ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΤΗΣ ΕΛΛΑΔΟΣ
Σχολη Θετικων Επιστημων
Τμημα Πληροφορικης
ΠΠΣ Μηχανικων Πληροφορικης

ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΚΩΝ/ΝΟΣ ΡΑΝΤΟΣ
krantos@cs.ihu.gr

1

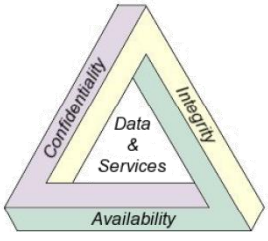
Τι είναι ασφάλεια

- Εννοιολογική θεμελίωση – βασικές αρχές ασφάλειας πληροφοριών
- Κρυπτογραφία – συμμετρικοί αλγόριθμοι
- Κρυπτογραφία δημοσίου κλειδιού – συναρτήσεις κατακερματισμού
- Ψηφιακές υπογραφές
- Ψηφιακά πιστοποιητικά και υποδομές δημοσίων κλειδιών
- Ακεραιότητα δεδομένων, αυθεντικοποίηση μηνύματος
- Αυθεντικοποίηση οντότητας – μέθοδοι και πρωτόκολλα
- Προστασία της ιδιωτικότητας
- Πολιτικές ασφαλείας
- Προστασία επικοινωνιών – ασφάλεια στο διαδίκτυο –
- Κακόβουλο λογισμικό
- Έλεγχος πρόσβασης

2

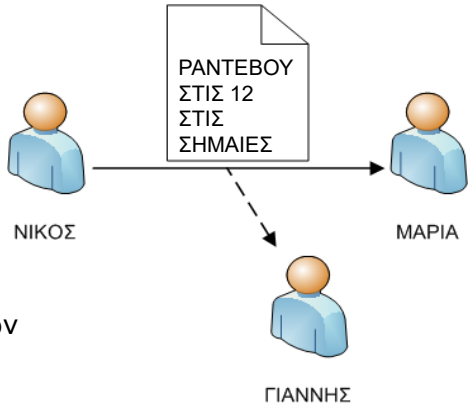
Τι είναι ασφάλεια

- Ασφάλεια ενός πληροφοριακού συστήματος είναι η προστασία των υπολογιστικών πόρων και δεδομένων από μη εξουσιοδοτημένη ή κακή χρήση τους.
- Στόχος είναι η προστασία όλων των περιουσιακών στοιχείων:
  - Υλικό
  - Λογισμικό
  - Δεδομένα
- Βασικές αρχές: το τρίπτυχο
  - Εμπιστευτικότητα (**C**onfidentiality)
  - Ακεραιότητα (**I**ntegrity)
  - Διαθεσιμότητα (**A**vailability)



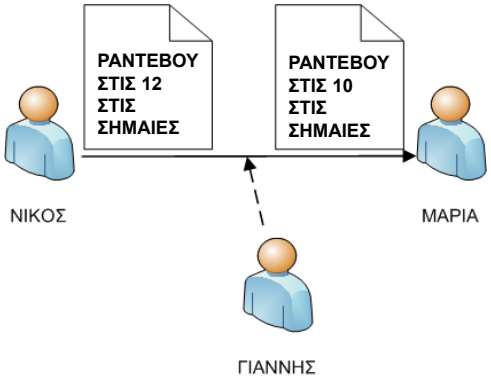
Εμπιστευτικότητα (Confidentiality)

- Προφυλάσσει από μη εξουσιοδοτημένη αποκάλυψη ευαίσθητων πληροφοριών.
  - Συνήθως είναι συνώνυμη με την ασφάλεια.
  - Επιτυγχάνεται με:
    - τη κρυπτογράφηση των δεδομένων η οποία καθιστά τα δεδομένα μη αναγνώσιμα,
    - έλεγχο πρόσβασης στα δεδομένα,
    - την απόκρυψη πληροφοριών (στεγανογραφία)



Ακεραιότητα (Integrity)

- Προφυλάσσει από μη εξουσιοδοτημένη τροποποίηση των δεδομένων.
  - Τροποποίηση περιλαμβάνει:
    - Εγγραφή/Δημιουργία νέων δεδομένων.
    - Εισαγωγή νέων δεδομένων στα υπάρχοντα.
    - Διαγραφή μέρους ή όλων των δεδομένων.
  - Επιτυγχάνεται με:
    - ψηφιακές υπογραφές
    - κώδικες αυθεντικοποίησης μηνύματος
    - κώδικες ανίχνευσης παραποίησης



Διαθεσιμότητα (Availability)

- Εξασφαλίζει ότι οι πόροι ενός συστήματος είναι πάντα διαθέσιμοι, σε εύλογο χρονικό διάστημα, σε όλους τους εξουσιοδοτημένους χρήστες και μόνο σε αυτούς.

Άλλες αρχές

- **Ταυτοποίηση (Identification)**
  - Μία οντότητα (π.χ. άνθρωπος, υπολογιστής, διαδικασία) **αναγνωρίζει** μία άλλη οντότητα
- **Αυθεντικοποίηση – Πιστοποίηση ταυτότητας (Authentication)**
  - Μια οντότητα **διαβεβαιώνεται** για την ταυτότητα μιας άλλης οντότητας
- **Εξουσιοδότηση (authorization)**
  - Η εκχώρηση σε μια οντότητα του δικαιώματος πρόσβασης στους πόρους ενός συστήματος.
  - Τυπικά ακολουθεί την ταυτοποίηση και αυθεντικοποίηση της οντότητας

Άλλες αρχές

- **Απόδοση ευθυνών (Accountability)**
  - Η οντότητα πρέπει να είναι αναγνωρίσιμη και υπεύθυνη των πράξεων της
- **Μη αποποίηση (Non-repudiation)**
  - Η διαθεσιμότητα αδιάψευστων αποδείξεων που μπορούν να χρησιμοποιηθούν σε μία διαφωνία.
  - Δύο κατηγορίες:
    - ✓ **Μη αποποίηση αποστολής**: να μη μπορεί ο αποστολέας ενός μηνύματος να αρνηθεί την αποστολή του.
    - ✓ **Μη αποποίηση παραλαβής**: να μη μπορεί ο παραλήπτης ενός μηνύματος να αρνηθεί τη λήψη του.

Προστασία από ποιούς;

- Οι περισσότερες επιθέσεις προέρχονται από μέσα παρά από έξω.
- Hackers-Εισβολείς: Επιτίθενται είτε από χόμπι είτε για οικονομικά οφέλη.
  - Τράπεζες
  - Κυβερνητικά συστήματα
  - Τηλεπικοινωνιακούς φορείς
  - Επιχειρήσεις
- Ατυχήματα – Ακούσιες βλάβες

Που εφαρμόζεται;

Που εφαρμόζεται η ασφάλεια;

Ασφάλεια επικοινωνιών: Η προστασία των πληροφοριών κατά την επικοινωνία ενός συστήματος με ένα άλλο.

Ασφάλεια υπολογιστών: Η προστασία των πληροφοριών μέσα σε ένα υπολογιστικό σύστημα (λειτουργικό σύστημα, βάσεις δεδομένων)

Φυσική ασφάλεια

Ασφάλεια προσωπικού

Βασικοί κανόνες

100% ασφάλεια ΔΕΝ ΥΠΑΡΧΕΙ

(Τα μέτρα που παίρνουμε είναι για να μειωθεί η επικινδυνότητα)

Η ασφάλεια ενός πληροφοριακού συστήματος
είναι μια αλυσίδα
και **το σύστημα είναι τόσο ασφαλές**
όσο ο πιο αδύναμος κρίκος αυτής της αλυσίδας

Ο πιο αδύναμος κρίκος της αλυσίδας είναι ο άνθρωπος

Το κόστος προστασίας των πληροφοριών δε θα πρέπει να υπερβαίνει το κόστος απώλειας των

Εννοιολογική θεμελίωση

- **Αδυναμία συστήματος (Vulnerability)**
  - Είναι ένα ελάττωμα στο λογισμικό, υλικό, ή στις διαδικασίες, το οποίο μπορεί να επιτρέψει την μη εξουσιοδοτημένη πρόσβαση ενός εισβολέα στους πόρους του συστήματος.
- **Απειλή (Threat)**
  - Οτιδήποτε μπορεί να προκαλέσει παραβίαση της ασφάλειας ενός συστήματος. Μπορεί να είναι:
    - Φυσική ή ανθρώπινη
    - Τυχαία ή σκόπιμη

Κυριότερες Απειλές

- Οι απειλές οι οποίες και αντικατοπτρίζουν τις αρχές ασφαλείας είναι:
  - Διαρροή πληροφοριών: Πληροφορίες αποκαλύπτονται σε μη εξουσιοδοτημένες οντότητες.
  - Παραβίαση ακεραιότητας: Μη εξουσιοδοτημένη δημιουργία, τροποποίηση ή καταστροφή δεδομένων.
  - Άρνηση παροχής υπηρεσίας: Παρεμποδίζεται η νόμιμη πρόσβαση σε δεδομένα ή πόρους.

Εννοιολογική θεμελίωση

- **Επικινδυνότητα (risk)**
  - Η πιθανότητα ενός φορέα απειλής να εκμεταλλευτεί μια αδυναμία.

ΣΚΟΠΟΣ ΤΩΝ ΜΕΤΡΩΝ ΠΡΟΣΤΑΣΙΑΣ ΕΙΝΑΙ
Η ΜΕΙΩΣΗ ΤΗΣ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

- **Επίθεση (attack)**
  - Η εκμετάλλευση μιας αδυναμίας από έναν εισβολέα για την πραγματοποίηση μιας απειλής.
- **Αντίμετρα (countermeasures)**
  - Είναι ένας μηχανισμός ή μια διαδικασία που περιορίζει ή εξαλείφει τις πιθανότητες ενός φορέα απειλής να εκμεταλλευτεί μια αδυναμία.

Τύποι επιθέσεων

- **Παθητική παρακολούθηση**: Περιορίζεται στην απλή παρακολούθηση των διακινουμένων δεδομένων με σκοπό την υποκλοπή πληροφοριών. Είναι πολύ δύσκολα ανιχνεύσιμη.
- **Ενεργή παρακολούθηση**: Έχει τα χαρακτηριστικά της παθητικής παρακολούθησης και επιπλέον αποσκοπεί στην τροποποίηση των πληροφοριών.
- **Προσποίηση**: Ένας εισβολέας προσποιείται ότι είναι μια άλλη οντότητα με σκοπό να αποκτήσει τα δικαιώματα πρόσβασης της εξουσιοδοτημένης οντότητας.

Τύποι επιθέσεων

- **Κακόβουλο λογισμικό (Ιοί, Δούρειοι Ίπποι):** Έχει ως σκοπό να παρεμποδίσουν την ομαλή και ασφαλή λειτουργία του συστήματος (π.χ. να καταστρέψουν ή να τροποποιήσουν δεδομένα ή να υποκλέψουν δεδομένα).
- **Ανάλυση επικοινωνίας:** Αποσκοπεί στην παρακολούθηση της ροής δεδομένων και έχει στόχο την εξαγωγή συμπερασμάτων για την συγκεκριμένη επικοινωνία (ποιοι εμπλέκονται, τι είδους δεδομένα ανταλλάσσουν). Σε αντίθεση με την παθητική παρακολούθηση, δε υπάρχει πρόσβαση στα διακινούμενα δεδομένα.

Τύποι επιθέσεων

- **Άρνηση Παροχής Υπηρεσίας (Denial of Service):** Έχει ως σκοπό την παρεμπόδιση της ομαλής λειτουργίας ενός συστήματος. Αποσκοπεί στο να αποτρέψει την παροχή υπηρεσίας στους νόμιμους χρήστες.
- **Αποποίηση (Repudiation):** Κάποια οντότητα αρνείται τη συμμετοχή σε μια επικοινωνία ή σε μία συναλλαγή.

Προστασία και Ασφάλεια Συστημάτων Υπολογιστών

Κρυπτογραφία

Εισαγωγή στην κρυπτογραφία
Συμμετρική κρυπτογράφηση
Αλγόριθμοι Αντικατάστασης
Αλγόριθμοι Αντιμετάθεσης

Εισαγωγή

- Κρυπτογραφία είναι η μελέτη των μαθηματικών τεχνικών που σχετίζονται με την ασφάλεια πληροφοριών όπως είναι η εμπιστευτικότητα, ακεραιότητα, πιστοποίηση ταυτότητας δεδομένων και αποστολέα.
- Προέρχεται από τις λέξεις
  - Κρυπτό: κρυφό, μυστικό
  - Γράφος: γραφή
  - Κρυπτογραφία: η μελέτη της κρυφής γραφής

Ιστορική αναδρομή

- Πρώτες αναφορές χρονολογούνται πριν τουλάχιστον 4000 χρόνια.
- Οι αρχαίοι Αιγύπτιοι διακοσμούσαν με ιερογλυφικά στους τάφους τους για να περιγράψουν τη ζωή του αποθανόντος.
- Ο Ηρόδοτος κάνει αναφορές για κρυπτογραφημένα μηνύματα που μετέφεραν οι αγγελιοφόροι.
- Το 400π.Χ. οι Σπαρτιάτες χρησιμοποιούσαν ένα σύστημα κρυπτογράφησης μηνυμάτων για να μεταφέρουν με ασφάλεια μηνύματα στους στρατιώτες τους.

Ιστορική αναδρομή

- Πριν 2000 χρόνια ο Ιούλιος Καίσαρας χρησιμοποίησε έναν αλγόριθμο κρυπτογράφησης (αντικατάστασης) γνωστό ως Caesar cipher.
- Η πιο εκτεταμένη αναφορά σε αλγόριθμους κρυπτογράφησης στη σύγχρονη ιστορία έγινε στο Δεύτερο Παγκόσμιο Πόλεμο με τη χρήση της μηχανής Enigma.

Βασικές έννοιες

Αλγόριθμος: Σύνολο μαθηματικών κανόνων που χρησιμοποιούνται στην κρυπτογράφηση και αποκρυπτογράφηση.

Κρυπτοσύστημα: Η υλοποίηση ενός αλγορίθμου κρυπτογράφησης.

Κρυπτανάλυση: Η μελέτη των μαθηματικών τεχνικών που αποσκοπούν στην αποκρυπτογράφηση δεδομένων χωρίς τη χρήση κλειδιών.

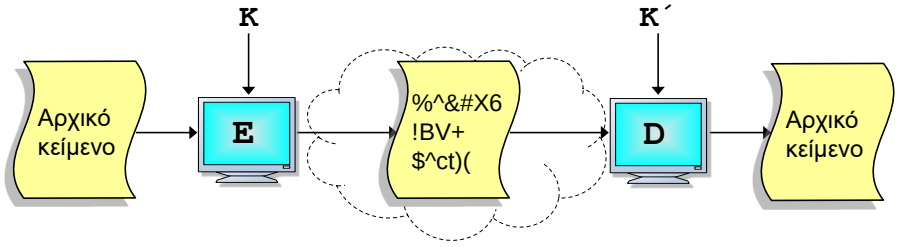
Κρυπτογράφηση: Η μετατροπή δεδομένων σε μη αναγνώσιμη μορφή.

Αποκρυπτογράφηση: Η μετατροπή δεδομένων σε αναγνώσιμη μορφή.

Plaintext: Το αρχικό μήνυμα.

Ciphertext: Το κρυπτογραφημένο μήνυμα.

Βασικό μοντέλο κρυπτογράφησης



E : Αλγόριθμος κρυπτογράφησης – γνωστός στους ενδιαφερόμενους

D : Αλγόριθμος αποκρυπτογράφησης – γνωστός στους ενδιαφερόμενους

K : Κλειδί κρυπτογράφησης

K΄ : Κλειδί αποκρυπτογράφησης

Κρυπτομήνυμα (ciphertext) $c = E_K(m)$

Αρχικό μήνυμα (plaintext) $m = D_{K'}(m)$

$$m = D_{K'}(E_K(m))$$

Η ΑΣΦΑΛΕΙΑ ΒΑΣΙΖΕΤΑΙ ΣΤΗ ΜΥΣΤΙΚΟΤΗΤΑ ΤΟΥ ΚΛΕΙΔΙΟΥ K΄

Κρυπτογραφία – Ο ρόλος των κλειδιών

- Ο κάθε αλγόριθμος έχει τις δικές του απαιτήσεις αναφορικά με το μέγεθος των κλειδιών
- Όσο μεγαλύτερο το κλειδί τόσο μεγαλύτερη ασφάλεια μας παρέχει
- Η ασφάλεια ενός κρυπτογραφημένου μηνύματος δε βασίζεται στη μυστικότητα του αλγορίθμου αλλά στην προστασία των κλειδιών

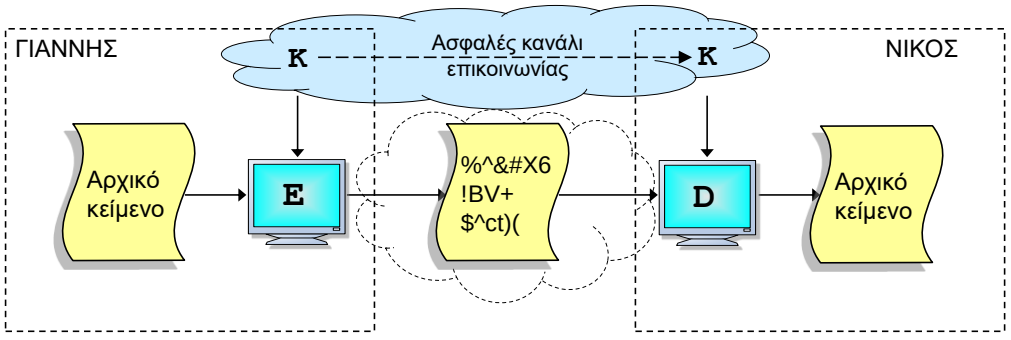
Συμμετρική κρυπτογράφηση

- Είναι επίσης γνωστή ως κρυπτογράφηση:
  - συμμετρικού κλειδιού
  - μυστικού κλειδιού
  - ενός κλειδιού
- Ένας αλγόριθμος κρυπτογράφησης λέγεται συμμετρικός εάν γνωρίζοντας το κλειδί κρυπτογράφησης k είναι υπολογιστικά "εύκολο" να προσδιορίσουμε το κλειδί αποκρυπτογράφησης k', και αντίστροφα.
- Πρακτικά, για τους περισσότερους συμμετρικούς αλγόριθμους k = k'.

Απαιτήσεις

- Η ασφαλής επικοινωνία μεταξύ δύο χρηστών με τη χρήση ενός συμμετρικού αλγορίθμου κρυπτογράφησης απαιτεί τα ακόλουθα:
  - Δυνατότητα χρήσης του ίδιου αλγορίθμου.
  - Χρήση ενός μυστικού κλειδιού το οποίο γνωρίζουν μόνο ο αποστολέας και ο παραλήπτης.
  - Ύπαρξη ενός ασφαλούς καναλιού για τη διανομή του κλειδιού.

Απαιτήσεις



Ερώτηση: Με ποιο τρόπο μπορεί ο Γιάννης να δώσει στον Νίκο το κλειδί **Κ**;

Συμμετρικά κρυπτοσυστήματα

- Πλεονεκτήματα
  - Ταχύτητα κρυπτογράφησης/αποκρυπτογράφησης.
  - Μέγεθος κλειδιών.
  - Μπορούν να χρησιμοποιηθούν ως βάση για τη κατασκευή άλλων μηχανισμών όπως παραγωγής τυχαίων αριθμών, συναρτήσεων κατακερματισμού, και ψηφιακών υπογραφών.
- Μειονεκτήματα
  - Μυστικότητα του κλειδιού.
  - Διαχείριση των κλειδιών:
    - Συμφωνία κλειδιών/Διανομή κλειδιών
    - Αλλαγή/Ανανέωση
    - Περίοδος ζωής

Επιθέσεις σε συστήματα κρυπτογράφησης

Επίθεση κρυπτογράμματος μόνο: Ο επιτιθέμενος (κρυπταναλυτής) προσπαθεί να ανακαλύψει το κλειδί ή το αρχικό κείμενο παρατηρώντας μόνο το κρυπτογράφημα. Κάθε κρυπτοσύστημα που είναι ευπαθές σε αυτό το είδος της επίθεσης λέγεται πως είναι τελείως ανασφαλές.

Επίθεση γνωστού κειμένου: Ο επιτιθέμενος (κρυπταναλυτής) έχει στην κατοχή του ένα μέρος του κειμένου και του αντίστοιχου κρυπτογραφήματος.

Επιθέσεις σε συστήματα κρυπτογράφησης

Επίθεση επιλεγμένου κειμένου: Ο επιτιθέμενος επιλέγει ένα κείμενο και αποκτά το αντίστοιχο κρυπτογράφημα. Κατόπιν, χρησιμοποιεί αυτά τα δύο για να ανακτήσει το κείμενο από άλλο κρυπτογράφημα.

Επίθεση επιλεγμένου κρυπτογραφήματος: Ο επιτιθέμενος επιλέγει το κρυπτογράφημα και αποκτά με κάποιο τρόπο πρόσβαση στο αντίστοιχο κείμενο.

Κατηγορίες συμμετρικών κρυπτοσυστημάτων

- **Block ciphers**

  Το αρχικό μήνυμα διασπάται σε κομμάτια (blocks), συγκεκριμένου μήκους *t,* και η κρυπτογράφηση γίνεται σε αυτά τα blocks του κειμένου.

- **Stream ciphers**

  Μπορούν να θεωρηθούν ως πολύ απλοί block ciphers όπου το μήκος του block είναι ίσο με 1 bit. Η κρυπτογράφηση γίνεται κρυπτογραφώντας τα bits ένα προς ένα.

Stream ciphers

- Ένας ισχυρός και αποτελεσματικός stream cipher έχει τα ακόλουθα χαρακτηριστικά:
  - Η γεννήτρια κλειδιών παράγει μεγάλες περιόδους από μη επαναλαμβανόμενα υποδείγματα.
  - Στατιστικά απρόβλεπτος.
  - Το κλειδί περιέχει τόσους 1 όσα και 0.
- Επειδή κρυπτογραφούν και αποκρυπτογραφούν ένα bit κάθε φορά, είναι πιο αποτελεσματικοί όταν υλοποιούνται σε υλικό παρά με λογισμικό.

Stream ciphers

Ο αλγόριθμος Vernam ορίζεται ως εξής:

Ένα δυαδικό μήνυμα μήκους t $m_1m_2…m_t$ κρυπτογραφείται χρησιμοποιώντας το κλειδί $k_1k_2…k_t$ ίδιου μήκους για να μας δώσει το κρυπτογράφημα $c_1c_2…c_t$ όπου:

$$c_i = m_i \oplus k_i \text{ , } 1 \le i \le t$$

Π.χ. Μήνυμα: 100111010100
Κλειδί: 010001101001
Κρυπτόγραμμα: 110110111101

Stream ciphers

- Εάν τα ψηφία του κλειδιού είναι τυχαία και ανεξάρτητα το ένα από το άλλο τότε ο Vernam cipher λέγεται one-time-pad.
- Ο one-time-pad προσφέρει τέλεια ασφάλεια απέναντι σε μια επίθεση επιλεγμένου κρυπτογράμματος. Απαραίτητη προϋπόθεση για τέλεια ασφάλεια είναι το μήκος του κλειδιού να είναι τουλάχιστον ίσο με το μήκος του μηνύματος.
- Ένας αλγόριθμος κρυπτογράφησης προσφέρει τέλεια ασφάλεια εάν το κρυπτογράφημα και το κείμενο είναι στατιστικά ανεξάρτητα.

Symmetric-key block ciphers

- Ένας block cipher είναι μία συνάρτηση που μετατρέπει τμήματα (blocks) κειμένου μεγέθους *n*-bit σε τμήματα κρυπτογραφήματος μεγέθους *n*-bit. Η συνάρτηση αυτή έχει ως παράμετρο ένα *k*-bit κλειδί.

  Κρυπτογράφηση: $c = E_K(m)$

  Αποκρυπτογράφηση: $m = D_K(c)$

  όπου *m* το μήνυμα

Τι γίνεται όμως στην περίπτωση που $m \bmod n \neq 0$;

Padding

- Πρόκειται για την τεχνική με την οποία το αρχικό κείμενο επεκτείνεται ώστε **να δημιουργηθεί ένας ακέραιος αριθμός από blocks** και έτσι να είναι δυνατή η κρυπτογράφηση του με έναν block cipher

- Π.χ. Προσθήκη ακολουθίας από bits που αποτελείται από έναν 1 και τα υπόλοιπα 0: 100000....

  Στην περίπτωση που τα δεδομένα τελειώνουν με μια τέτοια ακολουθία προστίθεται ένα ολόκληρο block

Τρόποι λειτουργίας block cipher

- Ορίζουν τον τρόπο με τον οποίο τα κρυπτογραφημένα blocks συνδέονται μεταξύ τους και επομένως αλληλοεξαρτώνται
- Καθιστούν την κρυπτογράφηση ενός κειμένου πιο ισχυρή.

Τέσσερις βασικοί τρόποι λειτουργίας:

Electronic CodeBook (ECB)
Cipher-block Chaining (CBC)
Cipher Feedback (CFB)
Output Feedback (OFB)

Λειτουργία ηλεκτρονικού βιβλίου κωδικών (Electronic CodeBook Mode; ECB mode)

Αλγόριθμος:

Είσοδος:

k-bit κλειδί K,

n-bit τμήματα κειμένου $m_1,m_2,\ldots,m_t$.

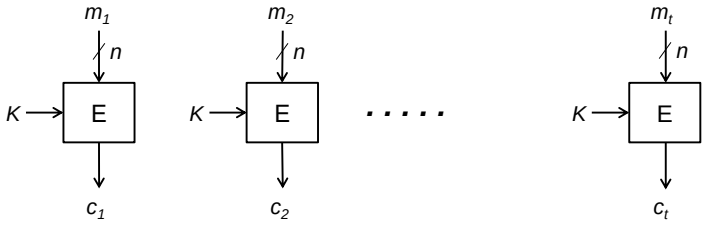
Έξοδος: Κρυπτογράφημα αποτελούμενο από τα τμήματα $c_1,c_2,\ldots,c_t$

Κρυπτογράφηση: για $1 \le j \le t$, $c_j \leftarrow E_K(m_j)$.

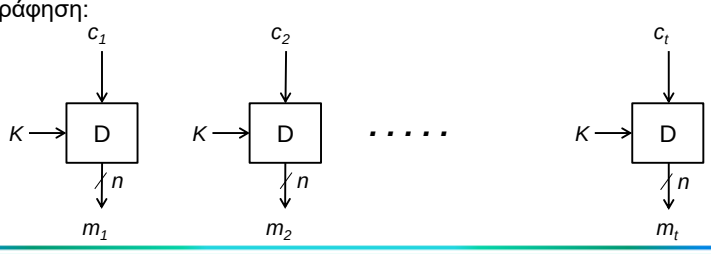
Αποκρυπτογράφηση: για $1 \le j \le t$, $m_j \leftarrow D_K(c_j)$.

Λειτουργία ηλεκτρονικού βιβλίου κωδικών (Electronic CodeBook Mode; ECB mode)

Κρυπτογράφηση:



Αποκρυπτογράφηση:



Λειτουργία ηλεκτρονικού βιβλίου κωδικών (Electronic CodeBook Mode; ECB).

- Ιδιότητες του τρόπου λειτουργίας ECB:
  - Ίδια τμήματα κειμένου δίνουν ίδια κρυπτογραφήματα (χρησιμοποιώντας το ίδιο κλειδί).
  - Κάθε τμήμα κρυπτογραφείται ανεξάρτητα από τα άλλα τμήματα.
  - Μετάδοση λάθους: ένα ή περισσότερα λάθη σε bits ενός τμήματος επηρεάζουν μόνο το συγκεκριμένο τμήμα.
- Που χρησιμοποιείται:
  - Συνιστάται η χρήση του μόνο για κρυπτογράφηση μηνυμάτων μεγέθους ενός τμήματος.

Λειτουργία κώδικα αλυσίδων μπλοκ (Cipher Block Chaining mode; CBC)

Αλγόριθμος:

Είσοδος:

k-bit κλειδί K,

n-bit διάνυσμα αρχικοποίησης IV

n-bit τμήματα κειμένου $m_1,m_2,\ldots,m_t$.

Έξοδος: Τμήματα κρυπτογραφήματος $c_1,c_2,\ldots,c_t$

Κρυπτογράφηση: για $2 \le j \le t$, $c_j \leftarrow E_K(c_{j-1} \oplus m_j)$

για $j=1$ $c_1 = E_K(\text{IV} \oplus m_1)$

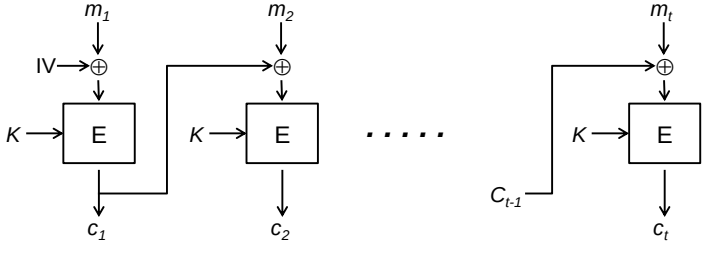
$c_2 = E_K(c_1 \oplus m_2)$ …

Αποκρυπτογράφηση: για $2 \le j \le t$, $m_j \leftarrow c_{j-1} \oplus D_K(c_j)$

για $j=1$ $m_1 \leftarrow IV \oplus D_K(c_1)$

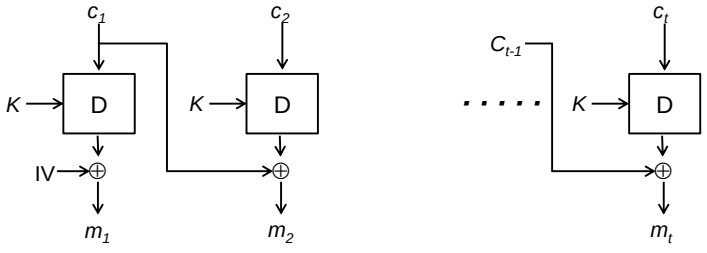
Λειτουργία κώδικα αλυσίδων μπλοκ (Cipher Block Chaining mode; CBC)

Κρυπτογράφηση:



Λειτουργία κώδικα αλυσίδων μπλοκ (Cipher Block Chaining mode; CBC)

Αποκρυπτογράφηση:



Λειτουργία κώδικα αλυσίδων μπλοκ (Cipher Block Chaining mode; CBC)

- Ιδιότητες του τρόπου λειτουργίας CBC:

  Ίδια τμήματα κρυπτογραφήματος δίνουν ίδια τμήματα κειμένου μόνο όταν έχουν κρυπτογραφηθεί χρησιμοποιώντας το ίδιο κλειδί και το ίδιο διάνυσμα αρχικοποίησης IV. Αλλάζοντας το κλειδί, το IV, ή το πρώτο τμήμα κειμένου παίρνουμε διαφορετικό κρυπτογράφημα.

  Ο μηχανισμός αλυσίδας έχει ως αποτέλεσμα το κρυπτογράφημα c_j να εξαρτάται από το x_j και όλα τα προηγούμενα τμήματα. Εάν αλλαχτεί η σειρά των τμημάτων κρυπτογραφήματος θα επηρεαστεί και η αποκρυπτογράφηση.

Λειτουργία κώδικα αλυσίδων μπλοκ (Cipher Block Chaining mode; CBC)

- Ιδιότητες του τρόπου λειτουργίας CBC:

  Διάδοση λάθους: ένα λάθος bit στο τμήμα c_j θα επηρεάσει την αποκρυπτογράφηση των τμημάτων c_j και c_{j+1} (αφού το x_j εξαρτάται από τα c_j και c_{j-1})

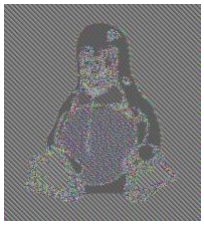
  Ανάκτηση λάθους: ο τρόπος λειτουργίας CBC είναι self-synchronizing υπό την έννοια ότι εάν έχουμε ένα λάθος στο τμήμα c_j αλλά όχι στο c_{j+1} , τότε θα έχουμε σωστή αποκρυπτογράφηση του c_{j+2} σε x_{j+2} .

Initialisation Vector

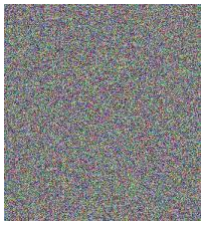
- Παρόλο που η μυστικότητα του IV δεν είναι απαραίτητη, η ακεραιότητα του είναι σημαντική γιατί αλλάζοντας το κάποιος μπορεί να προκαλέσει συγκεκριμένες αλλαγές στο πρώτο τμήμα κειμένου κατά την αποκρυπτογράφηση.

ECB vs CBC

Αρχικό κείμενο



Κρυπτογράφηση
σε ECB mode

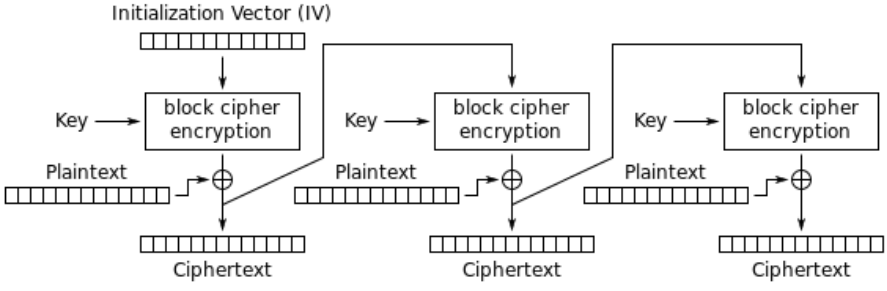


Κρυπτογράφηση
σε CBC mode

Πηγή: wikipedia.org

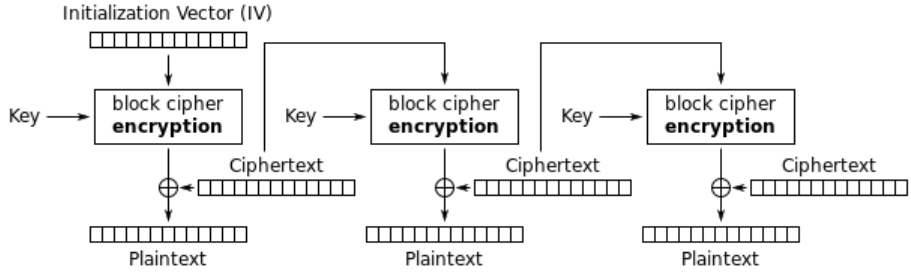
Cipher Feedback Mode (CFB)

Κρυπτογράφηση



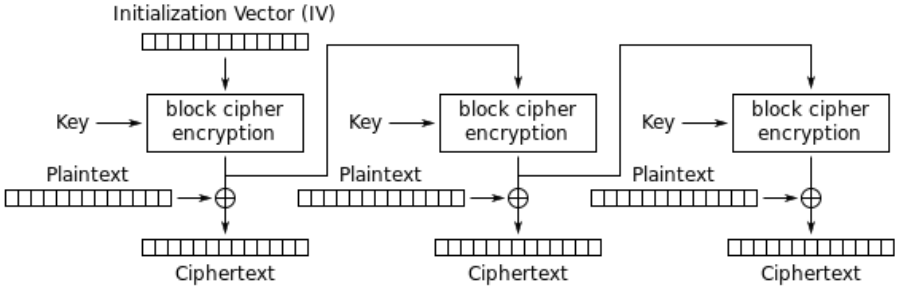
Cipher Feedback Mode

Αποκρυπτογράφηση



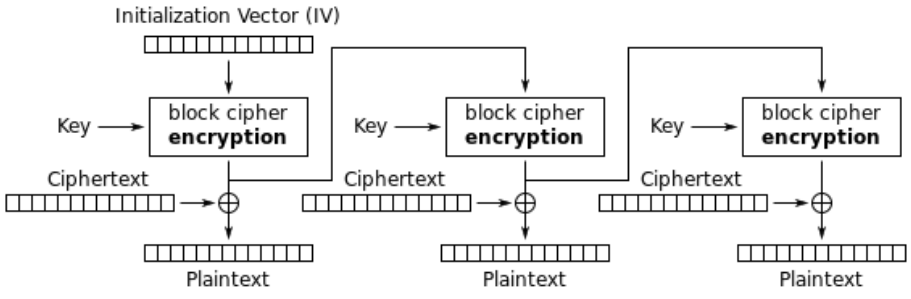
Output Feedback Mode (OFB)

Κρυπτογράφηση



Output Feedback Mode (OFB)

Αποκρυπτογράφηση



Πολλαπλή κρυπτογράφηση

Διπλή κρυπτογράφηση

$$E(m) = E_{K_2}(E_{K_1}(m))$$

Χρησιμοποιεί δύο ανεξάρτητα κλειδιά K_1 και K_2 για να κρυπτογραφήσει δύο φορές το μήνυμα

Τριπλή κρυπτογράφηση

$$E(x) = Y_{K_3}(Y_{K_2}(Y_{K_1}(x)))$$

Το Υ υποδηλώνει ότι μπορούμε να έχουμε είτε κρυπτογράφηση είτε αποκρυπτογράφηση. Η πιο συνηθισμένη χρήση είναι

$$E(x) = E_{K_3}(D_{K_2}(E_{K_1}(x))).$$

Τα κλειδιά δεν είναι απαραίτητο να είναι ανεξάρτητα και μπορούμε να έχουμε $K_1=K_3$ οπότε έχουμε τριπλή κρυπτογράφηση με διπλό κλειδί.

Εάν $K_1 \neq K_2 \neq K_3$ τότε έχουμε τριπλή κρυπτογράφηση με τριπλό κλειδί.

Κατηγορίες Block Ciphers

- Αλγόριθμοι αντικατάστασης (substitution cipher)
  - Κάθε γράμμα (ή ομάδα γραμμάτων) αντικαθίσταται από ένα άλλο γράμμα (ή ομάδα γραμμάτων).
  - Χαρακτηριστικό παράδειγμα ο Caesar cipher όπου έχουμε ολίσθηση των γραμμάτων του αλφαβήτου κατά 3 γράμματα:

    ```
    plaintext:    abcdefghijklmnopqrstuvwxyz
    ciphertext:   defghijklmnopqrstuvwxyzabc
    ```

  - **Γενίκευση του Caesar cipher** θέλει την ολίσθηση των γραμμάτων του αλφαβήτου Α κατά *k* γράμματα. Το *k* αποτελεί σε αυτήν την περίπτωση το κλειδί του αλγορίθμου αντικατάστασης:

    $$c_i = m_i + k \pmod{s}$$

    όπου m_i το *i*-οστό γράμμα του αρχικού κειμένου, c_i το *i*-οστό γράμμα του κρυπτογραφημένου κειμένου, και *s* το σύνολο των γραμμάτων του αλφαβήτου.

Symmetric-key Block Ciphers

- Αλγόριθμοι αντικατάστασης (substitution cipher)

  Ένας τύπος αλγορίθμου αντικατάστασης είναι η **μονοαλφαβητική αντικατάσταση,** όπου κάθε γράμμα αντικαθίσταται με κάποιο άλλο, "τυχαίο", γράμμα. Π.χ.

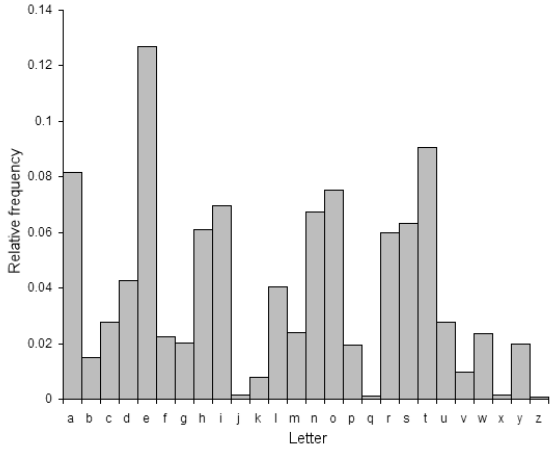
  ```
  plaintext:  a b x d e f g h i j k l m n o p q r s t u v w x y z
  ciphertext: j o e n a i z r d m w h c q v b t l k p u g y s f x
  ```

  Ο αριθμός των πιθανών κλειδιών είναι πολύ μεγάλος ($26!=4\times10^{26}$) ώστε να δοκιμάσει κάποιος όλα τα πιθανά κλειδιά.

  Ωστόσο κάποιος μπορεί να χρησιμοποιήσει στατιστικές μεθόδους για να βρεί ποιό γράμμα αντιστοιχεί σε ποιό. Για αυτό το σκοπό χρησιμοποιεί τον **αριθμό εμφάνισης των γραμμάτων σε ένα κείμενο**. Κατόπιν εξετάζει τις πιθανότητες εμφάνισης διγραμμάτων και τριγραμμάτων.

Στατιστική ανάλυση εμφάνισης γραμμάτων

- Αγγλικό αλφάβητο



Πηγή: wikipedia.org

55

Στατιστική ανάλυση εμφάνισης γραμμάτων

- Αγγλικό και ελληνικό αλφάβητο

A	B	C	D	E	F	G	H	I	J	K	L	M
8,2	1,4	2,8	3,8	12,7	2,9	2,0	5,3	6,3	0,1	0,4	3,4	2,3
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7,1	8,0	2,0	0,1	6,8	6,1	10,5	2,5	0,9	1,5	0,2	2,0	0,1
A	B	Γ	Δ	E	Z	H	Θ	I	K	Λ	M	N
12	0,8	2	1,7	8	0.5	2,9	1,3	7,8	4,2	3,3	4,4	7,9
Ξ	O	Π	P	Σ	T	Y	Φ	X	Ψ	Ω		
0,6	9,8	5,024	5,009	4,9	9,1	4,3	1,2	1,4	0,2	1,6		

56

Symmetric-key Block Ciphers

- Αλγόριθμοι αντικατάστασης (substitution cipher)
  - Στην **πολυαλφαβητική αντικατάσταση** (παράδειγμα της οποίας αποτελεί ο απλός Vigenere) έχουμε ένα κλειδί χαρακτήρων μεγέθους t $k_1k_2…k_t$. Η μετατροπή του κειμένου $m=m_1m_2m_3…$ σε κρυπτογραφημένο μήνυμα $c=c_1c_2c_3…$ γίνεται ως

$$c_1=m_1+k_t \bmod s$$

όπου s είναι το μέγεθος του αλφαβήτου μας. Ο αλγόριθμος λέμε ότι έχει περίοδο t.

Vigenère cipher

	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω
Α	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω
Β	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α
Γ	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β
Δ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ
Ε	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ
Ζ	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε
Η	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ
Θ	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η
Ι	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ
Κ	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι
Λ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ
Μ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ
Ν	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ
Ξ	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν
Ο	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ
Π	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο
Ρ	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π
Σ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ
Τ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ
Υ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ
Φ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ
Χ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ
Ψ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ
Ω	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ

Symmetric-key Block Ciphers

- Αλγόριθμοι αντιμετάθεσης (transposition)
  - Απλή **αναδιάταξη των γραμμάτων ενός κειμένου**. Για έναν απλό αλγόριθμο αντιμετάθεσης με περίοδο *t*, η κρυπτογράφηση περιλαμβάνει την ομαδοποίηση του κειμένου σε τμήματα των *t* χαρακτήρων το καθένα, και εφαρμογή σε κάθε ένα από αυτά τα τμήματα μιας απλής αντικατάστασης *e* πάνω στους αριθμούς *1* ως *t*.
  - Ένας αλγόριθμος αντιμετάθεσης διατηρεί τον αριθμό των συμβόλων μέσα σε ένα τμήμα και επομένως μπορεί εύκολα να κρυπταναλυθεί.

    Π.χ. Υποθέστε ένα απλό αλγόριθμο αντιμετάθεσης με περίοδο t = 6 και e = (641352). Το μήνυμα "ΚΡΥΠΤΟΓΡΑΦΙΑ" θα δώσει το κρυπτογράφημα "ΟΠΚΥΤΡΑΦΓΑΙΑ".

Symmetric-key Block Ciphers

- **Κώδικας γινομένου (Product cipher)**: Συνδυάζει δύο ή περισσότερες μετατροπές με τέτοιο τρόπο ώστε το αποτέλεσμα να είναι πιο ασφαλές από ότι είναι κάθε μια από τις μετατροπές που απαρτίζουν τον κώδικα γινομένου. Π.χ. Ένας κώδικας γινομένου μπορεί να αποτελείται από συνδυασμό κωδικών αντικατάστασης και αντιμετάθεσης. Σε μια τέτοια περίπτωση μπορούμε αρχικά να κρυπτογραφήσουμε το αρχικό κείμενο με τον κώδικα αντικατάστασης και το αποτέλεσμα να το ξανακρυπτογραφήσουμε χρησιμοποιώντας τον κώδικα αντιμετάθεσης.

Symmetric-key Block Ciphers

- **Επαναληπτικός block cipher (iterated block cipher):** ένας block cipher όπου έχουμε την ακολουθιακή επανάληψη μιας εσωτερικής συνάρτησης η οποία λέγεται κυκλική συνάρτηση (round function).

Symmetric-key Block Ciphers

- **Κώδικας Feistel:** Είναι ένας επαναληπτικός αλγόριθμος που "αντικαθιστά" 2*t*-bit κειμένου (L_0, R_0) μεγέθους *t*-bit το καθένα, σε ένα κρυπτογράφημα (L_r ,R_r) μέσω μιας διαδικασίας *r*-κύκλων, όπου $r \geq 1$.
  Για $1 \leq i \leq r$

$$L_i = R_{i-1},\ R_i = L_{i-1} \oplus f(R_{i-1},\ K_i)$$

  όπου κάθε κλειδί K_i προκύπτει από το κλειδί κρυπτογράφησης *K*. Η συνάρτηση *f* μπορεί να είναι ένας κώδικας γινομένου.
- Τυπικά $r \geq 3$ και είναι ζυγός αριθμός.

DES

- Ο Data Encryption Standard (DES) είναι ο πιο γνωστός block cipher συμμετρικού κλειδιού. Ορίζεται στο FIPS 46-2.
- Επεξεργάζεται τμήματα κειμένου μεγέθους n = 64bits και παράγει τμήματα κρυπτογραφημένου κειμένου μεγέθους επίσης 64bits.
- Το μέγεθος των κλειδιών που χρησιμοποιεί είναι 64bits αλλά 8 από αυτά (8,16,...,64) χρησιμοποιούνται ως bits ισοτιμίας (parity). Επομένως ο πραγματικός αριθμός των bits του κλειδιού είναι 56bits.
- Ο σχεδιασμός του βασίστηκε στους κώδικες γινομένου, και στον κώδικα Feistel.

DES

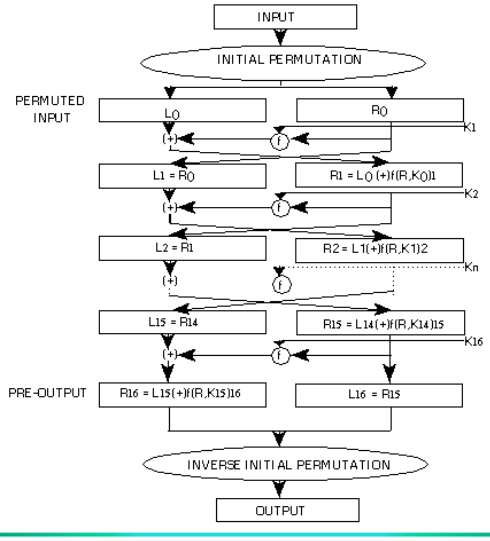
- Συνοπτική περιγραφή:
  - Η διαδικασία της κρυπτογράφησης γίνεται σε 16 επαναλήψεις.
  - Από το κλειδί εισόδου K δημιουργούνται βάσει κάποιων αντιμεταθέσεων 16 48-bit κλειδιά, ένα για κάθε επανάληψη.
  - Η κρυπτογράφηση αρχίζει με μια αντιμετάθεση του κειμένου των 64-bit.
  - Το αποτέλεσμα διασπάται σε 2 32-bit τμήματα L_0 και R_0.
  - Οι 16 επαναλήψεις είναι λειτουργικά ταυτόσημες όπου σε κάθε επανάληψη οι 32-bit είσοδοι L_{i-1} και R_{i-1} της προηγούμενης επανάληψης παράγουν 32-bit εξόδους L_i και R_i ως εξής:

$$L_i = R_{i-1}; \quad R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

DES

- Συνοπτική περιγραφή:
  - Η συνάρτηση *f* είναι μια σειρά από αντικαταστάσεις (βάσει κάποιων κουτιών αντικατάστασης ή S-boxes) και μια αντιμετάθεση.
  - Τα 8 S-boxes αποτελούν την καρδιά της ασφάλειας του DES.
  - Ο αλγόριθμος τελειώνει με μια αντιμετάθεση που είναι ακριβώς αντίθετη από την αρχική.
  - Η αποκρυπτογράφηση του DES γίνεται με τον ίδιο ακριβώς τρόπο όπως και η κρυπτογράφηση μόνο που τα 16 κλειδιά χρησιμοποιούνται αντίστροφα (από το K_{16} στο K_1).

DES



DES

- Αδύναμα κλειδιά του DES: είναι αυτά όπου για κάθε μήνυμα x, $E_K(E_K(x)) = x$
- Ημι-αδύναμα κλειδιά του DES: είναι ένα ζευγάρι κλειδιών K_1, K_2, για τα οποία $E_{K1}(E_{K2}(x)) = x$.
- Ο DES έχει 4 αδύναμα κλειδιά και έξι ζεύγη από ημι-αδύναμα.
- Λόγω της βελτιστοποίησης μεθόδων κρυπτανάλυσης και της υπολογιστικής ισχύος η οποία καθιστά επιθέσεις εφικτές συνιστάται η χρήση του 3-DES ή TDES (E-D-E) με διπλό ή με τριπλό κλειδί.

DES

- Το 1998 ερευνητές κατάφεραν να σπάσουν σε εργαστήριο ένα DES κλειδί σε 56 ώρες. Το 2007, ένα DES κλειδί μπορούσε να σπάσει μέσα σε 6 μέρες χρησιμοποιώντας ένα server αξίας < $10,000.

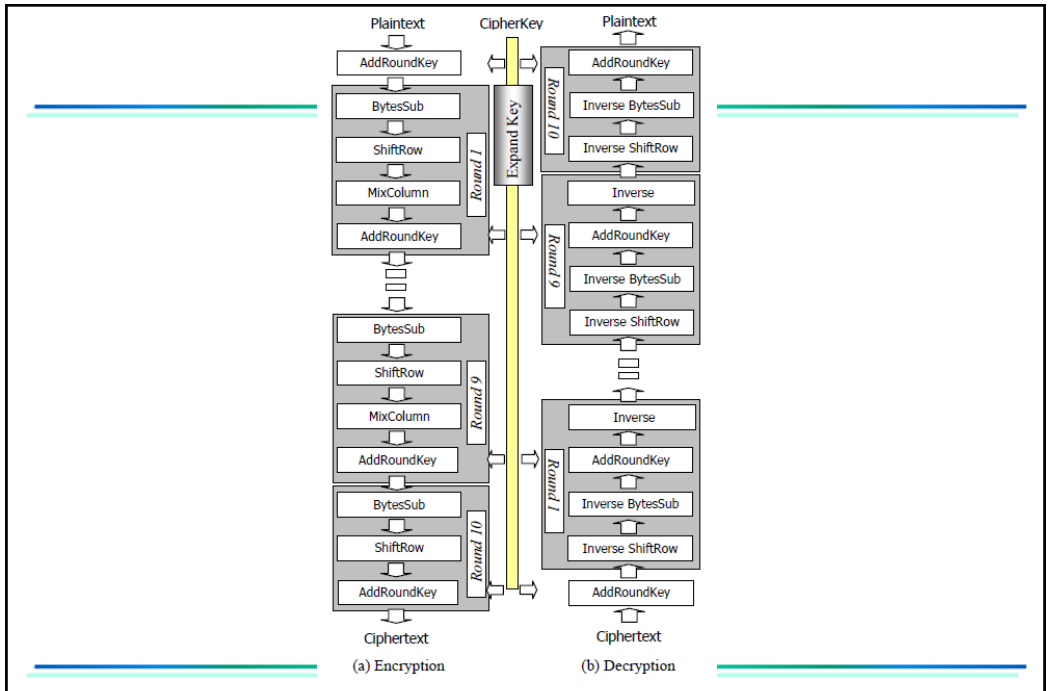
- Στη Ρωσία υπάρχει μια συμμορία που παρέχει υπηρεσίες σπασίματος κλειδιών DES για POS PEDs. Υπόσχονται την παράδοση των κλειδιών μέσα σε 72 ώρες από τη στιγμή που θα παραλάβουν τη συσκευή. Το κόστος ανέρχεται σε $250.000, ενώ υπόσχονται και επιστροφή χρημάτων.

AES – Advanced Encryption Standard

- Πρόκειται για τον αντικαταστάτη του DES. Ορίζεται από τον αλγόριθμο *Rijndael*. Ήταν ο νικητής ενός διαγωνισμού του NIST (National Institute of Standards and Technology).
- Κρυπτογραφεί τμήματα των 128bits χρησιμοποιώντας κλειδιά των 128, 192, και 256 bits.
- Προσφέρει μεγαλύτερη ασφάλεια από τον DES.
- Είναι ανθεκτικός σε όλες τις γνωστές μεθόδους κρυπτανάλυσης.
- Είναι σχεδιαστικά πιο απλός από τον DES.
- Είναι σχεδιασμένος για καλή απόδοση όταν υλοποιείται τόσο σε λογισμικό όσο και σε υλικό.

AES

- Χρησιμοποιεί πίνακες από bytes (γνωστοί ως States) μεγέθους 4x4, για να κάνει τις πράξεις σε κάποιες επαναλήψεις ο αριθμός των οποίων εξαρτάται από το μέγεθος του κλειδιού (10 για τον AES-128, 12 για τον AES-192, και 14 για τον AES-256).
- Το κλειδί της κάθε επανάληψης προκύπτει από το αρχικό κλειδί.
- Σε κάθε επανάληψη έχουμε τις ακόλουθες μετατροπές:
  - Αντικατάσταση bytes χρησιμοποιώντας ένα S-box
  - Ολίσθηση γραμμών
  - Ανάμειξη των δεδομένων σε κάθε στήλη του πίνακα
  - XOR του πίνακα με το κλειδί.



Προστασία και Ασφάλεια Συστημάτων Υπολογιστών

Κρυπτογραφία

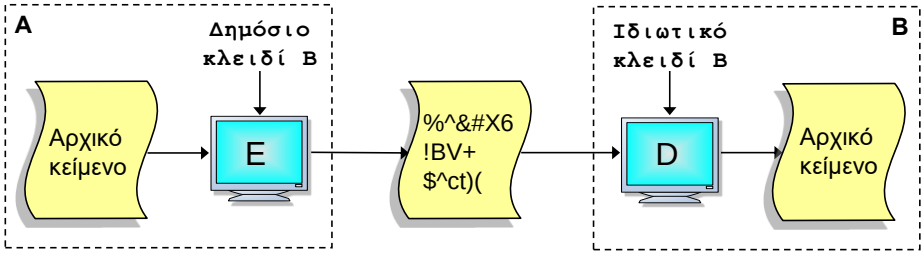
Κρυπτογραφία δημοσίου κλειδιού
Ψηφιακές υπογραφές
Συναρτήσεις κατακερματισμού

Κρυπτογραφία δημοσίου κλειδιού

- Κάθε οντότητα έχει ένα ζεύγος κλειδιών
  - ένα δημόσιο κλειδί *e* και
  - ένα ιδιωτικό κλειδί *d*.
- Σε ασφαλή κρυπτοσυστήματα, **ο υπολογισμός του *d* δεδομένου του *e* είναι υπολογιστικά αδύνατος**. Το δημόσιο κλειδί *e* ορίζει έναν μετασχηματισμό κρυπτογράφηση E_e , ενώ το ιδιωτικό κλειδί ορίζει έναν μετασχηματισμό αποκρυπτογράφησης D_d.

Κρυπτογραφία δημοσίου κλειδιού

- Τυπικές χρήσεις:
  - Ψηφιακές υπογραφές
  - Κρυπτογράφηση
    - Ο αποστολέας A κρυπτογραφεί με το δημόσιο κλειδί του παραλήπτη B, P_B.
    - Ο παραλήπτης αποκρυπτογραφεί με το ιδιωτικό του κλειδί, S_B



Κρυπτογραφία δημοσίου κλειδιού

- Όταν ο αποστολέας A θέλει να στείλει ένα μήνυμα m στον B θα πρέπει να πάρει ένα **αυθεντικοποιημένο** αντίγραφο του δημοσίου κλειδιού e του B και χρησιμοποιώντας τον μετασχηματισμό κρυπτογράφησης E_e παίρνει το κρυπτογράφημα $c = E_e(m)$.
- Για να αποκρυπτογραφήσει το μήνυμα ο Β πρέπει να χρησιμοποιήσει το ιδιωτικό του κλειδί d και το μετασχηματισμό αποκρυπτογράφησης D_d για να πάρει το μήνυμα $m = D_d(c)$.

Κρυπτογραφία δημοσίου κλειδιού

- Πλεονεκτήματα
  - Μόνο το μυστικό κλειδί πρέπει να κρατηθεί κρυφό
  - Εύκολη διαχείριση κλειδιών με τη βοήθεια μιας τρίτης έμπιστης οντότητας
  - Ανάλογα με τη χρήση του αλγορίθμου ένα ζεύγος μυστικού/δημοσίου κλειδιού μπορεί να χρησιμοποιηθεί για μεγάλες χρονικές περιόδους σε αντίθεση με τα κλειδιά ενός συμμετρικού κρυπτοσυστήματος που απαιτούν τακτικές αλλαγές.
  - Μπορούν να χρησιμοποιηθούν για ψηφιακές υπογραφές εξασφαλίζοντας μη αποποίηση.

Κρυπτογραφία δημοσίου κλειδιού

- Μειονεκτήματα
  - Είναι χαρακτηριστικά πιο αργοί σε σχέση με τους αλγορίθμους συμμετρικής κρυπτογράφησης.
  - Το μέγεθος των κλειδιών (είναι πολύ μεγαλύτερα από τα κλειδιά που χρησιμοποιούν οι αλγόριθμοι συμμετρικής κρυπτογράφησης).
  - Δεν υπάρχουν αποδείξεις ότι οι αλγόριθμοι είναι ασφαλείς (αν και το ίδιο μπορεί να ειπωθεί και για τους συμμετρικούς αλγορίθμους).
  - Απαιτεί τη χρήση πρόσθετων μηχανισμών που εξασφαλίζουν την αυθεντικοποίηση του δημοσίου κλειδιού.

RSA – Rivest, Shamir, Adleman

- Η ασφάλεια του βασίζεται στο πρόβλημα της παραγοντοποίησης μεγάλων ακεραίων.
- Το ζεύγος κλειδιών αποτελείται από:
  - μυστικό κλειδί *d* και
  - δημόσιο κλειδί (*n, e*), όπου *n* είναι το modulus και *e* ο εκθέτης κρυπτογράφησης.
- Το modulus *n* προσδιορίζει το μέγεθος του κλειδιού που χρησιμοποιούμε. Τυπικά μεγέθη είναι τα 512, 768, 1024, 2048, 4096 bits.
  - Για ασφαλή μεγέθη κλειδιών: http://www.keylength.com/

RSA - Κρυπτογράφηση

- Κατά την κρυπτογράφηση ο αποστολέας:
  - Παίρνει ένα αυθεντικοποιημένο αντίγραφο του δημοσίου κλειδιού του παραλήπτη.
  - Αναπαριστά το μήνυμα ως έναν ακέραιο m (μέσα στο διάστημα [0, n-1])
  - Κρυπτογράφηση

$$c = m^e \bmod n$$

  - Αποκρυπτογράφηση

$$m = c^d \bmod n$$

RSA

- Η ασφάλεια του RSA αλγορίθμου βασίζεται στη δυσκολία του να βρούμε τους πρώτους αριθμούς p και q από τους οποίους προκύπτει ο $n = pq$.
- Δημιουργία κλειδιών:
  - Επιλέγουμε δύο μεγάλους τυχαίους πρώτους αριθμούς p και q, του ίδιου περίπου μεγέθους.
  - Υπολογίζουμε $n = pq$ και φ = $(p-1)(q-1)$.
  - Επιλέγουμε έναν τυχαίο ακέραιο e, $1<e<\varphi$, τέτοιο ώστε $\gcd(e, \varphi) = 1$.
  - Υπολογίζουμε τον μοναδικό ακέραιο d $(1< d <\varphi)$ τέτοιο ώστε $ed = 1 \pmod{\varphi}$.
  - Το δημόσιο αποτελείται από τα (n, e) και το ιδιωτικό από το d.

Τυπικά το e επιλέγεται να είναι $e=3$ ή $e=2^{16}+1$

RSA - Παράδειγμα

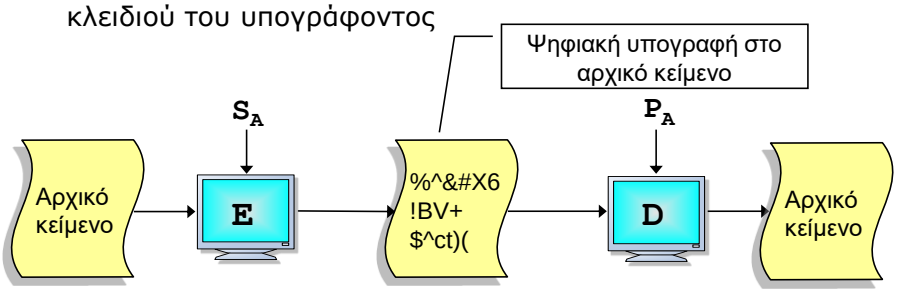
- Δημιουργία κλειδιών:
  - Επιλέγουμε $p = 2357$ και $q = 2551$.
  - Υπολογίζουμε $n = pq = 6012707$ και $\varphi = (p-1)(q-1) = 6007800$.
  - Επιλέγουμε $e = 3674911$, τέτοιο ώστε $\gcd(e, \varphi) = 1$.
  - Υπολογίζουμε $d = 422191$ $(1 < d < \varphi)$: $ed = 1 \pmod{\varphi}$.
  - Το δημόσιο αποτελείται από τα ($n=6012707$, $e=3674911$) και το ιδιωτικό από το d=422191.
- Για το μήνυμα m=5234673:
  - $c = m^e \bmod n = 5234673^{3674911} \bmod 6012707 = 3650502$
  - $m = c^d \bmod n = 3650502^{422191} \bmod 6012707 = 5234673$

Ψηφιακές υπογραφές – Digital signatures

- Είναι ο μηχανισμός που μας επιτρέπει να εξάγουμε συμπεράσματα όσον αφορά την σχέση κάποιων δεδομένων με κάποια οντότητα.
- Εξασφαλίζουν
  - αυθεντικοποίηση,
  - ακεραιότητα, και
  - μη-αποποίηση (κάτω από ορισμένες προϋποθέσεις)

Ψηφιακές υπογραφές και κρυπτογραφία δημοσίου κλειδιού

- Δημιουργία
  - Ο υπογράφων κρυπτογραφεί το μήνυμα κάνοντας χρήση του ιδιωτικού του κλειδιού
- Επαλήθευση
  - Με την αποκρυπτογράφηση κάνοντας χρήση του δημοσίου κλειδιού του υπογράφοντος



Ψηφιακές υπογραφές – Digital signatures

- **Βασική ιδιότητα**:
  - Είναι υπολογιστικά αδύνατο για κάποια οντότητα διαφορετική του υπογράφοντος *A* να μπορέσει να βρει, για κάποιο μήνυμα *m* μια υπογραφή *s* τέτοια ώστε η επαλήθευση της με το δημόσιο κλειδί της *A* να είναι επιτυχής.
- Άλλες ιδιότητες:
  - Θα πρέπει να είναι υπολογιστικά εύκολη η διαδικασία της επαλήθευσης της υπογραφής.
  - Θα πρέπει να έχει διάρκεια ζωής: Θα πρέπει να είναι υπολογιστικά ασφαλής μέχρι η υπογραφή να μην είναι πλέον απαραίτητη για τον αρχικό της σκοπό.

Ψηφιακές υπογραφές – Digital signatures

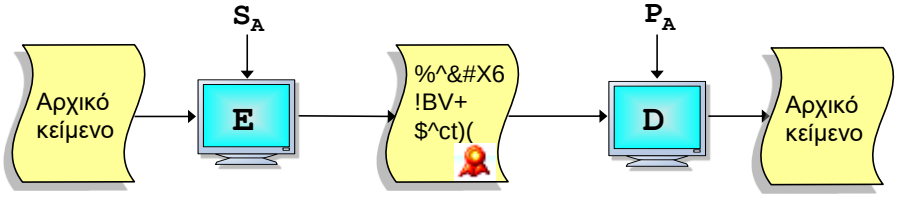
- Οι ψηφιακές υπογραφές χρησιμεύουν στην επίλυση των διαφορών με τη χρήση έμπιστων τρίτων οντοτήτων. Απαραίτητη προϋπόθεση είναι:
  - να ισχύει η βασική ιδιότητα των ψηφιακών υπογραφών,
  - να υπάρχει ένα αυθεντικοποιημένο αντίγραφο του δημοσίου κλειδιού επαλήθευσης της υπογραφής και να είναι διαθέσιμη η συνάρτηση επαλήθευσης της υπογραφής,
  - το μυστικό κλειδί υπογραφής να έχει παραμείνει μυστικό.

86

Ψηφιακές υπογραφές – Digital signatures

- Δύο κατηγορίες ψηφιακών υπογραφών:

  Ψηφιακές υπογραφές με ανάκτηση μηνύματος (with message recovery). Το αρχικό μήνυμα δεν αποτελεί είσοδο στη διαδικασία επαλήθευσης της υπογραφής, αλλά ανακτάται κατά τη διαδικασία επαλήθευσης της υπογραφής. Δεν απαιτείται μεταφορά του αρχικού μηνύματος για την επαλήθευση της υπογραφής.



87

Ψηφιακές υπογραφές – Digital signatures

- Δύο κατηγορίες ψηφιακών υπογραφών:

  Ψηφιακές υπογραφές με προσθήκη (with appendix). Σε αυτές τις υπογραφές απαιτείται η γνώση του αρχικού μηνύματος για την επαλήθευση της υπογραφής. Έτσι είναι απαραίτητο μαζί με την υπογραφή να μεταφέρουμε με κάποιο τρόπο και το μήνυμα (προστατευμένο ή μη).

  Τυπικά υπογράφουμε το αποτέλεσμα μιας συνάρτησης κατακερματισμού η είσοδος της οποίας είναι το αρχικό μήνυμα.

Hash functions

- Μια συνάρτηση κατακερματισμού ή σύνοψης ή ανάδευσης (**hash function** *h*) είναι μια συνάρτηση η οποία έχει τουλάχιστον τις δύο ακόλουθες ιδιότητες (δε κάνει χρήση κάποιου κλειδιού κρυπτογράφησης):
  - **Συμπίεση**: Η *h* μετατρέπει ένα μήνυμα αυθαίρετου μεγέθους *x*, σε ένα μήνυμα σταθερού μεγέθους.
  - **Ευκολία υπολογισμού:** Δεδομένης της *h* και του μηνύματος *x* είναι εύκολο να υπολογίσουμε το *h(x)*.

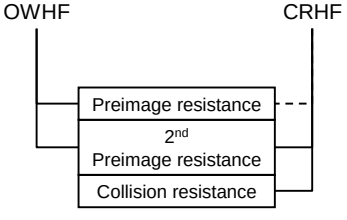
Hash functions

- Άλλες επιθυμητές ιδιότητες των hash functions είναι:
  - **Preimage resistance**: Δεδομένου του *h(x)* είναι υπολογιστικά αδύνατο να βρεθεί μια ακολουθία *x* η οποία να δίνει αποτέλεσμα *h(x)*
  - **2nd preimage resistance**: Δεδομένου του *x* είναι υπολογιστικά αδύνατο να βρεθεί μια δεύτερη ακολουθία *x′* τέτοια ώστε *h(x)=h(x′)*
  - **Collision resistance**: Είναι υπολογιστικά αδύνατο να βρεθούν δύο διαφορετικές *ακολουθίες x* και *x′* τέτοιες ώστε *h(x)=h(x′)*

Hash functions

- Μια μονόδρομη συνάρτηση κατακερματισμού (**one-way hash function**) είναι μια hash function με τις παρακάτω πρόσθετες ιδιότητες:
  - Preimage resistance
  - 2nd preimage resistance
- Μια συνάρτηση κατακερματισμού χωρίς συγκρούσεις (**collision resistant hash function**) είναι μια hash function με τις παρακάτω πρόσθετες ιδιότητες:
  - 2nd preimage resistance
  - collision resistance

  Τυπικά ωστόσο έχει και την ιδιότητα του Preimage resistance



Συναρτήσεις κατακερματισμού

- Δύο βασικοί τύποι συναρτήσεων κατακερματισμού:
  - **Block cipher based**: MDC-2, MDC-4 (βασίζονται στον DES και δίνουν hash-values των 128bits).
  - **Customised hash functions**: Σχεδιάζονται αποκλειστικά για αυτό το σκοπό: MD4 (128), MD5 (128), SHA-1 (160), SHA-224, SHA-256, SHA-384, SHA-512, RIPEMD-160 (160).
- Οι πιο συχνά χρησιμοποιούμενες συναρτήσεις είναι οι customised hash functions.

Συναρτήσεις κατακερματισμού

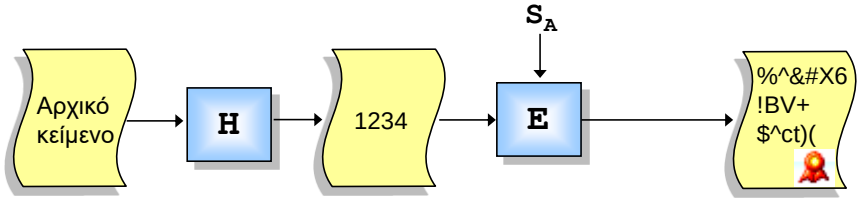
- Η πιο γνωστή επίθεση σε συναρτήσεις κατακερματισμού είναι η επίθεση γενεθλίων (birthday attack) η οποία βασίζεται στο εξής παράδοξο:
  - Ένα σε μια αίθουσα θέλουμε να βρούμε κάποιον που να έχει την ίδια ημέρα γενέθλια με εμάς τότε στην αίθουσα θα πρέπει να υπάρχουν 183 άτομα έτσι ώστε οι πιθανότητες να βρούμε κάποιον να είναι πάνω από 50%.
  - Ο αριθμός των ατόμων που πρέπει να είναι μέσα σε μια αίθουσα ώστε οι πιθανότητες δύο από αυτούς να έχουν γενέθλια την ίδια μέρα να είναι πάνω από 50% είναι **μόλις 23**.

Συναρτήσεις κατακερματισμού

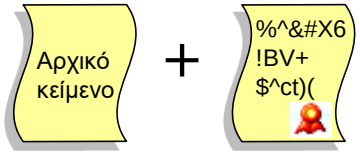
- Η επίθεση γενεθλίων σε συναρτήσεις κατακερματισμού εφαρμόζεται ως εξής:
  - Ο επιτιθέμενος προσπαθεί να βρει δύο οποιαδήποτε μηνύματα *m* και *m΄* για τα οποία *h*(*m*)=*h*(*m΄*). Με αυτόν τον τρόπο μπορεί αργότερα να δηλώσει ότι αυτό που έστειλε είναι το *m΄* και όχι το *m*.
- Εάν η συνάρτηση κατακερματισμού παράγει ένα αποτέλεσμα των *m* bits τότε η εύρεση ενός μηνύματος το οποίο δίνει μια συγκεκριμένη τιμή κατακερματισμού απαιτεί τον κατακερματισμό 2^m τυχαίων μηνυμάτων. Η εύρεση δύο οποιονδήποτε μηνυμάτων τα οποία δίνουν την ίδια τιμή κατακερματισμού απαιτεί τον κατακερματισμό μόλις $2^{m/2}$ τυχαίων μηνυμάτων.

Digital Signatures with Appendix

Δημιουργία υπογραφής

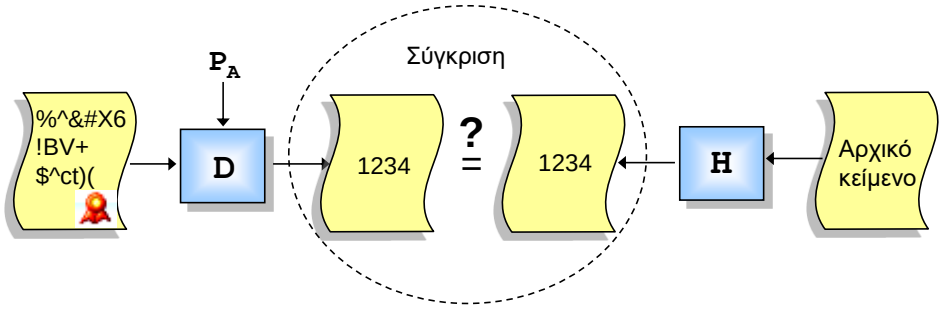


Αποστολή



Digital Signatures with Appendix

Επαλήθευση



Ψηφιακές Υπογραφές RSA (RFC 3447)

- Υπογραφή με τη χρήση του προτύπου **PKCS#1 (υπογραφή με προσθήκη)**.
- Διάταξη (format) δεδομένων – προετοιμασία block δεδομένων.
  - Έστω *k* το μήκος του modulus σε bytes ($k \geq 11$).
  - Τα δεδομένα είναι μια ακολουθία από bytes D, μήκους $||D|| \leq k-11$.
  - BT είναι ένα byte το οποίο είναι ίσο με 00 ή 01 (σε δεκαεξαδική μορφή).
  - PS είναι ένα **συμπλήρωμα (padding)**: μια ακολουθία από bytes το μήκος της οποίας είναι ίσο με $k-3-||D||$.
    - Εάν το BT είναι ίσο με 00 τότε όλα τα bytes του συμπληρώματος είναι 00. Εάν το BT είναι ίσο με 01 τότε όλα τα bytes του PS είναι ίσα με ff.

Ψηφιακές Υπογραφές RSA

- Το διαμορφωμένο μπλοκ δεδομένων θα είναι:

  EB=00||BT||PS||00||D.

  - Ο λόγος που το αρχικό byte είναι ίσο με 00 είναι για να σιγουρέψουμε ότι η ακολουθία EB όταν θα μετατραπεί σε ακέραιο θα είναι μικρότερη από το modulus n του αλγορίθμου.
  - Εάν BT=00, τότε τα δεδομένα D θα πρέπει είτε να αρχίζουν με ένα μη μηδενικό byte είτε να γνωρίζουμε το μέγεθος τους.
  - Εάν BT=01 τότε δεν υπάρχει πρόβλημα. Για αυτό το λόγο συνιστάται η χρήση του BT=01.

Ψηφιακές Υπογραφές RSA

Παράδειγμα: εάν το modulus n είναι μεγέθους 1024 bits. Τότε k=128. Εάν ||D|| = 20 bytes, τότε ||PS|| = 105 bytes, και ||EB||=128 bytes.

Διαδικασία υπογραφής με το PKCS#1:

1. **Κατακερματισμός μηνύματος**: Το μήνυμα M κατακερματίζεται για να πάρουμε την ακολουθία bytes MD.
2. **Κωδικοποίηση του κατακερματισμένου μηνύματος**: Το μήνυμα κωδικοποιείται σύμφωνα με τους κανόνες BER (Basic Encoding Rules) για να μας δώσει μια ακολουθία bytes D.
3. **Διάταξη του μπλοκ δεδομένων**: Η ακολουθία D τροποποιείται στην ακολουθία EB με την προσθήκη των απαραίτητων bytes.
4. **Μετατροπή των bytes σε ακέραιο *m***
5. **Υπολογισμός RSA**: $s=m^d \bmod n$.
6. **Μετατροπή του ακεραίου σε bytes.**

Ψηφιακές Υπογραφές RSA

Διαδικασία επαλήθευσης υπογραφής *S* με το PKCS#1:

1. **Μετατροπή της ακολουθίας bytes σε ακέραιο**:
   1. Εάν ο αριθμός των bits στην S δεν είναι πολλαπλάσιο του 8 τότε η επαλήθευση απέτυχε.
   2. Μετέτρεψε την S σε έναν ακέραιο s όπως στο βήμα 4 της υπογραφής.
   3. Εάν s>n τότε η επαλήθευση απέτυχε.
2. **Υπολογισμός RSA**: $m=s^e \bmod n$.
3. **Μετατροπή του ακεραίου σε ακολουθία bytes**: Η μετατροπή γίνεται όπως στο βήμα 6 της υπογραφής. Το αποτέλεσμα είναι *k* bytes.

Ψηφιακές Υπογραφές RSA

Διαδικασία επαλήθευσης υπογραφής *S* με το PKCS#1:

4. **Μετάφραση (parsing)**: Μετέφρασε το EB σε ένα block τύπου BT, μια ακολουθία συμπληρώματος PS, και τα δεδομένα D.
   1. Εάν το EB δε μπορεί να μετατραπεί μοναδικά τότε η επαλήθευση απέτυχε.
   2. Εάν το BT δε είναι 00 ή 01 η επαλήθευση απέτυχε.
   3. Εάν το PS<8 bytes ή δεν είναι συμβατό με το BT η επαλήθευση απέτυχε.
5. **Αποκωδικοποίηση μηνύματος**: Σύμφωνα με το BER για να πάρουμε την ταυτότητα της συνάρτησης κατακερματισμού και το κατακερματισμένο μήνυμα MD (τη σύνοψη μηνύματος).
6. **Κατακερματισμός μηνύματος**: Το μήνυμα M κατακερματίζεται για να πάρουμε την ακολουθία bytes MD΄. Εάν MD΄= MD τότε η υπογραφή είναι δεκτή.

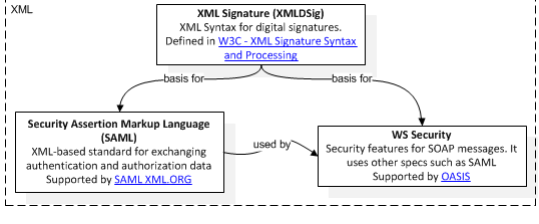
Ψηφιακές Υπογραφές DSA

- **Digital Signature Algorithm**: Είναι το πρώτο σχήμα ψηφιακών υπογραφών το οποίο αναγνωρίστηκε από κυβέρνηση, των ΗΠΑ. Είναι μια **υπογραφή με προσθήκη** και αποτελεί μια παραλλαγή του ElGamal.
- Για συνάρτηση κατακερματισμού χρησιμοποιεί την SHA-1.

XML Dsig

- Ορίζει τον τρόπο με τον οποίο υπογράφουμε ψηφιακά κάποια δεδομένα, π.χ. XML έγγραφα, σύμφωνα με το πρότυπο XML.

```
<Signature ID?>
     <SignedInfo>
       <CanonicalizationMethod/>
       <SignatureMethod/>
       (<Reference URI? >
         (<Transforms>)?
         <DigestMethod>
         <DigestValue>
       </Reference>)+
     </SignedInfo>
     <SignatureValue>
    (<KeyInfo>)?
    (<Object ID?>)*
   </Signature>
```



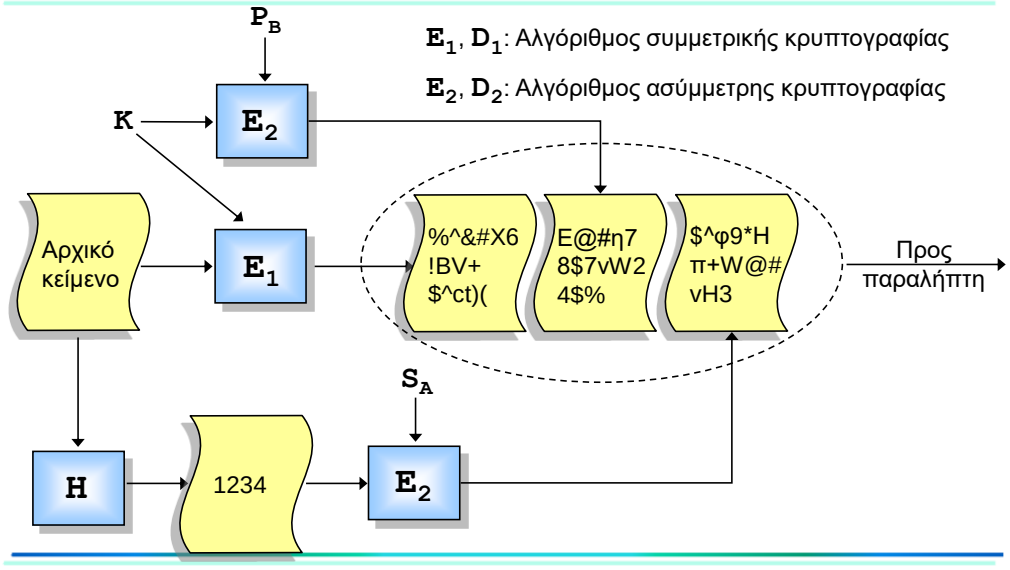
Στην πράξη

- Πως μπορούμε να παρέχουμε εμπιστευτικότητα, ακεραιότητα, και αυθεντικοποίηση σε ένα μήνυμα;

Στην πράξη

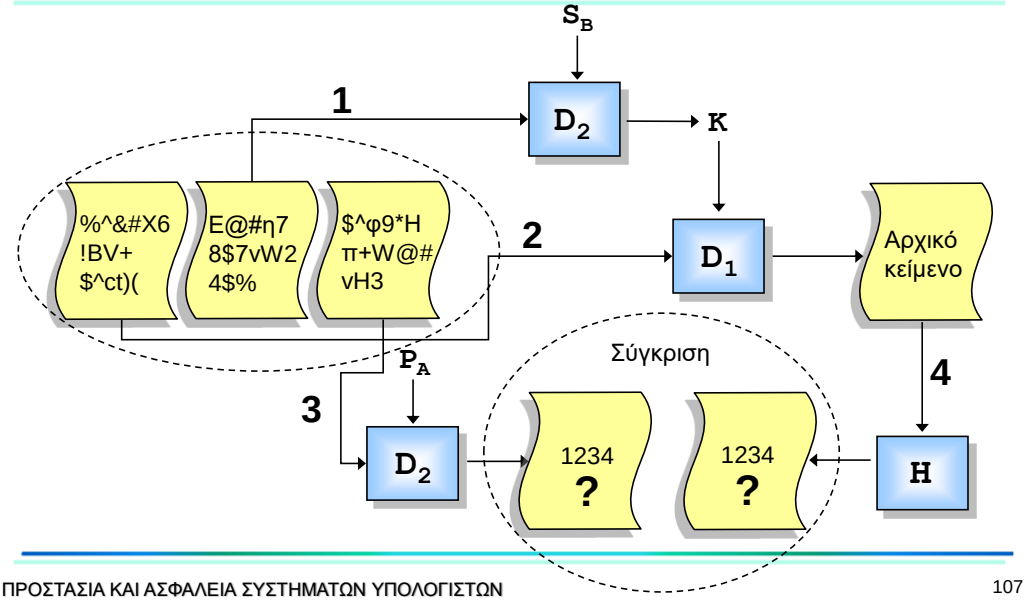
- Πως μπορούμε να παρέχουμε εμπιστευτικότητα, ακεραιότητα, και αυθεντικοποίηση σε ένα μήνυμα;
  - Εμπιστευτικότητα: Λόγω ταχύτητας αλγορίθμων επιλέγουμε τη χρήση ενός αλγορίθμου συμμετρικής κρυπτογραφίας
  - Για τη μεταφορά του κλειδιού επιλέγουμε τη χρήση κρυπτογραφίας δημοσίου κλειδιού (κρυπτογραφούμε με το δημόσιο κλειδί του παραλήπτη)
  - Αυθεντικοποίηση και ακεραιότητα: Κάνουμε χρήση ψηφιακών υπογραφών (κρυπτογραφούμε με το ιδιωτικό μας κλειδί)

Στην πράξη – Αποστολέας Α



106

Στην πράξη – Παραλήπτης Β



107

Στην πράξη

Πως είναι σίγουρος ο αποστολέας Α ότι το δημόσιο κλειδί που χρησιμοποιεί για την κρυπτογράφηση του συμμετρικού κλειδιού είναι του παραλήπτη Β;

Πως είναι σίγουρος ο παραλήπτης Β ότι το δημόσιο κλειδί που χρησιμοποιεί ο για την επαλήθευση της υπογραφής είναι του αποστολέα Α;

Προστασία και Ασφάλεια Συστημάτων Υπολογιστών

Στεγανογραφία

Στεγανογραφία

- «Τέχνη» της απόκρυψης πληροφοριών μέσα σε άλλα δεδομένα τα οποία προσφέρουν την απαραίτητη κάλυψη (π.χ. εικόνα, βίντεο, ήχος)
  - Στεγανογραφία = Στεγανός + γράφειν
- Τρεις τύποι
  - Pure Steganography: Τα ωφέλιμα δεδομένα «ανακατεύονται» με τα υπόλοιπα δεδομένα του κέλυφους βάσει συγκεκριμένου αλγορίθμου
  - Private Stego Key Steganography: Η απόκρυψη των ωφέλιμων δεδομένων και η εξαγωγή τους γίνεται με τη χρήση συμμετρικού κλειδιού.
  - Public Stego Key Steganography: Η απόκρυψη των ωφέλιμων δεδομένων και η εξαγωγή τους γίνεται με τη χρήση δημοσίου και ιδιωτικού κλειδιού αντίστοιχα.

Τεχνικές

- **Εισαγωγή**
  - Η ευαίσθητη πληροφορία εισάγεται μέσα στο κέλυφος π.χ. μετά το σύμβολο «τέλος αρχείου» (EOF), και έτσι παραμένουν κρυφά κατά την ανάγνωση του αρχείου με την αντίστοιχη εφαρμογή
- **Αντικατάσταση**
  - Τα LSB από κάθε byte του κέλυφους (π.χ. εικόνας) αντικαθίστανται από τα προς απόκρυψη bits. Εκμεταλλεύεται την αδυναμία του ανθρώπου να εντοπίσει κάποιες λεπτομέρειες.
- **Δημιουργία κέλυφους**
  - Το κέλυφος δημιουργείται βάσει των προς απόκρυψη δεδομένων.

Παράδειγμα

- http://mozaiq.org/encrypt/

Προστασία και Ασφάλεια Δικτύων

Αυθεντικοποίηση μηνύματος
Ακεραιότητα δεδομένων

Ακεραιότητα και αυθεντικοποίηση δεδομένων

- **Ακεραιότητα δεδομένων**: είναι η ιδιότητα που μας εξασφαλίζει ότι δεδομένα δεν έχουν παραποιηθεί με μη εξουσιοδοτημένο τρόπο από τη στιγμή που δημιουργήθηκαν, μεταδόθηκαν, ή αποθηκεύτηκαν από μια εξουσιοδοτημένη οντότητα.
- **Αυθεντικοποίηση μηνύματος**: Η διαδικασία σύμφωνα με την οποία επιβεβαιώνεται ότι μια οντότητα αποτελεί την πηγή κάποιων δεδομένων τα οποία δημιουργήθηκαν κάποια στιγμή στο παρελθόν (η χρονική αυτή στιγμή συνήθως δε δηλώνεται). Μέθοδοι που χρησιμοποιούνται:
  - Κώδικες αυθεντικοποίησης μηνύματος (MAC): Χρησιμοποιούν συμμετρικές μεθόδους.
  - Ψηφιακές υπογραφές

114

Ακεραιότητα και αυθεντικοποίηση δεδομένων

- **Η ακεραιότητα και η αυθεντικοποίηση δεδομένων είναι αλληλένδετες έννοιες:**
  - Εάν τα δεδομένα έχουν αλλοιωθεί τότε σίγουρα έχει αλλάξει και η πηγή τους,
  - Εάν δε μπορούμε να προσδιορίσουμε την πηγή των δεδομένων τότε δε μπορούμε να γνωρίζουμε και αν έχουν αλλοιωθεί ή όχι.

115

Ακεραιότητα δεδομένων

- Διαχωρισμός μεταξύ σκόπιμης και μη-σκόπιμης απειλής στην ακεραιότητα των δεδομένων:
  - Υπάρχει διαφορά μεταξύ των αλλοιώσεων που προκαλούνται στα δεδομένα από λάθη μετάδοσης στη γραμμή μετάδοσης και από σκόπιμες αλλοιώσεις.
  - Στην πρώτη περίπτωση ένας κυκλικός κώδικας πλεονασμού μπορεί να είναι αρκετός για την προστασία των δεδομένων. Γενικά η προστασία που παρέχεται από τέτοιου είδους λάθη χρησιμοποιεί μη κρυπτογραφικές μεθόδους, π.χ. κώδικες ανίχνευσης λαθών και κώδικες διόρθωσης λαθών.
  - **Οι κρυπτογραφικές μέθοδοι χρησιμοποιούνται για την προστασία των δεδομένων από σκόπιμες αλλοιώσεις.**

Ακεραιότητα δεδομένων

- Η κρυπτογράφηση δε παρέχει ακεραιότητα δεδομένων:
  - Υπάρχουν περιπτώσεις όπου ο επιτιθέμενος μπορεί απλά να επιφέρει κάποιες αλλαγές στο μήνυμα χωρίς να ξέρει είτε το αρχικό μήνυμα είτε το κλειδί. Παραδείγματα:
    - Ανακατάταξη των ECB .
    - Κρυπτογράφηση τυχαίων δεδομένων όπως κλειδιά κρυπτογράφησης. Σε μια τέτοια περίπτωση κάθε αποκρυπτογράφηση θα έχει νόημα.

Κώδικας ανίχνευσης παραποίησης Manipulation Detection Code (MDC)

- Πρόκειται για μηχανισμούς οι οποίοι όταν χρησιμοποιηθούν σε συνδυασμό με κάποιους άλλους μηχανισμούς, μπορούν να παρέχουν ακεραιότητα δεδομένων. Ένας κώδικας ανίχνευσης παραποίησης (manipulation detection code) μπορεί τυπικά να είναι
  - Μια one-way hash function ή
  - Μια one-way hash function με την επιπλέον ακόλουθη ιδιότητα: Είναι υπολογιστικά αδύνατο να βρεθούν δύο οποιεσδήποτε είσοδοι οι οποίες να δίνουν το ίδιο αποτέλεσμα (σύγκρουση). Αυτές οι συναρτήσεις κατακερματισμού ονομάζονται και strong one-way hash functions.

Ακεραιότητα δεδομένων

- **Ακεραιότητα δεδομένων χρησιμοποιώντας κρυπτογράφηση και κώδικα ανίχνευσης παραποίησης (MDC)**: Εάν απαιτείται τόσο εμπιστευτικότητα όσο και ακεραιότητα των δεδομένων τότε μπορεί να χρησιμοποιηθεί η ακόλουθη τεχνική:
  - Ο αποστολέας υπολογίζει την hash-value $h(x)$ για το μήνυμα x την επισυνάπτει στο μήνυμα και κρυπτογραφεί το σύνολο χρησιμοποιώντας συμμετρική κρυπτογράφηση
    $$C = E_k(x||h(x))$$
  - Ο παραλήπτης, αφού διαπιστώσει ποιο κλειδί θα χρησιμοποιήσει για την αποκρυπτογράφηση, αποκρυπτογραφεί το C, διαχωρίζει το μήνυμα x' από την hash-value $h(x)$, υπολογίζει εκ νέου την *hash-value* $h' = h(x')$ *και συγκρίνει* την h' με την τιμή $h(x)$.

Κώδικας αυθεντικοποίησης μηνύματος Message Authentication Code (MAC)

- Είναι ο μηχανισμός που παρέχει διαβεβαιώσεις αναφορικά με **την πηγή και την ακεραιότητα ενός μηνύματος**. Έχουν δύο παραμέτρους:
  - Το μήνυμα εισόδου,
  - Ένα μυστικό κλειδί
- Πρόκειται για μια **μονόδρομη συνάρτηση κατακερματισμού με κλειδί.**
- Βασίζονται στη χρήση συμμετρικών αλγορίθμων και έτσι δεν επιτρέπουν το διαχωρισμό μεταξύ των οντοτήτων που μοιράζονται το κλειδί. Επομένως δε παρέχουν μη αποποίηση της προέλευσης του μηνύματος.

Κώδικας αυθεντικοποίησης μηνύματος

- Πρόκειται για μια συνάρτηση h_k, η οποία χρησιμοποιεί ως παράμετρο ένα κλειδί k, με τις ακόλουθες ιδιότητες:
  - **Ευκολία υπολογισμού:** για μια γνωστή συνάρτηση h_k, είσοδο x και δεδομένο κλειδί k είναι εύκολο να υπολογίσουμε την MAC-τιμή $h_k(x)$.
  - **Συμπίεση**: Η h_k μετατρέπει μια είσοδο x αυθαίρετου μεγέθους σε μια έξοδο $h_k(x)$ συγκεκριμένου μεγέθους n.
  - **Αντίσταση στον υπολογισμό**: Δεδομένων 0 ή περισσοτέρων ζευγών $(x_i, h_k(x_i))$ είναι υπολογιστικά αδύνατο να υπολογίσουμε το $h_k(x)$ για οποιοδήποτε x διαφορετικό από τα x_i εάν δε γνωρίζουμε το κλειδί k.

Κώδικας αυθεντικοποίησης μηνύματος

- **Τρόπος χρήσης ενός MAC (ο οποίος αποτελεί ταυτόχρονα και τρόπο παροχής ακεραιότητας δεδομένων)**.
  - Ο αποστολέας του μηνύματος x υπολογίζει το MAC του μηνύματος $h_k(x)$ χρησιμοποιώντας ένα κλειδί k το οποίο μοιράζεται με τον παραλήπτη, και στέλνει τα x και $h_k(x)$.
  - Ο παραλήπτης, αφού διαπιστώσει με κάποιο τρόπο την ταυτότητα του μηνύματος, χρησιμοποιεί το κλειδί k για να υπολογίσει ο ίδιος το MAC για το μήνυμα x και το συγκρίνει με την MAC τιμή που έλαβε.
  - Αν οι τιμές είναι ίδιες ο παραλήπτης μπορεί να θεωρήσει ότι το μήνυμα παρελήφθη ακέραιο, όπως ακριβώς το έστειλε ο συγκεκριμένος αποστολέας.

Κώδικας αυθεντικοποίησης μηνύματος

- **MAC**: Ο πιο συχνά χρησιμοποιούμενος κώδικας MAC είναι αυτός που χρησιμοποιεί block ciphers σε CBC. **Ο MAC αποτελεί το τελευταίο block του κρυπτογραφημένου μηνύματος**.

- Προαιρετικά και για μεγαλύτερη ασφάλεια στο τελευταίο μπλοκ μπορούμε να χρησιμοποιήσουμε τριπλή κρυπτογράφηση με διπλό κλειδί.

Ακεραιότητα δεδομένων

- **Ακεραιότητα δεδομένων χρησιμοποιώντας κρυπτογράφηση και MAC**: Αντί για ένα MDC μπορεί να χρησιμοποιηθεί ένας MAC και έτσι το μήνυμα να είναι $C = E_k(x||h_{k'}(x))$.
  - Αν κάποιος προσβάλλει την εμπιστευτικότητα δε θα προσβάλει ταυτόχρονα και την ακεραιότητα του μηνύματος γιατί αυτή θα προστατεύεται από τον MAC.
  - Το μειονέκτημα είναι η χρήση δύο κλειδιών.
  - Η κρυπτογραφηση του MAC προστατεύει το MAC από μια επίθεση τύπου εξαντλητικής αναζήτησης κλειδιού (exhaustive key search).

Ακεραιότητα δεδομένων

- Δύο παραλλαγές:
  - **Υπολογισμός MAC στο κρυπτογραφημένο μήνυμα**: Ο παραλήπτης μπορεί να είναι σίγουρος ότι ο αποστολέας γνώριζε το μήνυμα;
  - **Ξεχωριστή κρυπτογράφηση και MAC**: Τα κλειδιά πρέπει να είναι διαφορετικά.

Ακεραιότητα δεδομένων

- Κακός συνδυασμός CBC-MAC και κρυπτογράφησης CBC: Έστω ότι η μέθοδος που χρησιμοποιούμε είναι της κρυπτογράφησης του MAC, δηλ. $C = E_k(x||h_{k'}(x))$ με $k=k'$ και το διάνυσμα αρχικοποίησης είναι το ίδιο τότε:

Ακεραιότητα δεδομένων

- Κακός συνδυασμός CBC-MAC και κρυπτογράφησης CBC: Έστω ότι η μέθοδος που χρησιμοποιούμε είναι της κρυπτογράφησης του MAC, δηλ. $C = E_k(x||h_{k'}(x))$ με $k=k'$ και το διάνυσμα αρχικοποίησης είναι το ίδιο τότε:
  - Έστω ότι το μήνυμα μας αποτελείται από τα δεδομένα $x=x_1x_2...x_t$. Το CBC-MAC θα είναι το τελευταίο κρυπτογραφημένο block $c_t=E_k(c_{t-1}\oplus x_t)$ και το τελευταίο block των δεδομένων θα είναι $x_{t+1}=c_t$ και επομένως η κρυπτογράφηση του θα δίνει $c_{t+1}=E_k(c_t\oplus x_{t+1})= E_k(0)$.
  - Το κρυπτογραφημένο MAC επομένως είναι ανεξάρτητο από το αρχικό μήνυμα και το κρυπτογραφημένο μήνυμα και έτσι καταστρέφεται η ακεραιότητα του μηνύματος.

Προστασία και Ασφάλεια Συστημάτων Υπολογιστών

Αυθεντικοποίηση Οντότητας – Πρωτόκολλα Αυθεντικοποίησης

Αυθεντικοποίηση

- Η πιστοποίηση της ταυτότητας.
- Διακρίνεται σε:
  - **Αυθεντικοποίηση οντότητας:** Η διαδικασία σύμφωνα με την οποία μια οντότητα Α βεβαιώνεται για την ταυτότητα μιας άλλης οντότητας Β (άτομο, τερματικό, πιστωτική κάρτα) και ότι η Β είναι ενεργή την ώρα που γίνεται η διαδικασία της αυθεντικοποίησης. Πρόκειται για μια **διαδικασία πραγματικού χρόνου**, με την έννοια ότι διαβεβαιώνει πως η οντότητα που αυθεντικοποιείται είναι λειτουργική την ώρα που αυθεντικοποιείται (παρέχουν διαβεβαιώσεις μόνο για τη συγκεκριμένη χρονική στιγμή).

Αυθεντικοποίηση

- Διακρίνεται σε:
  - **Αυθεντικοποίηση μηνύματος:** Η διαδικασία σύμφωνα με την οποία επιβεβαιώνεται ότι μια οντότητα αποτελεί την πηγή κάποιων δεδομένων τα οποία δημιουργήθηκαν κάποια στιγμή στο παρελθόν (η χρονική αυτή στιγμή συνήθως δε δηλώνεται). Μέθοδοι που χρησιμοποιούνται:
    - Κώδικες αυθεντικοποίησης μηνύματος (MAC): Χρησιμοποιούν συμμετρικές μεθόδους.
    - Ψηφιακές υπογραφές

Αυθεντικοποίηση οντότητας

- Δύο κατηγορίες

  Μονόδρομη αυθεντικοποίηση (unilateral authentication)

  Αμφίδρομη αυθεντικοποίηση (mutual authentication)
- Η αυθεντικοποίηση οντότητας γίνεται σύμφωνα με
  - κάτι που **ξέρει**
    - Password
    - PIN
  - κάτι που **έχει**
    - Security token (password generator)
    - Smart card, magnetic stripe card
  - κάτι που **είναι**
    - Βιομετρικές μέθοδοι

Passwords

- Ακολουθία χαρακτήρων γνώση της οποίας αποδέχεται ένα σύστημα ως διαβεβαίωση της ταυτότητας μιας οντότητας.
- Απειλές:
  - Password cracking:
    - Παρακολούθηση της γραμμής μετάδοσης
    - Dictionary attacks
    - Brute force attacks
  - Shoulder surfing
  - Social engineering
- Απαραίτητη η χρήση δύσκολων κωδικών (χρήση αλφαριθμητικών χαρακτήρων σε συνδυασμό με μη αλφαριθμητικούς χαρακτήρες)
- Μπορούμε να χρησιμοποιήσουμε password checkers για να ελέγξουμε την ποιότητα.

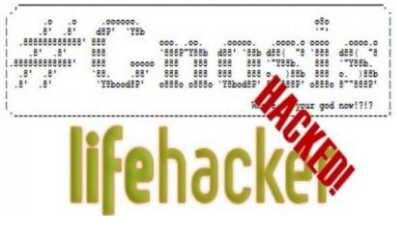
Passwords

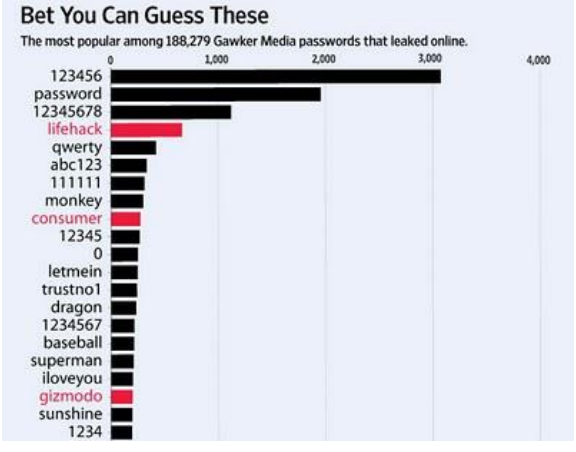
- Τρόποι μείωσης του κινδύνου εύρεσης ενός password:
  - Εκπαίδευση σε χρήστες και διαχειριστές
  - Περιορισμός των μη έγκυρων προσπαθειών αυθεντικοποίησης σε πολύ μικρό αριθμό
  - Χρήση τεχνητής καθυστέρησης στη διαδικασία επαλήθευσης για να δυσκολέψουμε την αποτελεσματικότητα των επιθέσεων τύπου dictionary attacks.
  - Χρήση μηχανισμών που αποτρέπουν τους χρήστες να επιλέξουν passwords που είναι πολύ μικρά, εύκολα, σχετίζονται με τα χαρακτηριστικά του χρήστη.
  - Συχνή αλλαγή των passwords – one-time passwords.
  - Αποφυγή των default passwords.
  - Ελεγχόμενη πρόσβαση στα passwords (κρυπτογράφηση, hash)

Passwords

- Από δικτυακή επίθεση που πραγματοποιήθηκε σε γνωστή εταιρία Media (12/2010) από την ομάδα hacker "Gnosis", διέρρευσαν πάνω από 1.3 εκατομμύρια διευθύνσεις email και κωδικοί στο internet.
  - Η ομάδα διέθεσε στο διαδίκτυο τους κλεμμένους κωδικούς και τα email σε μορφή αρχείου torrent με μέγεθος κοντά στα 500MB
  - Σύμφωνα με στατιστική ανάλυση που έγινε στους κωδικούς που διέρρευσαν, πάνω από 4.000 κωδικοί είναι οι αριθμοί "123456" και "12345678", 2000 χρήστες κάνουν χρήση του κωδικού "password" ενώ 150.000 χρήστες χρησιμοποιούν passwords μόνο με μικρά γράμματα.

Passwords





Passwords

- Τι γίνεται αν το ίδιο password χρησιμοποιείται και σε άλλα sites;
  - Σύμφωνα με το BBC από την αποκάλυψη αυτών των κωδικών hackers μπόρεσαν να αποκτήσουν τον έλεγχο χιλιάδων λογαριασμών του Twitter, στους οποίους προφανώς οι χρήστες χρησιμοποιούσαν τα ίδια συνθηματικά.

Passwords

- Το 2009 σε μια παραβίαση ασφάλειας του RockYou.com υπεκλάπησαν usernames, passwords και email διευθύνσεις από 32 εκατομμύρια χρήστες (με τη χρήση επίθεσης SQL injection). Τα passwords αυτά διοχετεύτηκαν στο διαδίκτυο. Μια εταιρία ονόματι Impreva έκανε στατιστική ανάλυση των passwords. Τα αποτελέσματα ήταν:
  - **Περισσότεροι από 290.000 χρήστες χρησιμοποιούσαν τον κωδικό «123456»**
  - **Το τέταρτο πιο συχνά χρησιμοποιούμενο password ήταν το «password» (62.000 χρήστες)**

Πρωτόκολλα Αυθεντικοποίησης

- Πρόκειται για πρωτόκολλα τα οποία έχουν ως σκοπό την αυθεντικοποίηση των οντοτήτων που συμμετέχουν σε μια συναλλαγή.
- Μπορούν να επιτύχουν:
  - Μονόδρομη αυθεντικοποίηση (unilateral authentication)
  - Αμφίδρομη αυθεντικοποίηση (mutual authentication)
  - Αυθεντικοποίηση και συμφωνία κλειδιών συνόδου

Πρόκληση – Απόκριση

- Η μια οντότητα να αποδεικνύει την ταυτότητα της σε μια άλλη οντότητα αποδεικνύοντας ότι γνωρίζει μια μυστική τιμή η οποία σχετίζεται με αυτήν την οντότητα, χωρίς όμως να αποκαλύπτει αυτήν την μυστική τιμή στην άλλη οντότητα κατά τη διάρκεια της εκτέλεσης του πρωτοκόλλου.
  - Επιτυγχάνεται με την απόκριση σε μια πρόκληση
  - Η απόκριση εξαρτάται τόσο από την μυστική τιμή όσο και από την πρόκληση.
- Το αποτέλεσμα είναι αν κάποιος παρακολουθεί τη γραμμή μετάδοσης να μην υπάρχει αποκάλυψη του μυστικού αυτού σε μη εξουσιοδοτημένους χρήστες.

Χρησιμοποιώντας συμμετρική κρυπτογράφηση

- Γίνεται με την επίδειξη γνώσης κοινού μυστικού κλειδιού μέσα από τη χρήση πρόκλησης-απόκρισης.
- Π.χ.

$A \rightarrow B: E_k(r_A)$
$B \rightarrow A: r_A$

ΜΗ ΑΣΦΑΛΕΣ

Χρησιμοποιώντας κρυπτογραφία δημοσίου κλειδιού

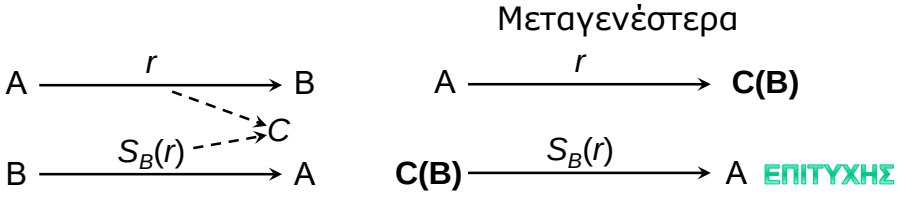
- Εκμεταλλεύονται το χαρακτηριστικό των αλγορίθμων όπου ο μόνος γνώστης κάποιου ιδιωτικού κλειδιού είναι ο κάτοχος του
- Π.χ. Οι δύο οντότητες χρησιμοποιούν ψηφιακές υπογραφές για να ανταλλάξουν υπογεγραμμένους τυχαίους αριθμούς.

$A \rightarrow B: r_A$
$B \rightarrow A: S_B(r_A)$

ΜΗ ΑΣΦΑΛΕΣ

Επιθέσεις σε πρωτόκολλα αυθεντικοποίησης

- **Επανάληψη στον χρήστη (Replay attacks)**: Ο επιτιθέμενος χρησιμοποιεί μηνύματα από μια κανονική αυθεντικοποίηση που έλαβε χώρα παλαιότερα.

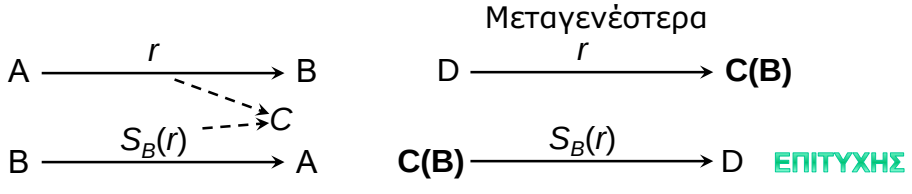


- **Προστασία**: Χρήση μη-επαναλαμβανόμενης τιμής (nonce), όπως ώρα και τυχαίο αριθμό. Χρήση ταυτότητας παραλήπτη.

142

Επιθέσεις σε πρωτόκολλα αυθεντικοποίησης

- **Επανάληψη σε άλλο χρήστη**: Ο επιτιθέμενος παρακολουθεί μια γραμμή όπου ο Α προσπαθεί να αυθεντικοποιήσει τον Β και χρησιμοποιεί αυτό το μήνυμα για να προσποιηθεί σε κάποιον τρίτο ότι πρόκειται για τον Β.



- **Προστασία**: Χρήση ταυτότητας του χρήστη που κάνει την αυθεντικοποίηση στο μήνυμα.

143

Επιθέσεις σε πρωτόκολλα αυθεντικοποίησης

- **Αντανάκλαση (Reflection attacks)**: Ο επιτιθέμενος χρησιμοποιεί κάποιο μήνυμα που προέρχεται από μια οντότητα και το οποίο αποτελεί μέρος μιας νόμιμης προσπάθειας αυθεντικοποίησης για να το στείλει πίσω στην ίδια οντότητα προσποιούμενος ότι προέρχεται από κάποια άλλη οντότητα. Είναι πιο επιτυχής σε πρωτόκολλα που χρησιμοποιούν συμμετρική κρυπτογράφηση.

Κανονική εκτέλεση	**Επίθεση**
$A \rightarrow B : E_k(r_A)$	$A \rightarrow C(B) : E_k(r_A)$
$B \rightarrow A : r_A$	$C(B) \rightarrow A : E_k(r_A)$
	$A \rightarrow C(B) : r_A$
	$C(B) \rightarrow A : r_A$

- **Προστασία**: Χρήση ταυτότητας πηγής ή προορισμού, και μη συμμετρικών μηνυμάτων

Επιθέσεις σε πρωτόκολλα αυθεντικοποίησης

- **Παρεμβολή (Interleaving)**: Ο επιτιθέμενος συνδυάζει πληροφορίες από μια ή περισσότερες εκτελέσεις του πρωτοκόλλου που έλαβε χώρα παλαιότερα ή που εκτελούνται παράλληλα με σκοπό να δημιουργήσει μηνύματα τα οποία θα φαίνονται ως σωστά για μια συγκεκριμένη εκτέλεση.

- **Προστασία**: Σύνδεση των μηνυμάτων του πρωτοκόλλου μεταξύ τους

Πρόκληση – Απόκριση

- Παράμετροι που μεταβάλλονται χρονικά μπορούν να προστατεύσουν από επιθέσεις επανάληψης (replay attacks).
- Σκοπός αυτών των μεταβλητών είναι να διαφοροποιήσουν μια εκτέλεση του πρωτοκόλλου από μια άλλη. Χρησιμοποιούνται για να παράσχουν μοναδικότητα, ή να προσδιορίσουν χρονικά την εκτέλεση ενός πρωτοκόλλου.
- Τρεις κατηγορίες παραμέτρων:
  - Τυχαίοι αριθμοί
  - Ακολουθιακοί αριθμοί
  - Χρονοσφραγίδες

Τυχαίοι αριθμοί

- Χρησιμοποιούνται εκτός των άλλων για να καταστήσουν την εκτέλεση των πρωτοκόλλων απρόβλεπτη.
  - Ο τυχαίος αριθμός αποτελεί μέρος της πρόκλησης.
  - Η απόκριση θα πρέπει να περιλαμβάνει τον ίδιο τυχαίο αριθμό για να θεωρηθεί αποτέλεσμα της πρόκλησης.

Μειονεκτήματα: Απαιτούν τη χρήση καλής γεννήτριας τυχαίων αριθμών αλλιώς μπορεί να είναι προβλέψιμοι. Τυπικά απαιτεί την ανταλλαγή ενός ακόμα μηνύματος σε σύγκριση με τα πρωτόκολλα που χρησιμοποιούν χρονοσφραγίδες.

Ακολουθιακοί αριθμοί

- Έχουν το χαρακτηριστικό της μοναδικότητας (τουλάχιστον για ένα μεγάλο χρονικό διάστημα).
- Τυπικά είναι διαφορετικοί για κάθε ζευγάρι οντοτήτων και για κάθε κατεύθυνση και πρέπει έμμεσα ή άμεσα να συνδέονται τόσο με τον αποστολέα όσο και με τον παραλήπτη.

Μειονεκτήματα: Η κάθε οντότητα πρέπει να διατηρεί όλους αυτούς τους αριθμούς για κάθε άλλη οντότητα με την οποία είναι σε επικοινωνία. Αποτυχία του συστήματος αποθήκευσης αριθμών θα έχει ως αποτέλεσμα την επανεκκίνηση των αριθμών.

148

Χρονοσφραγίδες

- Ο αποστολέας παίρνει μια χρονοσφραγίδα (ημερομηνία και ώρα) από το σύστημα και τη συνδέει με το μήνυμα. Ο παραλήπτης παίρνει τη χρονοσφραγίδα από το μήνυμα που έλαβε και αφού συμβουλευτεί την ώρα από το δικό του σύστημα θεωρεί ότι το μήνυμα που έλαβε είναι έγκυρο αν:
  - η διαφορά των χρονοσφραγίδων (του μηνύματος και του συστήματος του) είναι μέσα σε ένα παράθυρο το οποίο οι δύο οντότητες θεωρούν εύλογο (βάσει του χρόνου μετάδοσης διάδοσης και επεξεργασίας του μηνύματος).

Μειονεκτήματα: Απαιτούν τη χρήση συγχρονισμένων και προστατευμένων ρολογιών.

149

Αυθεντικοποίηση με συμμετρική κρυπτογράφηση

- Οι δύο οντότητες πρέπει να μοιράζονται ένα κοινό κλειδί.
- Η αυθεντικοποίηση γίνεται μέσα από την απόδειξη γνώσης του κλειδιού.

Μονόδρομη αυθεντικοποίηση βασισμένη σε χρονοσφραγίδες (ή ακολουθιακό αριθμό):

$$A \rightarrow B: A, E_k(t_A, B)$$

Τι μας εξασφαλίζει η παρουσία της ταυτότητας B;

Αυθεντικοποίηση με συμμετρική κρυπτογράφηση

Μονόδρομη αυθεντικοποίηση βασισμένη σε τυχαίους αριθμούς:

$$B \rightarrow A : r_B$$
$$A \rightarrow B : E_k(r_B, B)$$

Η χρήση της ταυτότητας του Β αποτρέπει επίθεση αντανάκλασης.

Αμοιβαία αυθεντικοποίηση βασισμένη σε τυχαίους αριθμούς:

$$B \rightarrow A : r_B$$
$$A \rightarrow B : E_k(r_A, r_B, B)$$
$$B \rightarrow A : E_k(r_B, r_A)$$

Αυθεντικοποίηση με τη χρήση MAC

- Η συνάρτηση κρυπτογράφησης μπορεί να αντικατασταθεί από MAC h_k.
- Π.χ.

$$B \rightarrow A : r_B$$
$$A \rightarrow B : r_A, h_k(r_A, r_B, B)$$
$$B \rightarrow A : h_k(r_B, r_A, A)$$

Αυθεντικοποίηση με κρυπτογραφία δημοσίου κλειδιού

- Η οντότητα που αυθεντικοποιείται αποδεικνύει τη γνώση του ιδιωτικού της κλειδιού με τους παρακάτω τρόπους:
  - Αποκρυπτογραφεί μια πρόκληση που κρυπτογραφήθηκε χρησιμοποιώντας το δημόσιο κλειδί της.
  - Υπογράφει ψηφιακά μια πρόκληση.

Αυθεντικοποίηση με κρυπτογραφία δημοσίου κλειδιού

- **Βάσει αποκρυπτογράφησης – μονόδρομη αυθεντικοποίηση**: Έστω r ένας τυχαίος αριθμός και $h(r)$ το αποτέλεσμα μιας μονόδρομης συνάρτησης κατακερματισμού, γνωστή ως **μάρτυρας (witness)**:

$$B \rightarrow A : h(r), B, E_{PA}(r, B)$$
$$A \rightarrow B : r$$

Με το $h(r)$ ο B αποδεικνύει στον A τη γνώση του r χωρίς φυσικά να το αποκαλύπτει στον A.

Αυθεντικοποίηση με κρυπτογραφία δημοσίου κλειδιού

- **Βάσει αποκρυπτογράφησης – Αμφίδρομη αυθεντικοποίηση:**

$$A \rightarrow B : E_{PB}(r_1, A)$$
$$B \rightarrow A : E_{PA}(r_1, r_2)$$
$$A \rightarrow B : r_2$$

Αυθεντικοποίηση με κρυπτογραφία δημοσίου κλειδιού

- **Βασισμένη σε ψηφιακές υπογραφές:**
  Μονόδρομη αυθεντικοποίηση με χρονοσφραγίδες:

$$A \rightarrow B : t_A, B, S_A(t_A, B)$$

όπου $S_A(t_A, B)$ η υπογραφή του A στην χρονοσφραγίδα t_A και στην ταυτότητα του παραλήπτη B.

Μονόδρομη αυθεντικοποίηση βάσει τυχαίων αριθμών:

$$B \rightarrow A : r_B$$
$$A \rightarrow B : r_A, B, S_A(r_A, r_B, B)$$

Ο τυχαίος αριθμός r_A στέλνεται για την αποφυγή επιθέσεων επιλεγμένου κειμένου.

156

Αυθεντικοποίηση με κρυπτογραφία δημοσίου κλειδιού

- **Βασισμένη σε ψηφιακές υπογραφές:**
  Αμφίδρομη αυθεντικοποίηση βάσει τυχαίων αριθμών:

$$B \rightarrow A : r_B$$
$$A \rightarrow B : r_A, B, S_A(r_A, r_B, B)$$
$$B \rightarrow A : A, S_B(r_B, r_A, A)$$

157

Πρόκληση – απόκριση

- Το πρόβλημα με αυτά τα πρωτόκολλα αυθεντικοποίησης είναι ότι δε συνοδεύονται από τη δημιουργία ενός κλειδιού το οποίο θα χρησιμοποιείται για τις ανταλλαγές των επόμενων μηνυμάτων.
- Ως αποτέλεσμα η αυθεντικοποίηση που επιτυγχάνεται χρησιμοποιώντας αυτά τα πρωτόκολλα είναι για εκείνη και μόνο εκείνη τη χρονική στιγμή.

158

Πρόκληση – απόκριση

- Ένας τρόπος για να σιγουρέψουμε ότι τα επόμενα μηνύματα που θα ανταλλάσσονται είναι από τις δύο οντότητες που αυθεντικοποιήθηκαν και όχι από κάποια άλλη, είναι να δημιουργήσουμε κάποια κλειδιά τα οποία θα μοιράζονται μεταξύ αυτών των οντοτήτων και τα οποία θα χρησιμοποιούνται:
  - για την κρυπτογράφηση των μηνυμάτων αν απαιτείται εμπιστευτικότητα, ή
  - για την παροχή ακεραιότητας αν αυτό απαιτείται, ή
  - και για τα δύο.

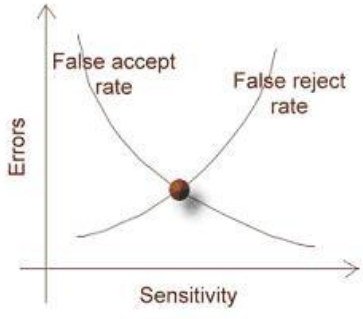
159

Βιομετρικές μέθοδοι

- Εξετάζουν κάποια στοιχεία που χαρακτηρίζουν μοναδικά έναν χρήστη.
- Πλεονεκτήματα
  - Αποτελεί την πιο αποτελεσματική μέθοδο πιστοποίησης ταυτότητας.
- Μειονεκτήματα
  - Κόστος
  - Όχι ιδιαίτερα αποδεκτό από τους χρήστες

Βιομετρικές μέθοδοι

- Χαρακτηριστικά
  - **Λάθος τύπου Ι**: το σύστημα απορρίπτει έναν εξουσιοδοτημένο (νόμιμο) χρήστη.
  - **Λάθος τύπου ΙΙ**: το σύστημα δέχεται μη εξουσιοδοτημένο χρήστη.
  - **Crossover Error Rate**: Αντιπροσωπεύει το σημείο στο οποίο το ποσοστό εσφαλμένης απόρριψης ισοδυναμεί με το ποσοστό εσφαλμένης αποδοχής.



Είδη βιομετρικών μεθόδων

- Δακτυλικά αποτυπώματα
- Σάρωση παλάμης (περιλαμβάνει και δακτυλικά αποτυπώματα)
- Γεωμετρία χεριού: μετρά το μήκος και το πλάτος ενός χεριού και των δακτύλων
- Σάρωση αμφιβληστροειδούς: Διαβάζει το σχέδιο των αιμοφόρων αγγείων στο πίσω μέρος του βολβού.
- Σάρωση ίριδας: Η ίριδα είναι το χρωματισμένο μέρος του ματιού που περιβάλλει την κόρη. Ελέγχει κάποια χαρακτηριστικά τα οποία είναι μοναδικά όπως χρώμα, κύκλους, ραβδώσεις.

Είδη βιομετρικών μεθόδων

- Αναγνώριση φωνής: Το άτομο πρέπει να εκφωνήσει κάποιες λέξεις που του ζητούνται και τις οποίες έχει εκφωνήσει και κατά τη διάρκεια της εγγραφής.
- Σάρωση προσώπου: Χρησιμοποιεί τη γεωμετρία του προσώπου και τα χαρακτηριστικά του.
- Δυναμική υπογραφής
- Δυναμική δακτυλογράφησης

Αποτελεσματικότητα βιομετρικών μεθόδων

- Σάρωση παλάμης
- Γεωμετρία χεριού
- Σάρωση ίριδας
- Σάρωση αμφιβληστροειδούς
- Δακτυλικά αποτυπώματα
- Αναγνώριση φωνής
- Αναγνώριση προσώπου
- Δυναμική υπογραφής
- Δυναμική δακτυλογράφησης

Αποδοχή βιομετρικών μεθόδων

- Σάρωση ίριδας
- Δυναμική δακτυλογράφησης
- Δυναμική υπογραφής
- Αναγνώριση φωνής
- Αναγνώριση προσώπου
- Δακτυλικά αποτυπώματα
- Σάρωση παλάμης
- Γεωμετρία χεριού
- Σάρωση αμφιβληστροειδούς

Προστασία και Ασφάλεια Συστημάτων Υπολογιστών

Διαχείριση κλειδιών

166

Διαχείριση κλειδιών – Κύκλος ζωής

- **Δημιουργία κλειδιού**: Σύμφωνα με τις απαιτήσεις του αλγορίθμου και τις ανάγκες της εφαρμογής. Το μέγεθος μπορεί να εξαρτηθεί από το είδος των δεδομένων που προστατεύουμε καθώς και από τη χρονική διάρκεια της κανονικής χρήσης του κλειδιού. Μπορεί να δημιουργηθεί:
  - Από τον ίδιο το χρήστη,
  - Από μια Έμπιστη Τρίτη Οντότητα
- **Καταχώρηση κλειδιού**: Ποιός κάνει χρήση αυτού του κλειδιού. Είναι ιδιαίτερα απαραίτητο στη διαχείριση δημοσίων κλειδιών και στη δημιουργία πιστοποιητικών.

167

Διαχείριση κλειδιών – Κύκλος ζωής

- **Διανομή κλειδιού**:
  - Έμπιστη τρίτη οντότητα: χρήση ψηφιακών πιστοποιητικών
  - Κέντρο διανομής κλειδιών: το κέντρο δημιουργεί το κλειδί και για τους δύο χρήστες και το διανέμει σε αυτούς
  - Κέντρα μετάφρασης κλειδιών: το κέντρο βοηθά στη μεταφορά του κλειδιού που δημιουργείται από έναν από τους δύο χρήστες
- **Ενεργοποίηση κλειδιού**: Μπορεί να περιλαμβάνει και την εγκατάσταση του κλειδιού στη μονάδα που θα το χρησιμοποιήσει (π.χ. Η τραπεζική κάρτα και η χρήση του PIN).

168

Διαχείριση κλειδιών – Κύκλος ζωής

- **Χρήση (η προβλεπόμενη)**: Το κλειδί θα πρέπει να είναι διαθέσιμο σε όλη τη διάρκεια της κανονικής του χρήσης για την προβλεπόμενη όμως μόνο χρήση (π.χ. Ζεύγος κλειδιών που έχει δημιουργηθεί για ψηφιακές υπογραφές)
- **Δημιουργία αντιγράφων ασφαλείας**: Όταν αυτό επιτρέπεται από το είδος του κλειδιού. Π.χ. Αντίγραφα ασφαλείας ιδιωτικών κλειδιών
- **Αντικατάσταση ή ανανέωση κλειδιού**: Όταν θα παρέλθει η διάρκεια χρήσης του κλειδιού θα πρέπει να υπάρχει τρόπος ώστε αυτό το κλειδί να αντικατασταθεί ή να ανανεωθεί με ασφαλείς μεθόδους έτσι ώστε να εξασφαλιστεί η αδιάλειπτη λειτουργία του κρυπτοσυστήματος.

169

Διαχείριση κλειδιών – Κύκλος ζωής

- **Ανάκληση κλειδιού**: Κάτω από ορισμένες συνθήκες, όπως η υποψία ότι η ασφάλεια ενός κλειδιού διακυβεύεται, πρέπει να αποφασιστεί η παύση χρήσης αυτού του κλειδιού.
- **Απενεργοποίηση κλειδιού**: Όταν παρέλθει ο χρόνος χρήσης του κλειδιού.
- **Ανάκτηση κλειδιού**: Από εξουσιοδοτημένους χρήστες έτσι ώστε να αποτραπεί η ανεπιθύμητη αδυναμία πρόσβασης σε κρυπτογραφημένα δεδομένα.
- **Αρχειοθέτηση κλειδιού**: Όταν πλέον το κλειδί τεθεί εκτός λειτουργίας.
- **Καταστροφή κλειδιού**: Με την ολοκλήρωση του κύκλου.

Διαχείριση κλειδιών – Κύκλος ζωής

- **Κάθε κλειδί πρέπει να προστατεύεται σε όλες τις περιόδους του κύκλου ζωής του.**
- Ο κύκλος ζωής των συμμετρικών κλειδιών διαφέρει από τον κύκλο ζωής ενός ζεύγους δημοσίου/ιδιωτικού κλειδιού και γενικά είναι λιγότερο πολύπλοκος. Παρόλα αυτά η διαχείριση των κλειδιών ασύμμετρων κρυπτοσυστημάτων σε πολλές φάσεις του κύκλου ζωής είναι ευκολότερη

Πρωτόκολλα Εγκαθίδρυσης Κλειδιών (Key Establishment Protocols)

- Δίνουν τη δυνατότητα σε δύο ή περισσότερες οντότητες να μοιραστούν ένα ή περισσότερα κλειδιά συμμετρικής κρυπτογράφησης.
- Χωρίζονται σε δύο κατηγορίες:
  - **Μεταφορά κλειδιών (key transport)**: η μία από τις δύο οντότητες δημιουργεί ένα κλειδί και το μεταφέρει με ασφαλή τρόπο στην άλλη οντότητα.
  - **Συμφωνία κλειδιών (key agreement)**: ένα κοινό κλειδί δημιουργείται από δύο ή περισσότερες οντότητες σαν συνάρτηση πληροφοριών που συνεισφέρουν ή που σχετίζονται με κάθε μια από αυτές τις οντότητες, έτσι ώστε καμία από αυτές τις οντότητες να μπορεί να προκαθορίσει το αποτέλεσμα.

172

Πρωτόκολλα Εγκαθίδρυσης Κλειδιών (Key Establishment Protocols)

- Βασίζονται τόσο σε συμμετρική κρυπτογράφηση όσο και σε κρυπτογραφία δημοσίου κλειδιού.
- Τα κλειδιά που δημιουργούνται με τη χρήση αυτών των πρωτοκόλλων τυπικά ονομάζονται **κλειδιά συνόδου (session keys)**:
  - εφήμερα κλειδιά τα οποία τυπικά χρησιμοποιούνται για ένα συγκεκριμένο χρονικό διάστημα το οποίο μπορεί να καθορίζεται από τη διάρκεια μιας επικοινωνίας.

173

Εφήμερα κλειδιά

- Λόγοι που επιβάλλουν τη χρήση εφήμερων κλειδιών:
  - Περιορισμό των διαθέσιμων κρυπτογραμμάτων που έχουν κρυπτογραφηθεί με το ίδιο κλειδί (αποφυγή κρυπτανάλυσης).
  - Περιορισμό της έκθεσης του κλειδιού, από πλευράς τόσο χρόνου όσο και ποσότητας δεδομένων για την περίπτωση που αποκαλυφθεί το κλειδί.
  - Αποφυγή της αποθήκευσης κλειδιών για μεγάλο χρονικό διάστημα – μπορούν να είναι διαθέσιμα μόνο τη στιγμή που θα χρησιμοποιηθούν.
  - Για την ανεξαρτητοποίηση συνόδων επικοινωνιών ή εφαρμογών.

Διαχείριση κλειδιών – Με συμμετρική κρυπτογράφηση

- **Κέντρα διανομής κλειδιών (key distribution centers)**
- **Κέντρα μετάφρασης κλειδιών (key translation centers)**

- Πλεονεκτήματα:
  - Είναι εύκολο να προσθέσουμε ή να αφαιρέσουμε οντότητες από το δίκτυο
  - Κάθε οντότητα χρειάζεται μόνο να αποθηκεύσει ένα μυστικό κλειδί μακράς διαρκείας
- Μειονεκτήματα:
  - Όλες οι επικοινωνίες απαιτούν μια αρχική επικοινωνία με την έμπιστη τρίτη οντότητα (Trusted Third Party – TTP).
  - Η TTP πρέπει να αποθηκεύσει η κλειδιά μακράς διαρκείας.
  - Η TTP έχει τη δυνατότητα να διαβάσει όλα τα μηνύματα.
  - Εάν παραβιαστεί η ασφάλεια της TTP τότε όλες οι επικοινωνίες είναι ανασφαλείς.

Διαχείριση κλειδιών – Με κρυπτογραφία δημοσίου κλειδιού

- Χρησιμοποιώντας τεχνικές δημοσίου κλειδιού: Τυπικά τα δημόσια κλειδιά μπορούν να χρησιμοποιηθούν για την κρυπτογράφηση κλειδιών συνόδου συμμετρικής κρυπτογράφησης.
- Απαιτούν τη χρήση TTP η οποία θα εγγυηθεί για την αυθεντικότητα των κλειδιών.
- Πλεονεκτήματα χρήσης τεχνικών δημοσίου κλειδιού με TTP:
  - Η TTP δε μπορεί να παρακολουθήσει τις επικοινωνίες.
  - Η επικοινωνία με το TTP μπορεί να περιοριστεί αν οι οντότητες αποθηκεύουν τα κλειδιά τοπικά.
- Μειονεκτήματα:
  - Πρέπει να υπάρχει εμπιστοσύνη στην TTP από όλες τις οντότητες.

Diffie-Hellman

- **Diffie-Hellman**: Επιτρέπει δύο οντότητες που δεν έχουν συναντηθεί στο παρελθόν και δε μοιράζονται ένα κοινό μυστικό κλειδί, να μπορέσουν να δημιουργήσουν ένα κοινό κλειδί K ανταλλάσοντας μηνύματα μέσω ενός μη προστατευμένου καναλιού.

  Οι δύο χρήστες πρέπει να έχουν συμφωνήσει, έστω και έμμεσα, στη χρήση ενός τυχαίου αριθμού p και ενός αριθμού a τέτοιο ώστε $2 \le a \le p\text{-}2$.

  Ο Α επιλέγει μια τυχαία μυστική τιμή x, $1 \le x \le p\text{-}2$ και στέλνει στον Β

  $$A \rightarrow B: a^x \bmod p$$

  Ο Β επιλέγει μια τυχαία μυστική τιμή y, $1 \le y \le p\text{-}2$ και στέλνει στον Α

  $$B \rightarrow A: a^y \bmod p$$

  Ο Β λαμβάνει το a^x και υπολογίζει το κοινό κλειδί ως $K = (a^x)^y \bmod p$

  Ο Α λαμβάνει το a^y και υπολογίζει το κοινό κλειδί ως $K = (a^y)^x \bmod p$

Diffie-Hellman

- Οι χρήστες μπορούν να χρησιμοποιήσουν το κοινό κλειδί K αυτούσιο ή μέρος αυτού ανάλογα με τις ανάγκες του αλγορίθμου.
- Γνωρίζουν οι συμμετέχοντες σε ποιόν ανήκει το κλειδί που λαμβάνουν;
  - Η βασική έκδοση του πρωτοκόλλου προστατεύει τη μυστικότητα του κοινού κλειδιού από ένα παθητικό επιτιθέμενο, αλλά όχι από κάποιον ενεργό επιτιθέμενο που μπορεί να υποκλέψει αλλά και να τροποποιήσει ή να εισάγει δεδομένα στη γραμμή μετάδοσης.
- Απαραίτητη η χρήση ψηφιακών πιστοποιητικών.
  - Οι τιμές των κλειδιών παραμένουν σταθερές
  - Το κοινό κλειδί θα είναι το ίδιο
    - Απαιτείται η χρήση χρονοσφραγίδας ή τυχαίου αριθμού σε συνδυασμό με μια συνάρτηση κατακερματισμού για τη δημιουργία του κοινού κλειδιού συνόδου

178

Διαχείριση συμμετρικών κλειδιών με τη χρήση τεχνικών δημοσίου κλειδιού

- **Μεταφορά κλειδιών βασισμένη σε κρυπτογράφηση δημοσίου κλειδιού**:
- Τυπικά θα μπορούσε η μία από τις δύο οντότητες, Α, να επιλέξει ένα συμμετρικό κλειδί και να το στείλει κρυπτογραφημένο στην άλλη οντότητα, Β.

$$A \rightarrow B: P_B(k, T_A)$$

  - Πόσο σίγουρος είναι ο Β ότι αυτό το κλειδί το μοιράζεται με τον Α;
- Απαραίτητη η αυθεντικοποίηση του μηνύματος και κατ' επέκταση του κλειδιού που χρησιμοποιείται:
  - **Έμμεση αυθεντικοποίηση** μέσω της αποκρυπτογράφησης χρησιμοποιώντας τεχνικές δημοσίου κλειδιού
  - **Άμεση αυθεντικοποίηση** μηνύματος με τη χρήση ψηφιακών υπογραφών

179

Μεταφορά κλειδιών με τη χρήση ΚΔΚ χωρίς υπογραφές

- **Μεταφορά με τη χρήση ενός μόνο μηνύματος:**
  - Είναι ιδανικά για επικοινωνίες μιας κατεύθυνσης όπως είναι το e-mail.
- Αποστολή κλειδιού συνόδου από τον αποστολέα κρυπτογραφημένη με το δημόσιο κλειδί του παραλήπτη :

$$A \rightarrow B: P_B(k, T_A)$$

- Με ποιόν τρόπο μπορεί ο Β να είναι σίγουρος για την ταυτότητα του αποστολέα;

Συμφωνία κλειδιών με τη χρήση ΚΔΚ χωρίς υπογραφές

- **Needham-Schroeder πρωτόκολλο**: Γίνεται με την ανταλλαγή τριών μηνυμάτων:

  Ο Α δημιουργεί ένα κλειδί k_1 και στέλνει στον Β το ακόλουθο μήνυμα:

$$A \rightarrow B: P_B(k_1, A)$$

  Ο Β παίρνει το k_1 από το μήνυμα, δημιουργεί ένα κλειδί k_2 και στέλνει στον Α το

$$B \rightarrow A: P_A(k_1, k_2)$$

  Αν το k_1 είναι το ίδιο με αυτό που έστειλε ο A στο πρώτο μήνυμα:

$$A \rightarrow B: P_B(k_2)$$

  Ο Β ελέγχει το k_2.

  Το κλειδί συνόδου μπορεί να δημιουργηθεί χρησιμοποιώντας μια μόνοδρομη συνάρτηση f ως $f(k_1, k_2)$.

Πρωτόκολλα που συνδυάζουν ΚΔΚ και ψηφιακές υπογραφές

- Η χρήση ψηφιακών υπογραφών παρέχει αυθεντικοποίηση μηνύματος.
- Πρωτόκολλα μεταφοράς κλειδιών που κάνουν χρήση κρυπτογράφησης δημοσίου κλειδιού και υπογραφών:
  - Κρυπτογράφηση του υπογεγραμμένου κλειδιού.
  - Υπογραφή κλειδιού και ξεχωριστή κρυπτογράφηση του (μη υπογεγραμμένο) κλειδιού.
  - Υπογραφή κρυπτογραφημένου κλειδιού.
- Η ψηφιακή υπογραφή δε θα πρέπει να επιτρέπει την ανάκτηση μηνύματος

Πρωτόκολλα που συνδυάζουν ΚΔΚ και ψηφιακές υπογραφές

- **Κρυπτογράφηση υπογεγραμμένων κλειδιών:**

$$A \rightarrow B: P_B(k, t_A^*, S_A(B, k, t_A^*))$$

Η χρονοσφραγίδα είναι προαιρετική. Η χρήση της παρέχει εγγύηση ως προς το χρόνο δημιουργίας του μηνύματος.

Γιατί περιλαμβάνεται η ταυτότητα του Β στο μήνυμα;

Τι μορφή θα πρέπει να έχει το μήνυμα αν χρησιμοποιούμε ψηφιακές υπογραφές με ανάκτηση μηνύματος;

Πρωτόκολλα που συνδυάζουν ΚΔΚ και ψηφιακές υπογραφές

- **Κρυπτογραφώντας και υπογράφοντας ξεχωριστά:**

  Μπορεί να χρησιμοποιηθεί **μόνο με υπογραφές που δε παρέχουν ανάκτηση μηνύματος**.

  $$A \rightarrow B: P_B(k, t_A^*), S_A(B, k, t_A^*)$$

  Εάν το κλειδί k χρησιμοποιείται μόνο για την κρυπτογράφηση ενός αρχείου y τότε η υπογραφή μπορεί να είναι πάνω στο y και όχι στο κλειδί.

184

Πρωτόκολλα που συνδυάζουν ΚΔΚ και ψηφιακές υπογραφές

- **Υπογράφοντας κρυπτογραφημένα κλειδιά:**

  $$A \rightarrow B: t_A^*, P_B(A, k), S_A(B, t_A^*, P_B(A, k))$$

  Η παράμετρος Α μέσα στο κρυπτογραφημένο μήνυμα αποτρέπει από την ακόλουθη επίθεση: Εάν υπογράφαμε μόνο το κρυπτογραφημένο μήνυμα $S_A(P_B(k))$ ο επιτιθέμενος C θα μπορούσε να πάρει τα κρυπτογραφημένα δεδομένα $P_B(k)$ και να τα υπογράψει με το δικό του κλειδί και έτσι να καταφέρει να πείσει τον Β ότι το μήνυμα το έστειλε ο C.

  Θα πρέπει το μέγεθος της ταυτότητας του Α μαζί με το κλειδί να μη ξεπερνούν το μέγεθος του block του αλγορίθμου κρυπτογράφησης, έτσι ώστε η κρυπτογράφηση να περιοριστεί σε ένα μόνο block.

185

Προστασία και Ασφάλεια Συστημάτων Υπολογιστών

Έμπιστες Τρίτες Οντότητες
Ψηφιακά πιστοποιητικά
Υποδομές δημοσίου κλειδιού

186

Έμπιστες Τρίτες Οντότητες ή Trusted Third Parties – TTPs

- Πρόκειται για μια οντότητα την οποία εμπιστεύονται όλες οι οντότητες μέσα σε ένα σχήμα και για συγκεκριμένες υπηρεσίες.
- Ο βαθμός εμπιστοσύνης διαφέρει και μπορεί να είναι μια **άνευ όρων εμπιστοσύνη** ή **μια λειτουργική εμπιστοσύνη**
- **Μπορεί να είναι:**
  - Φορέας του δημοσίου
  - Τράπεζα
  - Ιδιωτική εταιρία

187

Έμπιστες Τρίτες Οντότητες ή Trusted Third Parties – TTPs

- Από την πλευρά των επικοινωνιών υπάρχουν τρεις κατηγορίες έμπιστων οντοτήτων TTP βάσει της σχετικής τους θέσης και της αλληλεπίδρασης τους με τις οντότητες που επικοινωνούν Α και Β:
  - **In-line**: Λειτουργεί ως μεσάζων και αποτελεί το μέσο επικοινωνίας μεταξύ Α και Β.
  - **On-line**: Συμμετέχει ενεργά (σε πραγματικό χρόνο) κατά τη διάρκεια της εκτέλεσης του πρωτοκόλλου. Οι Α και Β όμως επικοινωνούν άμεσα από ότι μέσω του TTP.
  - **Off-line**: Το TTP δε συμμετέχει σε πραγματικό χρόνο αλλά ετοιμάζει τις σχετικές πληροφορίες οι οποίες είναι διαθέσιμες στους Α και Β πριν την εκτέλεση του πρωτοκόλλου.

TTPs

- Ρόλοι μιας Έμπιστης Τρίτης Οντότητας περιλαμβάνουν:
  - **Αρχή Πιστοποίησης:** Χρησιμοποιείται σε υποδομές δημοσίου κλειδιού και είναι η αρχή που εκδίδει τα ψηφιακά πιστοποιητικά.
  - **Registration Authority (Αρχή εγγραφής):** Χρησιμοποιείται σε υποδομές δημοσίου κλειδιού και είναι η αρχή που χρησιμεύει στην εγγραφή ενός χρήστη σε μια υποδομή δημοσίου κλειδιού.
  - **Key Generator (Γεννήτρια κλειδιών):** Χρησιμοποιείται για τη διαχείριση κλειδιών, και πιο συγκεκριμένα στη δημιουργία κλειδιών για τους χρήστες.
  - **Certificate Directory (Κατάλογος Πιστοποιητικών):** Χρησιμεύει ως χώρος αποθήκευσης ψηφιακών πιστοποιητικών.

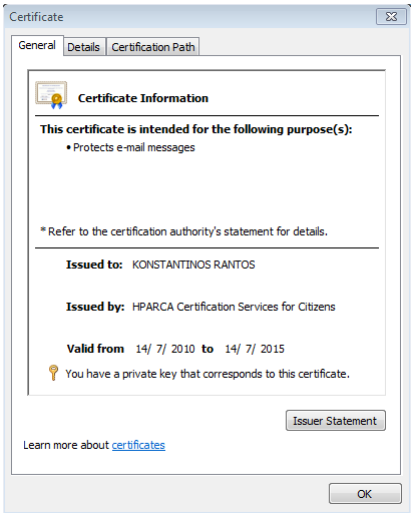
TTPs

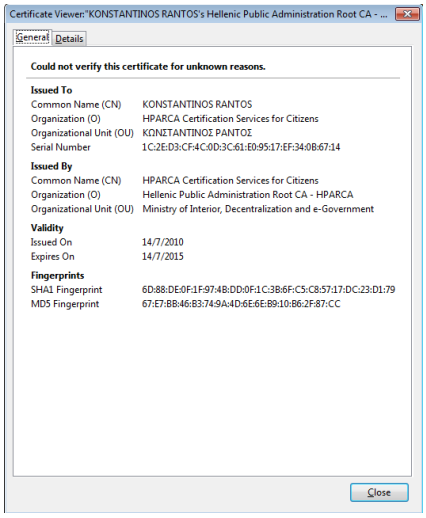
- Ρόλοι μιας Έμπιστης Τρίτης Οντότητας περιλαμβάνουν:
  - **Key server (Εξυπηρετητής κλειδιών):** Χρησιμοποιείται για την αποθήκευση και διαχείριση κλειδιών κρυπτογράφησης. Παραδείγματα αποτελούν τα Κέντρα Διανομής Κλειδιών και Κέντρα Διαχείρισης Κλειδιών.
  - **Timestamp Agent:** Πιστοποιεί τη χρονική στιγμή την οποία έγινε μια συναλλαγή.
  - **Notary Agent:** Χρησιμεύει ως αρχή επίλυσης διαφορών.
  - **Key Escrow Agent:** Πρόκειται για μια αρχή στην οποία εμπιστευόμαστε αντίγραφα κλειδιών κρυπτογράφησης.

Ψηφιακά πιστοποιητικά

- Είναι ο μηχανισμός που χρησιμοποιείται για να σχετίσει κάποιες πληροφορίες που αφορούν μια οντότητα με την ταυτότητα αυτής της οντότητας. Αποτελείται από **ένα τμήμα δεδομένων** και από ένα τμήμα υπογραφής.
  - **Ένα τμήμα δεδομένων**: το στοιχεία της οντότητας που πιστοποιείται, τα στοιχεία του εκδότη, το δημόσιο κλειδί της οντότητας, καθώς και άλλες πληροφορίες που αφορούν αυτήν την οντότητα.
  - **Ένα τμήμα υπογραφής**: η ψηφιακή υπογραφή μιας έμπιστης τρίτης οντότητας (εκδότη) στο τμήμα δεδομένων.
- Μέσω των πιστοποιητικών είναι δυνατή η διακίνηση **αυθεντικοποιημένων αντιγράφων δημοσίων κλειδιών**.
- Βασίζονται στο πρότυπο ITU-T X.509 (RFC 5280)

Ψηφιακά πιστοποιητικά



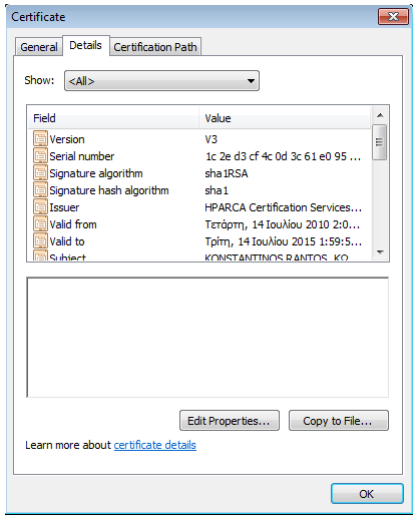


Ψηφιακά πιστοποιητικά

- Είδη πιστοποιητικών
  - **Πιστοποιητικά δημοσίου κλειδιού (public-key certificates)**: Συνδέουν την ταυτότητα μιας οντότητας, και προαιρετικά κάποιες πληροφορίες οι οποίες αναγνωρίζουν μοναδικά αυτή την οντότητα, με το δημόσιο κλειδί της.
  - **Πιστοποιητικά ιδιότητας (attribute certificates)**: Πιστοποιούν την ιδιότητα μιας οντότητας (θέση σε εταιρία, δικαιώματα πρόσβασης).

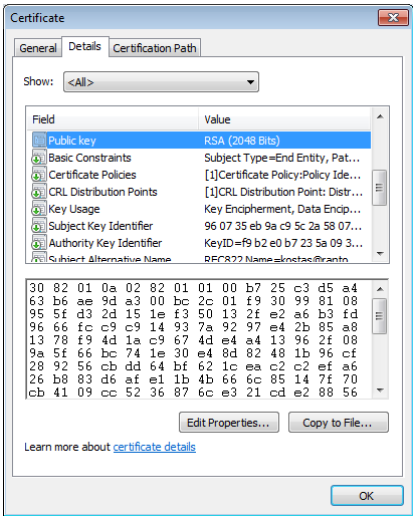
Ψηφιακά πιστοποιητικά

- Πληροφορίες που υπάρχουν στο τμήμα δεδομένων:
  - **Έκδοση X.509 προτύπου**
  - **Σειριακό αριθμό**
  - **Αλγόριθμος υπογραφής**
  - **Εκδότης**
  - **Ημερομηνία έναρξης ισχύος**
  - **Ημερομηνία λήξης ισχύος**
  - **Στοιχεία υποκειμένου**



Ψηφιακά πιστοποιητικά

- Πληροφορίες που υπάρχουν στο τμήμα δεδομένων:
  - **Δημόσιο κλειδί**
  - **Περιορισμοί**: προσδιορίζουν αν πρόκειται για Αρχή Πιστοποίησης ή για τελική οντότητα
  - **Πολιτικές πιστοποίησης**
  - **Σημεία διανομή CRL**
  - **Χρήση κλειδιού**
  - **Αναγνωριστικό κλειδιού**
  - **...**



Υποδομή Δημοσίου Κλειδιού

- Πρόκειται για την υποδομή η οποία κάνει χρήση κρυπτογραφίας δημοσίου κλειδιού για να προσφέρει σε οντότητες που συμμετέχουν σε αυτή υπηρεσίες προστασίας πληροφοριών όπως αυθεντικοποίηση, εμπιστευτικότητα, μη αποποίηση, και ακεραιότητα των ανταλλασσόμενων μηνυμάτων.
- Μια υποδομή δημοσίου κλειδιού αποτελείται από εκείνα **τα προγράμματα, δομές δεδομένων, διαδικασίες, πρωτόκολλα επικοινωνίας, πολιτικές ασφαλείας, και μηχανισμούς κρυπτογραφίας δημοσίου κλειδιού** που επιτρέπουν τις συμμετέχουσες οντότητες να επικοινωνήσουν με ασφαλή τρόπο.

196

Υποδομή Δημοσίου Κλειδιού

- Η διαφορά μεταξύ **κρυπτογραφίας δημοσίου κλειδιού** και **υποδομής δημοσίου κλειδιού** είναι ότι η πρώτη περιλαμβάνει τους αλγορίθμους, τα κλειδιά, και την τεχνολογία που απαιτείται για την κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων ενώ η δεύτερη περιλαμβάνει εκείνα τα κομμάτια που αναγνωρίζουν τους χρήστες, διαχειρίζονται πιστοποιητικά, διανέμουν και ανακαλούν κρυπτογραφικά κλειδιά.
- Η κρυπτογραφία δημοσίου κλειδιού είναι μόνο ένα τμήμα της υποδομής δημοσίου κλειδιού.

197

Υποδομή Δημοσίου Κλειδιού

- Μια υποδομή δημοσίου κλειδιού απαρτίζεται από:
  - **Αρχές πιστοποίησης**
  - **Αρχές εγγραφής**
  - **Πιστοποιητικά**
  - **Χρήστες**
  - **Αποθήκη πιστοποιητικών (repository)**
  - **Κλειδιά**
  - **Μηχανισμό ανάκλησης κλειδιών**

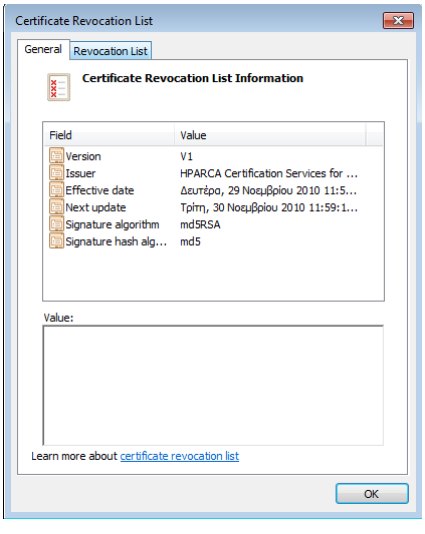
Αρχή Πιστοποίησης

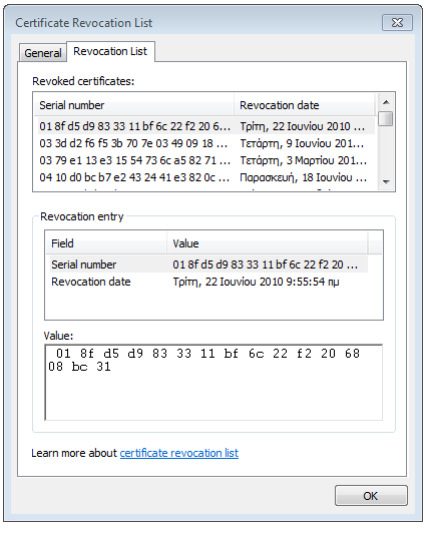
- Κάθε οντότητα που συμμετέχει σε μια υποδομή χρειάζεται ένα **ψηφιακό πιστοποιητικό**.
  - Τα στοιχεία του πιστοποιητικού συγκεντρώνονται από την **αρχή εγγραφής**.
  - Το πιστοποιητικό υπογράφεται από μια αρχή πιστοποίησης.
- **Αρχή Πιστοποίησης**: Οργανισμός ο οποίος εκδίδει και διαχειρίζεται ψηφιακά πιστοποιητικά. Μέρος των διαδικασιών της διεκπεραιώνεται από την αρχή εγγραφής.

Ανάκληση πιστοποιητικών

- Υπάρχουν περιπτώσεις όπου κάποιο πιστοποιητικό θα πρέπει να πάψει να είναι έγκυρο πριν την ημερομηνία λήξης του:
  - Αποκάλυψη του ιδιωτικού κλειδιού ή υποψία αποκάλυψης.
  - Αλλαγή των στοιχείων της οντότητας
  - Αλλαγή της ιδιότητας της οντότητας
- Σε μια τέτοια περίπτωση γίνεται χρήση ενός **μηχανισμού ανάκλησης πιστοποιητικών**.
  - **Λίστα ανακληθέντων πιστοποιητικών (certificate revocation list – CRL)**: Υπογεγραμμένη από την αρχή πιστοποίησης λίστα με όλα τα πιστοποιητικά που δεν έχουν λήξει αλλά δε πρέπει να θεωρούνται έγκυρα πια. Εκδίδεται ανά τακτά χρονικά διαστήματα.
  - **Online Certificate Status Protocol (OCSP)**

CRL





Αρχή Εγγραφής

- **Αρχή εγγραφής (Registration Authority)**: Πρόκειται για φορέα, ο οποίος μπορεί να είναι ανεξάρτητος από την αρχή πιστοποίησης, και είναι υπεύθυνος
  - Για την υποδοχή αιτημάτων χρηστών
  - Για τη συλλογή των στοιχείων μιας οντότητας που αιτείται ένα πιστοποιητικό καθώς και για την επαλήθευση της εγκυρότητας των.
  - Την παράδοση ενός πιστοποιητικού.
- **Δεν εκδίδει πιστοποιητικά.**

Υποδομή Δημοσίου Κλειδιού

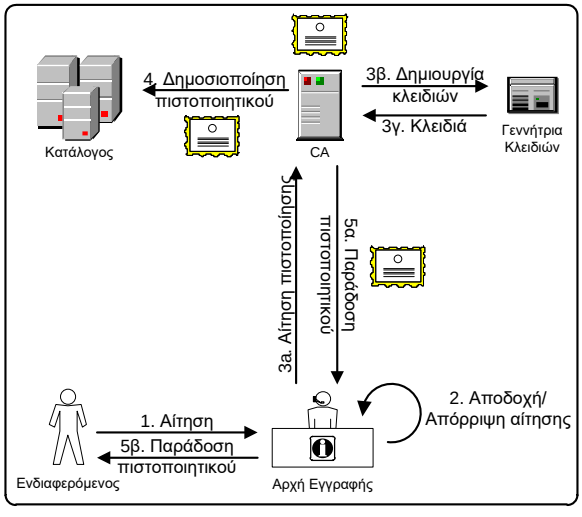
- **Κατάλογο πιστοποιητικών (certificate directory)**: Βάση δεδομένων από την οποία οι χρήστες έχουν τη δυνατότητα άντλησης πιστοποιητικών αλλά και διαχείρισης των δικών τους.
- Για την πρόσβαση στις υπηρεσίες καταλόγου τυπικά χρησιμοποιείται το LDAP (Light Directory Access Protocol)

Υποδομή Δημοσίου Κλειδιού

- **Εγγραφή και έκδοση πιστοποιητικού:**
  - Ο χρήστης Α υποβάλλει την αίτηση του για πιστοποιητικό στην Αρχή Εγγραφής.
  - Η Αρχή Εγγραφής με τον έλεγχο της εγκυρότητας των στοιχείων του χρήστη ζητά από την Αρχή Πιστοποίησης να πιστοποιήσει το δημόσιο κλειδί του χρήστη. Το δημόσιο κλειδί του χρήστη μπορεί να δημιουργηθεί από
    - Την αρχή πιστοποίησης η οποία όμως θα πρέπει μετά να του δώσει με πολύ ασφαλή τρόπο το ιδιωτικό κλειδί (αυτός ο τρόπος δε συνηθίζεται για κλειδιά που χρησιμοποιούνται για ψηφιακές υπογραφές).
    - Τον ίδιο το χρήστη ο οποίος όμως θα πρέπει να αποδείξει ότι είναι κάτοχος του αντίστοιχου ιδιωτικού κλειδιού.
  - Το πιστοποιητικό δημοσιεύεται στον κατάλογο πιστοποιητικών – ένα αντίγραφο δίνεται στον χρήστη

204

Εγγραφή και έκδοση πιστοποιητικού



205

Χρήση πιστοποιητικών για την επαλήθευση υπογραφής

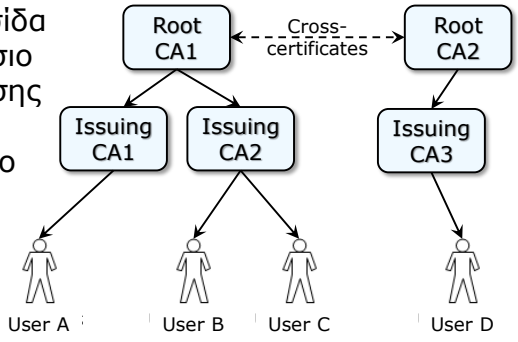
- **Το πιστοποιητικό στέλνεται μαζί με το υπογεγραμμένο έγγραφο:**
  - Η Β ελέγχει τα στοιχεία του πιστοποιητικού και ότι ανήκει στον υπογράφοντα
  - Επαληθεύει ότι τη συγκεκριμένη μέρα και ώρα που χρησιμοποιεί το πιστοποιητικό είναι σε ισχύ
  - Επαληθεύει την εγκυρότητα του πιστοποιητικού
    - Χρησιμοποιώντας το δημόσιο κλειδί της Αρχής Πιστοποίησης (αυθεντικοποιημένο αντίγραφο της οποίας θεωρούμε ότι έχουν όλες οι οντότητες που χρησιμοποιούν κλειδιά σε αυτήν την υποδομή)
    - Θα ελέγξει εάν το πιστοποιητικό έχει ανακληθεί
  - Αν δεν υπάρχουν προβλήματα η Β δέχεται ότι το δημόσιο κλειδί στο πιστοποιητικό είναι ένα αυθεντικοποιημένο κλειδί της Α

Υποδομή Δημοσίου Κλειδιού

- **Τελικός Χρήστης**: Το υποκείμενο για το οποίο έχει εκδοθεί ένα πιστοποιητικό ύστερα από αίτηση του. Ο Τελικός Χρήστης είναι εξουσιοδοτημένος να χρησιμοποιεί το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που αναγράφεται στο πιστοποιητικό.
- **Τρίτος Συμμετέχων**: Το φυσικό πρόσωπο ή φορέας που ενεργεί βασιζόμενος στις πληροφορίες οι οποίες περιέχονται σε ένα ψηφιακό πιστοποιητικό.
- **Πολιτική Πιστοποίησης**: Πρόκειται για ένα σύνολο κανόνων αναφορικά με τη χρήση ενός πιστοποιητικού μέσα σε μια κοινωνία ή σύνολο εφαρμογών

Αλυσίδες πιστοποιητικών

- Μας δίνουν τη δυνατότητα να οδηγηθούμε σε ένα σημείο εμπιστοσύνης για την επαλήθευση ενός πιστοποιητικού τελικού χρήστη.
- Η αλυσίδα πιστοποιητικών ανταποκρίνεται σε μια αλυσίδα εμπιστοσύνης από το δημόσιο κλειδί της αρχής πιστοποίησης την οποία ο χρήστης εμπιστεύεται εως το δημόσιο κλειδί που θέλει να επαληθεύσει.



Υπηρεσίες εμπιστοσύνης στην ΕΕ – Κανονισμός No 910/2014 (eIDAS)

«**υπηρεσία εμπιστοσύνης**»: ηλεκτρονική υπηρεσία, συνήθως παρεχόμενη έναντι αμοιβής, η οποία συνίσταται:

- στη δημιουργία, εξακρίβωση και επικύρωση ηλεκτρονικών υπογραφών, ηλεκτρονικών σφραγίδων ή ηλεκτρονικών χρονοσφραγίδων, ηλεκτρονικών υπηρεσιών συστημένης παράδοσης και πιστοποιητικών που σχετίζονται με τις υπηρεσίες αυτές, ή
- στη δημιουργία, εξακρίβωση και επικύρωση πιστοποιητικών για επαλήθευση της ταυτότητας ιστοτόπων, ή
- στη διαφύλαξη ηλεκτρονικών υπογραφών, σφραγίδων ή πιστοποιητικών που σχετίζονται με τις υπηρεσίες αυτές·

Ηλεκτρονικές Υπογραφές στην ΕΕ – Κανονισμός Νο 910/2014 (eIDAS)

«**ηλεκτρονική υπογραφή**»: δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με άλλα δεδομένα σε ηλεκτρονική μορφή και τα οποία χρησιμοποιούνται από τον υπογράφοντα για να υπογράφει

Υπογραφές στην ΕΕ – Κανονισμός Νο 910/2014 (eIDAS)

«**προηγμένη ηλεκτρονική υπογραφή**»: ηλεκτρονική υπογραφή που πληροί τις ακόλουθες απαιτήσεις

- συνδέεται κατά τρόπο μοναδικό με τον υπογράφοντα·
- είναι ικανή να ταυτοποιεί τον υπογράφοντα·
- δημιουργείται με δεδομένα δημιουργίας ηλεκτρονικής υπογραφής τα οποία ο υπογράφων μπορεί, με υψηλό βαθμό εμπιστοσύνης, να χρησιμοποιεί υπό τον αποκλειστικό του έλεγχο, και
- συνδέεται με τα δεδομένα που έχουν υπογραφεί σε σχέση με αυτήν κατά τρόπο ώστε να μπορεί να ανιχνευθεί οποιαδήποτε επακόλουθη τροποποίηση των εν λόγω δεδομένων.

Υπογραφές στην ΕΕ – Κανονισμός Νο 910/2014 (eIDAS)

«**εγκεκριμένη ηλεκτρονική υπογραφή**»: προηγμένη ηλεκτρονική υπογραφή που δημιουργείται από **εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής υπογραφής** και η οποία βασίζεται σε **εγκεκριμένο πιστοποιητικό** ηλεκτρονικής υπογραφής·

Υπογραφές στην ΕΕ – Κανονισμός Νο 910/2014 (eIDAS)

Οι εγκεκριμένες διατάξεις δημιουργίας ηλεκτρονικής υπογραφής διασφαλίζουν, με τα κατάλληλα τεχνικά και διαδικαστικά μέσα, τουλάχιστον ότι:

α) διασφαλίζεται ευλόγως η εμπιστευτικότητα των δεδομένων δημιουργίας ηλεκτρονικής υπογραφής που χρησιμοποιούνται για τη δημιουργία της ηλεκτρονικής υπογραφής·

β) τα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής που χρησιμοποιούνται για τη δημιουργία της ηλεκτρονικής υπογραφής μπορούν να προκύψουν στην πράξη μία μόνο φορά·

γ) τα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής που χρησιμοποιούνται για τη δημιουργία ηλεκτρονικής υπογραφής δεν μπορούν, με εύλογη βεβαιότητα, να είναι παράγωγα και ότι η ηλεκτρονική υπογραφή προστατεύεται με τρόπο αξιόπιστο από πλαστογραφία με τη χρήση της τρέχουσας τεχνολογίας·

δ) τα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής που χρησιμοποιούνται για τη δημιουργία ηλεκτρονικής υπογραφής μπορούν να προστατεύονται κατά τρόπο αξιόπιστο από τον νόμιμο υπογράφοντα έναντι της χρησιμοποίησης τους από τρίτους.