public key), και το οποίο διανέμεται (δίνεται)

ελεύθερα μέσω του Internet ή και ως συνημμένο σ' ένα e-mail. Οι δύο αυτοί κωδικοί αποτελούν από κοινού ένα μοναδικό ζεύγος κλειδιού με το οποίο επιτυγχάνεται η αποκρυπτογράφηση των δεδομένων.

Registered User - Όρος που αναφέρεται σ' έναν εγγεγραμμένο χρήστη μιας online υπηρεσίας, ο οποίος προσδιορίζεται από το όνομα χρήστη και τον προσωπικό (απόρρητο) κωδικό πρόσβασης και ενδεχομένως από κάποια επιπλέον στοιχεία.

RSA - Μια μέθοδος κρυπτογράφησης δημόσιου κλειδιού που μπορεί να χρησιμοποιηθεί και για την κρυπτογράφηση μηνυμάτων και για τη δημιουργία ψηφιακών υπογραφών, δηλ. για την επιβεβαίωση της ταυτότητας του αποστολέα ενός μηνύματος. Το RSA είναι η μέθοδος κρυπτογράφησης δημοσίου κλειδιού που χρησιμοποιείται στο PGP. Τα αρχικά του RSA αναφέρονται στους δημιουργούς του αλγορίθμου *(Rivest-Shamir-Adleman)*. Η βασική ασφάλεια στο RSA προέρχεται από το γεγονός ότι, ενώ είναι σχετικά εύκολο να πολλαπλασιάσουμε δύο μεγάλους πρώτους αριθμούς και να πάρουμε το γινόμενό τους, είναι υπολογιστικά δύσκολο να κάνουμε το αντίστροφο, δηλ. το να βρούμε τους δύο πρώτους παράγοντες ενός δεδομένου σύνθετου αριθμού. Είναι αυτή η φύση του RSA που επιτρέπει τη δημιουργία και την αποκάλυψη στον κόσμο ενός κλειδιού κρυπτογράφησης, ενώ από την άλλη μεριά δεν επιτρέπει την αποκρυπτογράφηση ενός μνηνύματος.

Secret Key Encryption - Αποδίδεται στα ελληνικά με τον όρο *Κρυπτογράφηση με Κρυφό Κλειδί* και πρόκειται για ένα σύστημα κρυπτογράφησης με το οποίο αποστέλλεται στον παραλήπτη το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση ενός μηνύματος.

Secure Web Server - Ένας Web server που εργάζεται με πιστοποιητικά (πρωτόκολλα) ασφαλείας. Οι συνδέσεις που γίνονται μ' έναν τέτοιο Web server είναι ασφαλείς και όλα

τα μηνύματα (δεδομένα) που ανταλλάσσονται με τους πελάτες (clients) του είναι κρυπτογραφημένα.

SET (Secure Electronic Transaction) - Πρόκειται για ένα σύστημα ασφαλών τραπεζικών πληρωμών που έχει δημιουργηθεί από γνωστές εταιρείες πιστωτικών καρτών. Χρησιμοποιεί τη λεγόμενη *Έμπιστη Τρίτη Οντότητα (Third Trusted Party)* στις συναλλαγές εμπόρου-πελάτη, δηλ. μια ιδιωτική εταιρεία εμπιστοσύνης που παρεμβάλλεται ως τρίτος στις συνδιαλλαγές και εκδίδει τα ψηφιακά πιστοποιητικά ταυτότητας των συναλλασσομένων. Τα κρυπτογραφικά αυτά πρωτόκολλα σχεδιάστηκαν και αναπτύχθηκαν από κοινού από τις εταιρείες Visa, MasterCard, Netscape & Microsoft προκειμένου να παρέχουν ασφαλείς συναλλαγές με πιστωτικές κάρτες στο Διαδίκτυο για τους καταναλωτές (επλάτες) και τους πωλητές.

Spam e-mail - Έτσι αποκαλούνται τα e-mails που έχουν ενοχλητικό και συνήθως διαφημιστικό περιεχόμενο και που έχουν κατακλείσει το Internet τελευταία. Αποτελούν μια πολύ φθηνή μέθοδο διαφήμισης και προώθησης προϊόντων αλλά και marketing. Στα spam e-mails συγκαταλέγονται ανεπιθύμητες διαφημίσεις για προϊόντα, υπηρεσίες και sites καθώς επίσης και διάφοροι άλλοι τύποι e-mail (newsletters, chain mails κ.ά.).

SSL (Secure Sockets Layer)- Πρόκειται για ένα σύστημα (πρωτόκολλο) κρυπτογράφησης που έχει δημιουργήσει η γνωστή εταιρεία Netscape, με σκοπό την ασφαλή σύνδεση (επικοινωνία) ενός φυλλομετρητή με τον Web server. Τα δεδομένα που στέλνονται ανάμεσα στους δύο είναι κρυπτογραφημένα αλλά το σύστημα δεν εξασφαλίζει την ταυτότητα ούτε του αποστολέα ούτε του παραλήπτη. Είναι ειδικό πρωτόκολλο επικοινωνίας ανάμεσα σε browsers και servers και το οποίο κρυπτογραφεί κάθε online επικοινωνία. Το πρωτόκολλο

αυτό διασφαλίζει συναλλαγές με διαφάνεια στους τελικούς χρήστες.

Steganography - Αποδίδεται στα ελληνικά με τον όρο *Στεγανογραφία* και είναι η διαδικασία απόκρυψης πληροφοριών μέσα σ' ένα άλλο πακέτο πληροφοριών και δεδομένων. Με τον τρόπο αυτό μπορούμε να αποκρύψουμε ένα αρχείο κειμένου μέσα σε κάποιο αρχείο εικόνας ή και ήχου, ώστε να μην γίνεται κατανοητό από τον παραλήπτη του αρχείου εικόνας ή ήχου.

Symmetric Encryption - Αποδίδεται στα ελληνικά με τον όρο *Συμμετρική Κρυπτογράφηση* και είναι μια από τις πρώτες μορφές κρυπτογραφίας που χρησιμοποιεί το ίδιο κλειδί τόσο για την κωδικοποίηση όσο και για την αποκωδικοποίηση του μηνύματος. Υπάρχει και η *Ασύμμετρη Κρυπτογράφηση (Asymmetric Encryption)*, η οποία χρησιμοποιεί δύο διαφορετικά κλειδιά (δημόσιο και ιδιωτικό).

Symmetric Key - Αποδίδεται στα ελληνικά με τον όρο *Συμμετρικό Κλειδί* και είναι η παλιά μέθοδος κρυπτογράφησης που χρησιμοποιεί το ίδιο κλειδί τόσο για την κωδικοποίηση όσο και για την αποκωδικοποίηση του μηνύματος. Δεν χρησιμοποιείται σήμερα καθώς δεν είναι ασφαλής μέθοδος επικοινωνίας.

TripleDES - Είναι μια μέθοδος βελτίωσης των δυνατοτήτων του αλγορίθμου DES, η οποία χρησιμοποιεί τον ίδιο αλγόριθμο τρεις φορές σε αλληλουχία με διαφορετικά κλειδιά, για μεγαλύτερη ασφάλεια.

User Identification - Αναφέρεται στην πιστοποίηση, δηλ. στον έλεγχο της ταυτότητας ή του δικαιώματος πρόσβασης σ' έναν δικτυακό τόπο, που γίνεται με το όνομα χρήστη και τον κωδικό πρόσβασης.

Username - Αποδίδεται στα ελληνικά με τον όρο *Όνομα Χρήστη* ή και *Αναγνωριστικό* και χρησιμοποιείται συνήθως

σε συνδυασμό μ' έναν Κωδικό Πρόσβασης (Password) για την εισαγωγή σ' ένα σύστημα ή δίκτυο πολλαπλών χρηστών. Συνήθως ο χρήστης μπορεί να επιλέξει ο ίδιος το δικό του username (που πρέπει να είναι μοναδικό, στο πλαίσιο ενός δικτύου ή συστήματος) και το password, το οποίο δεν είναι απαραίτητο να είναι μοναδικό αλλά θα πρέπει να είναι απόρρητο και δύσκολο στο να μπορέσει να το εντοπίσει κάποιος.

Verisign - Μια από τις πιο γνωστές διεθνώς εταιρείες που λειτουργεί ως Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ) και εκδίδει ψηφιακές ταυτότητες (digital ID's) σε τρίτους (ιδιώτες ή και εταρείες). Οι εταιρείες αυτές αποκαλούνται και Έμπιστες Τρίτες Οντότητες (ΕΤΟ), δηλ. Trusted Third Parties (TTP), ή και Αρχές Πιστοποίησης (CA, Certification Authorities). Μια εταιρεία Παροχής Υπηρεσιών Πιστοποίησης μπορεί να εξουσιοδοτήσει άλλες εταιρείες σ' άλλες χώρες ή και σ' άλλες πόλεις για να κάνουν πιστοποίηση και να σχηματιστεί έτσι ένα δένδρο από τους Οργανισμούς Πιστοποίησης.

X.509 - Ένα από τα πιο διαδεδομένα πρότυπα για τη δημιουργία ψηφιακών πιστοποιητικών.

Πηγη:κεντρο πληνετ νομου φλωρινας,wikipedia.org