Εισαγωγή στην επιστήμη της Πληροφορικής και των Τηλεπικοινωνιών

Ασφάλεια

Περιεχόμενα

- **Πλευρές Ασφάλειας**
- **Ιδιωτικό Απόρρητο**
  - **Μέθοδος Μυστικού Κλειδιού (Συμμετρική Κρυπτογράφηση)**
  - **Μέθοδος Δημόσιου Κλειδιού (Ασύμμετρη Κρυπτογράφηση)**
  - **Συνδυασμός Μεθόδων**
- **Ψηφιακή Υπογραφή**
  - **Υπογραφή Ολόκληρου του Εγγράφου**
  - **Υπογραφή Σύνοψης του Εγγράφου**

Πλευρές Ασφάλειας

- Ιδιωτικό Απόρρητο (confidentiality)
- Πιστοποίηση Αυθεντικότητας (authentication)
- Ακεραιότητα (integrity)
- Μη - απάρνηση (non-repudiation)

Περιεχόμενα

- **Πλευρές Ασφάλειας**
- **Ιδιωτικό Απόρρητο**
  - **Μέθοδος Μυστικού Κλειδιού (Συμμετρική Κρυπτογράφηση)**
  - **Μέθοδος Δημόσιου Κλειδιού (Ασύμμετρη Κρυπτογράφηση)**
  - **Συνδυασμός Μεθόδων**
- **Ψηφιακή Υπογραφή**
  - **Υπογραφή Ολόκληρου του Εγγράφου**
  - **Υπογραφή Σύνοψης του Εγγράφου**

Ιδιωτικό Απόρρητο

- Απαιτεί
  - Κρυπτογράφηση στη θέση του αποστολέα
  - Αποκρυπτογράφηση στη θέση του παραλήπτη
- Μέθοδοι Κρυπτογράφησης/ Αποκρυπτογράφησης
  - Διαφυλάσσουν το Ιδιωτικό Απόρρητο
  - Δύο είδη
    - Μέθοδοι μυστικού κλειδιού
    - Μέθοδοι δημόσιου κλειδιού

Περιεχόμενα

- **Πλευρές Ασφάλειας**
- **Ιδιωτικό Απόρρητο**
  - **Μέθοδος Μυστικού Κλειδιού (Συμμετρική Κρυπτογράφηση)**
  - **Μέθοδος Δημόσιου Κλειδιού (Ασύμμετρη Κρυπτογράφηση)**
  - **Συνδυασμός Μεθόδων**
- **Ψηφιακή Υπογραφή**
  - **Υπογραφή Ολόκληρου του Εγγράφου**
  - **Υπογραφή Σύνοψης του Εγγράφου**

Εξασφάλιση Ιδιωτικού Απόρρητου με τη μέθοδο μυστικού κλειδιού

- Ο αποστολέας χρησιμοποιεί το κλειδί κι έναν αλγόριθμο κρυπτογράφησης (encryption)
- Ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί και τον αντίστοιχο αλγόριθμο αποκρυπτογράφησης (decryption)
- Ίδιο μυστικό κλειδί
- Αντίστροφοι αλγόριθμοι
- Απλό κείμενο -> plain text
- Κρυπτοκείμενο -> cipher text

Συμμετρική Κρυπτογράφηση

- Είναι η άλλη ονομασία της μεθόδου του μυστικού κλειδιού, επειδή το ίδιο κλειδί μπορεί να χρησιμοποιηθεί σε αμφίδρομη επικοινωνία

- Οι αλγόριθμοι κρυπτογράφησης μυστικού κλειδιού συχνά ονομάζονται *αλγόριθμοι συμμετρικής κρυπτογράφησης*

- Η μέθοδος αυτή χρησιμοποιείται πάνω από 2.000 χρόνια

ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ
Κρυπταλγόριθμοι Συμμετρικού Κλειδιού

Κρυπτογράφηση συμμετρικού κλειδιού.
Αναπαρίσταται ως «κλείδωμα» και «ξεκλείδωμα» με το ίδιο κλειδί

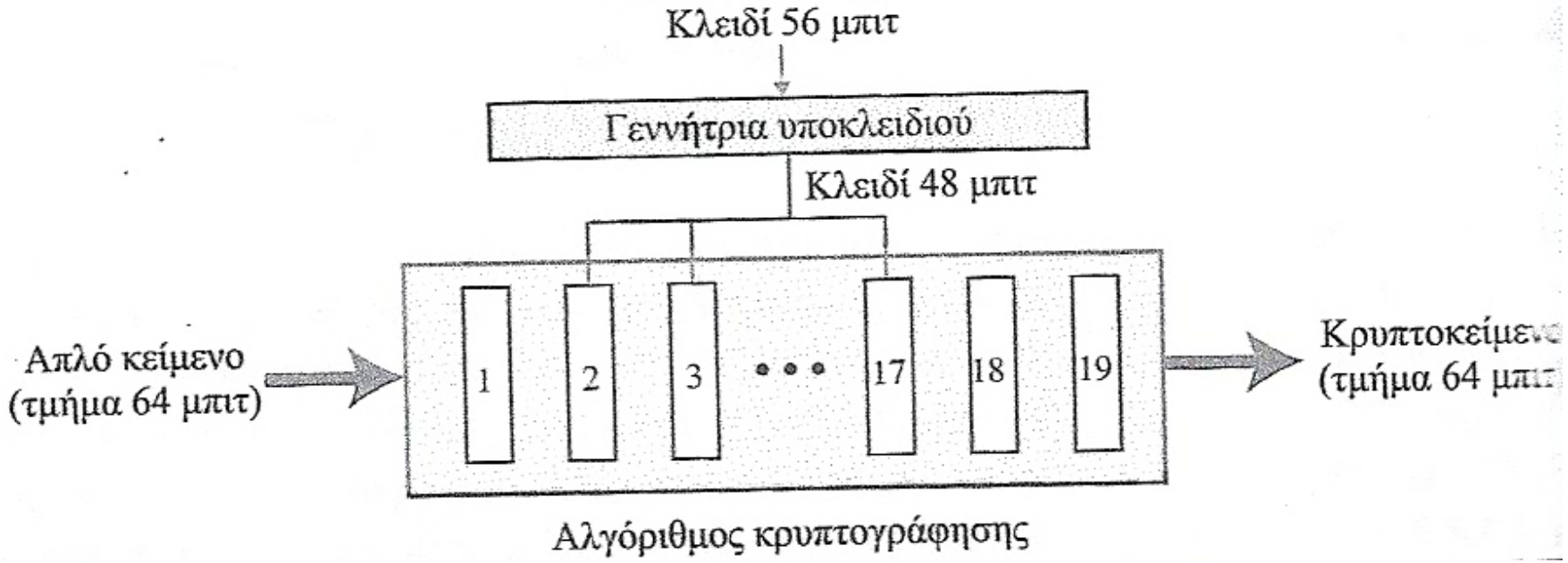
Αλγόριθμοι Συμμετρικής Κρυπτογράφησης

- Στην αρχή οι αλγόριθμοι ήταν απλοί
  - Κάποιος μπορούσε εύκολα να μαντέψει τα κλειδιά
- Σήμερα χρησιμοποιούνται εξελιγμένοι αλγόριθμοι
  - Ο πιο γνωστός είναι το **πρότυπο κρυπτογράφησης δεδομένων**

Πρότυπο Κρυπτογράφησης Δεδομένων (Data Encryption Standard – DES) (1/2)

- Η κ/α γίνεται σε επίπεδο μπιτ
- Μετατροπή δεδομένων σε ακολουθίες 64 μπιτ
- Κάθε τμήμα κρυπτογραφείται με ένα κλειδί 56 μπιτ
- Ιδέα της μεθόδου:
  - μίξη δεδομένων και κλειδιού ώστε κάθε μπιτ του κρυπτοκειμένου να εξαρτάται από κάθε μπιτ του απλού κειμένου και του κλειδιού

Πρότυπο Κρυπτογράφησης Δεδομένων (Data Encryption Standard – DES) (2/2)



Πλεονεκτήματα και Μειονεκτήματα αλγορίθμων μυστικού κλειδιού

Πλεονεκτήματα

- Απαιτούν λιγότερο χρόνο για κ/α από τους αλγόριθμους δημόσιου κλειδιού -> καλές λύσεις για μεγάλα μηνύματα

Μειονεκτήματα

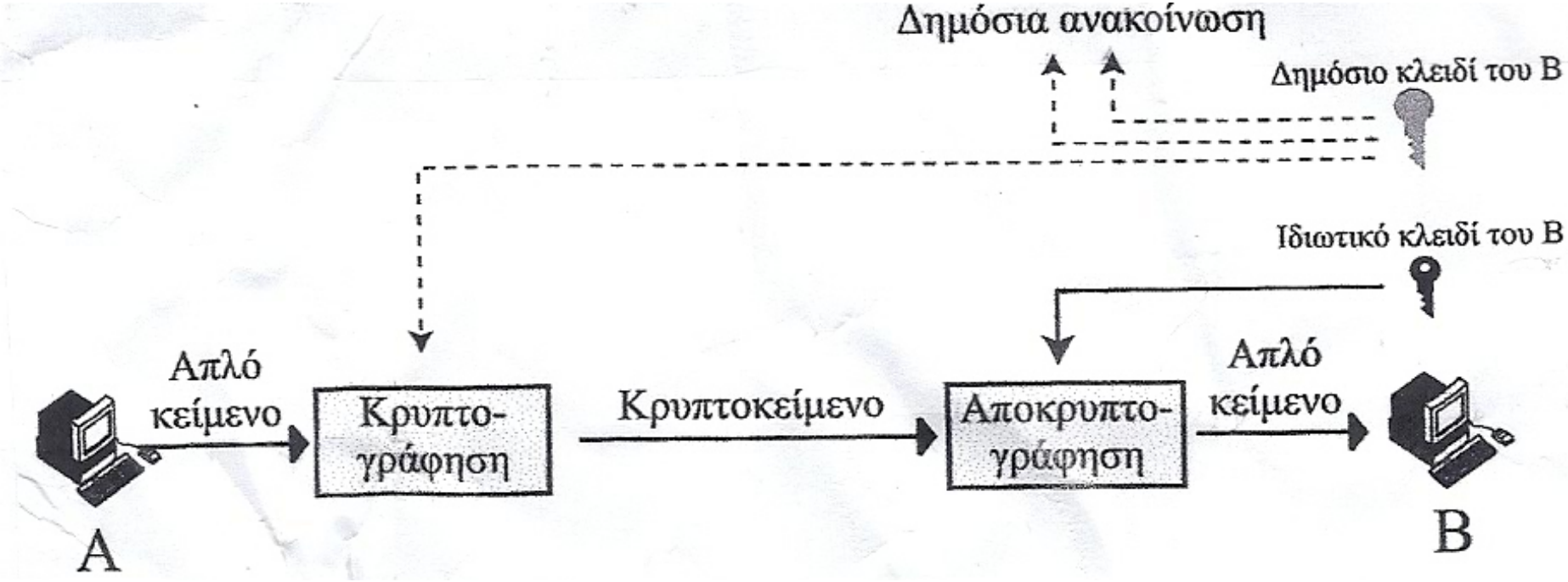
- Κάθε ζεύγος χρηστών χρειάζεται ένα ξεχωριστό μυστικό κλειδί.
  - Δηλ: Ν χρήστες -> **N(N-1)/2** μυστικά κλειδιά.
  - π.χ. 1 εκατομ. Χρήστες -> μισό τρισεκατομ. κλειδιά
- Η διανομή των κλειδιών στα δύο μέρη μπορεί να είναι δύσκολη

Περιεχόμενα

- **Πλευρές Ασφάλειας**
- **Ιδιωτικό Απόρρητο**
  - **Μέθοδος Μυστικού Κλειδιού (Συμμετρική Κρυπτογράφηση)**
  - **Μέθοδος Δημόσιου Κλειδιού (Ασύμμετρη Κρυπτογράφηση)**
  - **Συνδυασμός Μεθόδων**
- **Ψηφιακή Υπογραφή**
  - **Υπογραφή Ολόκληρου του Εγγράφου**
  - **Υπογραφή Σύνοψης του Εγγράφου**

Κρυπτογράφηση Δημόσιου Κλειδιού (Ασσύμετρη κρυπτογράφηση)

- Δύο κλειδιά: ιδιωτικό και δημόσιο
- Διαφορετικοί αλγόριθμοι κ/α



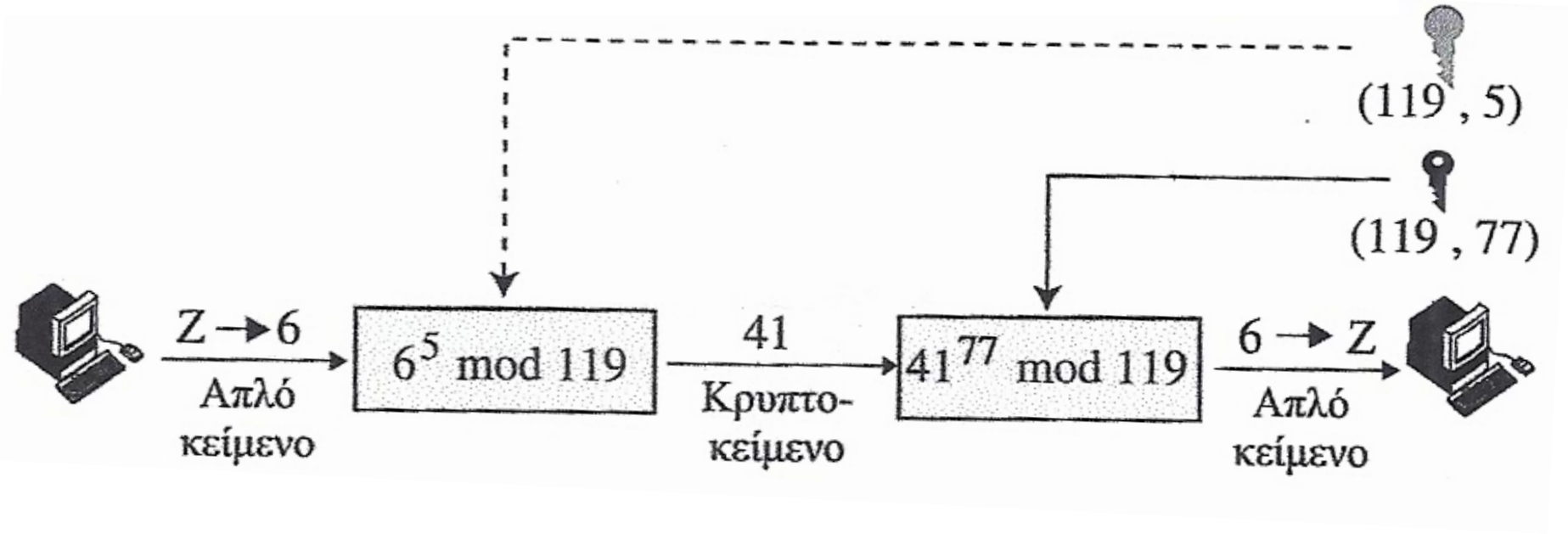
Αλγόριθμος Δημόσιου Κλειδιού RSA
(River-Shamir-Adleman 1978)

- Το ιδιωτικό κλειδί αποτελείται από ένα ζεύγος αριθμών ***(N, d)***
- Το δημόσιο κλειδί αποτελείται από ένα άλλο ζεύγος αριθμών ***(N, e)***
- Αλγόριθμος κρυπτογράφησης: $\boldsymbol{C = P^e \bmod N}$
  - *P: αριθμός που αναπαριστά το απλό κείμενο*
  - *C: αριθμός που αναπαριστά το κρυπτοκείμενο. Είναι το υπόλοιπο της διαίρεσης του* P^e διά του *N*
- Αλγόριθμος αποκρυπτογράφησης: $\boldsymbol{P = C^d \bmod N}$
- Η ασφάλεια του RSA προκύπτει από τη δυσκολία παραγοντοποίησης μεγάλων αριθμών. Γι αυτό, τα ***d*** και ***e*** είναι πολύ μεγάλοι αριθμοί (σήμερα, συνήθως της τάξης των 1024 με 2048 μπιτς)

Παράδειγμα Αλγορίθμου RSA (1/2)

- Ιδιωτικό κλειδί ***(N=119, d=77)***
- Δημόσιο κλειδί ***(N=119, e=5)***
- Αλγόριθμος κρυπτογράφησης: $C = P^e \bmod N$
  - Απλό κείμενο: το γράμμα Z. Το αντιστοιχίζουμε με τον αριθμό 6. Άρα $P = 6$
  - $C = 6^5 \bmod 119 = 41$
- Αλγόριθμος αποκρυπτογράφησης: $P = C^d \bmod N \rightarrow 41^{77} \bmod 119 = 6$

Παράδειγμα Αλγορίθμου RSA (2/2)



Επιλογή Δημόσιου και Ιδιωτικού Κλειδιού

- Επιλέγονται δυο τυχαίοι μεγάλοι πρώτοι αριθμοί, ***p*** και ***q***

  (δηλ. αριθμοί που οι μόνοι φυσικοί διαιρέτες τους είναι η μονάδα και ο εαυτός τους)

- Υπολογίζεται το ***N*** = ***p*** x ***q***
- Επιλέγεται το ***e*** έτσι ώστε
  - ***e*** < ***N*** και
  - ***e*** είναι σχετικά πρώτος με το (***p*** -1)(***q***-1)
- Επιλέγεται το ***d*** έτσι ώστε έτσι ώστε

  (***e*** x ***d***) mod [(***p*** -1)(***q***-1)] να ισούται με 1

Πλεονεκτήματα και Μειονεκτήματα Αλγόριθμου δημόσιου κλειδιού

Πλεονέκτημα

- Το πλήθος των κλειδιών: κάθε οντότητα δημιουργεί ένα ζεύγος κλειδιών, κρατά το ένα μυστικό και δημοσιοποιεί το άλλο
  - -> για επικοινωνία N χρηστών χρειάζονται μόνο **2N** κλειδιά

Μειονέκτημα

- Πολυπλοκότητα: για την αποτελεσματικότητα του αλγόριθμου απαιτούνται μεγάλοι αριθμοί
  - χρονοβόρος υπολογισμός του κρυπτοκειμένου
  - δεν συνιστάται για μεγάλα κείμενα

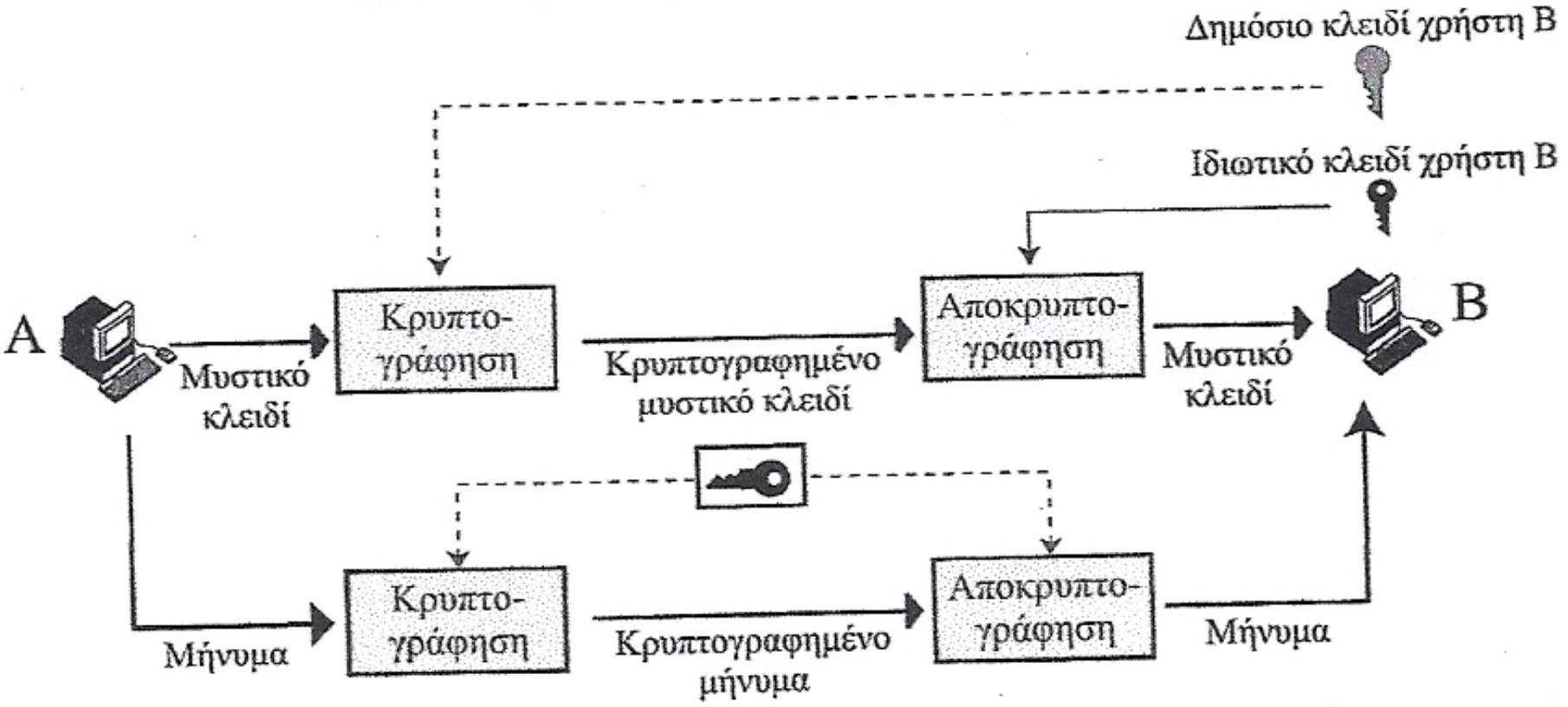
Περιεχόμενα

- **Πλευρές Ασφάλειας**
- **Ιδιωτικό Απόρρητο**
  - **Μέθοδος Μυστικού Κλειδιού (Συμμετρική Κρυπτογράφηση)**
  - **Μέθοδος Δημόσιου Κλειδιού (Ασύμμετρη Κρυπτογράφηση)**
  - **Συνδυασμός Μεθόδων**
- **Ψηφιακή Υπογραφή**
  - **Υπογραφή Ολόκληρου του Εγγράφου**
  - **Υπογραφή Σύνοψης του Εγγράφου**

Εξασφάλιση Ιδιωτικού Απόρρητου με Συνδυασμό Μεθόδων (1/2)

- Συνδυάζει το πλεονέκτημα του αλγόριθμου μυστικού κλειδιού (αποδοτικότητα) με το πλεονέκτημα του αλγόριθμου δημόσιου κλειδιού (εύκολη διανομή κλειδιών)
- Το δημόσιο κλειδί χρησιμοποιείται για την κρυπτογράφηση του μυστικού κλειδιού
- Το μυστικό κλειδί χρησιμοποιείται για την κρυπτογράφηση του μηνύματος
- Η διαδικασία έχει ως εξής:
  - Ο αποστολέας
    - Διαλέγει ένα μυστικό κλειδί μιάς χρήσης
    - Το κρυπτογραφεί (ως κείμενο) με το δημόσιο κλειδί του παραλήπτη και το στέλνει στον παραλήπτη ως σύντομο μήνυμα κειμένου
    - Κρυπτογραφεί το κείμενό του με το μυστικό κλειδί μιάς χρήσης και το στέλνει στον παραλήπτη
  - Ο παραλήπτης χρησιμοποιεί
    - Το ιδιωτικό του κλειδί για να αποκρυπτογραφήσει το μυστικό κλειδί
    - Το μυστικό κλειδί για να αποκρυπτογραφήσει το πραγματικό μήνυμα

Εξασφάλιση Ιδιωτικού Απόρρητου με Συνδυασμό Μεθόδων (2/2)



Περιεχόμενα

- **Πλευρές Ασφάλειας**
- **Ιδιωτικό Απόρρητο**
  - **Μέθοδος Μυστικού Κλειδιού (Συμμετρική Κρυπτογράφηση)**
  - **Μέθοδος Δημόσιου Κλειδιού (Ασύμμετρη Κρυπτογράφηση)**
  - **Συνδυασμός Μεθόδων**
- **Ψηφιακή Υπογραφή**
  - **Υπογραφή Ολόκληρου του Εγγράφου**
  - **Υπογραφή Σύνοψης του Εγγράφου**

Ψηφιακή Υπογραφή (1/2)

- Ιδιωτικό Απόρρητο (confidentiality)
- Πιστοποίηση Αυθεντικότητας (authentication)
- Ακεραιότητα (integrity)
- Μη - απάρνηση (non-repudiation)

Ψηφιακή Υπογραφή (2/2)

- Βασίζεται στην ιδέα υπογραφής εγγράφου από το δημιουργό του -> μετά από αυτό, το έγγραφο δεν μπορεί να τροποποιηθεί

- Υλοποιείται με δύο τρόπους
  - Υπογραφή ολόκληρου του εγγράφου
  - Υπογραφή σύνοψης του εγγράφου

Περιεχόμενα

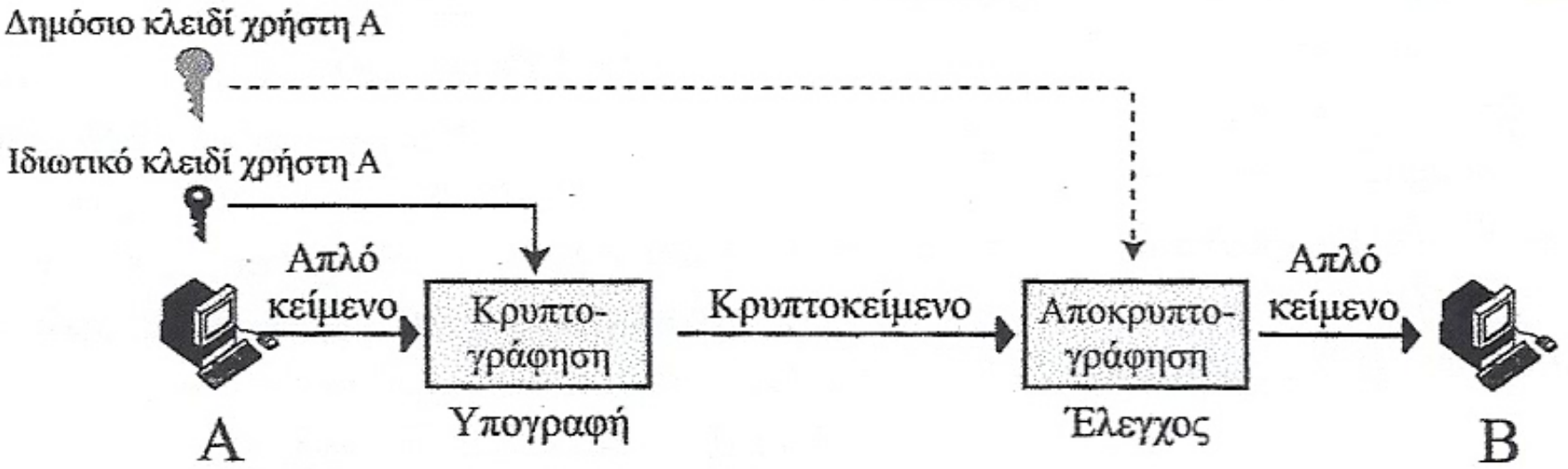
- **Πλευρές Ασφάλειας**
- **Ιδιωτικό Απόρρητο**
  - **Μέθοδος Μυστικού Κλειδιού (Συμμετρική Κρυπτογράφηση)**
  - **Μέθοδος Δημόσιου Κλειδιού (Ασύμμετρη Κρυπτογράφηση)**
  - **Συνδυασμός Μεθόδων**
- **Ψηφιακή Υπογραφή**
  - **Υπογραφή Ολόκληρου του Εγγράφου**
  - **Υπογραφή Σύνοψης του Εγγράφου**

Υπογραφή Ολόκληρου του Εγγράφου (1/4)

- Μπορεί να χρησιμοποιηθεί η κρυπτογράφηση δημόσιου κλειδιού

- Διαφορές:
  - Ο αποστολέας κρυπτογραφεί το μήνυμα με το δικό του ιδιωτικό κλειδί (και όχι με το δημόσιο κλειδί του παραλήπτη)
  - Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του αποστολέα
  - Αυτό είναι εφικτό γιατί οι αλγόριθμοι κ/α που χρησιμοποιούνται σήμερα, όπως ο RSA, είναι μαθηματικοί τύποι με την ίδια δομή.

Υπογραφή Ολόκληρου του Εγγράφου (2/4)



Υπογραφή Ολόκληρου του Εγγράφου (3/4)

Πως εξασφαλίζει αυτός ο τύπος υπογραφής ακεραιότητα, αυθεντικότητα και μη-απάρνηση;

Ακεραιότητα

Αν κάποιος υποκλέψει ή αλλάξει ολοκληρωτικά ή εν μέρει το κρυπτοκείμενο, το αποκρυπτογραφημένο κείμενο θα είναι μη αναγνώσιμο

Αυθεντικότητα

Αν ο Χ στείλει μήνυμα προσποιούμενος ότι είναι ο Ζ, αναγκαστικά θα χρησιμοποιήσει το δικό του ιδιωτικό κλειδί. Άρα το μήνυμα δεν θα αποκρυπτογραφηθεί σωστά με το δημόσιο κλειδί του Ζ

Μη-απάρνηση

Αν ο Χ έστειλε ένα μήνυμα και μετά το αρνηθεί, θα μπορούσε να υποχρεωθεί με δικαστική εντολή να αποκαλύψει το ιδιωτικό του κλειδί που αντιστοιχεί στο δημόσιό του κλειδί. Αν το μήνυμα που παραλήφθηκε κρυπτογραφηθεί και αποκρυπτογραφθεί με αυτά τα δύο κλειδιά, θα προκύψει το απεσταλμένο μήνυμα

Υπογραφή Ολόκληρου του Εγγράφου (4/4)

- Η μέθοδος δεν παρέχει μυστικότητα
  - Οποιοσδήποτε μπορεί να χρησιμοποιήσει το δημόσιο κλειδί του αποστολέα και να διαβάσει το μήνυμα
- Για μυστικότητα, χρειάζεται ένα ακόμη επίπεδο ασφάλειας

Περιεχόμενα

- Πλευρές Ασφάλειας
- Ιδιωτικό Απόρρητο
  - Μέθοδος Μυστικού Κλειδιού (Συμμετρική Κρυπτογράφηση)
  - Μέθοδος Δημόσιου Κλειδιού (Ασύμμετρη Κρυπτογράφηση)
  - Συνδυασμός Μεθόδων
- Ψηφιακή Υπογραφή
  - Υπογραφή Ολόκληρου του Εγγράφου
  - Υπογραφή Σύνοψης του Εγγράφου

Υπογραφή Σύνοψης Εγγράφου (1/9)

- Αντιμετωπίζει το μειονέκτημα της κρυπτογράφησης δημόσιου κλειδιού (*χαμηλή απόδοση* όταν χρησιμοποιείται για υπογραφή ολόκληρου του εγγράφου)

- Για βελτίωση της απόδοσης, ο αποστολέας υπογράφει (κρυπτογραφεί με το ιδιωτικό του κλειδί) μια σύνοψη (μικρογραφία) του εγγράφου

- Ο παραλήπτης αποκρυπτογραφεί τη μικρογραφία με το δημόσιο κλειδί του αποστολέα

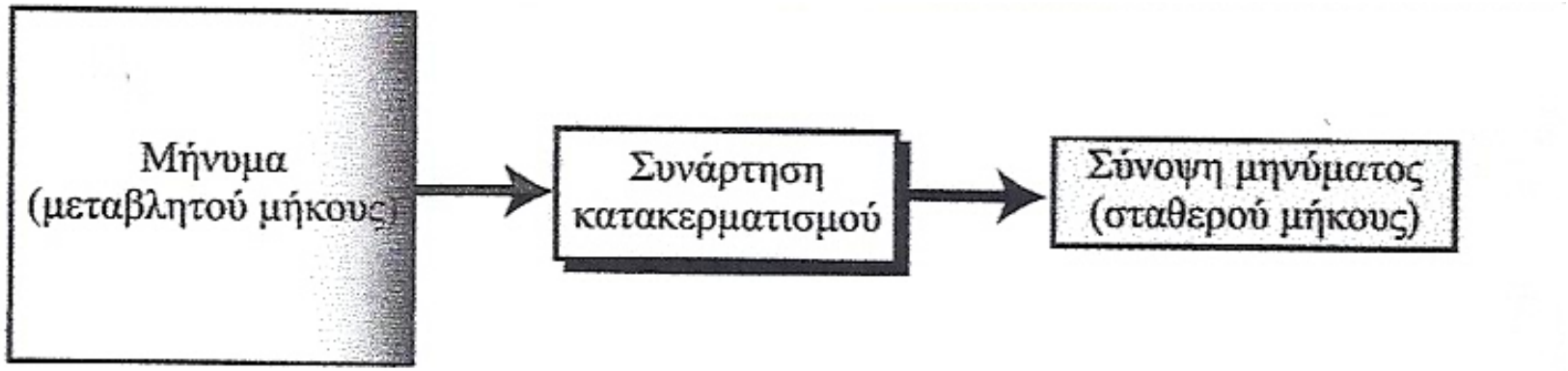
Υπογραφή Σύνοψης Εγγράφου (2/9)

- Για τη δημιουργία της σύνοψης του εγγράφου, χρησιμοποιείται ένας αλγόριθμος κατακερματισμού (hash function)

- Η σύνοψη έχει πάντα σταθερό μήκος (συνήθως 128 μπιτ) ανεξαρτήτως του μεγέθους του μηνύματος

- Γνωστοί αλγόριθμοι κατακερματισμού
  - MD5 (Message Digest 5) -> παράγει συνόψεις 128 μπιτ
  - SHA-1 (Secure Hash Algorithm 1) -> παράγει συνόψεις 160 μπιτ

Υπογραφή Σύνοψης Εγγράφου (3/9)

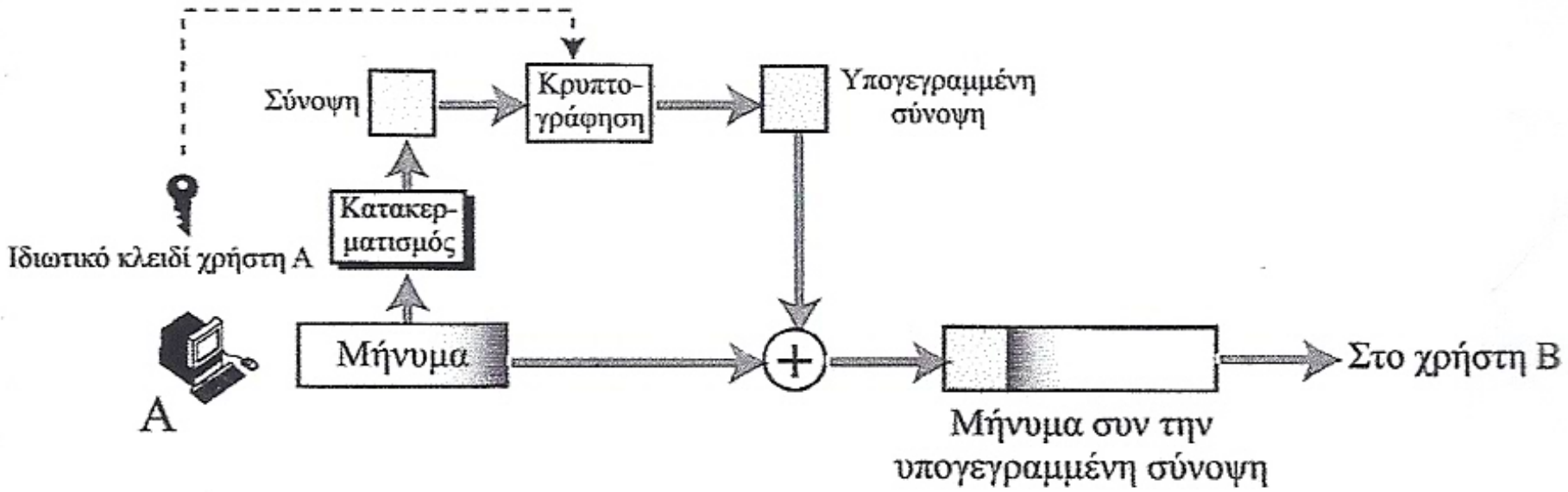


Υπογραφή Σύνοψης Εγγράφου (4/9)

- Η επιτυχία της μεθόδου του κατακερματισμού εξασφαλίζεται από το ότι ο ***κατακερματισμός***:
  - Είναι ***μιάς κατεύθυνσης***, δηλ. μπορούμε να δημιουργήσουμε τη σύνοψη από το μήνυμα αλλά το αντίστροφο δεν είναι εφικτό
  - Πρέπει να είναι ***μονοσήμαντος,*** δηλ. θα πρέπει να είναι πολύ δύσκολο να βρεθούν δύο μηνύματα που έχουν την ίδια σύνοψη

- Η σύνοψη κρυπτογραφείται (υπογράφεται) με το ιδιωτικό κλειδί του αποστολέα, επισυνάπτεται στο αρχικό μήνυμα και αποστέλλεται στον παραλήπτη

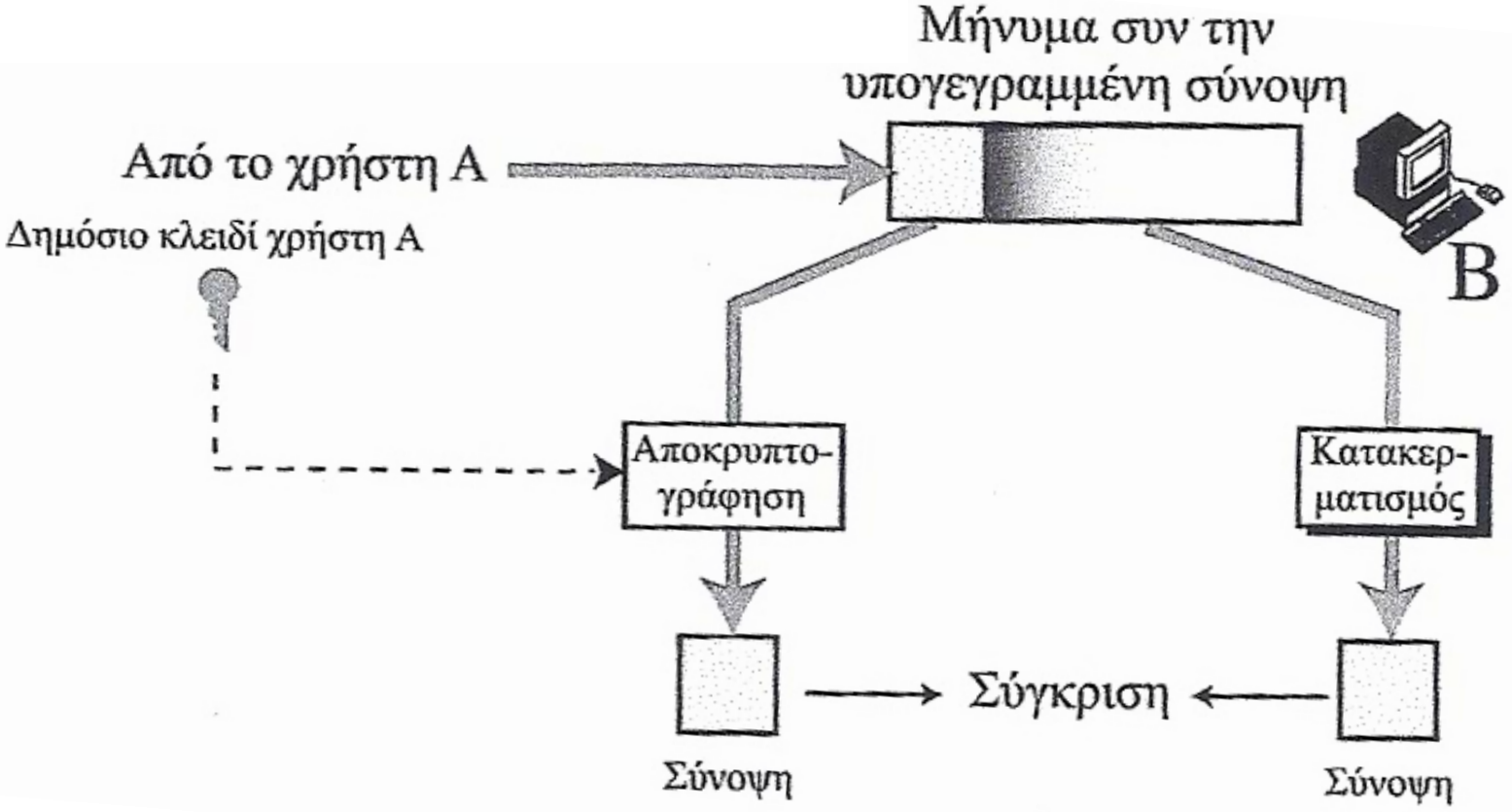
Υπογραφή Σύνοψης Εγγράφου (5/9)
Πλευρά του Αποστολέα



Υπογραφή Σύνοψης Εγγράφου (6/9)

- Ο παραλήπτης παίρνει το αρχικό μήνυμα και την κρυπτογραφημένη σύνοψη
- Εφαρμόζει στο αρχικό μήνυμα τον ίδιο αλγόριθμο κατακερματισμού και δημιουργεί μια δεύτερη σύνοψη
- Αν οι δύο συνόψεις είναι ίδιες, τότε έχουν τηρηθεί όλες οι πλευρές ασφάλειας

Υπογραφή Σύνοψης Εγγράφου (7/9)
Πλευρά Παραλήπτη



Υπογραφή Σύνοψης Εγγράφου (8/9)

- Οι τρεις πλευρές της ασφάλειας ισχύουν για το αντίγραφο της σύνοψης που παρέλαβε ο παραλήπτης.

  Γιατί ισχύουν και για το ίδιο το μήνυμα;

  - Από το παραληφθέν μήνυμα δημιουργείται ένα ίδιο αντίγραφο σύνοψης. Άρα ούτε το αρχικό μήνυμα έχει μεταβληθεί
  - Η σύνοψη προέρχεται από τον πραγματικό αποστολέα, άρα και το ίδιο το μήνυμα. Αν προερχόταν από άλλον δεν θα είχε δημιουργήσει την ίδια σύνοψη.
  - Ο αποστολέας δεν μπορεί να αρνηθεί ότι έστειλε το μήνυμα, επειδή δεν μπορεί να αρνηθεί την αποστολή της σύνοψης. Το μόνο μήνυμα που μπορει να δημιουργήσει τη συγκεκριμένη σύνοψη είναι το παραληφθέν

Υπογραφή Σύνοψης Εγγράφου (9/9)

- Ούτε αυτή η μέθοδος ψηφιακής υπογραφής παρέχει εμπιστευτικότητα

- Αν απαιτείται εμπιστευτικότητα, θα πρέπει να προστεθεί και ένα άλλο επίπεδο κρυπτογράφησης [είτε με τη μέθοδο δημόσιου κλειδιού ή μυστικού κλειδιού ή με συνδυασμό των δύο μεθόδων]

ΕΡΩΤΗΣΕΙΣ?