ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
ΤΜΗΜΑ ΙΣΤΟΡΙΑΣ-ΑΡΧΑΙΟΛΟΓΙΑΣ

ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΕΜΠΙΣΤΟΣΥΝΗΣ ΣΕ ΠΟΛΙΤΙΣΜΙΚΑ ΠΕΡΙΒΑΛΛΟΝΤΑ

ΔΙΔΑΚΤΙΚΗ ΕΝΟΤΗΤΑ 7

ΘΕΜΑ: ΑΣΦΑΛΕΙΑ ΚΑΙ ΕΜΠΙΣΤΟΣΥΝΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ-ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Δημήτριος Κ. Κουκόπουλος
Αναπληρωτής Καθηγητής

Περιεχόμενα

- Στόχοι-Ανάγκες Ασφαλούς Διακίνησης στο Διαδίκτυο
- Ψηφιακά Πιστοποιητικά
- Ψηφιακές Υπογραφές
- Συναρτήσεις Κατακερματισμού
- Κρυπτογράφηση
- Βιβλιογραφία

Μη Ασφαλείς Ιδιότητες Διαδικτύου 1/2

- Περιορισμένη δυνατότητα ελέγχου δικτυακού περιβάλλοντος
  - Χρήση διαφόρων ειδών συσκευών και συνδέσεων
  - Αλληλεπίδραση μεταξύ χρηστών και παρόχου υπηρεσίας
- Ευαισθησία σε εσωτερικές επιθέσεις
- Χρήση ανασφαλών δημοσίων δικτύων
  - Υποκλοπή (line tapping)
  - Αλλαγή δεδομένων (data interception and alteration)
- Ύπαρξη μη-φυσικού μονοπατιού επικοινωνίας εξαιτίας φύσης Διαδικτύου (δημόσιο δίκτυο δικτύων)
  - Υποκλοπές (eavesdropping)
  - Ενεργείς παρεμβολές

Μη Ασφαλείς Ιδιότητες Διαδικτύου 2/2

- Ανοιχτό σύστημα
  - Δυσκολία σε καθορισμό ταυτότητας επικοινωνούντων μερών

- Ed Gerck: “Η επικοινωνία στο Internet μοιάζει με το να στέλνεις ανώνυμες κάρτες που απαντώνται από ανώνυμους παραλήπτες”

Βασικά Προβλήματα

- Παραποίηση ταυτότητας (spoofing)
- Υποκλοπή (eavesdropping)
- Αλλαγή δεδομένων (data alteration)

Στόχοι

- Αυθεντικοποίηση (authentication)-παρεμπόδιση παραποίησης ταυτότητας
- Ιδιωτικότητα (privacy) - παρεμπόδιση υποκλοπής
- Ακεραιότητα δεδομένων (data integrity) – αποφυγή αλλαγής δεδομένων
- Μη απόκρυψη προηγούμενης ενέργειας (non-repudiation)

Γνωστές Λύσεις

- Χρήση ψηφιακών πιστοποιητικών (digital certificates) και ψηφιακών υπογραφών (digital signatures) για ασφάλεια των Web servers.
- Χρήση κρυπτογραφικών αλγορίθμων
- Χρήση τεχνικών έμπιστης επικοινωνίας
  - Secure Sockets Layer (SSL) σε διαδικτυακούς φυλλομετρητές

Ψηφιακές Υπογραφές/Πιστοποιητικά

- Αυθεντικοποίηση
- Ακεραιότητα δεδομένων
- Υπηρεσίες αποφυγής άρνησης προηγούμενων ενεργειών

Κρυπτογραφικοί Αλγόριθμοι

Εξασφάλιση ιδιωτικότητας

Δημήτριος Κ. Κουκόπουλος
Αναπληρωτής Καθηγητής

SSL

- Πιο δημοφιλές πρωτόκολλο ασφαλείας στο διαδίκτυο.
- Διαθέτει υπηρεσίες κρυπτογράφησης και πιστοποίησης σε ένα TCP/IP περιβάλλον.
- Βάση για έμπιστη υποδομή στο διαδίκτυο, κυρίως e-banking, e-business.

Ανάγκη Ψηφιακής Πιστοποίησης

- Τα προβλήματα ψευδούς πιστοποίησης δεν επιλύονται με την κρυπτογράφηση ή με την χρήση ασφαλών πρωτοκόλλων.
- Παράδειγμα: Ασφαλής σύνδεση με έναν spoofing ιστότοπο.
- Επίλυση προβλήματος σύνδεσης ταυτότητας με δημόσιο κλειδί

Ορισμός Ψηφιακού Πιστοποιητικού

- Το ψηφιακό πιστοποιητικό είναι ένα ηλεκτρονικό αρχείο που προσδιορίζει μοναδικά τις επικοινωνούσες οντότητες στο διαδίκτυο.
- Τα πιστοποιητικά παρέχονται και υπογράφονται από την αρχή πιστοποίησης (certification authority).
- Η αρχή πιστοποίησης είναι αξιόπιστη και υπεύθυνη για τη σύνδεση ονόματος-δημοσίου κλειδιού.

Σκοπός Πιστοποίησης

- Συσχέτιση ονόματος οντότητας με δημόσιο κλειδί της.

- Εισαγωγή κατάλληλων ιδιοτήτων (tamperproof) ώστε ο λήπτης ενός μηνύματος να μπορεί να αποφασίσει αν το μήνυμα, το κλειδί και ο αποστολέας είναι αυτό που φαίνεται χωρίς να χρειαστεί να ρωτήσει τον αποστολέα.

Πρότυπα

ITU-T recommendation X.509 (πλαίσιο παροχής υπηρεσιών αυθεντικοποίησης)

Οντότητες

- **Αρχή πιστοποίησης** (CA): παρέχει πιστοποιητικά.
- **Συνδρομητές** (CA clients): παίρνουν πιστοποιητικά
- **Χρήστες**: το κοινό που αποφασίζει αξιολογώντας πιστοποιητικά

Αρχή Πιστοποίησης

- Έλεγχος υπηρεσιών αυθεντικοποίησης και διαχείριση πιστοποιητικών
- Ονομάζεται και πάροχος (issuer)
- Είναι ανεξάρτητες αρχές:
  - Δημόσιες (τράπεζες)
  - Εμπορικές (VeriSign)
  - Ιδιωτικές
  - Προσωπικές
- Η σχέση αρχής πιστοποίησης, συνδρομητών και χρηστών καθορίζεται από το Certification Practice Statement(CPS) που καθορίζεται από την αρχή

Συνδρομητής

- Ο συνδρομητής είναι μια οντότητα που παρέχει στην αρχή πιστοποίησης όλες τις αναγκαίες πληροφορίες για τη δημιουργία του δικού του πιστοποιητικού. Το πιστοποιητικό τελικά υπογράφεται από την αρχή πιστοποίησης.

- Εμπορικός πελάτης σε αρχή πιστοποίησης.

- Η αρχή πιστοποίησης δεν παρέχει εγγυήσεις για τις πληροφορίες που τις δίνει ο συνδρομητής για να ενσωματώσει στο πιστοποιητικό του.

Χρήστης

Οντότητα που εμπιστεύεται την αξιοπιστία ενός πιστοποιητικού που εκδίδει μια αρχή πιστοποίησης για να συλλέξει πληροφορίες για έναν συνδρομητή.

Αρχή Ονοματοδοσίας

- Η αρχή ονοματοδοσίας (naming authority-NA) καθορίζει το σχήμα ονοματοδοσίας που χρησιμοποιείται από την αρχή πιστοποίησης.
- Η αρχή πιστοποίησης μπορεί να λειτουργήσει ως αρχή ονοματοδοσίας.
- Η αρχή πιστοποίησης αναφέρεται σε ένα όνομα, ενώ η αρχή ονοματοδοσίας το δηλώνει.

Πιστοποιητικό X.509

- Τιμή δημοσίου κλειδιού του κατόχου του πιστοποιητικού
- Μοναδική ταυτότητα (όνομα) του κατόχου του πιστοποιητικού (DN)
- Έκδοση του προτύπου του πιστοποιητικού
- Σειριακός αριθμός πιστοποιητικού
- Προσδιοριστής αλγορίθμου υπογραφής (για υπογραφή χρηστών)
- Όνομα αρχής πιστοποίησης
- Περίοδος χρήσης
- Επεκτάσεις

Υπογράφεται ψηφιακά από αρχή πιστοποίησης με ιδιωτικό της κλειδί.

Διαδικασία Απόκτησης Πιστοποιητικού X.509

1. Δημιουργία δημόσιου/ιδιωτικού κλειδιού για υπογραφή
2. Επιλογή αρχής πιστοποίησης και συλλογή πληροφοριών που απαιτεί η αρχή
3. Αποστολή αίτησης μαζί με δημόσια κλειδιά και πληροφορίες
4. Αξιολόγηση πληροφοριών από αρχή πιστοποίησης
5. Δημιουργία πιστοποιητικού από αρχή πιστοποίησης
6. Αποστολή πιστοποιητικού
7. Φόρτωση πιστοποιητικού σε υπολογιστή και χρήση

Σχήμα Ονοματοδοσίας σε X.509 Πιστοποιητικά

- Ένα πιστοποιητικό συσχετίζει ένα δημόσιο κλειδί με το μοναδικό διακριτό όνομα ενός χρήστη.
- Το διακριτό όνομα ενός χρήστη δηλώνεται από μια αρχή ονοματοδοσίας και γίνεται αποδεκτό από μια αρχή πιστοποίησης ως μοναδικό μέσα στο πεδίο της συγκεκριμένης αρχής πιστοποίησης.
- Ένας χρήστης μπορεί να έχει διαφορετικά διακριτά ονόματα σε διαφορετικές αρχές πιστοποίησης

Σχήμα Ονοματοδοσίας σε X.509 Πιστοποιητικά

- Ένας χρήστης μπορεί να έχει το ίδιο διακριτό όνομα σε διαφορετικές αρχές πιστοποίησης ακόμη και αν αυτό έχει ήδη χρησιμοποιηθεί.

Πιστοποίηση σε Φυλλομετρητή Χρήστη

1. Ο φυλλομετρητής λαμβάνει ένα ψηφιακό πιστοποιητικό.
2. Ελέγχει αν η ημερομηνία λήψης είναι έγκυρη και αν το πιστοποιητικό έχει ανακληθεί.
3. Ο φυλλομετρητής προσπαθεί να βρει ένα διακριτό όνομα αρχής από τη λίστα έμπιστων αρχών πιστοποίησης, ενώ ελέγχει αν η αιτούσα αρχή πιστοποίησης είναι έμπιστη.
4. Αν η αρχή είναι έμπιστη, ο φυλλομετρητής ελέγχει αν το δημόσιο κλειδί της αιτούσας αρχής εγκρίνει την ψηφιακή υπογραφή του αιτούντα.
5. Ελέγχει αν το όνομα πεδίου που καθορίζεται στο διακριτό όνομα του εξυπηρετητή ταιριάζει με το πραγματικό όνομα πεδίου του εξυπηρετητή.

Πρόβλημα Πιστοποίησης

- Ένα πιστοποιητικό δε μπορεί να πιστοποιήσει τον εαυτό του.
- Ανάγκη ανώτερης αρχής πιστοποίησης.
- Το δημόσιο κλειδί των αρχών πιστοποίησης είναι στόχος εκτεταμένων επιθέσεων αποκρυπτογράφησης. Λύση με χρήση μεγάλων κλειδιών και με αυξημένη συχνότητα αλλαγής τους.

Γνωστές Αρχές Πιστοποίησης

- VeriSign (www.verisign.com)
- Thawte (www.thawte.com)

Ψηφιακές Υπογραφές

Στόχοι:

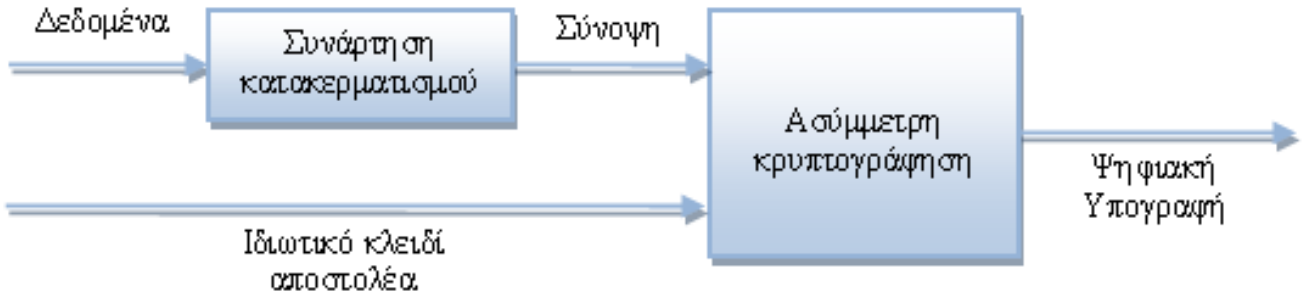
- Αυθεντικοποίηση πηγής
- Αυθεντικοποίηση ακεραιότητας δεδομένων
- Αποφυγή άρνησης προηγούμενης ενέργειας

Δημιουργία Ψηφιακής Υπογραφής

Έστω ότι έχουμε ένα μήνυμα με μεταβλητό μέγεθος που θέλουμε να υπογράψουμε ψηφιακά.

- Δημιουργία περίληψης μηνύματος (message digest) με τη χρήση αλγορίθμου κατακερματισμού μονής κατεύθυνσης (RSA-MD2, RSA-MD5, NIST-SHS). Η περίληψη μηνύματος έχει σταθερό μέγεθος 128 ή 160 bits.
- Κρυπτογράφηση της περίληψης μηνύματος με ιδιωτικό κλειδί.
- Το αποτέλεσμα της κρυπτογράφησης είναι η ψηφιακή υπογραφή.

Απεικόνιση Δημιουργίας Ψηφιακής Υπογραφής



Δημήτριος Κ. Κουκόπουλος
Αναπληρωτής Καθηγητής

Χρήση Ψηφιακής Υπογραφής

Η ψηφιακή υπογραφή στέλνεται μαζί με το μήνυμα μέσω ενός μη-ασφαλούς καναλιού.

Αυθεντικοποίηση Μηνύματος με Ψηφιακή Υπογραφή

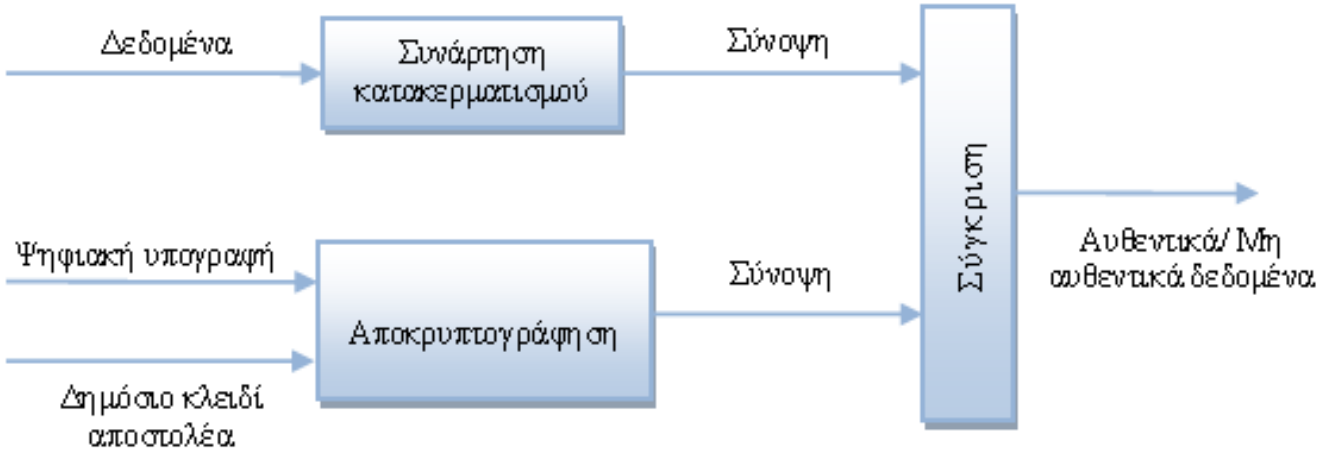
1. Λήψη μηνύματος και ψηφιακής υπογραφής σε παραλήπτη.

2. Χρήση δημοσίου κλειδιού αποστολέα για αποκρυπτογράφηση ψηφιακής υπογραφής σε περίληψη μηνύματος (D’).

3. Δημιουργία νέας περίληψης μηνύματος (D’’) από ληφθέν μήνυμα με τη χρήση του ίδιου αλγορίθμου κατακερματισμού όπως ο αποστολέας.

4. Σύγκριση D’ και D’’. Αν είναι ίσα το ληφθέν μήνυμα είναι αυθεντικό.

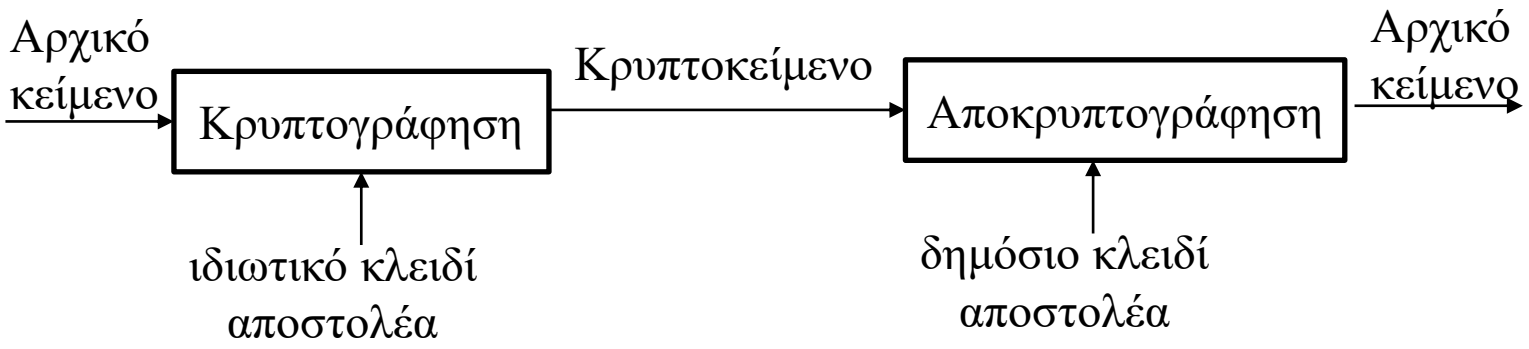
Έλεγχος Ψηφιακής Υπογραφής



Δημήτριος Κ. Κουκόπουλος
Αναπληρωτής Καθηγητής

Μηχανισμός Ψηφιακής Υπογραφής RSA

- Όταν ο RSA χρησιμοποιείται για δημιουργία και επαλήθευση ψηφιακών υπογραφών, ονομάζεται μηχανισμός (σχήμα) ψηφιακής υπογραφής RSA.
- Στο μηχανισμό ψηφιακής υπογραφής RSA χρησιμοποιείται το ζεύγος ιδιωτικού και δημοσίου κλειδιού του αποστολέα και όχι του παραλήπτη.
- Στην ασύμμετρη κρυπτογραφία η ακεραιότητα διασφαλίζεται όταν ο αποστολέας υπογράφει με το ιδιωτικό κλειδί του και ο παραλήπτης επαληθεύει με το δημόσιο κλειδί του αποστολέα.



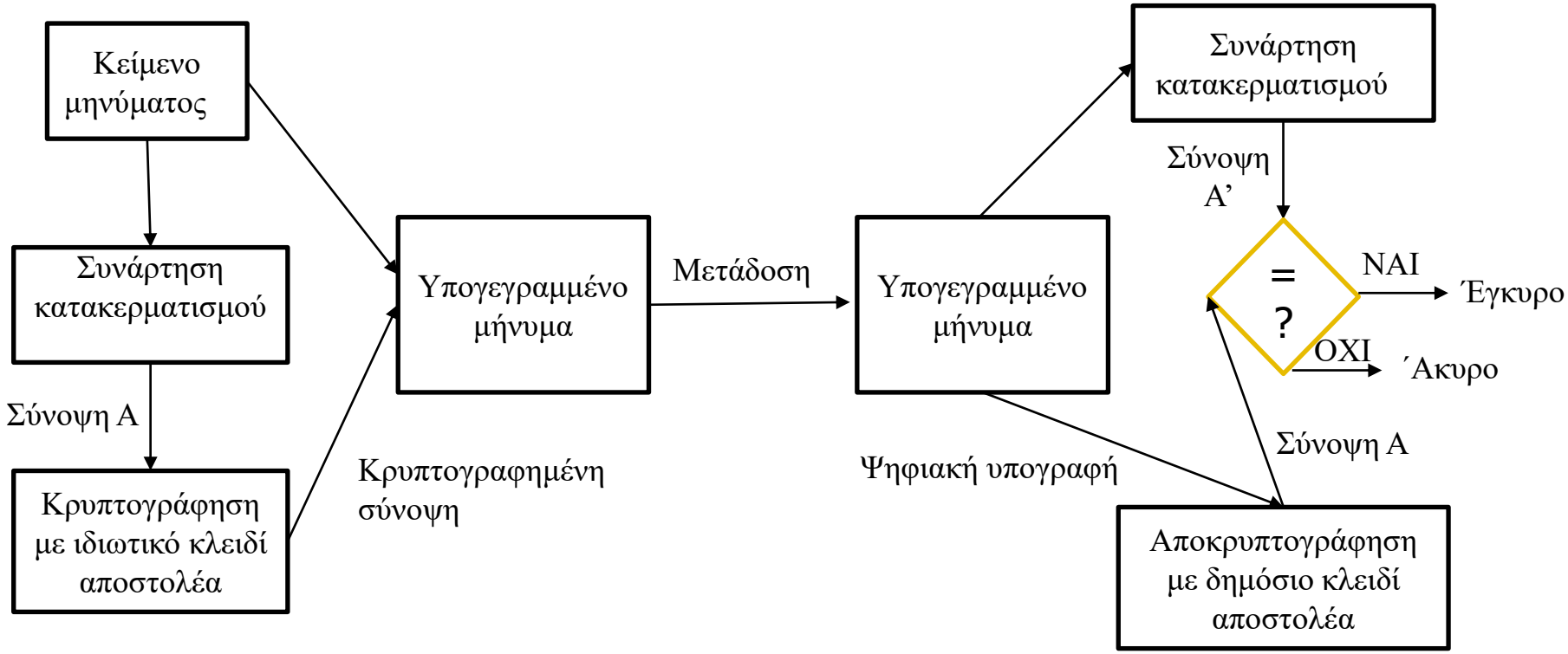
Σχήμα RSA – Αποστολέας

- Δημιουργία σύνοψης μηνύματος **A** (μικρό και σταθερό σε μέγεθος μήνυμα) με τη χρήση μιας συνάρτησης κατακερματισμού.
- Κρυπτογράφηση σύνοψης με τη χρήση του ιδιωτικού κλειδιού του αποστολέα (ψηφιακή υπογραφή μηνύματος).
- Αποστολή μηνύματος ως αρχικό κείμενο, συνοδευόμενο από την ψηφιακή υπογραφή του (το κρυπτοκείμενο της σύνοψης και την ταυτότητα της συνάρτησης κατακερματισμού που χρησιμοποιήθηκε για την παραγωγή της σύνοψης)

Σχήμα RSA – Παραλήπτης

- Λήψη μηνύματος.
- Παραγωγή σύνοψης μηνύματος **A'** με τη χρήση της ίδιας συνάρτησης κατακερματισμού, όπως σε αποστολέα.
- Αποκρυπτογράφηση της ψηφιακής υπογραφής με το δημόσιο κλειδί του αποστολέα και εξαγωγή της σύνοψης **A** που είχε στείλει ο αποστολέας.
- Αν οι δύο συνόψεις είναι ίδιες, **A = A'**, τότε το κείμενο δεν έχει αλλοιωθεί (διαφύλαξη της ακεραιότητας), ενώ η επιτυχής αποκρυπτογράφηση με χρήση του δημόσιου κλειδιού επιβεβαιώνει την ταυτότητα του αποστολέα (αυθεντικοποίηση πηγής προέλευσης).

Σχήμα RSA



Δημήτριος Κ. Κουκόπουλος
Αναπληρωτής Καθηγητής

Δημιουργία/Επαλήθευση Ψηφιακών Υπογραφών με Χρήση RSA Online tool

- https://8gwifi.org/rsasignverifyfunctions.jsp

DSA/DSS

- Το Digital Signature Standard (DSS) αποτελεί πρότυπο του NIST από το 1994.
- Το πρότυπο DSS στηρίζεται στον αλγόριθμο Digital Signature Algorithm (DSA) που βασίζεται στο μηχανισμό El-Gamal.
- Χρησιμοποιείται μόνο για ψηφιακή υπογραφή.
- Η ανθεκτικότητά του βασίζεται στο δύσκολο πρόβλημα υπολογισμού των διακριτών λογαρίθμων.

DSA/DSS – Δημιουργία Δημόσιου/Ιδιωτικού Κλειδιού

- Επιλογή ενός πρώτου αριθμού q
- Επιλογή ενός πρώτου αριθμού p μήκους 512 - 1024 bits, τέτοιος ώστε το q να διαιρεί το $p – 1$
- Επιλέγεται $g = n\ (p - 1) / q \bmod p$, όπου n ακέραιος και $1 < n < (p – 1)$
- Επιλέγεται τυχαία το ιδιωτικό κλειδί x που είναι αριθμός με $0 < x < (q - 1)$
- Υπολογισμός δημόσιου κλειδιού (p, q, g, y) από το x, όπου $y = g^x \bmod p$

DSA/DSS – Δημιουργία Υπογραφής σε Αποστολέα

Για τη σύνοψη h η ψηφιακή υπογραφή αποτελείται από τους αριθμούς r και s:

- $r = (g^k \bmod p) \bmod q$
- $s = (k^{-1} (h + x\, r)) \bmod q$, όπου k μια τυχαία τιμή διαφορετική για κάθε υπογραφή.

DSA/DSS – Έλεγχος Υπογραφής σε Παραλήπτη

- Ο παραλήπτης, λαμβάνει τα r και s και υπολογίζει τη συνόψιση h.

- Στη συνέχεια, επιβεβαιώνει την υπογραφή εκτελώντας τα ακόλουθα βήματα:
  - $w = s^{-1} \bmod q$
  - $u1 = (h\ w) \bmod q$
  - $u2 = (r\ w) \bmod q$
  - $u = (g^{u1}\ y^{u2} \bmod p) \bmod q$
  - Η υπογραφή είναι έγκυρη, αν $w = u$

Δημιουργία/Επαλήθευση Ψηφιακών Υπογραφών με Χρήση DSA Online tool

- https://8gwifi.org/dsafunctions.jsp

Συναρτήσεις Κατακερματισμού

- **Ορισμός**: Μια κρυπτογραφική συνάρτηση κατακερματισμού (hashing function) h δέχεται ως είσοδο μια σειρά m από bits αυθαιρέτου μεγέθους, και παράγει στην έξοδο μια σειρά $h(m)$ από bits (σύνοψη μηνύματος-message digest/hash value) με ένα προκαθορισμένο σταθερό μέγεθος, έστω k bits.

- Η διαδικασία κατακερματισμού αποτελεί στην ουσία μια λειτουργία συμπίεσης.

- Μια βασική ιδιότητα των συναρτήσεων κατακερματισμού είναι η ευκολία υπολογισμού της εξόδου.

Ιδιότητες Συνάρτησης Κατακερματισμού

Μια ιδανική κρυπτογραφική συνάρτηση κατατεμαχισμού έχει τις παρακάτω ιδιότητες:

- Είναι εύκολο να υπολογιστεί η σύνοψη για οποιαδήποτε είσοδο.
- Δεν είναι εφικτό να βρεις την είσοδο από την σύνοψη (αντοχή προαπεικόνισης ή μονόδρομη συμπεριφορά).
- Δεν είναι εφικτό να τροποποιήσεις την είσοδο, χωρίς να τροποποιηθεί η σύνοψη (αντοχή δεύτερης προ-απεικόνισης).
- Δεν είναι εφικτό να βρεθούν δύο διαφορετικές είσοδοι που δίνουν την ίδια σύνοψη (αντοχή σε συγκρούσεις).

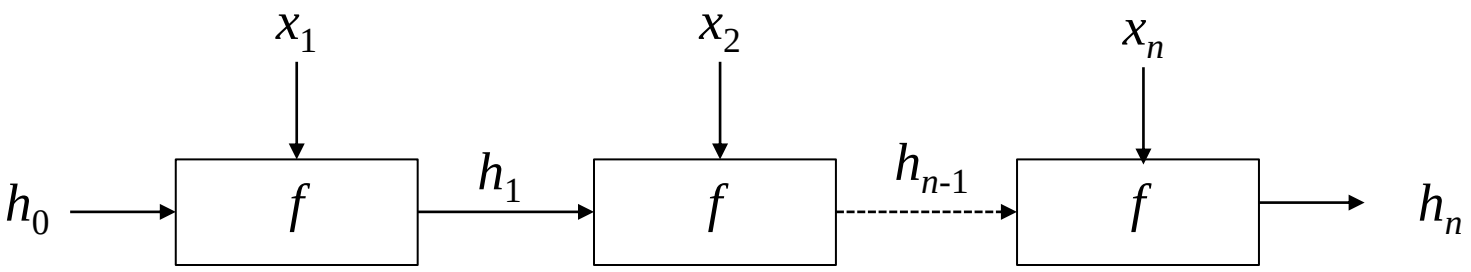
Βασική Λειτουργία

- Ο υπολογισμός της συνόψισης h ενός μηνύματος m γίνεται με επαναληπτική εφαρμογή μιας συνάρτησης συμπίεσης f στις δέσμες, που χωρίζεται το μήνυμα, όπου x_i η i-στη δέσμη του μηνύματος με $i = 1 \ldots n$.
- Ξεκινώντας από μια σταθερή αρχική τιμή συνόψισης h_0, υπολογίζονται οι ενδιάμεσες συνοψίσεις, ως εξής:

  $h_i = f\,(x_i \,||\, h_{i-1})$, για $i = 1 \ldots n$, όπου || σημαίνει συνένωση.

- Η τελευταία υπολογισμένη συνόψιση h_n είναι η τελική συνόψιση h του μηνύματος m.
- Η συνάρτηση συμπίεσης f δέχεται ως είσοδο σειρές από bits σταθερού μήκους.

Βασική Λειτουργία



Δημήτριος Κ. Κουκόπουλος
Αναπληρωτής Καθηγητής

Σκοπός Κρυπτογράφησης

Ιδιωτικότητα

Δημήτριος Κ. Κουκόπουλος
Αναπληρωτής Καθηγητής

Κρυπτογραφημένη Μετάδοση Μηνύματος

- Ο αποστολέας κρυπτογραφεί ένα απλό μήνυμα με τη χρήση ενός αλγορίθμου κρυπτογράφησης και κατάλληλων κλειδιών.
- Μετά την κρυπτογράφηση το μήνυμα στέλνεται στον παραλήπτη μέσω ενός μη ασφαλούς καναλιού.
- Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με τη χρήση του κατάλληλου αλγορίθμου αποκρυπτογράφησης και των κατάλληλων κλειδιών.

SSL

- Παρέχει υπηρεσίες κρυπτογράφησης και πιστοποίησης σε περιβάλλον TCP/IP.
- Είναι η βάση για έμπιστες υπηρεσίες στο διαδίκτυο.
- Στηρίζεται στη διαστρωμάτωση των δικτύων σε επίπεδα (ISO/OSI).
- Παίζει το ρόλο υποεπιπέδου στο επίπεδο δικτύου και προστατεύει πρωτόκολλα υψηλότερων επιπέδων, όπως telnet, ftp, http, s-http.

Βιβλιογραφία

- ITU-T, “Summary of ITU-T Recommendation X.509”, 2001.
- E. Gerck, “Overview of Certification Systems”, 2000
- A. Shostack, “An Overview of SSL”, 1995.
- Digital Signature Standard (DSS), Federal Information Processing Standard (FIPS) 186-4, 2013.
- Q. Dang, Recommendation for applications using approved hash algorithms, NIST SP 800-107, 2012.