Ηλεκτρονικό εμπόριο

ΗΕ 7

Τεχνολογίες ασφάλειας

Πρόκληση ανάπτυξης ασφαλών συστημάτων

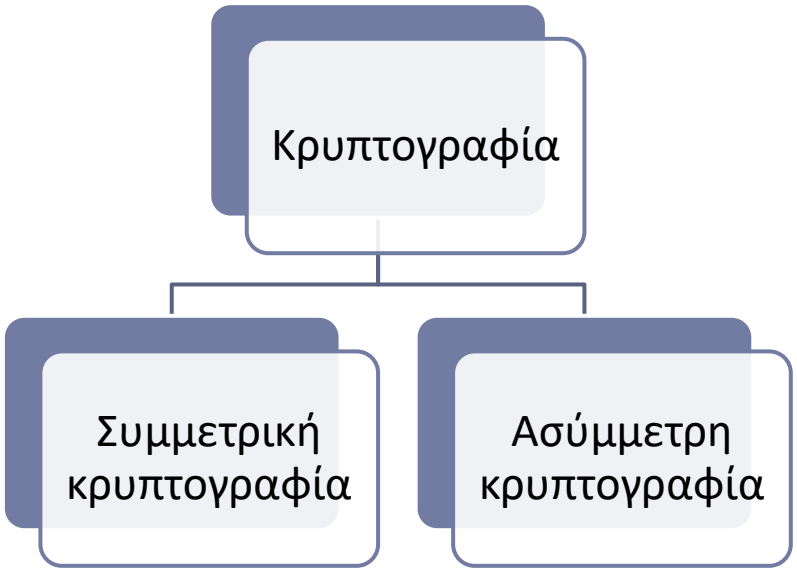
- Η υποδομή του διαδικτύου παρουσίαζε έλλειψη υπηρεσιών ασφάλειας καθώς η οικογένεια πρωτοκόλλων TCP/IP στην οποία στηρίζεται είναι μη ασφαλής

- Επιχειρήθηκε και επιχειρείται η ανάπτυξη πρωτοκόλλων και προτύπων που καταστούν το διαδίκτυο αξιόπιστο χώρο συναλλαγών

- Συχνά ο άνθρωπος είναι ο αδύναμος κρίκος στην προσπάθεια τω επιχειρήσεων να σημιουργήσουν ένα ασφαλές περιβάλλον

Κρυπτογραφία

- Η κρυπτογραφία χρησιμοποιείται για να καλύψει την ανάγκη της εμπιστευτικότητας στο ηλεκτρονικό εμπόριο
- **Κλειδί:** σειρά από bits συγκεκριμένου μήκους που χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση



Στην πράξη η συμμετρική και η ασύμμετρη κρυπτογραφία συνδυάζονται έτσι ώστε να χρησιμοποιούνται τα καλύτερα χαρακτηριστικά κάθε μεθόδου

Κρυπτανάλυση

- Η **κρυπτανάλυση** είναι η μελέτη για την επινόηση μεθόδων που εξασφαλίζουν την κατανόηση του νοήματος της κρυπτογραφημένης πληροφορίας, έχοντας ως άγνωστες ποσότητες τον κρυφό μετασχηματισμό, το κλειδί, με βάση το οποίο αυτός πραγματοποιήθηκε και το κρυπτογραφημένο μήνυμα. Βασικός στόχος της είναι, ανάλογα με της απαιτήσεις του αναλυτή κρυπτοσυστημάτων ή αλλιώς κρυπταναλυτή, να βρει το κλειδί, το μήνυμα ή ένα ισοδύναμο αλγόριθμο που θα τον βοηθά να αναγνώσει το (κρυφό) μήνυμα. (πηγή:wikipedia)

Συμμετρική κρυπτογραφία

- Ο αποστολέας και ο παραλήπτης γνωρίζουν **το ίδιο μυστικό κλειδί**
- Το κλειδί χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση
- Θεωρείται γρήγορη και αποδοτική μέχρι ενός ορίου

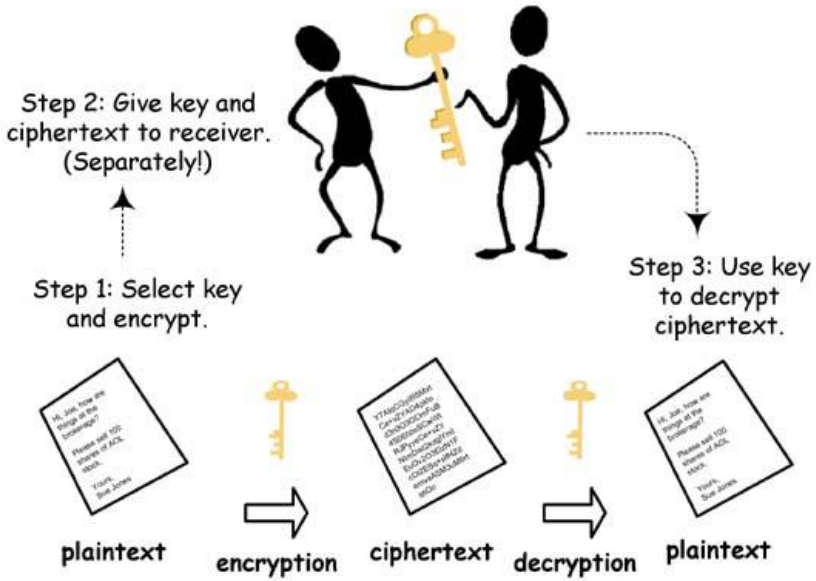
Μειονεκτήματα

- Προβληματική διαχείριση κλειδιών πάνω από δημόσια δίκτυα με πληθώρα χρηστών
- Αυθεντικότητα
- Αποποίηση ευθύνης

Symmetric cryptography

Αλγόριθμοι συμμετρικής κρυπτογράφησης

- DES
- 3DES
- AES
- RC2
- RC4
- RC5
- IDEA



Ασύμμετρη κρυπτογραφία

- **Χρησιμοποιεί 2 κλειδιά** ένα για την **κωδικοποίηση** και ένα για την **αποκωδικοποίηση**
- **Δημόσιο κλειδί:** είναι γνωστό σε όλους
- **Ιδιωτικό κλειδί:** παραμένει μυστικό
- **Οποιοσδήποτε μπορεί να στείλει μήνυμα με το δημόσιο κλειδί** αλλά το μήνυμα μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί
- Ο αποστολέας στέλνει το μήνυμα του κρυπτογραφημένο με το **δημόσιο κλειδί του παραλήπτη** έτσι ώστε να παραμείνει εμπιστευτικό μέχρι να αποκρυπτογραφηθεί από τον παραλήπτη με το ιδιωτικό κλειδί του
- Ο αποστολέας κρυπτογραφεί το μήνυμα (επιπλέον), χρησιμοποιώντας **το ιδιωτικό του κλειδί.** Έτσι κατά την αποκρυπτογράφηση ο παραλήπτης βεβαιώνει την ταυτότητα του αποστολέα.
- Μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ταχύτητα της

Ασύμμετροι αλγόριθμοι

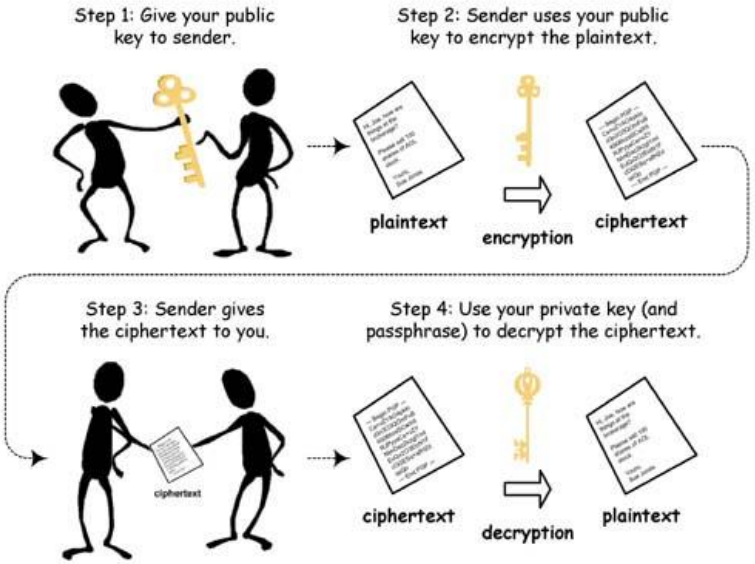
- Ένας ασύμμετρος αλγόριθμος λειτουργεί ως μια μονόδρομη συνάρτηση (trap-door) δηλαδή είναι εύκολη η πραγματοποίηση μια λειτουργίας στην μια κατεύθυνση αλλά είναι δύσκολη ή αδύνατη η αντιστροφή της λειτουργίας

- Παράδειγμα: Είναι εύκολος ο πολλαπλασιασμός 2 ακεραίων αλλά είναι δύσκολο να βρεθούν οι αριθμοί που έδωσαν το γινόμενο αυτό. Αν απο την άλλη όμως κάποιος γνωρίζει το γινόμενο και έναν από τους δύο αριθμούς τότε αποκαλύπτεται και ο άλλος αριθμός

Asymmetric cryptography

Αλγόριθμοι ασύμμετρης κρυπτογράφησης

- Diffie-Hellman Key Exchange Algorithm
- RSA



Βήματα ασύμμετρης κρυπτογράφησης

- Ο αποστολέας κρυπτογραφεί το μήνυμα χρησιμοποιώντας έναν κοινό αλγόριθμο κρυπτογράφησης και **το ιδιωτικό του κλειδί**.
- Στο **αποτέλεσμα ο αποστολέας προσθέτει την ψηφιακή υπογραφή** του και κρυπτογραφεί το συνολικό μήνυμα ξανά χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη.

- Ο παραλήπτης αποκρυπτογραφεί το μήνυμα που δέχεται χρησιμοποιώντας το δικό του ιδιωτικό κλειδί αποκαλύπτοντας την ταυτότητα του αποστολέα στο μήνυμα (**αυθεντικότητα**).
- Ο παραλήπτης αποκρυπτογραφεί το υπόλοιπο μήνυμα με το **δημόσιο κλειδί του αποστολέ**α.

- Με αυτό τον τρόπο ο παραλήπτης διασφαλίζει ότι όποιος συνέθεσε το μήνυμα είχε πρόσβαση στο ιδιωτικό κλειδί του αποστολέα και ότι κανένας δεν τροποποίησε ή ανάγνωσε το μήνυμα κατά την διαδρομή

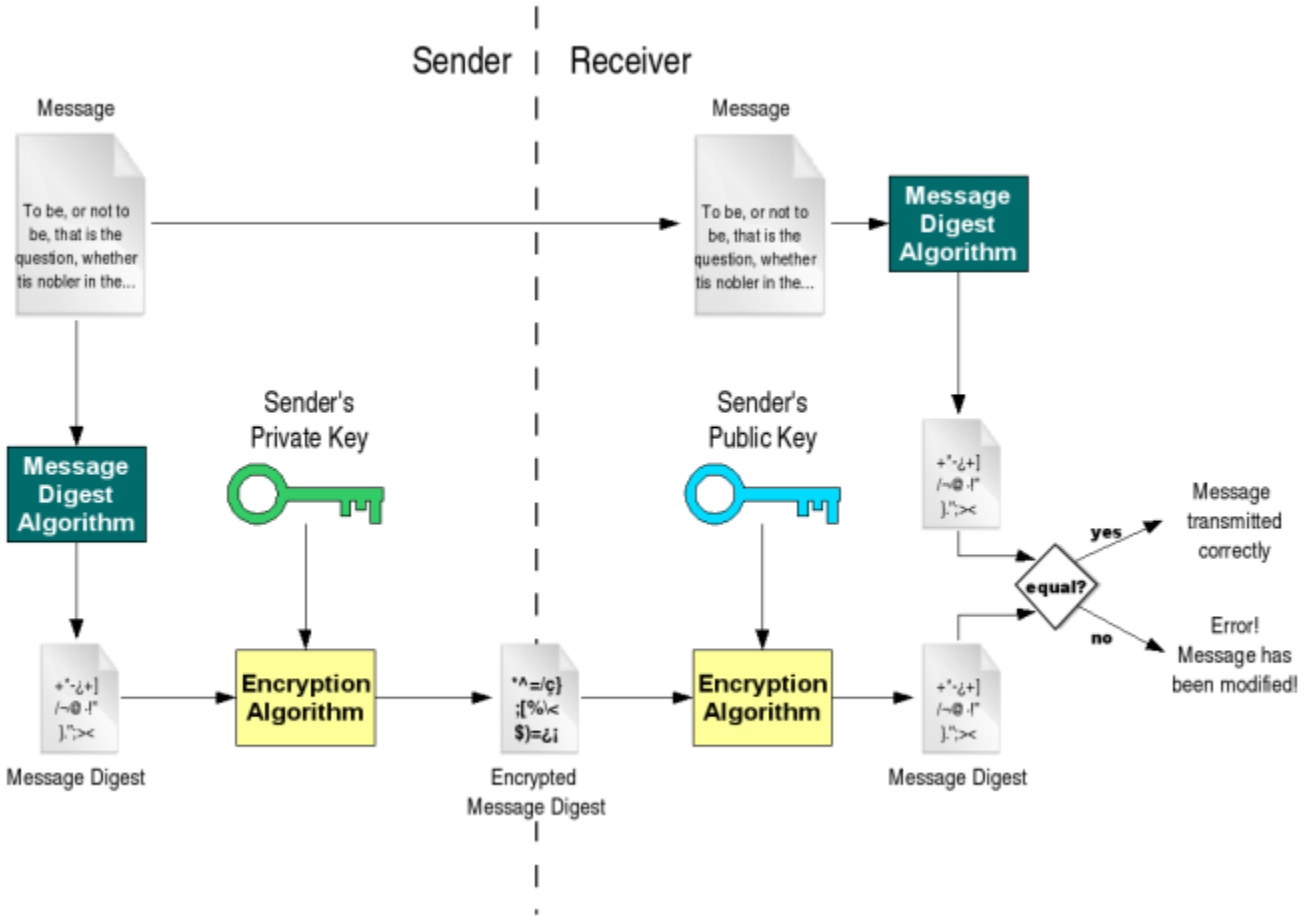
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci836964,00.html

Ψηφιακές υπογραφές

- Συναρτήσεις hash: εκτελούν μαθηματικούς υπολογισμούς με όρισμα ένα μήνυμα και παράγουν μια αριθμητική τιμή (MD = Message Digest) από την οποία δεν μπορεί να επαναδημιουργηθεί το μήνυμα
- Το MD είναι μικρού μεγέθους (μικρότερο από το αρχικό μήνυμα)
- Η πιθανότητα δυο διαφορετικά μηνύματα να δώσουν το ίδιο MD είναι εξαιρετικά μικρή
- Ψηφιακή υπογραφή είναι το κρυπτογραφημένο MD.

- Ο Α στέλνει στον Β το μήνυμα Τ και το MD του μηνύματος κρυπτογραφημένο με το ιδιωτικό κλειδί του Α έστω MD_A
- Ο Β εφαρμόζει την ίδια συνάρτηση hash στο μήνυμα και δημιουργεί την δική του εκδοχή για το MD έστω MD_B
- Ο Β αποκρυπτογραφεί το MD_A που έχει λάβει με το δημόσιο κλειδί του Α
- Ο Β συγκρίνει το MD_A και το MD_B και αν είναι ίδια τότε έχει επιτυχώς αυθεντικοποιήσει τον Α

Digital signatures



Ψηφιακά πιστοποιητικά

- Πως συνδέεται μια οντότητα με το δημόσιο κλειδί της;
  - Με τα ψηφιακά πιστοποιητικά
- Τα ψηφιακά πιστοποιητικά υπάρχουν με σκοπό να δημιουργήσουν εμπιστοσύνη στην νομιμότητα του δημόσιου κλειδιού
- Είναι ψηφιακές υπογραφές που προστατεύουν τα δημόσια κλειδιά από παραχάραξη
- Η δημιουργία από οποιονδήποτε ενδιαφερόμενο ζευγών δημόσιων και ιδιωτικών κλειδιών και ο διαμοιρασμός τους (π.χ. μέσω email) εμπεριέχει κινδύνους
- Η αξιόπιστη διανομή δημοσίων κλειδιών μπορεί να γίνει με χρήση κάποιας αρχής πιστοποίησης

Αρχές πιστοποίησης

- Δέχεται το δημόσιο κλειδί ενός χρήστη μαζί με ντοκουμέντα ταυτότητας και δημιουργεί ένα ψηφιακό πιστοποιητικό το οποίο διαθέτει σε οποιονδήποτε ενδιαφερόμενο
- Αρχές πιστοποίησης
  - Verisign
  - Cybertrust
  - Globalsign
- Το πρότυπο πιστοποιητικών δημοσίου κλειδιού είναι το X.509 και περιέχει:
  - Όνομα κατόχου
  - Το δημόσιο κλειδί του
  - Χρονική περιόδο εγκυρότητας πιστοποιητικού

Κλάσεις πιστοποίησης

- Κλάση 1
  - Ευκολότερη απόκτηση
  - Επαληθεύεται μόνο το όνομα και το email
- Κλάση 2
  - Έλεγχος άδειας οδήγησης, αριθμό κοινωνικής ασφάλισης, ημερομηνία γέννησης
- Κλάση 3
  - Πιστωτικός έλεγχος
- Κλάση 4
  - Επιπλέον έλεγχος σχετικά με την θέση ενός ιδιώτη σε έναν οργανισμό

- Κόστος πιστοποιητικών
- Εξυπηρετητής πιστοποιητικών
- Λίστες ανάκλησης πιστοποιητικών
- Αλυσίδες πιστοποιητικών

Πρωτόκολλα ασφαλείας

- Ασφάλεια σύνδεσης (SSL)
  - https://...
- Ασφάλεια εφαρμογών (S-HTTP, S/MIME)
- Ασφάλεια συναλλαγών ηλεκτρονικού εμπορίου (SET)
  - Visa, MasterCard, Microsoft, …

PGP

- Pretty Good Privacy

GnuPG

THE ENIGMAIL PROJECT
OPENPGP EMAIL SECURITY FOR MOZILLA APPLICATIONS

Home | Download | Documentation | Support | News | Links

A simple interface for OpenPGP email security

Φράγματα ασφαλείας (firewalls)

- Μηχανισμός που ελέγχει την κυκλοφορία της πληροφορίας μεταξύ ενός τοπικού δικτύου και του διαδικτύου και **προστατεύει το τοικό δίκτυο από εξωτερικές απειλές και παραβιάσεις**
- Κακόβουλο λογισμικό (ιοί, σκουλήκια, δούρειοι ίπποι) που διακινείται εντός του τοπικού δικτύου μπορεί να υποβιβάσει το επίπεδο ασφάλειας που παρέχει ένα φράγμα ασφαλείας
- Ένα firewall μπορεί να δίνει την αίσθηση του αδικαιολόγητου περιορισμού ενώ γενικά δεν είναι ιδιαίτερα εύκολα στην χρήση τους
- Ένα firewall μπορεί:
  - **να μπλοκάρει** ή να παρακολουθεί μετάδοση συγκεκριμένου είδους μηνυμάτων (βάσει τύπου και προορισμού)
  - **Πρόσβαση συγκεκριμένων εφαρμογών σε υπηρεσίες**

- Διαδεδομένα firewalls
  - Comodo
  - Sygate
  - ZoneAlarm
  - Sunbelt