ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν
Πανεπιστήμιον Αθηνών

Δίκτυα Επικοινωνιών ΙΙ

Ενότητα 5: Ασφάλεια Δικτύων

Διδάσκων: Χριστόφορος Πάνος

Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Εθνικό & Καποδιστριακό Πανεπιστήμιο Αθηνών

Δίκτυα Επικοινωνιών ΙΙ

Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Εθνικό & Καποδιστριακό
Πανεπιστήμιο Αθηνών

Θεματικές Ενότητες (ΘΕ) μαθήματος:

ΘΕ1: Εισαγωγή

(Κεφ. 1 του βιβλίου)

ΘΕ2: Συστήματα Αναμονής (M/M/1 και παραλλαγές, M/G/1, συστήματα με προτεραιότητες, δίκτυα ουρών)

ΘΕ3: Ασύρματα/Κινητά Δίκτυα (ασύρματα τοπικά δίκτυα, υποστήριξη κινητικότητας στο διαδίκτυο, κινητά δίκτυα 3ης γενιάς)

(Κεφ. 6 του βιβλίου)

ΘΕ4: Δικτύωση Πολυμέσων

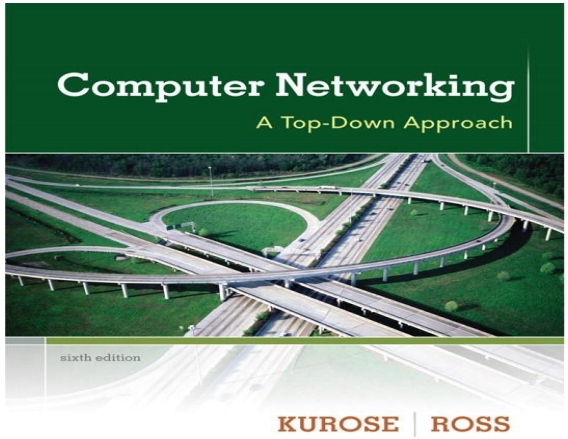
(Κεφ. 7 του βιβλίου)

ΘΕ5: Ασφάλεια Δικτύων

(Κεφ. 8 του βιβλίου)

Συνιστώμενο Βιβλίο:
Computer Networking: A Top-Down Approach, by Kurose & Ross, Addison-Wesley

Ελληνική Μετάφραση:
Εκδόσεις : Μ. Γκιούρδας



Οι περισσότερες από τις διαφάνειες αυτές αποτελούν προσαρμογή και απόδοση στα ελληνικά των διαφανειών που συνοδεύουν το βιβλίο Computer Networking : A Top-Down Approach, J.F Kurose and K.W. Ross, 6/E, Addison-Wesley.

Προσαρμογή και επιμέλεια της απόδοσης των πρωτότυπων διαφανειών για την θεματική ενότητα της Ασφάλειας Δικτύων στα ελληνικά : Χριστόφορος Πάνος

Ασφάλεια Δικτύων

Στόχοι:

- Κατανόηση βασικών θεμάτων ασφάλειας δικτύων:
  - Κρυπτογραφία και οι εφαρμόγες της πέρα από την κρυπτογράφηση δεδομένων
  - Αυθεντικοποίηση
  - Ακεραιότητα μηνύματος
- Η ασφάλεια στη πράξη:
  - Firewalls και συστήματα εντοπισμού παρεισφρήσεων
  - Ασφάλεια σε επίπεδο εφαρμογής, μεταφοράς, δικτύου και ζεύξης

Ασφάλεια Δικτύων

- Τι είναι η ασφάλεια δικτύων;
- Αρχές κρυπτογραφίας
- Ακεραιότητα μηνύματος
- Αυθεντικοποίηση
- Διασφαλίζοντας το e-mail
- Διασφαλίζοντας συνδέσεις TCP: SSL
- Ασφάλεια επιπέδου δικτύου: IPsec
- Διασφαλίζοντας ασύρματα τοπικά δίκτυα
- Firewalls και IDS

Τι είναι η ασφάλεια δικτύων;

Εμπιστευτικότητα: μόνο ο αποστολέας και ο παραλήπτης θα πρέπει να διαβάσουν το περιεχόμενο του μηνύματος

- Ο αποστολέας κρυπτογραφεί το μήνυμα
- Ο παραλήπτης αποκρυπτογραφεί το μήνυμα

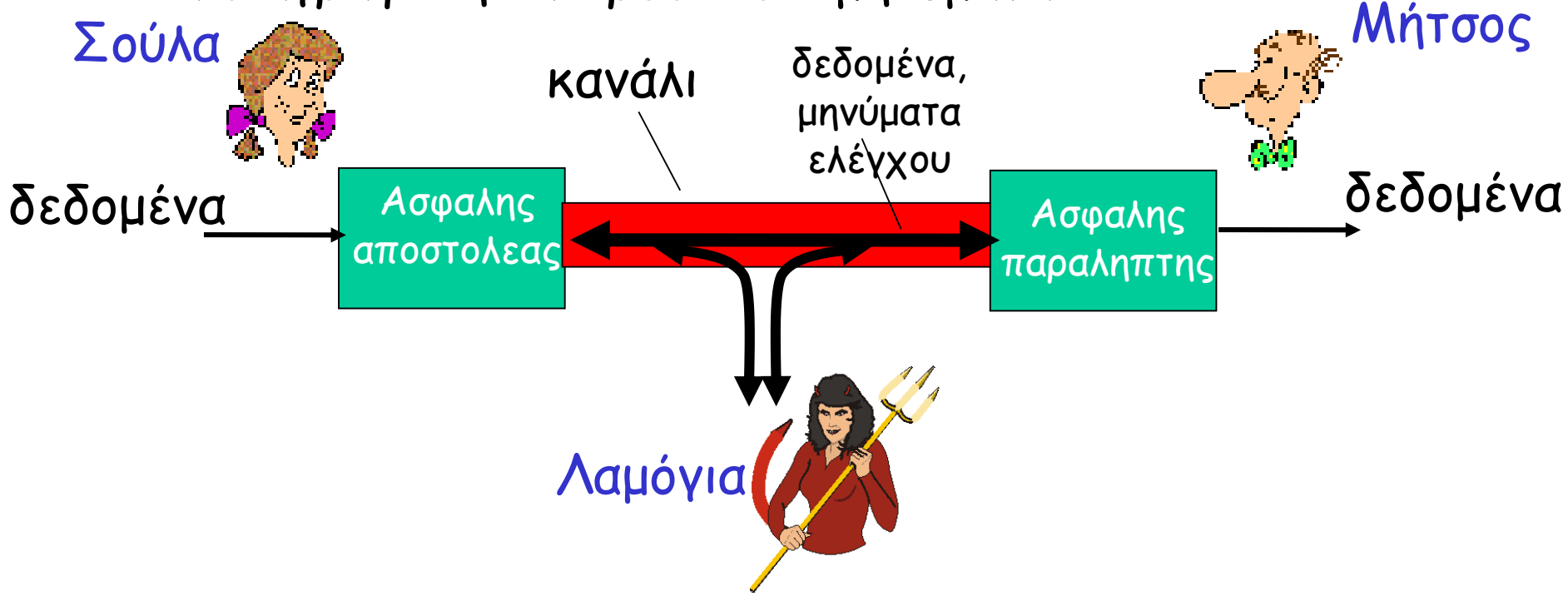
Αυθεντικοποίηση: αποστολέας και παραλήπτης θέλουν να εξακριβώσουν ο ένας την ταυτότητα του άλλου

Ακεραιότητα μηνύματος: αποστολέας και παραλήπτης θέλουν να διαβεβαιωθούν ότι τα μηνύματα δεν τροποποιήθηκαν (ή αν τροποποιήθηκαν να το αντιληφθούν)

Πρόσβαση και διαθεσιμότητα: οι υπηρεσίες πρέπει πάντα να είναι προσβάσιμες και διαθέσιμες στους τελικούς χρήστες

Φίλοι και εχθροί: Σούλα, Μήτσος, Λαμόγια

- Γνωστά πρόσωπα στο κόσμο της ασφάλειας
- Ο Μήτσος και η Σούλα επιθυμούν να επικοινωνήσουν με ασφαλή τρόπο
- Η Λαμόγια (κακόβουλος χρήστης) μπορεί να παρέμβει, να διαγράψει ή να προσθέσει μηνύματα



Ποιοί μπορεί να είναι οι: Μήτσος, Σούλα;

- Φυσικά Πρόσωπα!
- Προγράμματα περιήγησης στο διαδίκτυο (Web browser), Web εξυπηρέτες
- on-line τραπεζικές/ηλεκτρονικές συναλλαγές, πελάτες/εξυπηρέτες
- DNS εξυπηρέτες
- Δρομολογητές που ανταλλάσουν δεδομένα για τους πίνακες δρομολόγησης

Οι κακοί!

Ε: Τι μπορεί να κάνει ένας κακόβουλος;

Α:

- Παθητικά να *ακούσει* και να *διαβάσει* τα μηνύματα
- Ενεργά να *εισάγει* δικά του μηνύματα στην σύνδεση
- *Να υποδυθεί μια άλλη οντότητα:* μπορεί να χρησιμοποιήσει IP διευθύνσεις άλλων χρηστών
- *hijacking:* να εισχωρήσει σε μια σύνδεση και να διώξει τον αποστολέα ή τον παραλήπτη
- *Άρνηση παροχής υπηρεσιών* : οι χρήστες δεν μπορούν να έχουν πρόσβαση στις επιθυμητές υπηρεσίες (θα μελετήσουμε αναλυτικά την επίθεση αυτή αργότερα)

Ασφάλεια Δικτύων

- Τι είναι η ασφάλεια δικτύων;
- Αρχές κρυπτογραφίας
- Ακεραιότητα μηνύματος
- Αυθεντικοποίηση
- Διασφαλίζοντας το e-mail
- Διασφαλίζοντας συνδέσεις TCP: SSL
- Ασφάλεια επιπέδου δικτύου: IPsec
- Διασφαλίζοντας ασύρματα τοπικά δίκτυα
- Firewalls και IDS

Βασικοί όροι κρυπτογραφίας

m καθαρό κείμενο

$K_\Sigma(m)$ κρυπτοκείμενο, κρυπτογραφημένο με το κλειδί K_Σ

$m = K_M(K_\Sigma(m))$

Μια απλή μέθοδος κρυπτογράφησης

Κρυπτοκείμενο αντικατάστασης: αντικαθιστά ένα γράμμα με ένα άλλο (μονο-αλφαβητικά)

καθαρό κείμενο: abcdefghijklmnopqrstuvwxyz

κρυπτοκείμενο: mnbvcxzasdfghjklpoiuytrewq

π.χ.: καθαρό κείμενο: bob. i love you. alice

κρυπτοκείμενο: nkn. s gktc wky. mgsbc

"Mapping" του σετ των 26 γραμμάτων σε ένα σετ 26 γραμμάτων

Πολύ-αλφαβητική κρυπτογραφία

- n κρυπτοκείμενα αντικατάστασης, $M_1, M_2, \ldots, M_n$
- Κυκλική σειρά:
  - Π.χ., n=3, M_1, M_3, M_4; M_1, M_3, M_4;
- ΄Για κάθε νέο σύμβολο καθαρού κειμένου, χρησιμοποιούμε κυκλικά τη σειρά μονο-αλβαβητικών κρυπτοκείμενων αντικατάστασης
  - dog: d from M_1, o from M_3, g from M_4
- Κλειδί: τα n κρυπτοκείμενα αντικατάστασης και η κυκλική σειρά

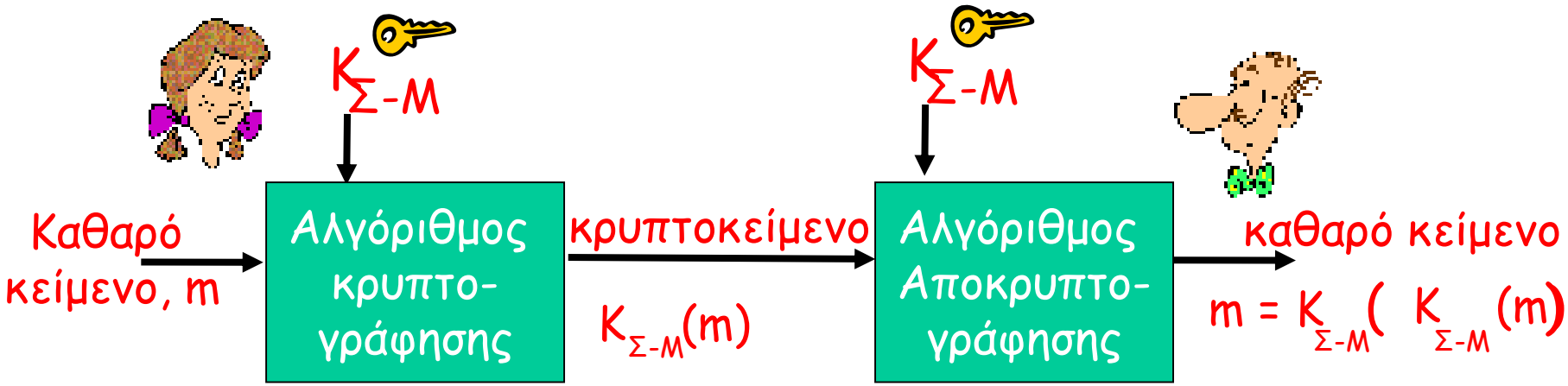
Σπάζοντας ένα μηχανισμό κρυπτογράφησης

- Επίθεση κρυπτοκειμένου: Η Λαμόγια κατέχει κρυπτοκείμενο που μπορεί να αναλύσει
- Δύο προσεγγίσεις:
  - Δοκιμή όλων των κλειδιών (Brute-Force). Απαιτείται η ικανότητα κατανόησης του αποτελέσματος
  - Στατιστική ανάλυση
- Επίθεση καθαρού κειμένου: Η Λαμόγια κατέχει ένα κομμάτι καθαρού κειμένου που αντιστοιχεί σε κάποιο κρυπτοκείμενο
  - Π.χ., γνωρίζει τα ονόματα των οντοτήτων
- Επίθεση επιλεγμένου καθαρού κειμένου: Η Λαμόγια μπορεί να λάβει το κρυπτοκείμενο για ένα επιλεγμένο καθαρό κείμενο

Τύποι Κρυπτογραφίας

- Η κρυπτογραφία βασίζεται στα κλειδιά:
  - Ο αλγόριθμος είναι γνωστός σε όλους
  - Μόνο τα κλειδιά είναι μυστικά
- Κρυπτογραφία δημόσιου κλειδιού
  - Χρήση δύο κλειδιών
- Συμμετρική κρυπτογραφία
  - Χρήση ενός κλειδιού
- Συναρτήσεις κατακερματισμού
  - Δεν γίνεται χρήση κλειδιών
  - Τίποτα μυστικό. Πώς είναι χρήσιμες;

Συμμετρικό κλειδί κρυπτογράφησης



Συμμετρικό κλειδί κρυπτογράφησης: Μήτσος και Σούλα μοιράζονται το ίδιο (συμμετρικό) γνωστό κλειδί: $K_{Σ-M}$

- π.χ., το κλειδί στο κρυπτοκείμενο αντικατάστασης είναι το μοτίβο αντικατάστασης των γραμμάτων
- Ε: πως οι δύο οντότητες αποφασίζουν την τιμή του κλειδιού ;

Δύο τύποι συμμετρικής κρυπτογράφησης

- Stream ciphers
  - Κρυπτογράφηση ενός bit τη φορά
- Block ciphers
  - Διαχωρισμός καθαρού κειμένου σε κομμάτια (ίσου μεγέθους)
  - Κρυπτογράφηση κάθε κομματιού σα μονάδα

Stream Ciphers

- Συνδύασε κάθε bit ενός keystream με κάθε bit καθαρού κειμένου
- m(i) = ith bit του μηνύματος
- ks(i) = ith bit του keystream
- c(i) = ith bit του κρυπτοκειμένου
- $c(i) = ks(i) \oplus m(i)$ ($\oplus$ = exclusive or)
- $m(i) = ks(i) \oplus c(i)$

Block ciphers

- Το μήνυμα κρυπτογραφείται σε blocks των k bits (π.χ., 64-bit blocks).
- 1-προς-1 mapping

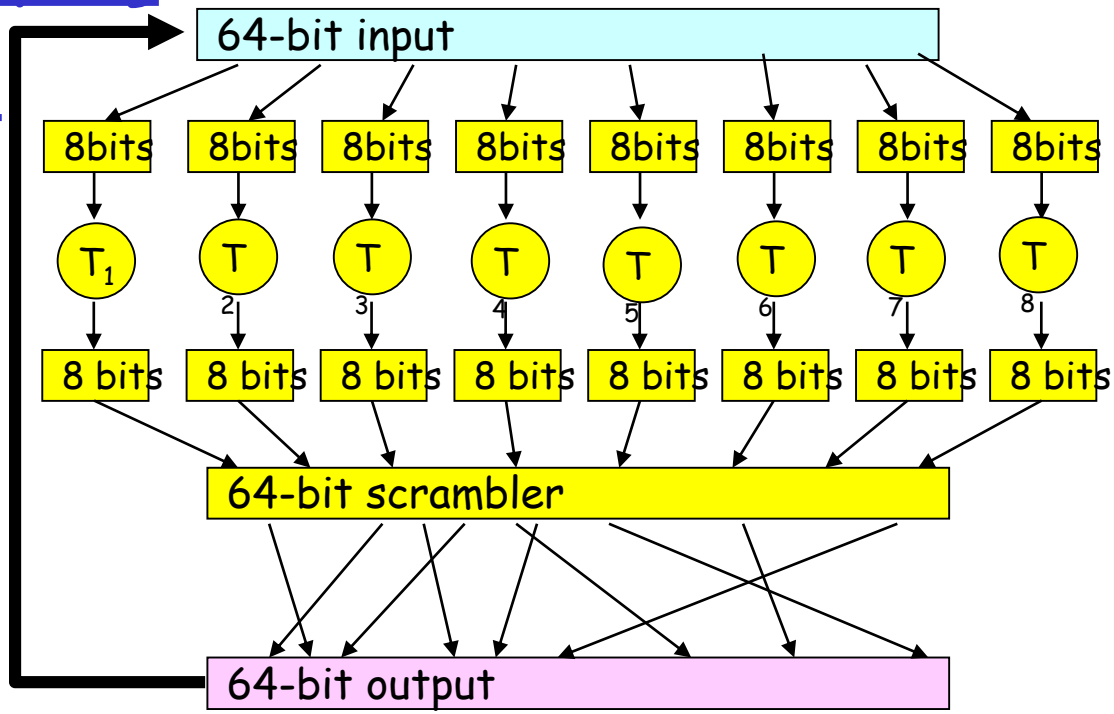
Παράδειγμα με k=3:

input	output
000	110
001	111
010	101
011	100

input	output
100	011
101	010
110	000
111	001

Κρυπτογραφικοί αλγόριθμοι δέσμης (Block Cipher)

Επανάληψη n φορές



- Ένας γύρος: κάθε ένα bit εισόδου επηρεάζει οκτώ bits εξόδου
- Πολλαπλοί γύροι: κάθε ένα bit εισόδου επηρεάζει όλα τα bits εξόδου
- block ciphers: DES, 3DES, AES

Κρυπτογράφηση συμμετρικού κλειδιού DES

DES: Data Encryption Standard

- US πρότυπο [NIST 1993]
- 56-bit συμμετρικό κλειδί, 64-bit καθαρό κείμενο είσοδος
- Πόσο ασφαλές είναι το DES;
  - Διαγωνισμός DES Challenge: η φράση ("Strong cryptography makes the world a safer place") κρυπτογραφήθηκε με ένα 56-bit κλειδί και αποκρυπτογραφήθηκε (εξαντλητική μέθοδος) σε 4 μήνες
  - Καμία γνωστή "backdoor" προσέγγιση για δυνατότητα αποκρυπτογράφησης
- το DES μπορεί να γίνει ακόμα πιο ισχυρό:
  - Χρήση τριών κλειδιών στη σειρά (3-DES)
  - Χρήση αλυσίδωσης μπλοκ κρυπτομεθόδου

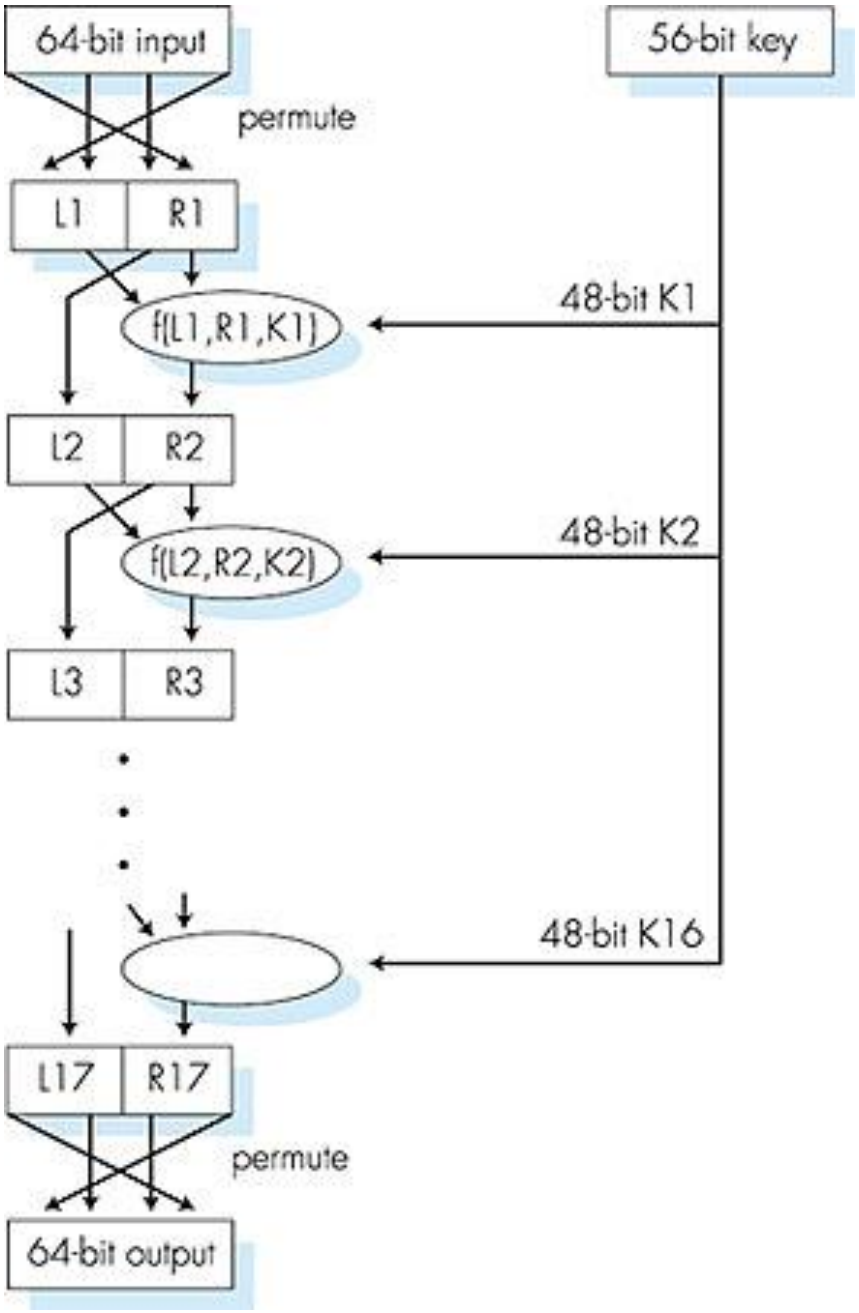
Κρυπτογράφηση συμμετρικού κλειδιού DES

DES λειτουργία

Αρχική μετάθεση

16 παρόμοιοι «κύκλοι» ίδιας διαδικασίας, κάθε διαδικασία χρησιμοποιεί διαφορετικό κλειδί 48 bits

Τελική μετάθεση

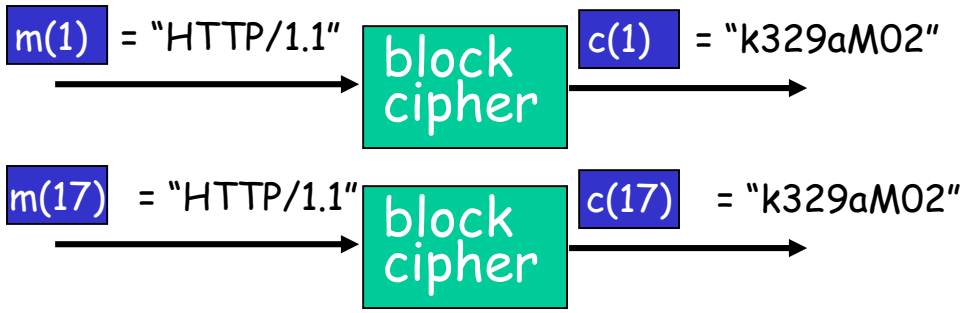


AES: Advanced Encryption Standard

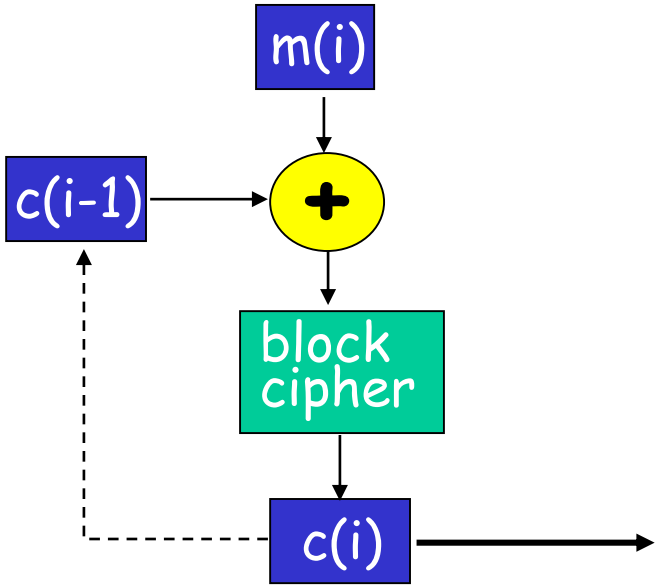
- καινούργιο NIST προτύπο (Nov. 2001) συμμετρικού κλειδιού, αντικαθιστά το DES
- Επεξεργάζεται δεδομένα με 128 bit μπλοκ
- 128, 192, ή 256 bit κλειδιά
- Αποκρυπτογράφηση εξαντλητικής μεθόδου (brute force) (δοκιμή κάθε πιθανού κλειδιού). Αν μια μηχανή θέλει 1 sec στο DES, τότε θέλει 149 τρισεκατομμύρια χρόνια στο AES

Κρυπταλγόριθμος αλυσιδωτής δέσμης

- Αλγόριθμος δέσμης: σε περίπτωση επανάληψης του μπλοκ εισόδου παράγεται το ίδιο κρυπτόγραμμα.



- *Κρυπταλγόριθμος αλυσιδωτής δέσμης:* Το μπλοκ εισαγωγής m(i), υποβάλλεται σε XOR με το προηγούμενο μπλοκ, c(i-1)
  - c(0) αποστέλλεται στο παραλήπτη
  - Τι γίνεται στο "HTTP/1.1" βάση του παραπάνω σεναρίου;



Κρυπτογραφία δημόσιου κλειδιού

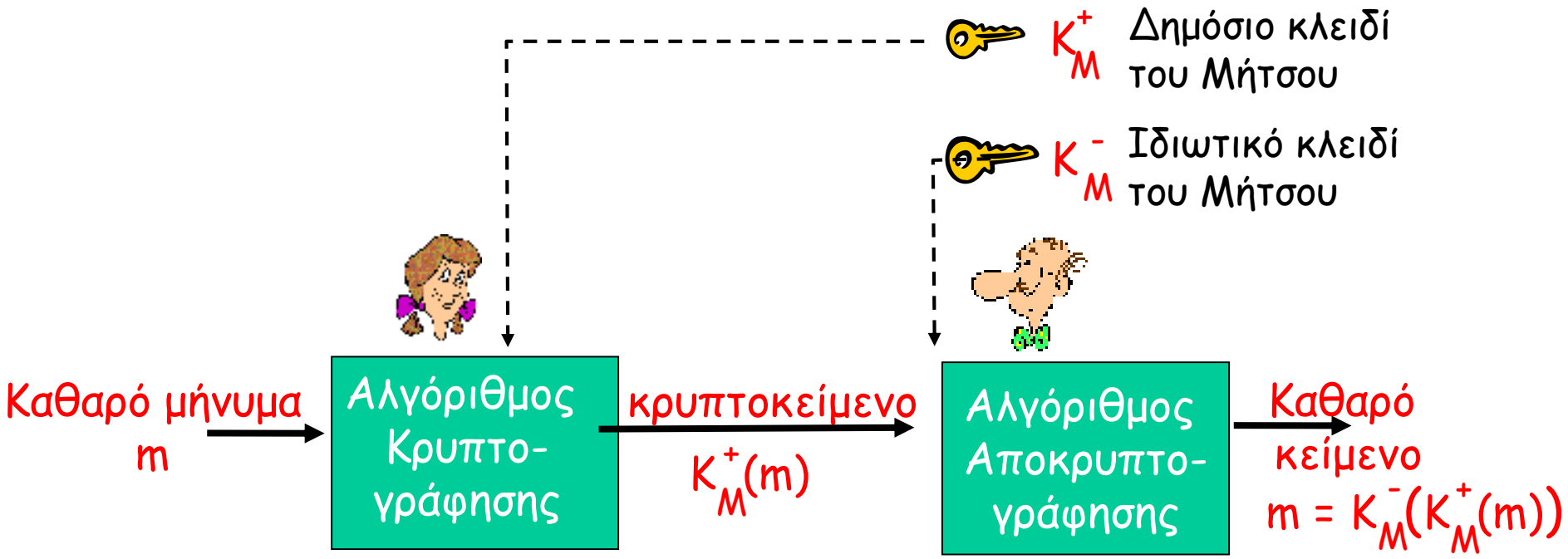
Κρυπτογραφία συμμετρικού κλειδιού

- προϋποθέτει ο αποστολέας και ο παραλήπτης να γνωρίζουν ένα μυστικό κλειδί
- Ε: πώς μπορούν να συμφωνήσουν για το μυστικό κλειδί με ασφαλή τρόπο (και ιδιαίτερα αν δεν έχουν συναντηθεί ποτέ τους);

Κρυπτογραφία δημόσιου κλειδιού

- Διαφορετική προσέγγιση [Diffie-Hellman76, RSA78]
- Αποστολέας και παραλήπτης δεν μοιράζονται κάποιο μυστικό κλειδί
- *Δημόσιο* κλειδί κρυπτογράφησης γνωστό σε όλους
- *Ιδιωτικό* κλειδί αποκρυπτογράφησης γνωστό μόνο στον παραλήπτη

Κρυπτογραφία δημόσιου κλειδιού



Αλγόριθμοι κρυπτογράφησης δημόσιου κλειδιού

Απαιτούμενα:

1. Χρειάζεται $K_M^+(\cdot)$ και $K_M^-(\cdot)$ τέτοια ώστε
$$K_M^-(K_M^+(m)) = m$$
2. Με δεδομένο ένα δημόσιο κλειδί K_M^+, πρέπει να είναι αδύνατο να υπολογιστεί το αντίστιχο ιδιωτικό κλειδί K_M^-

RSA: Rivest, Shamir, Adelson αλγόριθμος

Προαπαιτούμενο: modular αριθμητική

- x mod n = υπόλοιπο του x όταν διαιρούμε με n
- Facts:

  [(a mod n) + (b mod n)] mod n = (a+b) mod n
  [(a mod n) - (b mod n)] mod n = (a-b) mod n
  [(a mod n) * (b mod n)] mod n = (a*b) mod n
- Οπότε

  $(a \bmod n)^d \bmod n = a^d \bmod n$
- Π.χ.: x=14, n=10, d=2:
  $(x \bmod n)^d \bmod n = 4^2 \bmod 10 = 6$
  $x^d = 14^2 = 196 \quad x^d \bmod 10 = 6$

RSA: Διαλέγοντας κλειδιά

1. Διάλεξε δύο μεγάλους πρώτους αριθμούς *p, q.* (π.χ., 1024 bits το κάθε ένα)
2. Υπολόγισε $n = pq$, $z = (p-1)(q-1)$
3. Διάλεξε e (με $e<n$) τέτοιο ώστε να μην έχει κανένα κοινό παράγοντα με το z εκτός από το 1. (*e, z* είναι σχετικά πρώτοι).
4. Διάλεξε d τέτοιο ώστε το $ed-1$ να διαιρείται ακριβώς με το *z*. (με άλλα λόγια: $ed \bmod z = 1$).
5. Το δημόσιο κλειδί είναι το (n,e). Ιδιωτικό είναι το (n,d).

K_M^+ K_M^-

RSA: Κρυπτογράφηση Αποκρυπτογράφηση

0. Υπολόγισε (n,e) και (n,d) όπως περιγράφτηκε προηγουμένως

1. Για την κρυπτογράφηση του m, υπολόγισε

   $c = m^e \bmod n$ (δηλ. το υπόλοιπο όταν το m^e διαιρείται με το n)

2. Για την αποκρυπτογράφηση του c, υπολόγισε

   $m = c^d \bmod n$ (δηλ. το υπόλοιπο όταν το c^d διαιρείται με το n)

Μαγικό! $m = (\underbrace{m^e \bmod n}_{c})^d \bmod n$

RSA Παράδειγμα:

Ο Μήτσος διαλέγει $p=5$, $q=7$. Μετά $n=35$, $z=24$.

$e=5$ (άρα e, z σχετικά πρώτοι).

$d=29$ (άρα $ed-1$ διαιρείται ακριβώς με το z).

Κρυπτογράφηση:

γράμμα	m	m^e	$c = m^e \bmod n$
l	12	1524832	17

Αποκρυπτογράφηση:

c	c^d	$m = c^d \bmod n$	γράμμα
17	481968572106750915091411825223071697	12	l

RSA: γιατί $m = (m^e \bmod n)^d \bmod n$

Χρήσιμο θεώρημα από θεωρία αριθμών: Αν p,q πρώτοι και $n = pq$, τότε:

$$x^y \bmod n = x^{y \bmod (p-1)(q-1)} \bmod n$$

$$(m^e \bmod n)^d \bmod n = m^{ed} \bmod n$$

$$= m^{ed \bmod (p-1)(q-1)} \bmod n$$

(με την παραπάνω θεωρία)

$$= m^1 \bmod n$$

(αφού επιλέξαμε ed να διαιρείται από το $(p-1)(q-1)$ με υπόλοιπο 1)

$$= m$$

RSA: άλλη μια σημαντική ιδιότητα

Η παρακάτω ιδιότητα θα είναι *πολύ χρήσιμη* αργότερα

$$K_M^-(K_M^+(m)) = m = K_M^+(K_M^-(m))$$

Χρήση δημόσιου κλειδιού πρώτα, και έπειτα ακολουθεί το ιδιωτικό κλειδί

Χρήση ιδιωτικού κλειδιού πρώτα, και έπειτα ακολουθεί το δημόσιο κλειδί

Το αποτέλεσμα είναι το ίδιο!

Ασφάλεια Δικτύων

- Τι είναι η ασφάλεια δικτύων;
- Αρχές κρυπτογραφίας
- Ακεραιότητα μηνύματος
- Αυθεντικοποίηση
- Διασφαλίζοντας το e-mail
- Διασφαλίζοντας συνδέσεις TCP: SSL
- Ασφάλεια επιπέδου δικτύου: IPsec
- Διασφαλίζοντας ασύρματα τοπικά δίκτυα
- Firewalls και IDS

Ακεραιότητα Μηνύματος

Ο Bob λαμβάνει ένα μήνυμα m από την Alice και θέλει να διαπιστώσει πώς:

Το μήνυμα προέρχεται πραγματικά από την Alice

Το μήνυμα δεν έχει τροποποιηθεί μετά την αποστολή του

Το μήνυμα δεν έχει γίνει «replayed»

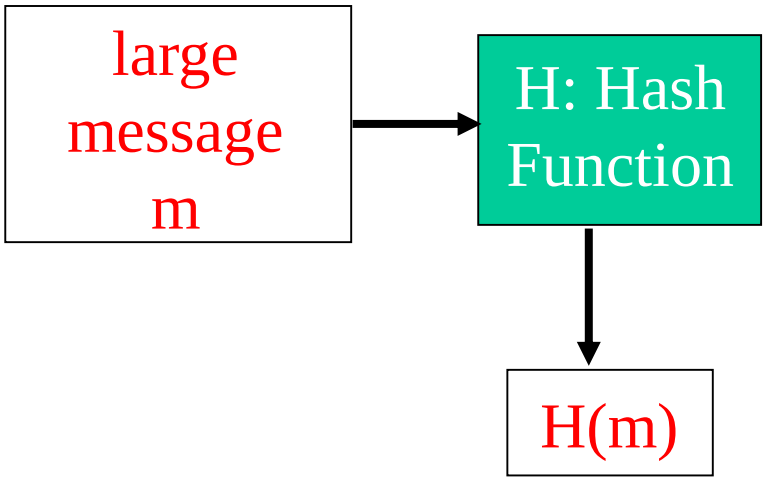
Ακεραιότητα Μηνύματος

Σύνοψη μηνύματος:

Στόχος: ένα σταθερού μήκους, εύκολο να υπολογιστεί, ψηφιακό «αποτύπωμα»

Εφαρμογή συνάρτησης κατακερματισμού H στο *m*, με έξοδο μια σταθερού μήκους σύνοψη μηνύματος, *H(m)*.

Με δεδομένη σύνοψη μηνύματος x, είναι υπολογιστικά ανέφικτο να βρεθεί m τέτοιο ώστε x = H(m) (no collisions)



Άθροισμα ελέγχου κεφαλίδας IP: κακή συνάρτηση κατακερματισμού.

Το άθροισμα ελέγχου κεφαλίδας IP έχει κάποιες ιδιότητες συναρτήσεων κατακερματισμού:

- ✓ Παράγει σύνοψη σταθερού μήκους (16-bit) του μηνύματος
- ✓ many-to-1

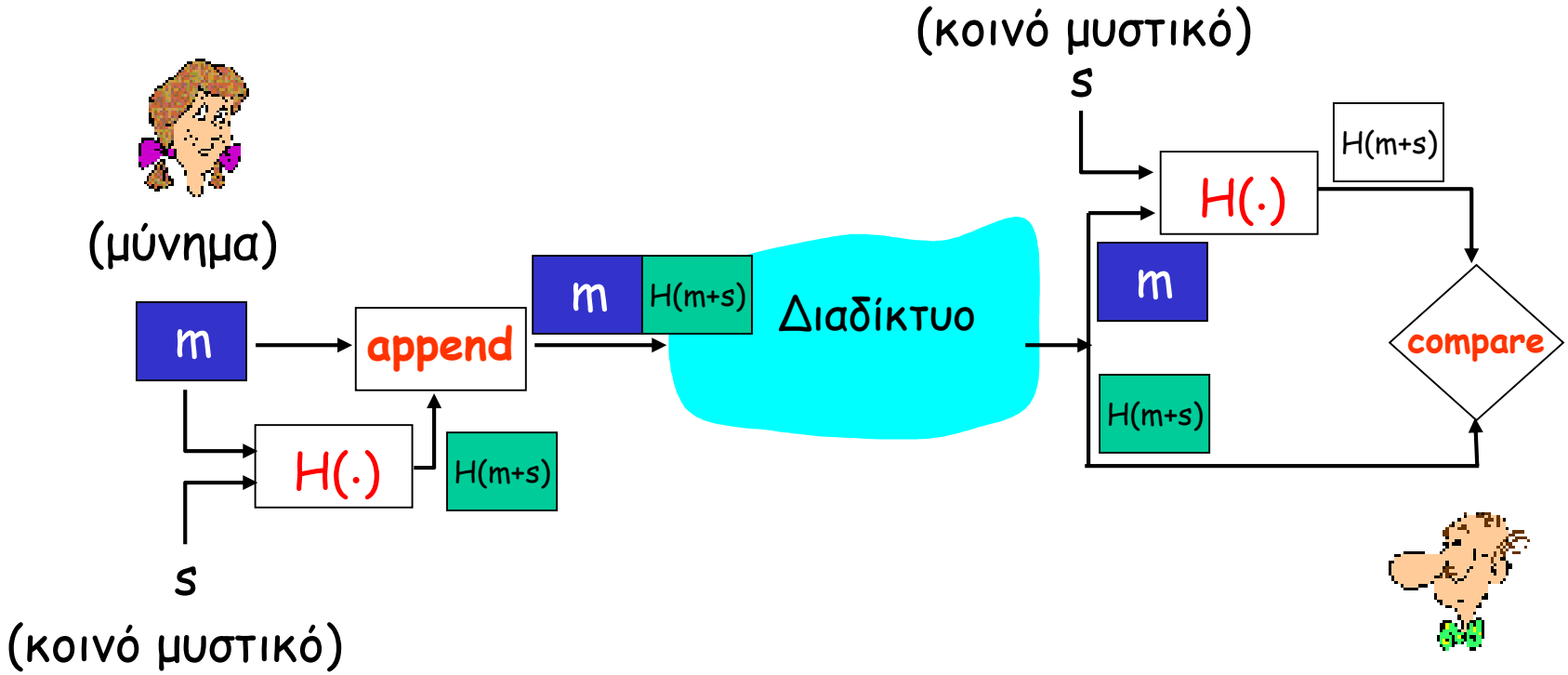
Αλλά με δεδομένο ένα μήνυμα και τιμή σύνοψης, είναι εύκολο να βρεθεί ένα άλλο μήνυμα με την ίδια τιμή σύνοψης:

message	ASCII format
I O U 1	49 4F 55 31
0 0 . 9	30 30 2E 39
9 B O B	39 42 D2 42
	B2 C1 D2 AC

message	ASCII format
I O U 9	49 4F 55 39
0 0 . 1	30 30 2E 31
9 B O B	39 42 D2 42
	B2 C1 D2 AC

διαφορετικά μηνύματα αλλά με την ίδια σύνοψη

Σύνοψη Μηνύματος (MAC)



Αλγόριθμοι συναρτήσεων κατακερματισμού

- MD5 συνάρτηση κατακερματισμού ευρέως χρησιμοποιούμενη (RFC 1321)
  - Υπολογίζει 128-bit σύνοψη μηνύματος με μια διαδικασία 4 βημάτων.
  - Για τυχαίο 128-bit x, «φαίνεται» να είναι δύσκολο να κατασκευαστεί μήνυμα m με MD5 σύνοψη ίσο με x.
- SHA-1 χρησιμοποιείται επίσης
  - US standard [NIST, FIPS PUB 180-1]
  - 160-bit σύνοψη μηνύματος

Ψηφιακές Υπογραφές

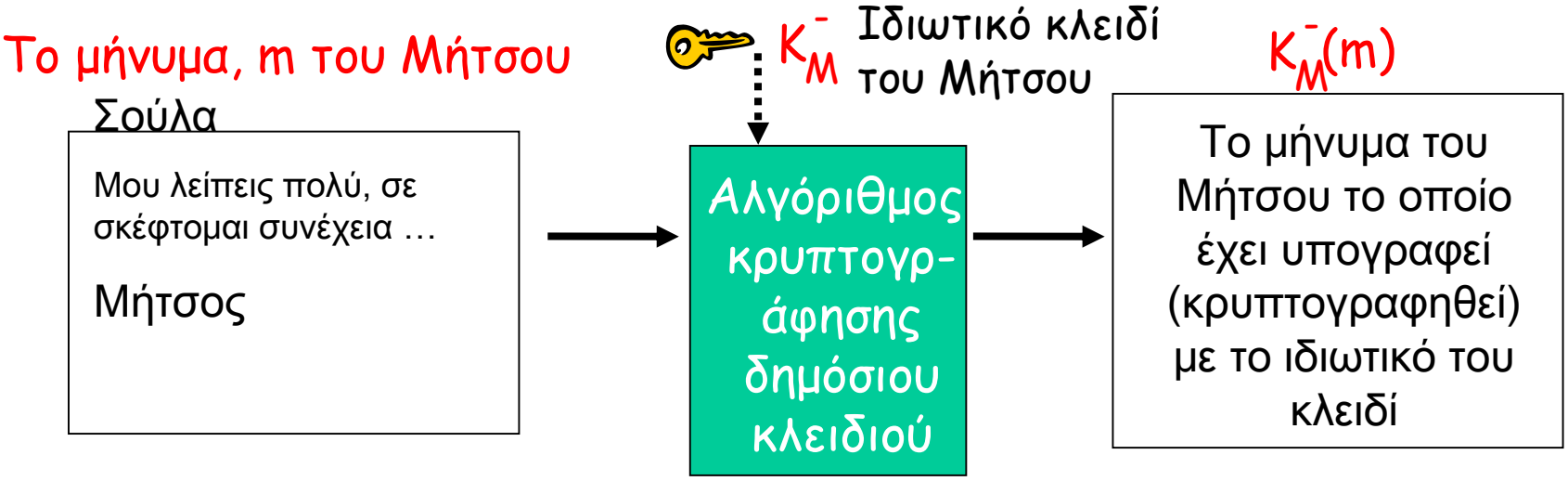
Κρυπτογραφική τεχνική ανάλογη με τις χειρόγραφες υπογραφές.

- Ο αποστολέας (Μήτσος) υπογράφει ψηφιακά τα δεδομένα του, για να κατοχυρώσει ότι ανήκουν στην ιδιοκτησία του.
- Εξακριβώνεται η εγκυρότητα της υπογραφής και δεν μπορεί να πλαστογραφηθεί: Ο παραλήπτης (Σούλα) μπορεί να αποδείξει σε οποιονδήποτε, ότι μόνο ο Μήτσος και κάνεις άλλος υπέγραψε τα δεδομένα που έλαβε.

Ψηφιακές υπογραφές

Απλή ψηφιακή υπογραφή για το μήνυμα m:

- Ο Μήτσος υπογράφει το m με την κρυπτογράφηση του μηνύματος με το ιδιωτικό του κλειδί K_B, δημιουργώντας το $K_M^-(m)$



Ψηφιακές Υπογραφές (περισσότερα)

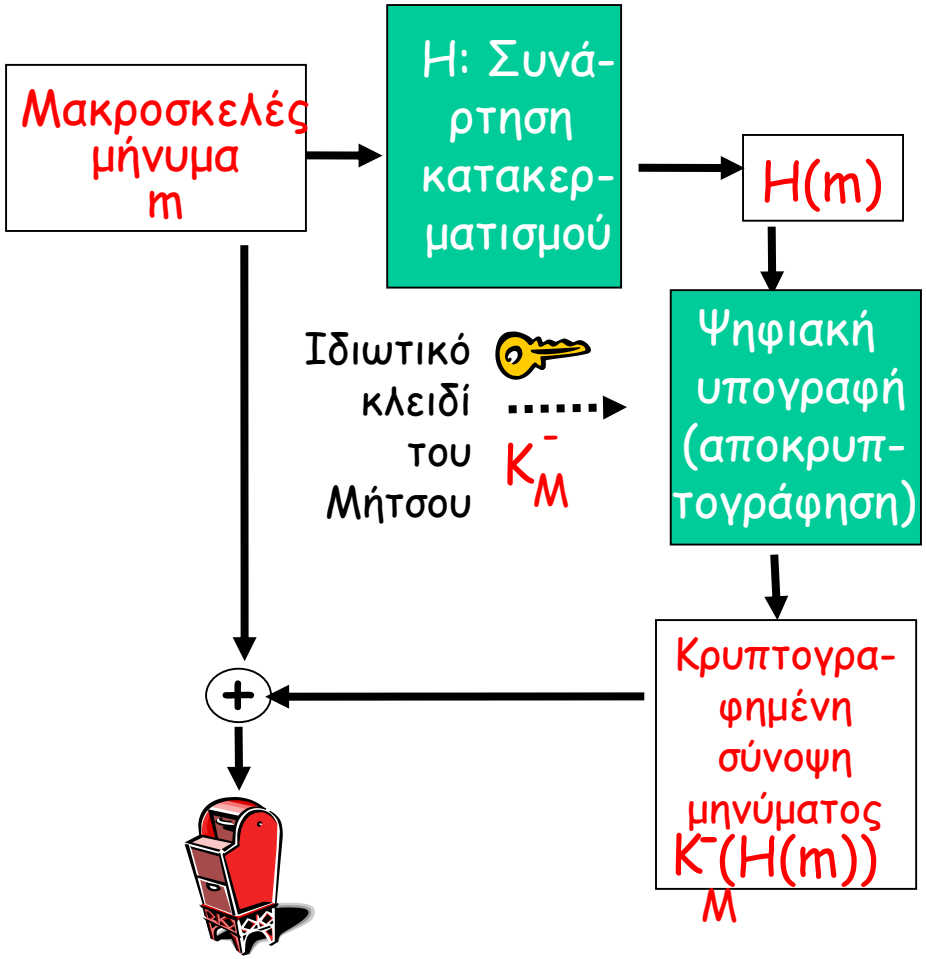
- Υποθέστε ότι η Σούλα λαμβάνει το μήνυμα m, ψηφιακή υπογραφή $K_M^-(m)$.
- Η Σούλα εξακριβώνει το m το οποίο έχει υπογραφεί από τον Μήτσο με το δημόσιο κλειδί του K_M^+ στο $K_M^-(m)$, δηλ. ελέγχει αν $K_M^+(K_M^-(m)) = m$.
- Αν $K_M^+(K_M^-(m)) = m$, τότε όποιος υπέγραψε το m πρέπει να χρησιμοποίησε το ιδιωτικό κλειδί του Μήτσου.

  Η Σούλα εξακριβώνει έτσι ότι:
  - ✓ Ο Μήτσος υπέγραψε το m.
  - ✓ Κανείς άλλος δεν υπέγραψε το m.
  - ✓ Ο Μήτσος υπέγραψε το m και όχι το m′.

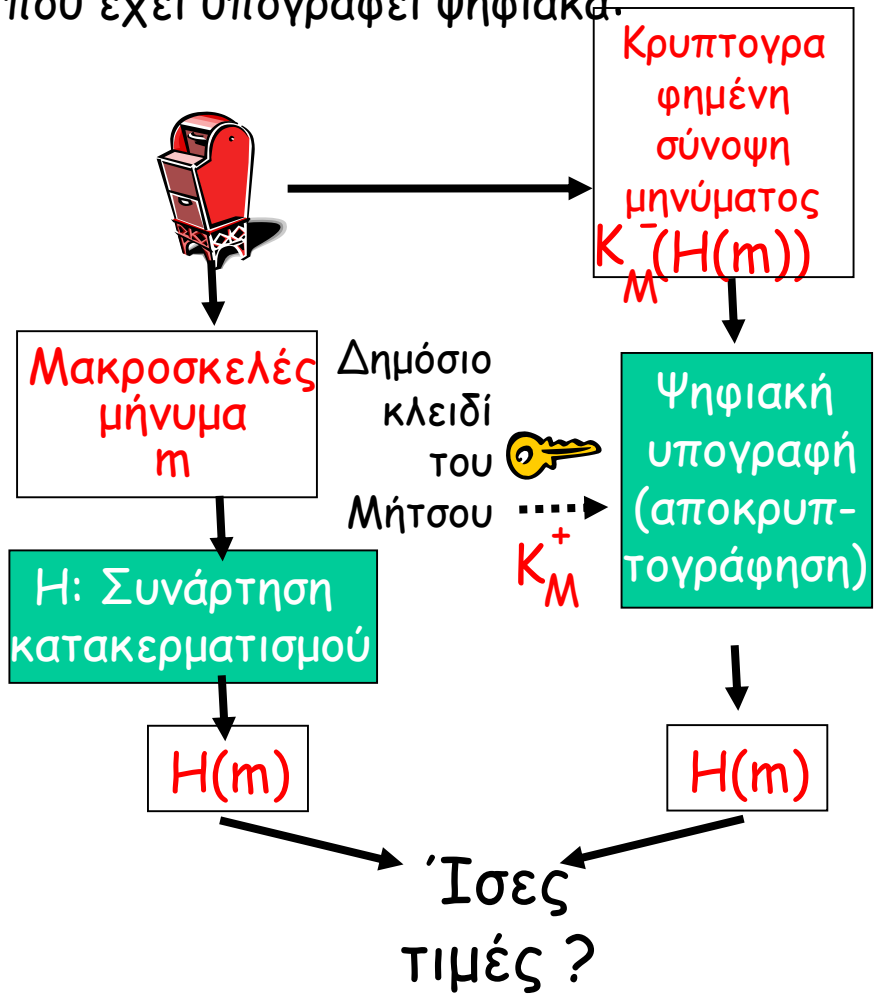
  Μη-αποκύρηξη:
  - ✓ Η Σούλα έχει το δικαίωμα να πάρει το m, και την υπογραφή $K_M^-(m)$ για δικαστικό έλεγχο για να αποδείξει ότι ο Μήτσος υπέγραψε το m.

Ψηφιακή υπογραφή = υπογραφή σύνοψης μηνύματος

Ο Μήτσος στέλνει ένα μήνυμα που έχει υπογραφεί ψηφιακά:



Η Σούλα ελέγχει την υπογραφή και την ακεραιότητα του μηνύματος που έχει υπογραφεί ψηφιακά:



Πιστοποίηση δημόσιου κλειδιού

Πρόβλημα δημόσιου κλειδιού:

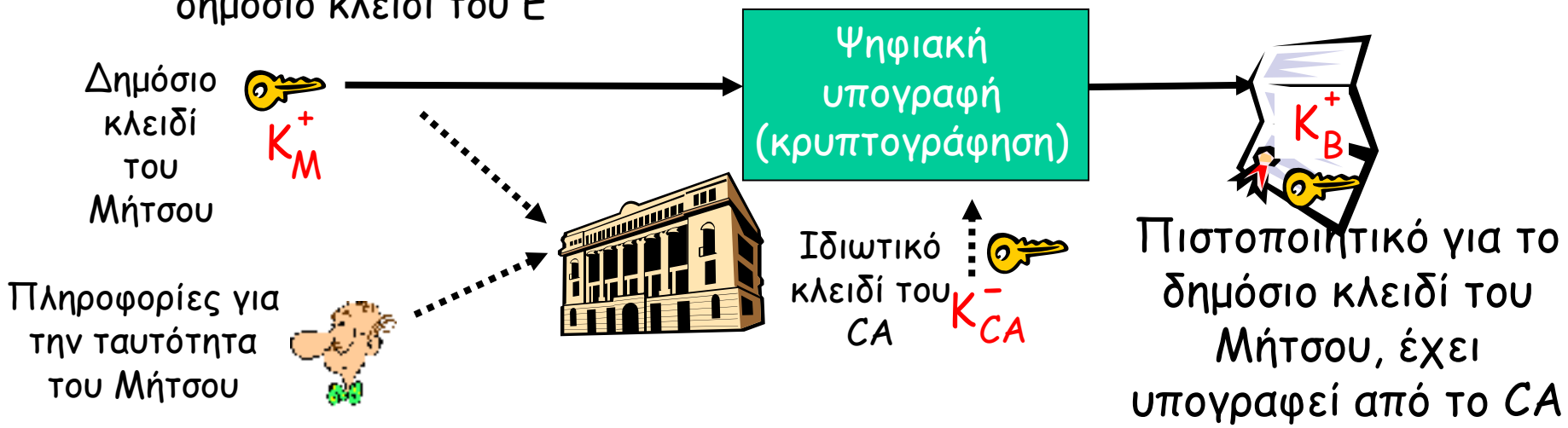
- Όταν η Σούλα αποκτήσει το δημόσιο κλειδί του Μήτσου (από μια ιστοσελίδα, e-mail, δισκέτα), πως είναι σίγουρη ότι είναι πράγματι το δημόσιο κλειδί του Μήτσου και όχι της Λαμόγια;

Λύση:

- Έμπιστη αρχή πιστοποίησης (CA)

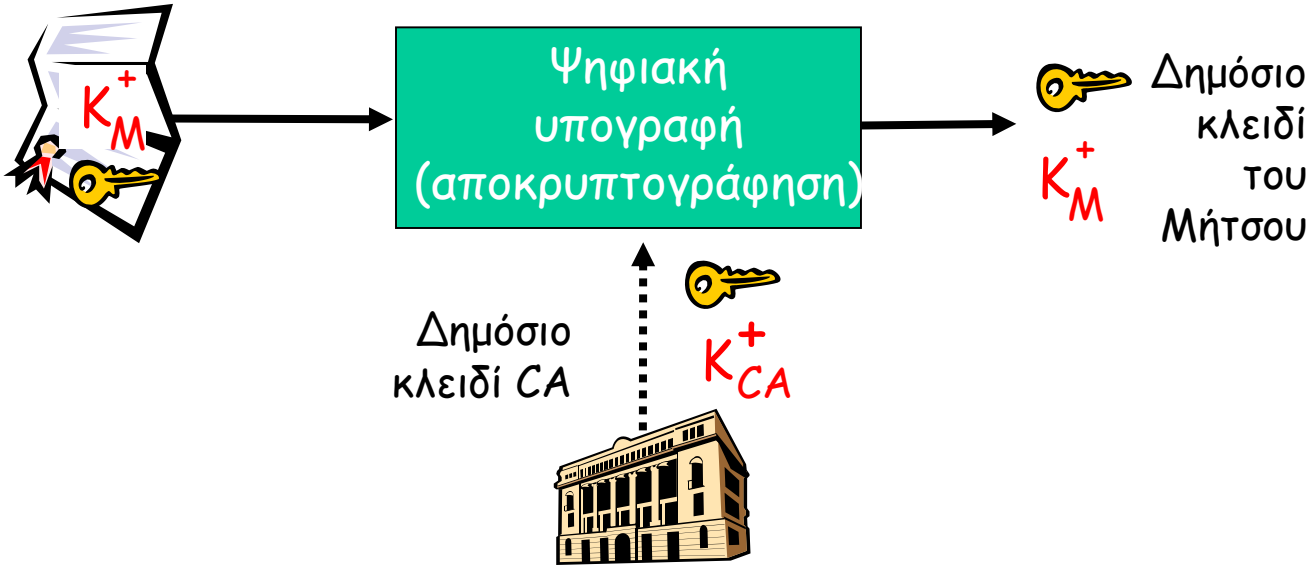
Αρχή Πιστοποίησης-Certificate Authority (CA)

- Αρχή πιστοποίησης (CA): δέσμευση δημόσιου κλειδιού με μια συγκεκριμένη οντότητα Ε.
- Ε (φυσικό πρόσωπο, δρομολογητής) εγγράφει το δημόσιο κλειδί του με το CA.
  - Ε δίνει μια απόδειξη της ταυτότητας του στο CA.
  - CA δημιουργεί το πιστοποιητικό δεσμεύοντας το Ε με το δημόσιο κλειδί του.
  - Το πιστοποιητικό περιέχει το δημόσιο κλειδί του Ε το όποιο έχει υπογραφεί ψηφιακά από το CA, δηλ. το CA λεει "αυτό είναι το δημόσιο κλειδί του Ε"



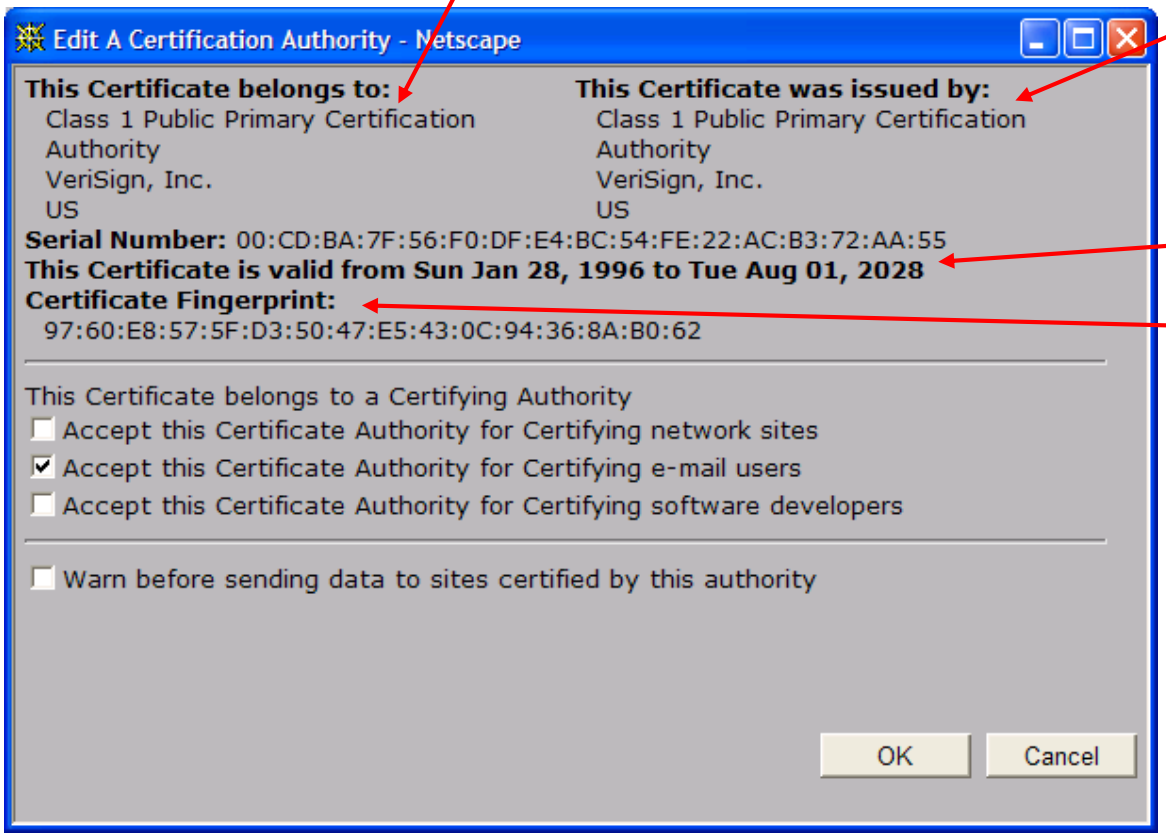
Αρχή πιστοποίησης

- Όταν η Σούλα θέλει το δημόσιο κλειδί του Μήτσου:
  - Αποκτά το πιστοποιητικό του Μήτσου.
  - Εφαρμόζει το δημόσιο κλειδί της αρχής πιστοποίησης στο πιστοποιητικό του Μήτσου, ανακτά το δημόσιο κλειδί του Μήτσου



Ένα πιστοποιητικό περιέχει:

- Serial number (μοναδικό για τον εκδότη)
- Πληροφορίες για τον κάτοχο του πιστοποιητικού, όπως αλγόριθμοι και κλειδιά (δε φαίνονται στο σχήμα)



- Πληροφορίες για τον εκδότη
- Έγκυρες ημερομηνίες
- Ψηφιακή υπογραφή του εκδότη

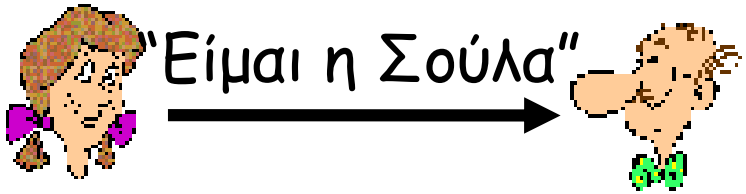
Ασφάλεια Δικτύων

- Τι είναι η ασφάλεια δικτύων;
- Αρχές κρυπτογραφίας
- Ακεραιότητα μηνύματος
- Αυθεντικοποίηση
- Διασφαλίζοντας το e-mail
- Διασφαλίζοντας συνδέσεις TCP: SSL
- Ασφάλεια επιπέδου δικτύου: IPsec
- Διασφαλίζοντας ασύρματα τοπικά δίκτυα
- Firewalls και IDS

Αυθεντικοποίηση

Στόχος: Ο Μήτσος θέλει από την Σούλα να του "αποδείξει" την ταυτότητά της.

πρωτόκολλο ap1.0: Η Σούλα λέει "Είμαι η Σούλα"

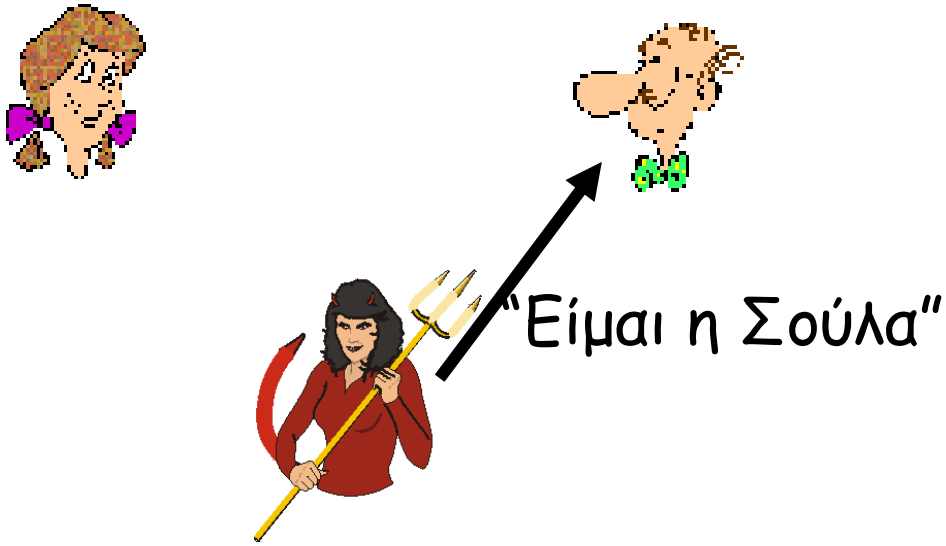


Σενάριο Αποτυχίας:

Αυθεντικοποίηση

Στόχος: Ο Μήτσος θέλει από την Σούλα να του "αποδείξει" την ταυτότητά της.

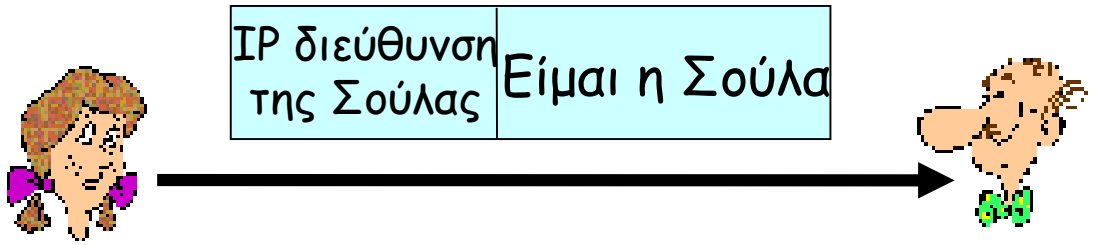
πρωτόκολλο ap1.0: Η Σούλα λέει "Είμαι η Σούλα"



Σε ένα δίκτυο, Ο Μήτσος δεν «βλέπει»την Σούλα, έτσι η Λαμόγια απλά δηλώνει ότι αυτή είναι η Σούλα

Αυθεντικοποίηση: άλλη μια προσπάθεια

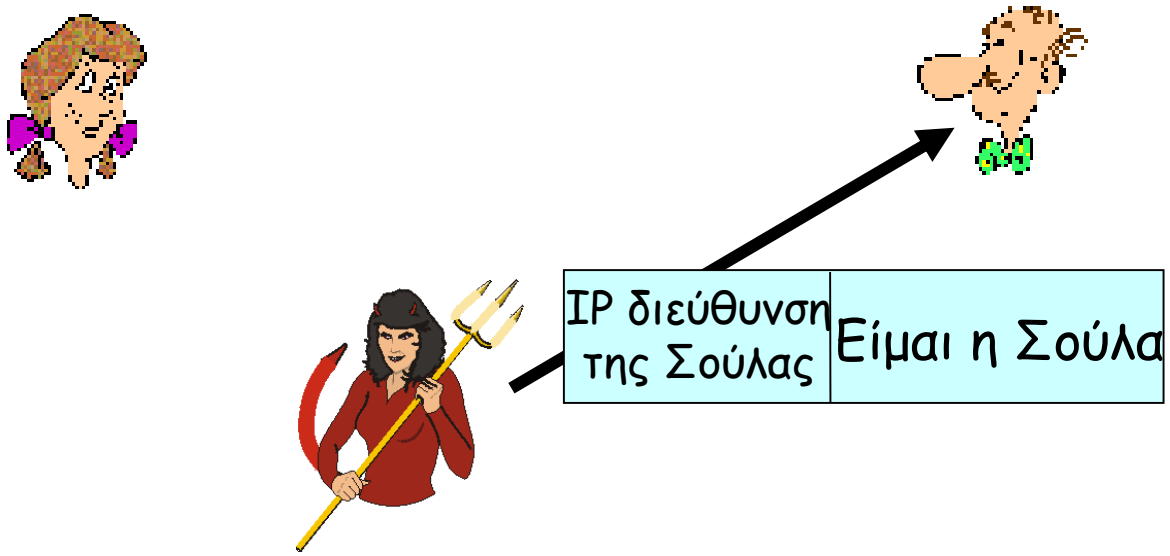
πρωτόκολλο ap2.0: Η Σούλα λέει "Είμαι η Σούλα" μέσα σε ένα IP πακέτο το οποίο περιέχει την IP διεύθυνση της



Σενάριο αποτυχίας;

Αυθεντικοποίηση: άλλη μια προσπάθεια

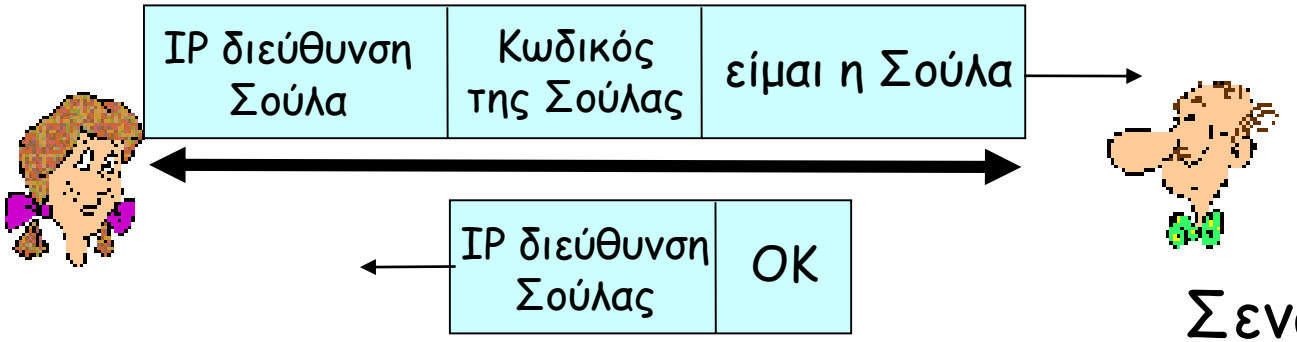
πρωτόκολλο ap2.0: Η Σούλα λέει "Είμαι η Σούλα" μέσα σε ένα IP πακέτο το οποίο περιέχει την IP διεύθυνσή της



Η Λαμόγια απλά δημιουργεί ένα πακέτο με την IP διεύθυνση της Σούλας

Αυθεντικοποίηση: άλλη μια προσπάθεια

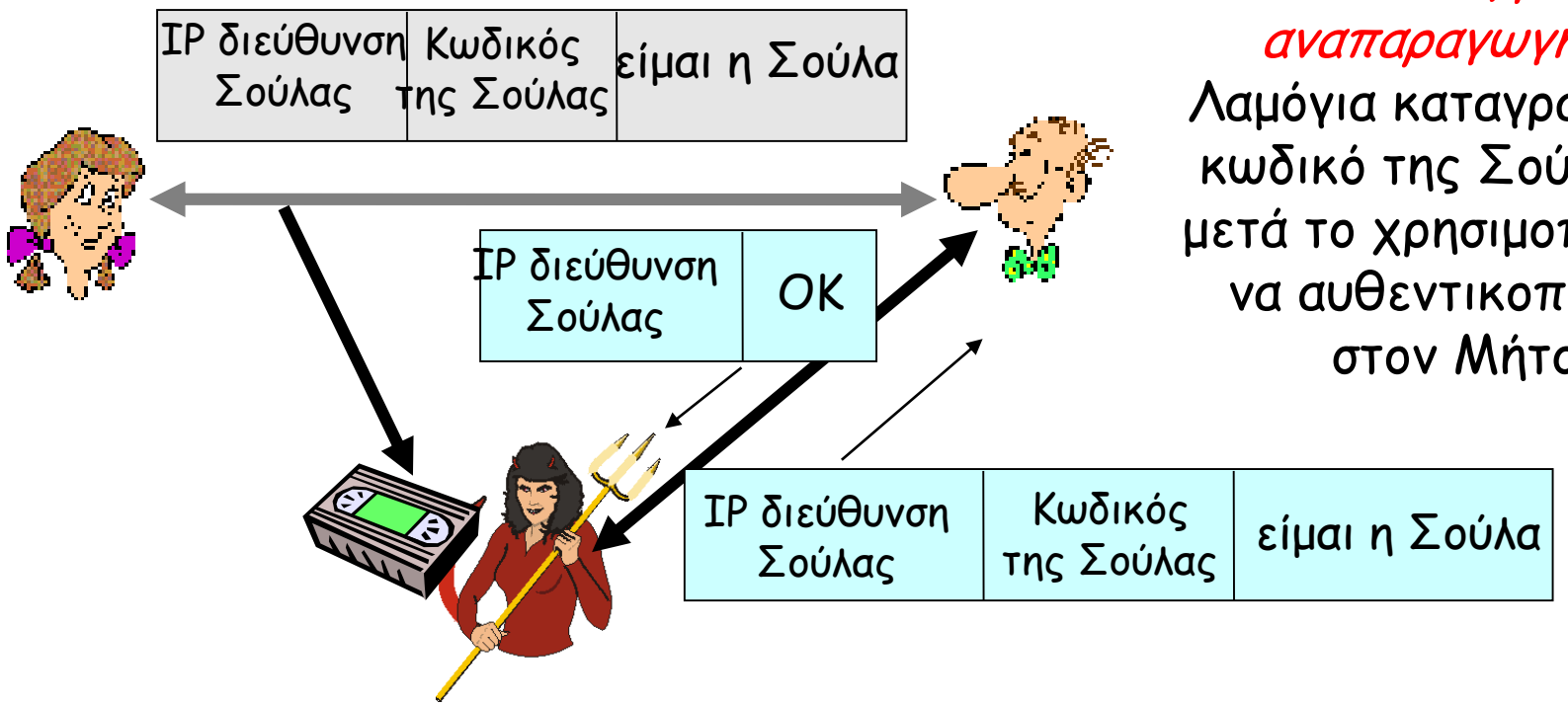
πρωτόκολλο ap3.0: Η Σούλα λέει "είμαι η Σούλα" και στέλνει τον κωδικό πρόσβασης της για να το αποδείξει



Σενάριο αποτυχίας;

Αυθεντικοποίηση: άλλη μια προσπάθεια

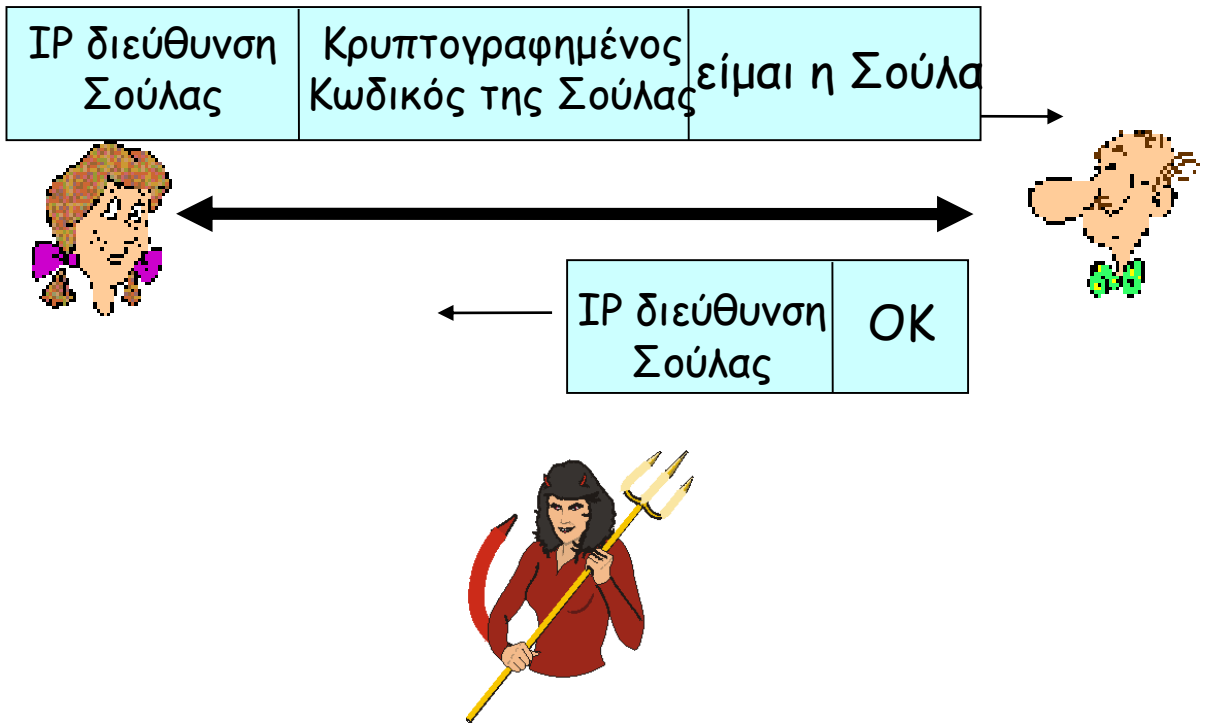
πρωτόκολλο ap3.0: Η Σούλα λέει "είμαι η Σούλα" και στέλνει τον κωδικό πρόσβασης της για να το αποδείξει



Επίθεση μέσω αναπαραγωγής: Η Λαμόγια καταγράφει τον κωδικό της Σούλας και μετά το χρησιμοποιεί για να αυθεντικοποιηθεί στον Μήτσο

Αυθεντικοποίηση: άλλη μια προσπάθεια

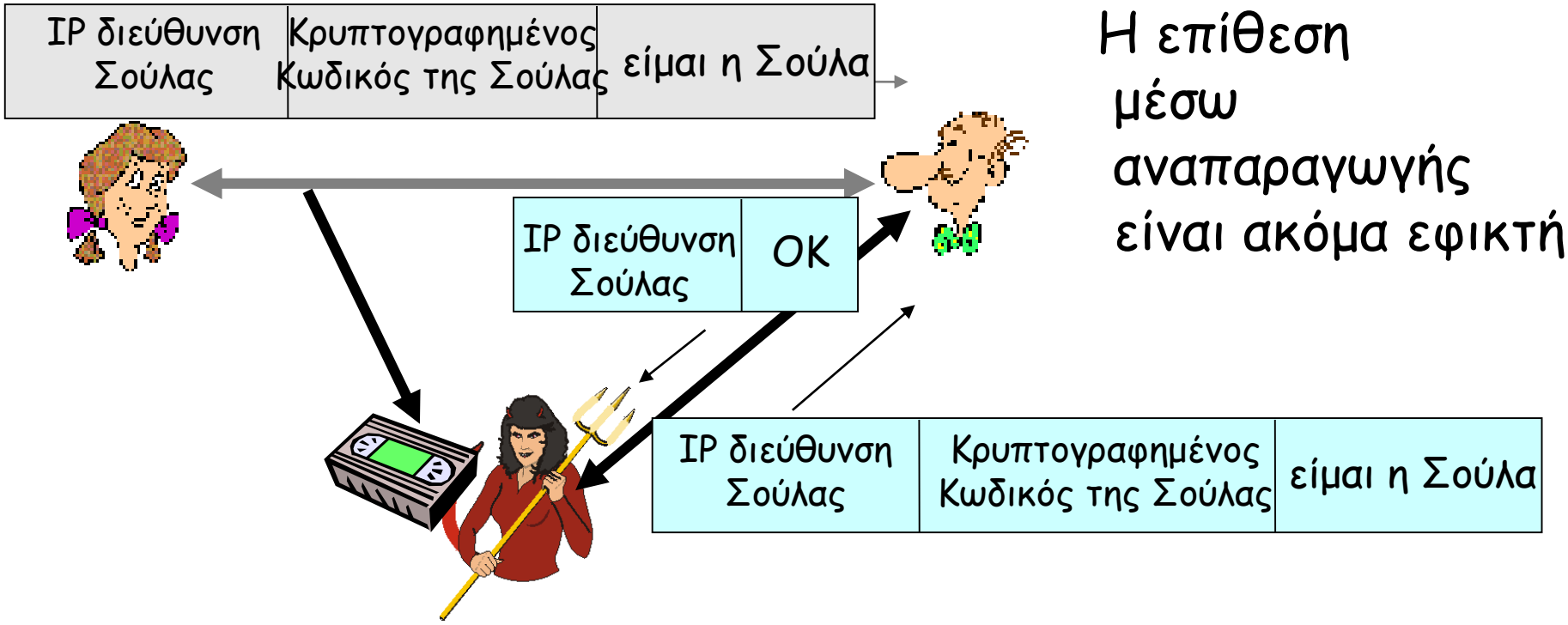
πρωτόκολλο ap3.1: Η Σούλα λέει "είμαι η Σούλα" και στέλνει τον κωδικό πρόσβασης της *κρυπτογραφημένο* για να το αποδείξει



Σενάριο αποτυχίας;

Αυθεντικοποίηση: άλλη μια προσπάθεια

πρωτόκολλο ap3.1: Η Σούλα λέει "είμαι η Σούλα" και στέλνει τον κωδικό πρόσβασης της *κρυπτογραφημένο* για να το αποδείξει



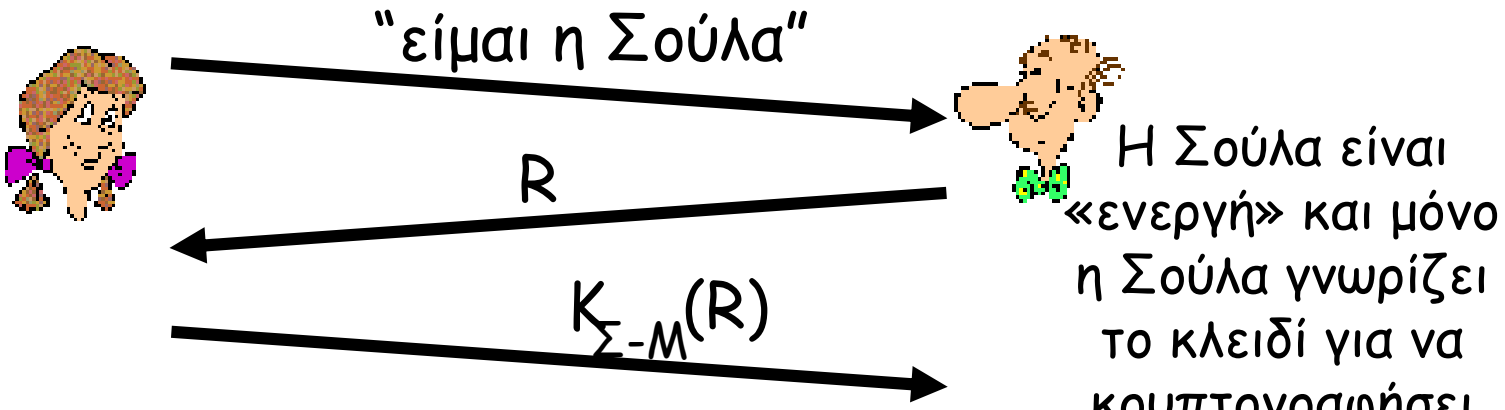
Η επίθεση μέσω αναπαραγωγής είναι ακόμα εφικτή!

Αυθεντικοποίηση: άλλη μια προσπάθεια

Στόχος: την αποφυγή της επίθεσης μέσω αναπαραγωγής

Nonce: ένας αριθμός (R) που θα χρησιμοποιηθεί μόνο μια φορά

ap4.0: Για να αποδείξει ότι η Σούλα είναι «ενεργή», ο Μήτσος στέλνει στην Σούλα nonce, R. Η Σούλα πρέπει να επιστρέψει το R, κρυπτογραφημένο με ένα διαμοιρασμένο μυστικό κλειδί



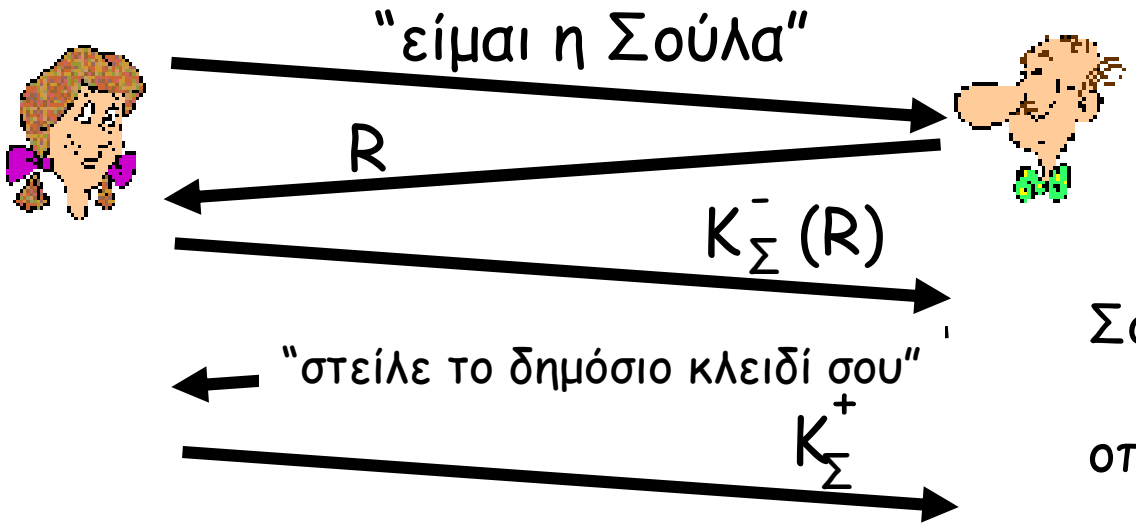
μειονεκτήματα;

Αυθεντικοποίηση: ap5.0

ap4.0 απαιτεί ένα διαμοιρασμένο συμμετρικό κλειδί

- Μπορούμε να αυθεντικοποιήσουμε με χρήση κρυπτογραφίας δημόσιου κλειδιού;

ap5.0: χρήση nonce, κρυπτογραφία δημόσιου κλειδιού



Ο Μήτσος υπολογίζει

$K_\Sigma^+(K_\Sigma^-(R)) = R$

και ξέρει ότι μόνο η Σούλα μπορεί να έχει το ιδιωτικό κλειδί με το οποίο κρυπτογραφήθηκε το R, έτσι ώστε

$K_\Sigma^+(K_\Sigma^-(R)) = R$

ap5.0: κενό ασφάλειας

Επίθεση μέσω ενδιάμεσου: Η Λαμόγια υποδύεται την Σούλα (στον Μήτσο) και τον Μήτσο (στην Σούλα)

Είμαι η Σούλα

Είμαι η Σούλα

R

$K^-_{\Lambda}(R)$

στείλε το δημόσιο κλειδί σου

K^+_{Λ}

R

$K^-_{\Sigma}(R)$

στείλε το δημόσιο κλειδί σου

K^+_{Σ}

$K^+_{\Lambda}(m)$

Η Λαμόγια λαμβάνει το $m = K^-_{\Lambda}(K^+_{\Lambda}(m))$

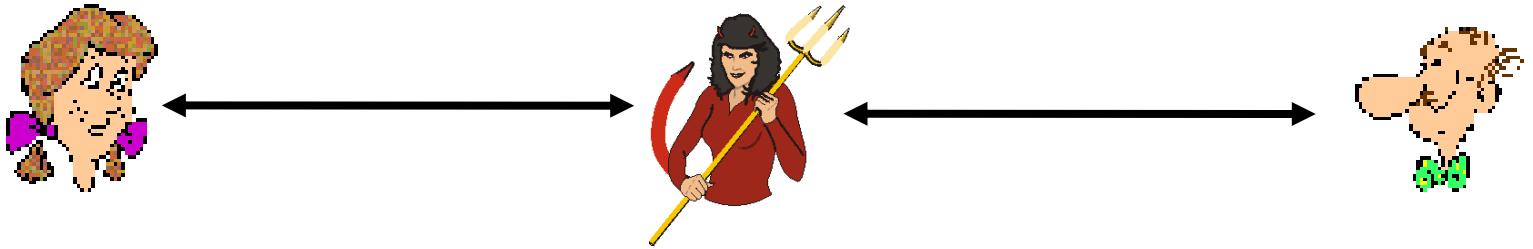
Στέλνει το m στην Σούλα κρυπτογραφημένο με το δημόσιο κλειδί της

$K^+_{\Sigma}(m)$

$m = K^-_{\Sigma}(K^+_{\Sigma}(m))$

ap5.0: κενό ασφάλειας

Επίθεση μέσω ενδιάμεσου: Η Λαμόγια υποδύεται την Σούλα (στον Μήτσο) και τον Μήτσο (στην Σούλα)



Δύσκολες να εντοπιστούν:

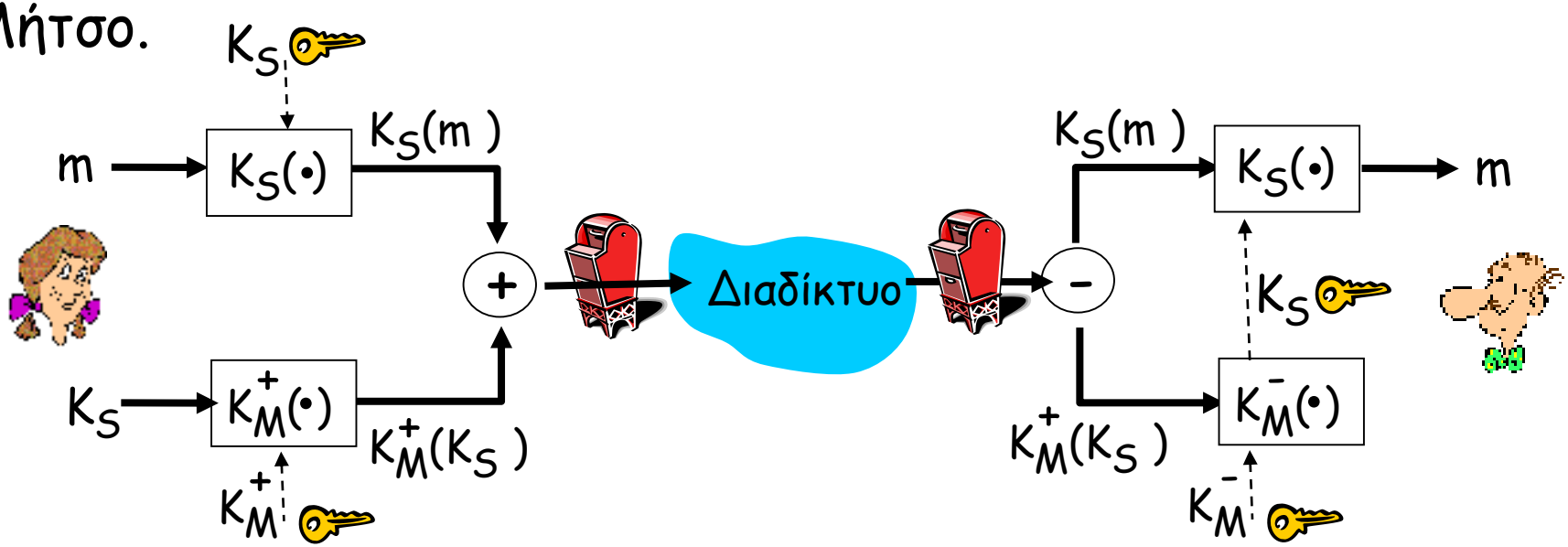
- Ο Μήτσος λαμβάνει οτιδήποτε στέλνει η Σούλα, και αντίστροφα. (π.χ., έτσι ο Μήτσος και η Σούλα μπορούν να συναντηθούν μια εβδομάδα αργότερα και να ξαναδούν την συνομιλία)
- το πρόβλημα είναι ότι η Λαμόγια λαμβάνει επίσης όλα τα μηνύματα!

Ασφάλεια Δικτύων

- Τι είναι η ασφάλεια δικτύων;
- Αρχές κρυπτογραφίας
- Ακεραιότητα μηνύματος
- Αυθεντικοποίηση
- Διασφαλίζοντας το e-mail
- Διασφαλίζοντας συνδέσεις TCP: SSL
- Ασφάλεια επιπέδου δικτύου: IPsec
- Διασφαλίζοντας ασύρματα τοπικά δίκτυα
- Firewalls και IDS

Ασφάλεια στην ηλεκτρονική αλληλογραφία

- Η Σούλα θέλει να στείλει ένα εμπιστευτικό e-mail, m, στον Μήτσο.

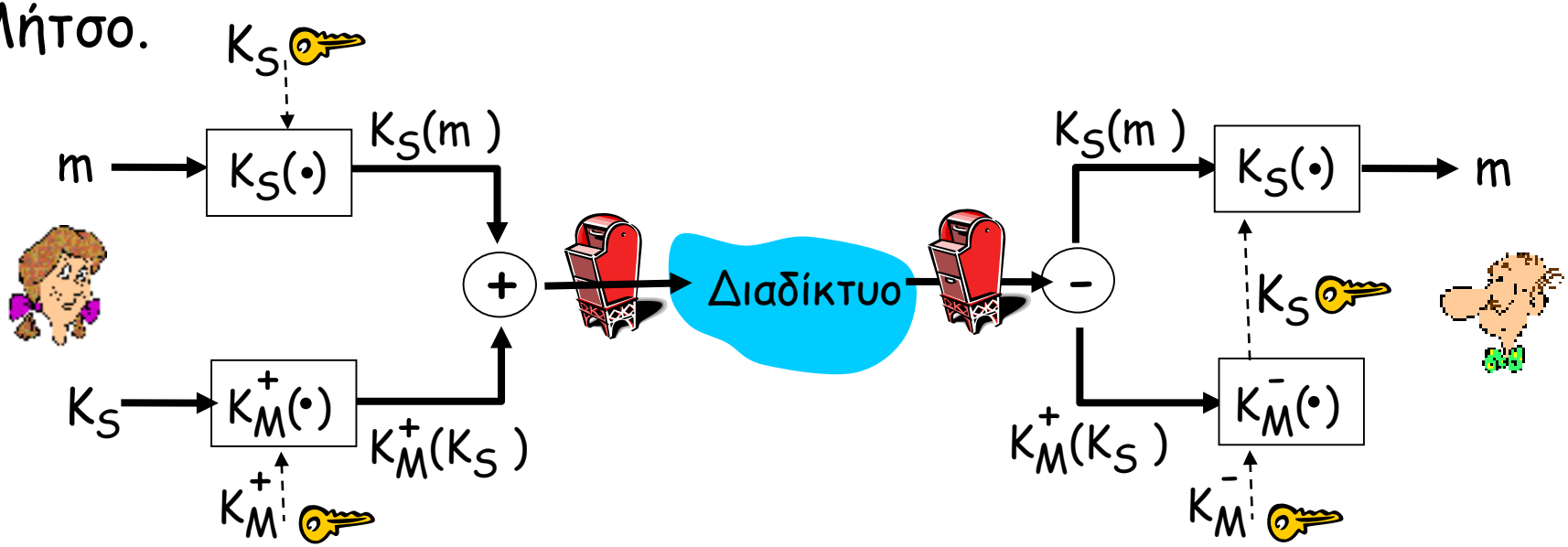


Σούλα:

- παράγει τυχαίο συμμετρικό κλειδί K_S.
- κρυπτογραφεί το μήνυμα με το K_S (για αποδοτικότητα)
- κρυπτογραφεί το K_S με το δημόσιο κλειδί του Μήτσου.
- στέλνει το $K_S(m)$ και $K_M(K_S)$ στον Μήτσο.

Ασφάλεια στην ηλεκτρονική αλληλογραφία

- Η Σούλα θέλει να στείλει ένα εμπιστευτικό e-mail, m, στον Μήτσο.

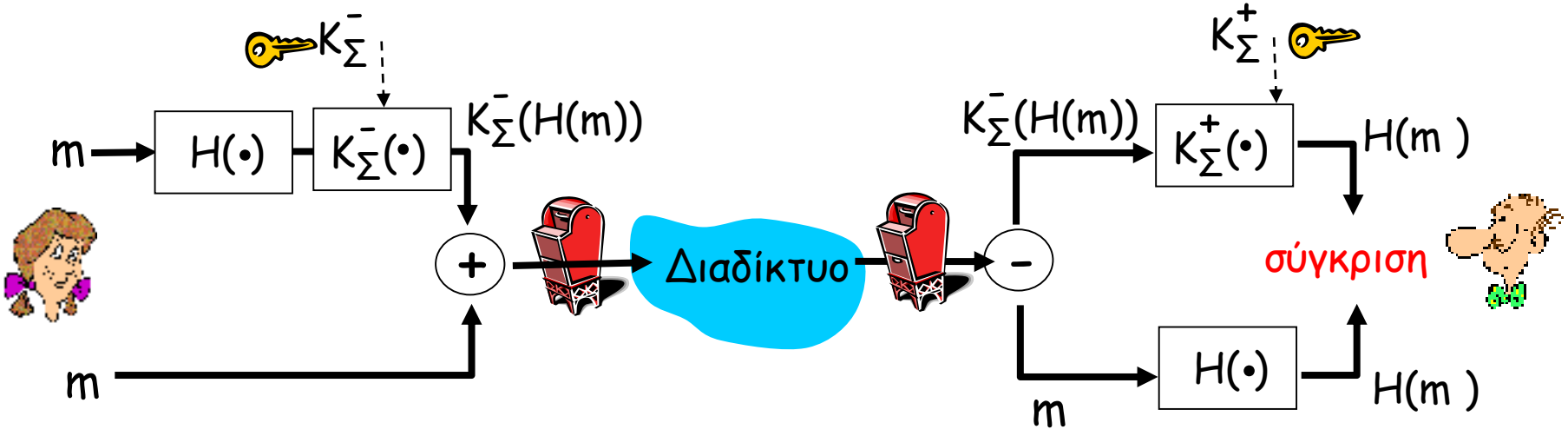


Μήτσος:

- χρησιμοποιεί το ιδιωτικό του κλειδί για να αποκρυπτογραφήσει και να ανακτήσει το K_S
- χρησιμοποιεί το K_S για να αποκρυπτογραφήσει το $K_S(m)$ και να ανακτήσει το m

Ασφάλεια στην ηλεκτρονική αλληλογραφία (συνέχεια)

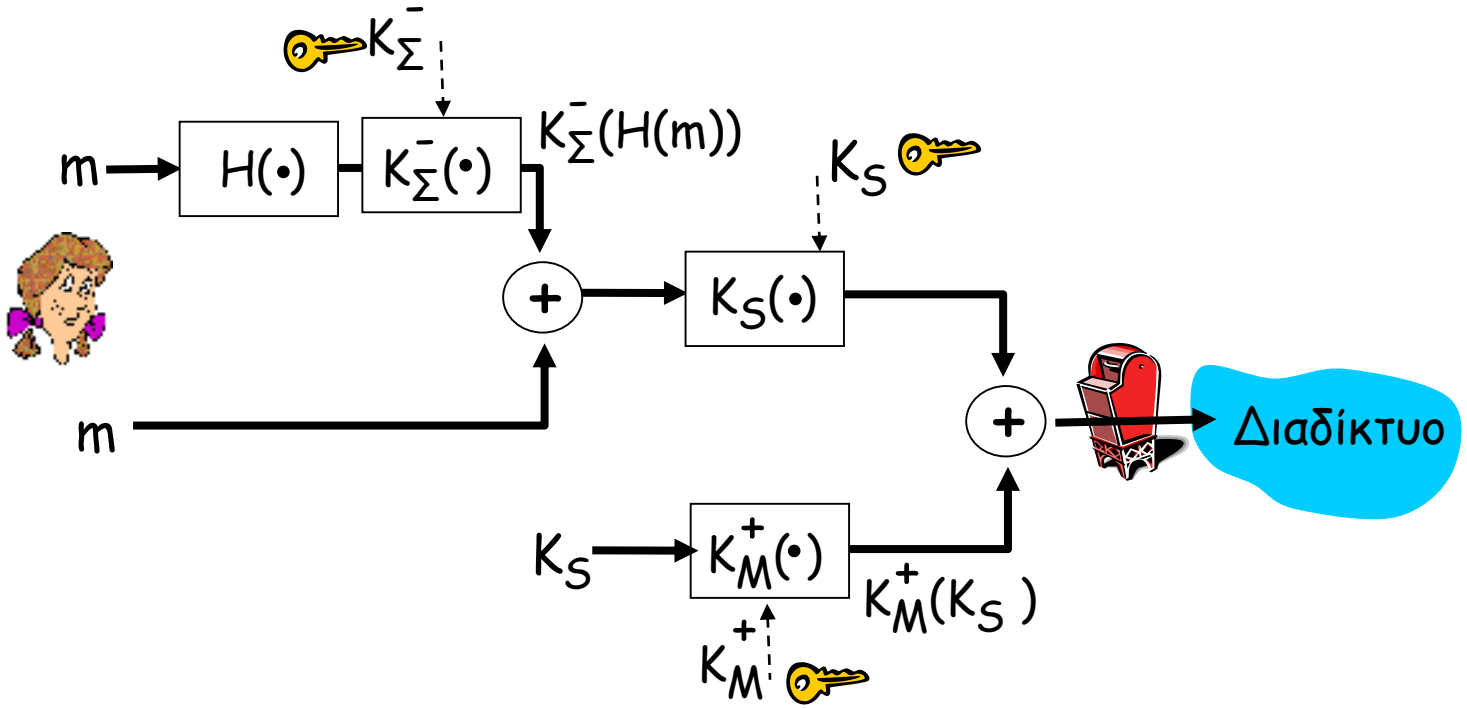
- Η Σούλα θέλει να παρέχει αυθεντικοποίηση αποστολέα, ακεραιότητα μηνύματος



- Η Σούλα υπογράφει ψηφιακά το μήνυμα.
- Στέλνει το μήνυμα (καθαρό κείμενο) και την ψηφιακή υπογραφή

Ασφάλεια στην ηλεκτρονική αλληλογραφία (συνέχεια)

- Η Σούλα θέλει να παρέχει εμπιστευτικότητα, αυθεντικοποίηση αποστολέα, ακεραιότητα μηνύματος



Η Σούλα χρησιμοποιεί τρία κλειδιά: το ιδωτικό της κλειδί, το δημόσιο κλειδί του Μήτσου, το νέο συμμετρικό κλειδί

Pretty good privacy (PGP)

- Σχήμα ασφαλούς ηλεκτρονικής αλληλογραφίας, de-facto πρότυπο.
- Χρησιμοποιεί κρυπτογράφηση συμμετρικού κλειδιού, δημόσιου κλειδιού, συναρτήσεις κατακερματισμού και ψηφιακές υπογραφές.
- Παρέχει εμπιστευτικότητα, αυθεντικοποίηση αποστολέα, ακεραιότητα.
- Ο δημιουργός Phil Zimmerman, ήταν επί 3 χρόνια στόχος ομοσπονδιακής έρευνας.

Ένα PGP μήνυμα με υπογραφή:

```
---BEGIN PGP SIGNED MESSAGE---
Hash: SHA1

Bob:My husband is out of town
   tonight.Passionately yours,
   Alice

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3mqJ
   hFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

Ασφάλεια Δικτύων

- Τι είναι η ασφάλεια δικτύων;
- Αρχές κρυπτογραφίας
- Ακεραιότητα μηνύματος
- Αυθεντικοποίηση
- Διασφαλίζοντας το e-mail
- Διασφαλίζοντας συνδέσεις TCP: SSL
- Ασφάλεια επιπέδου δικτύου: IPsec
- Διασφαλίζοντας ασύρματα τοπικά δίκτυα
- Firewalls και IDS

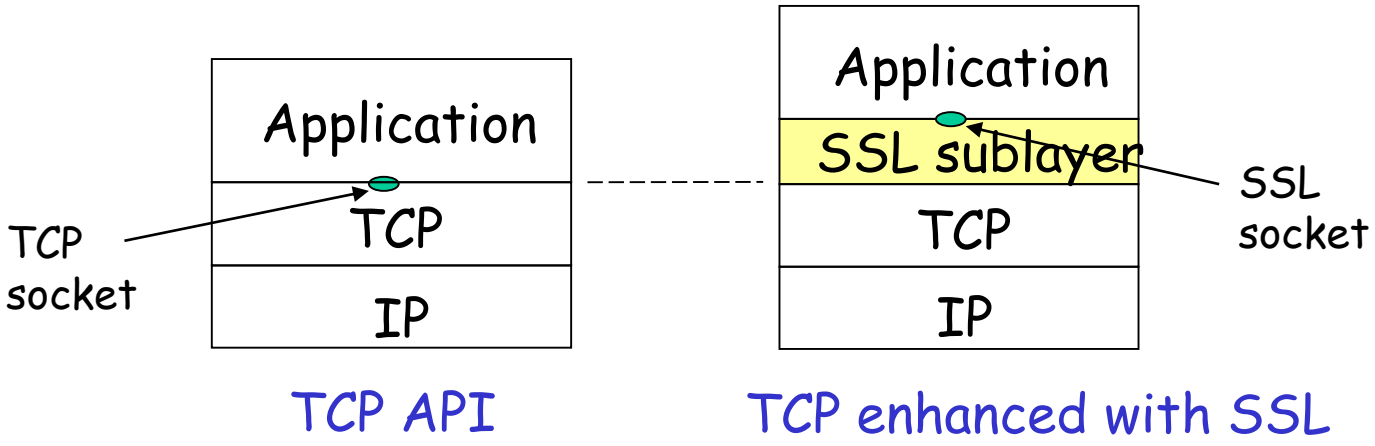
Secure sockets layer (SSL)

Παρέχει ασφάλεια επιπέδου μεταφοράς σε οποιαδήποτε εφαρμογή βασισμένη στοTCP.

Χρησιμοποιείται μεταξύ προγραμμάτων περιήγησης (Web browsers), εξυπηρέτες για e-commerce (shttp).

Υπηρεσίες ασφάλειας:

Αυθεντικοποίηση εξυπηρέτη, Κρυπτογράφηση δεδομένων, Αυθεντικοποίηση πελάτη (προαιρετικό)



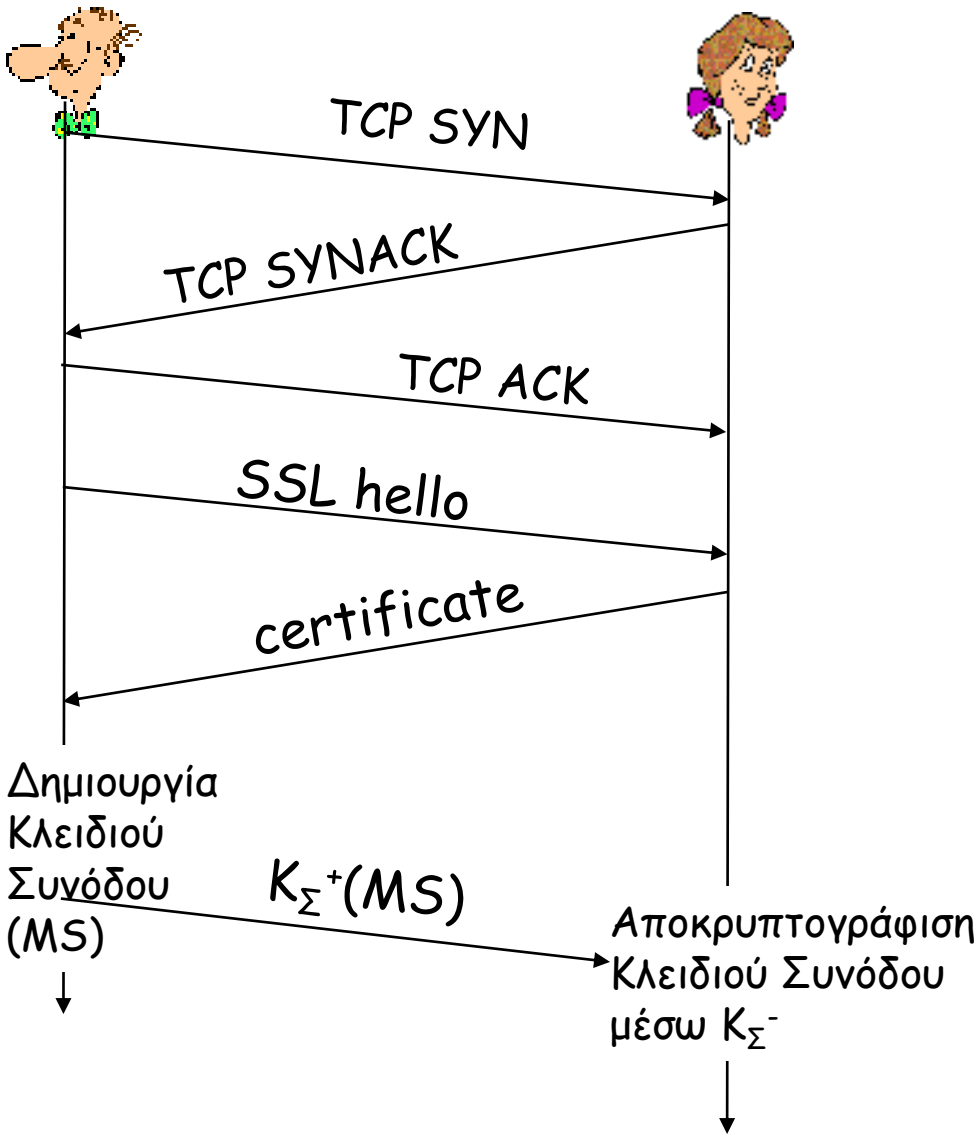
SSL: τρία στάδια

- *Χειραψία:* Χρήση ψηφιακών πιστοποιητικών για την αυθεντικοποίηση της Σούλας και του Μήτσου και για την ανταλλαγή κλειδιού συνόδου
- *Παραγωγή κλειδιών:* Χρήση του κλειδιού συνόδου για τη παραγωγή κλειδιών
- *Μεταφορά δεδομένων:* Διαχωρισμός των δεδομένων σε μια σειρά από records

SSL: τρία στάδια

1. Χειραψία:

- Ο Μήτσος δημιουργεί μια νέα σύνδεση TCP με την Σούλα
- Ο Μήτσος αυθεντικοποιεί την Σούλα μέσω μίας Αρχής Πιστοποίησης
- Ο Μήτσος δημιουργεί, κρυπτογραφεί (χρησιμοποιώντας το δημόσιο κλειδί της Σούλας), και αποστέλλει στην Σούλα το κλειδί συνόδου



SSL: τρία στάδια

2. Παραγωγή κλειδιών:

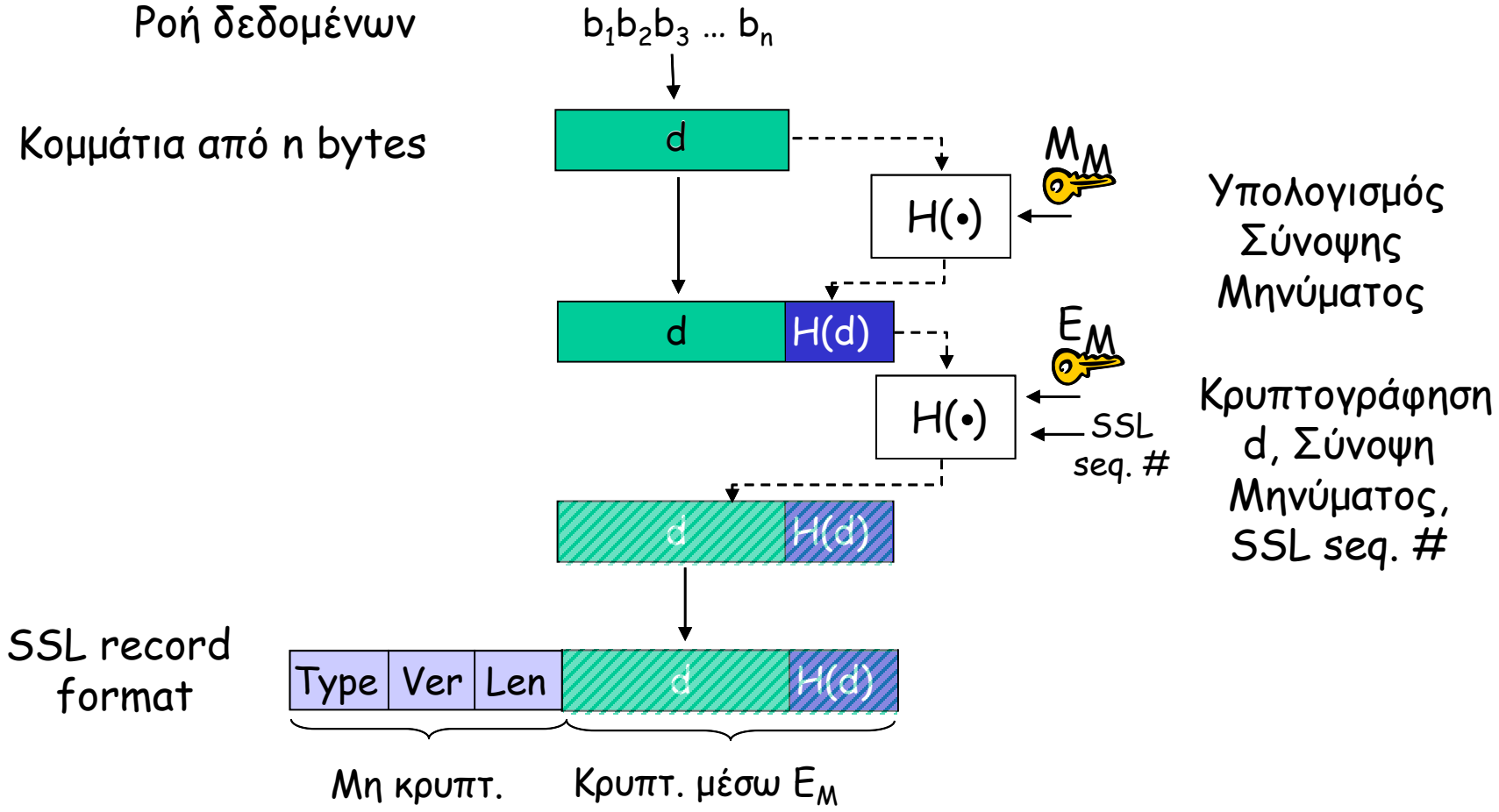
Η Σούλα και ο Μήτσος χρησιμοποιούν το κοινό κλειδί συνόδου για να παράγουν 4 κλειδιά:

- E_M: Μ->Σ κλειδί κρυπτογράφησης δεδομένων
- E_Σ: Σ->Μ κλειδί κρυπτογράφησης δεδομένων
- M_M: Μ->Σ κλειδί συνάρτησης κατακερματισμού
- M_Σ: Σ->Μ κλειδί συνάρτησης κατακερματισμού

Γιατί 4 κλειδιά?

SSL: τρία στάδια

3. Μεταφορά δεδομένων



SSL: Επιθέσεις;

- Replay or re-order?
- Λύσεις;

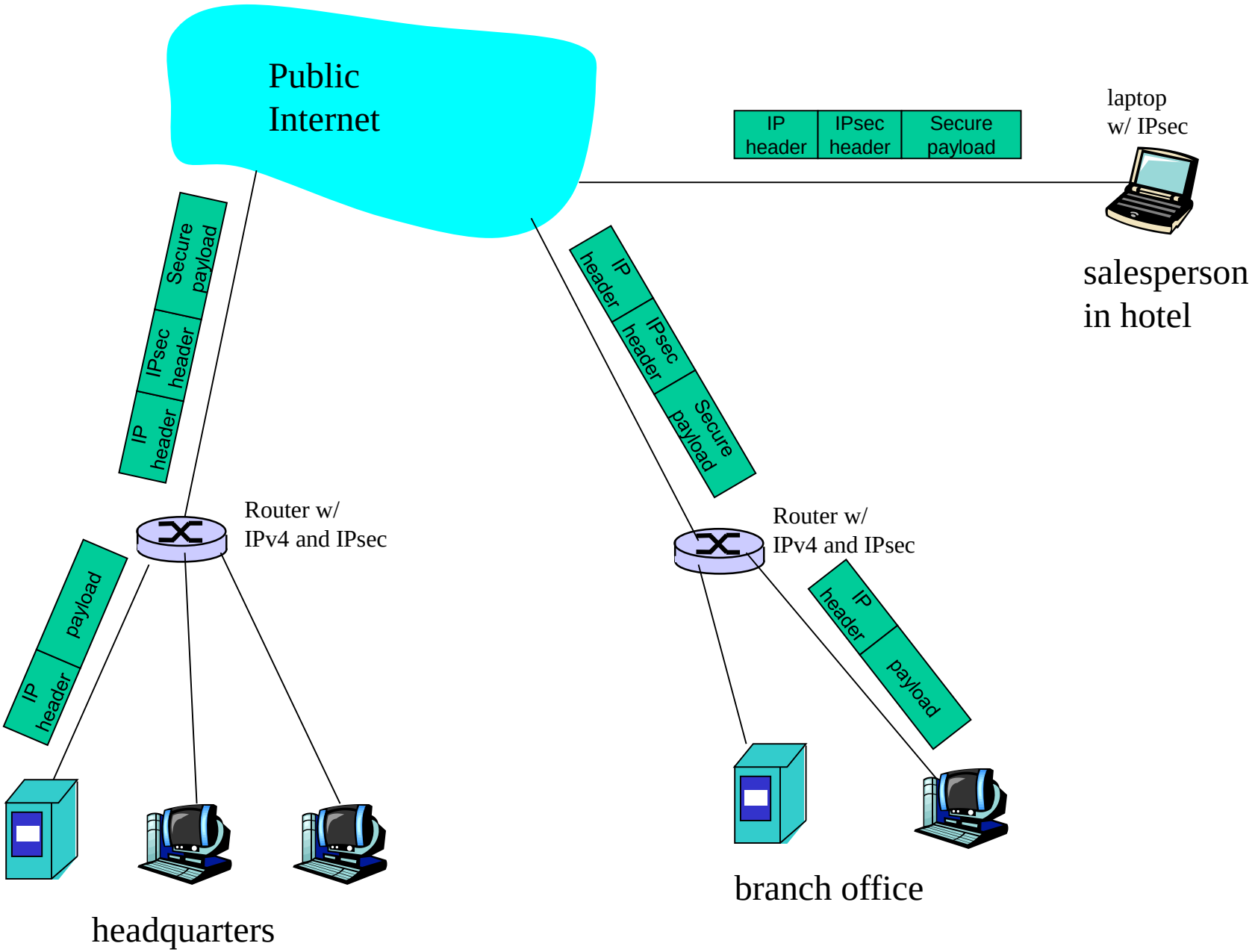
Ασφάλεια Δικτύων

- Τι είναι η ασφάλεια δικτύων;
- Αρχές κρυπτογραφίας
- Ακεραιότητα μηνύματος
- Αυθεντικοποίηση
- Διασφαλίζοντας το e-mail
- Διασφαλίζοντας συνδέσεις TCP: SSL
- Ασφάλεια επιπέδου δικτύου: IPsec
- Διασφαλίζοντας ασύρματα τοπικά δίκτυα
- Firewalls και IDS

Ασφάλεια επιπέδου δικτύου: IPsec

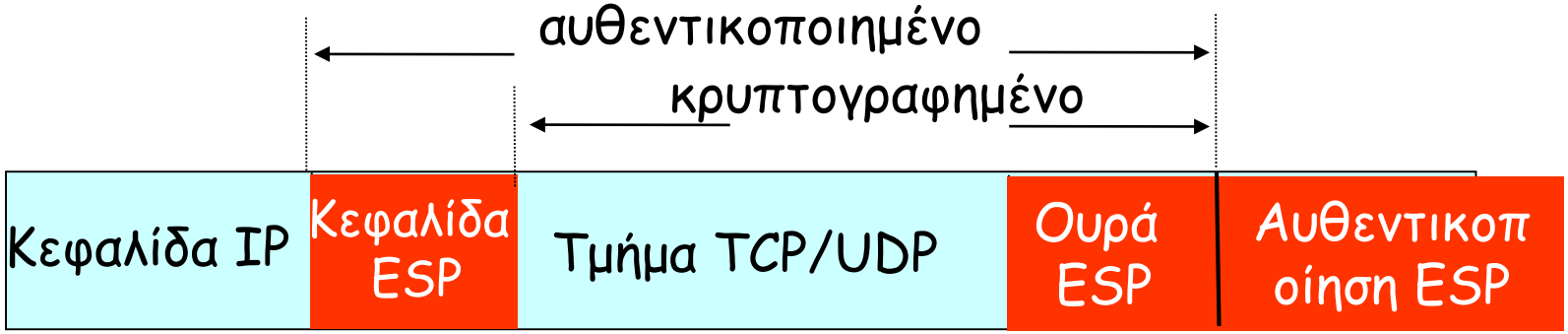
- Εμπιστευτικότητα επιπέδου δικτύου:
  - Αποστολέας κρυπτογραφεί τα δεδομένα του IP δεδομενογράμματος
  - Τμήματα TCP και UDP, ICMP και SNMP μηνύματα
- Αυθεντικοποίηση επιπέδου δικτύου
  - Ο παραλήπτης μπορεί να αυθεντικοποιήσει την IP διεύθυνση του αποστολέα
- Δύο κύρια πρωτόκολλα:
  - authentication header (AH)
  - encapsulation security payload (ESP)
- Στο AH και στο ESP, ο αποστολέας και ο παραλήπτης κάνουν μια δικτυακή χειραψία:
  - Δημιουργία μιας λογικής σύνδεσης επιπέδου δικτύου ονομαζόμενο συσχέτιση ασφαλείας
- Κάθε συσχέτιση ασφαλείας είναι μονοκατευθυντική.
- Μοναδικά προσδιορίζεται με:
  - Πρωτόκολλο ασφαλείας (AH ή ESP)
  - Την διεύθυνση προέλευσης IP
  - Ταυτότητα σύνδεσης 32-bit

Virtual Private Network (VPN)



Το πρωτόκολλο ESP

- Παρέχει εμπιστευτικότητα, αυθεντικοποίηση υπολογιστή υπηρεσίας, ακεραιότητα δεδομένων.
- Δεδομένα και ουρά ESP κρυπτογραφημένα.
- Η ουρά ESP περιέχει padding και πεδίο κεφαλίδας πακέτου.
- Η κεφαλίδα ESP περιέχει το sequence number
- πρωτόκολλο = 50.
- Αυθεντικοποίηση ESP = MAC



Ασφάλεια Δικτύων

- Τι είναι η ασφάλεια δικτύων;
- Αρχές κρυπτογραφίας
- Ακεραιότητα μηνύματος
- Αυθεντικοποίηση
- Διασφαλίζοντας το e-mail
- Διασφαλίζοντας συνδέσεις TCP: SSL
- Ασφάλεια επιπέδου δικτύου: IPsec
- Διασφαλίζοντας ασύρματα τοπικά δίκτυα
- Firewalls και IDS

Ασφάλεια στο IEEE 802.11

- *War-driving:* οδήγηση σε μια γεωγραφική περιοχή των ΗΠΑ (Bay area), για τον εντοπισμό ασύρματων δικτύων IEEE 802.11
  - Περισσότερα από 9000 διαθέσιμα ασύρματα δίκτυα σε κεντρικούς δρόμους
  - 85% δεν εφαρμόζουν κρυπτογράφηση/αυθεντικοποίηση
  - Παρακολούθηση πακέτων και διάφορες επιθέσεις εύκολες να πραγματοποιηθούν!
- *Διασφαλίζοντας το 802.11:*
  - κρυπτογράφηση, αποκρυπτογράφηση
  - Πρώτη προσπάθεια: το πρωτόκολλο WEP, αποτυχία.
  - State of the art: Το πρωτόκολλο 802.11i

Wired Equivalent Privacy (WEP):

αυθεντικοποίηση όπως στο πρωτόκολλο *ap4.0*

- Υπολογιστής υπηρεσίας κάνει μια αίτηση αυθεντικοποίησης στο σημείο προσπέλασης (access point)
- Το σημείο προσπέλασης στέλνει ένα 128 bit nonce
- Ο υπολογιστής υπηρεσίας κρυπτογραφεί το nonce χρησιμοποιώντας ένα συμμετρικό κλειδί
- Το σημείο προσπέλασης αποκρυπτογραφεί το nonce, και αυθεντικοποιεί τον υπολογιστή υπηρεσίας

Δεν απαιτείται μηχανισμός διανομής κλειδιού

Αυθεντικοποίηση: αρκεί η γνώση του διαμοιραζόμενου κλειδιού

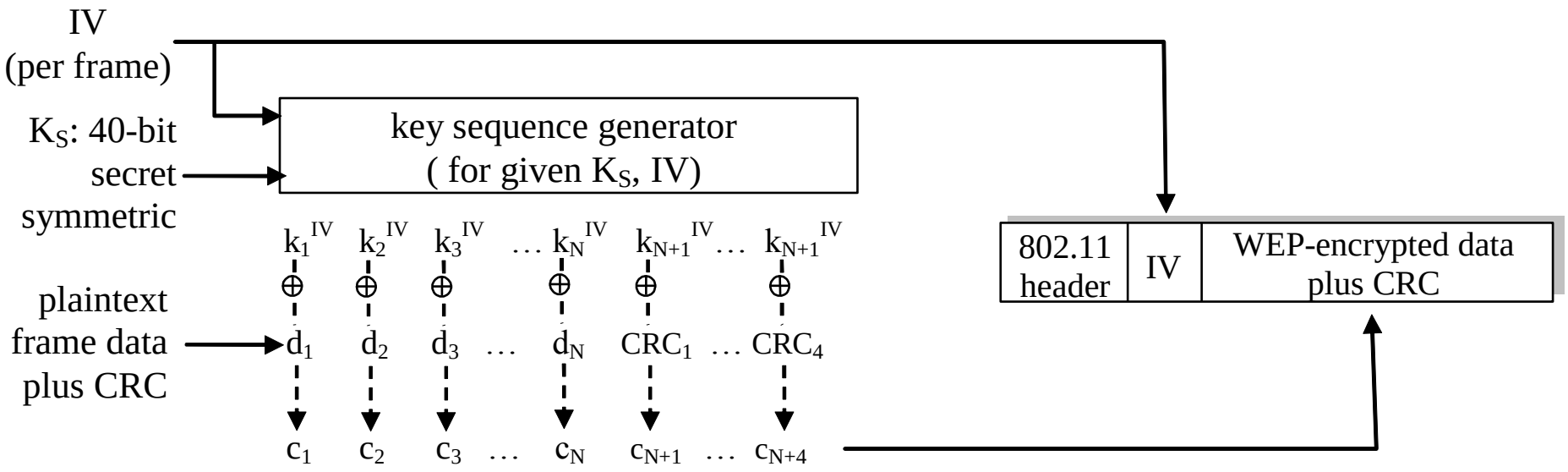
WEP: κρυπτογράφηση δεδομένων

- Υπολογιστής υπηρεσίας και σταθμός βάσης μοιράζονται ένα 40 bit συμμετρικό κλειδί (σχεδόν μόνιμο)
- Ένα 24-bit initialization vector (IV) προσαρτάται για να δημιουργηθεί ένα 64-bit κλειδί
- 64 bit κλειδί χρησιμοποιείται για να παράγει ένα ρεύμα τιμών κλειδιών , k_i^{IV}
- k_i^{IV} χρησιμοποιείται για να κρυπτογραφήσει το i-οστο byte, d_i, του πλαισίου:

$$c_i = d_i \text{ XOR } k_i^{IV}$$

- Το IV και τα κρυπτογραφημένα bytes, c_i στέλνονται μέσα στο πλαίσιο

802.11 WEP κρυπτογράφηση



WEP κρυπτογράφηση (αποστολέας)

Παραβιάζοντας την ασφάλεια του 802.11 WEP

Κενό ασφαλείας:

- 24-bit IV, ένα IV ανά πλαίσιο, -> χρησιμοποίηση ίδιων τιμών IV
- IV μεταδίδονται σε καθαρό κείμενο -> γνώση της χρησιμοποίησης ίδιων τιμών IV

Επίθεση:

- Η Λαμόγια προκαλεί την Σούλα να κρυπτογραφήσει ένα γνωστό καθαρό κείμενο $d_1\ d_2\ d_3\ d_4$ …
- Η Λαμόγια βλέπει: $c_i = d_i$ XOR k_i^{IV}
- Η Λαμόγια γνωρίζει τα $c_i\ d_i$, έτσι μπορεί να υπολογίσει το k_i^{IV}
- Η Λαμόγια γνωρίζει την ακολουθία κλειδιών $k_1^{IV}\ k_2^{IV}\ k_3^{IV}$ …
- Την επόμενη φορά που θα χρησιμοποιηθεί ξανά το ίδιο IV, η Λαμόγια μπορεί να αποκρυπτογραφήσει!

802.11i: Βελτιωμένη ασφάλεια

Πολλαπλοί (ισχυρότεροι) μηχανισμοί κρυπτογράφησης

Παρέχεται διανομή κλειδιού

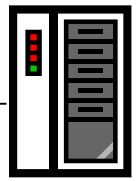
Γίνεται χρήση διακομιστή αυθεντικοποίησης διαφορετικού από το σημείο προσπέλασης

802.11i: 4 φάσεις λειτουργίας

STA: Υπολογιστής υπηρεσίας

AP: Σημείο προσπέλασης

Ενσύρματο δίκτυο



AS: Διακομιστής αυθεντικοποίησης

1 Εντοπισμός δυνατοτήτων ασφάλειας

2 STA και AS αμοιβαία αυθεντικοποιούνται και από κοινού παράγουν το Master Key (MK).

3 Το AS παράγει το ίδιο PMK, Το οποίο και αποστέλλει στο AP

3o STA παράγει το Pairwise Master Key (PMK)

4 STA και AP κάνουν χρήση του PMK για να παράξουν το Temporal Key (TK) το οποίο χρησιμοποιείται για κρυπτογράφηση και ακεραιότητα

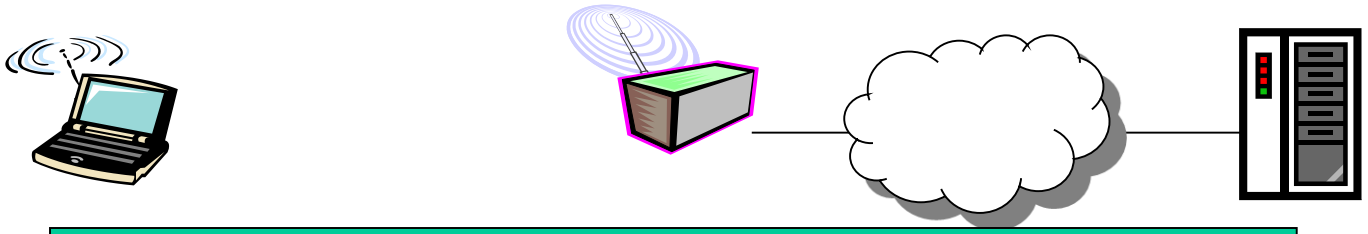
EAP: extensible authentication protocol

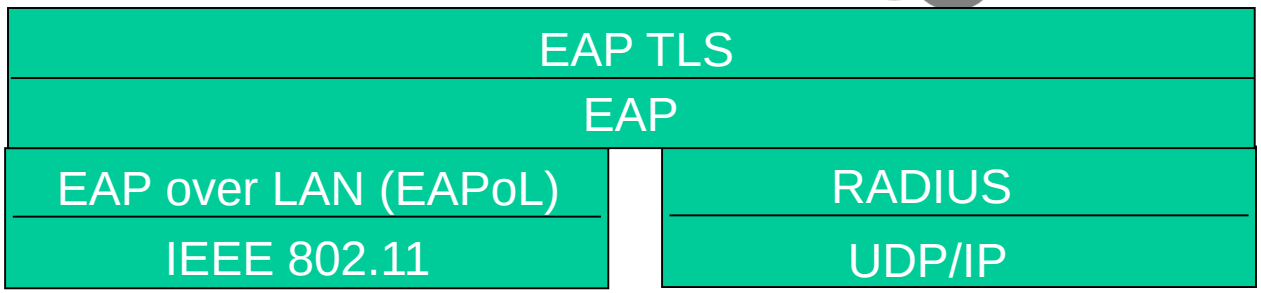
EAP: πρωτόκολλο πιστοποίησης ταυτότητας μεταξύ υπολογιστή υπηρεσίας και διακομιστή αυθεντικοποίησης

Το EAP κάνει χρήση χωριστών συνδέσεων

Υπολογιστής υπηρεσίας-προς-AP (EAP over LAN)

AP προς διακομιστή αυθεντικοποίησης(RADIUS over UDP)





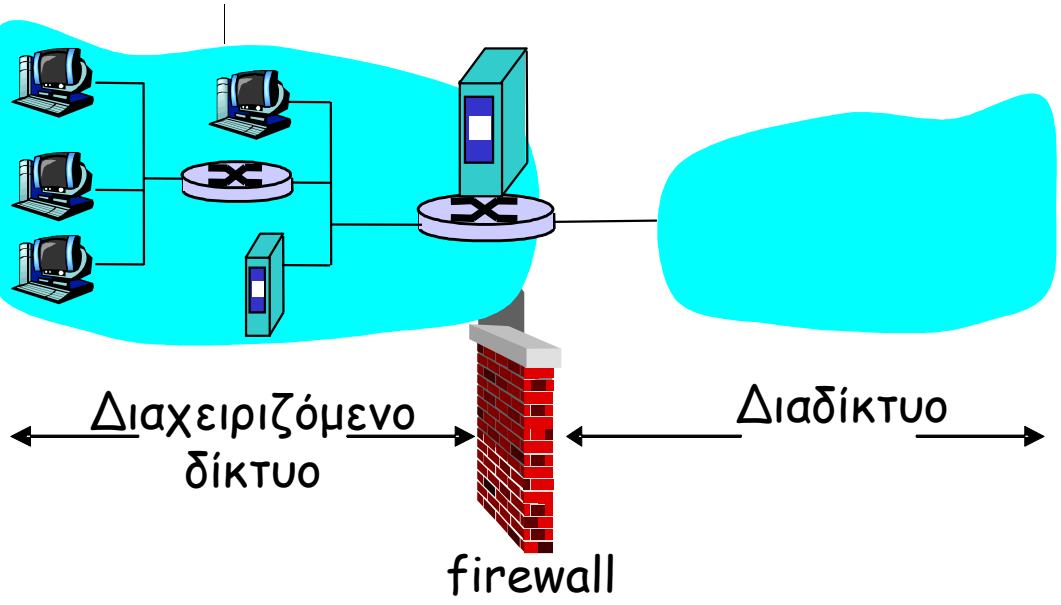
Ασφάλεια Δικτύων

- Τι είναι η ασφάλεια δικτύων;
- Αρχές κρυπτογραφίας
- Ακεραιότητα μηνύματος
- Αυθεντικοποίηση
- Διασφαλίζοντας το e-mail
- Διασφαλίζοντας συνδέσεις TCP: SSL
- Ασφάλεια επιπέδου δικτύου: IPsec
- Διασφαλίζοντας ασύρματα τοπικά δίκτυα
- Firewalls και IDS

Firewalls

firewall

Απομονώνει το εσωτερικό δίκτυο ενός υπολογιστή από το διαδίκτυο, επιτρέποντας σε ορισμένα πακέτα να περνούν και μπλοκάροντας τα άλλα πακέτα.



Firewalls: Τι προσφέρουν;

Παρεμπόδιση επιθέσεων άρνησης υπηρεσιών:

- Πλημμύρα SYN: ο επιτιθέμενος εγκαθιστά πολλές ψεύτικες TCP συνδέσεις και δεν αφήνει πόρους για πραγματικές συνδέσεις.

Αποτρέπει παράνομη μετατροπή/πρόσβαση σε εσωτερικά δεδομένα

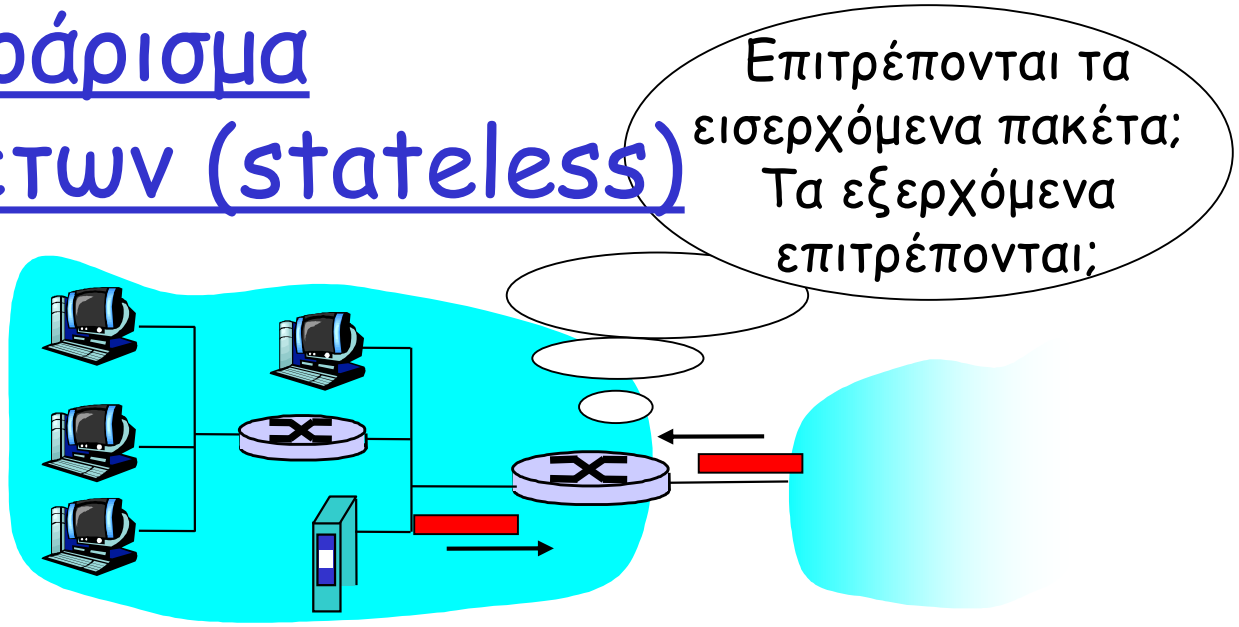
- π.χ. επιτιθέμενος αντικαθιστά μια ιστοσελίδα με μια άλλη

Επιτρέπει μόνο την εξουσιοδοτημένη πρόσβαση στο εσωτερικό δίκτυο (σύνολο από αυθεντικοποιημένους χρήστες/υπολογιστές)

Τρεις τύποι firewall:

- Φιλτραρίσματος πακέτων (stateless)
- Φιλτραρίσματος πακέτων (stateful)
- Επιπέδου εφαρμογής

Φιλτράρισμα πακέτων (stateless)



- Εσωτερικό δίκτυο συνδέεται με το διαδίκτυο με έναν δρομολογητή firewall
- Ο δρομολογητής φιλτράρει ένα προς ένα τα πακέτα, η απόφαση για το αν θα προωθηθούν τα πακέτα ή όχι εξαρτάται από:
  - IP Διευθύνσεις προέλευσης και προορισμού
  - Θύρα προέλευσης και προορισμούTCP/UDP
  - ICMP τύπος μηνύματος
  - bits του TCP: SYN ή ACK

Φιλτράρισμα πακέτων (stateless)

- Παράδειγμα 1: Μπλόκαρε όλα τα εισερχόμενα και εξερχόμενα δεδομενογράμματα με IP πρωτόκολλο πεδίο = 17 και με θύρα προέλευσης ή προορισμού= 23.
  - Όλη η εξερχόμενη και εισερχόμενη UDP ροή και όλες οι συνδέσεις telnet έχουν μπλοκαριστεί.
- Παράδειγμα 2: μπλόκαρε εισερχόμενα τμήματα TCP με ACK=0.
  - Αποτρέπει εξωτερικούς πελάτες από το να κάνουν TCP συνδέσεις με εσωτερικούς πελάτες, αλλά επιτρέπει εσωτερικούς πελάτες να συνδεθούν με εξωτερικούς.

Φιλτράρισμα πακέτων (Stateless): περισσότερα παραδείγματα

Πολιτική	Ρύθμιση Firewall
Αποκλεισμός εξωτερικής πρόσβασης διαδικτύου.	Απόρριψε όλα τα εξερχόμενα πακέτα προς οποιαδήποτε IP address, στη θύρα 80
Αποκλεισμός εισερχόμενων συνδέσεων TCP, εκτός εκείνων που προορίζονται για τον Web server του τμήματος.	Απόρριψε όλα τα εισερχόμενα TCP SYN πακέτα προς οποιαδήποτε IP εκτός της 130.207.244.203, θύρα 80
Προστασία του εύρους ζώνης από υπηρεσίες δικτυακού ράδιο.	Απόρριψε όλα τα εισερχόμενα UDP πακέτα εκτός των DNS και αναμεταδόσεων του δρομολογητών
Αποκλεισμός της δυνατότητας χρήσης του δικτύου για τη πραγματοποίηση επιθέσεων smurf DoS.	Απόρριψε όλα τα ICMP πακέτα που προορίζονται για διεύθυνση αναμετάδοσης
Προστασία δικτύου από raceroute	Απόρριψε όλα τα εξερχόμενα ICMP πακέτα που έχουν λήξει

Λίστες έλεγχου προσπέλασης

- *ACL:* πίνακας με κανόνες, οι οποίοι εφαρμόζονται σε κάθε εισερχόμενο πακέτο

Ενεργεία	Διεύθυνση αποστολέα	Διεύθυνση παραλήπτη	πρωτόκολλο	Θύρα αποστολέα	Θύρα παραλήπτη	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

Φιλτράρισμα πακέτων (Stateful)

Φιλτράρισμα πακέτων (stateless):

Δέχεται πακέτα τα οποία "δεν έχουν λογική" π.χ., θύρα παραλήπτη = 80, ACK bit set, αν και δεν έχει δημιουργηθεί καμία σύνδεση TCP:

Ενεργεία	Διεύθυνση αποστολέα	Διεύθυνση παραλήπτη	πρωτόκολλο	Θύρα αποστολέα	Θύρα παραλήπτη	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

- *Φιλτράρισμα μακέτων (stateful):* ακολουθούν τη κατάσταση κάθε σύνδεσης TCP
  - Παρακολούθηση διαδικασίας έναρξης σύνδεσης (SYN) και τερματισμού (FIN): επιτρέπει να προσδιορίσουμε πότε τα εισερχόμενα/εξερχόμενα πακέτα "έχουν λογική"

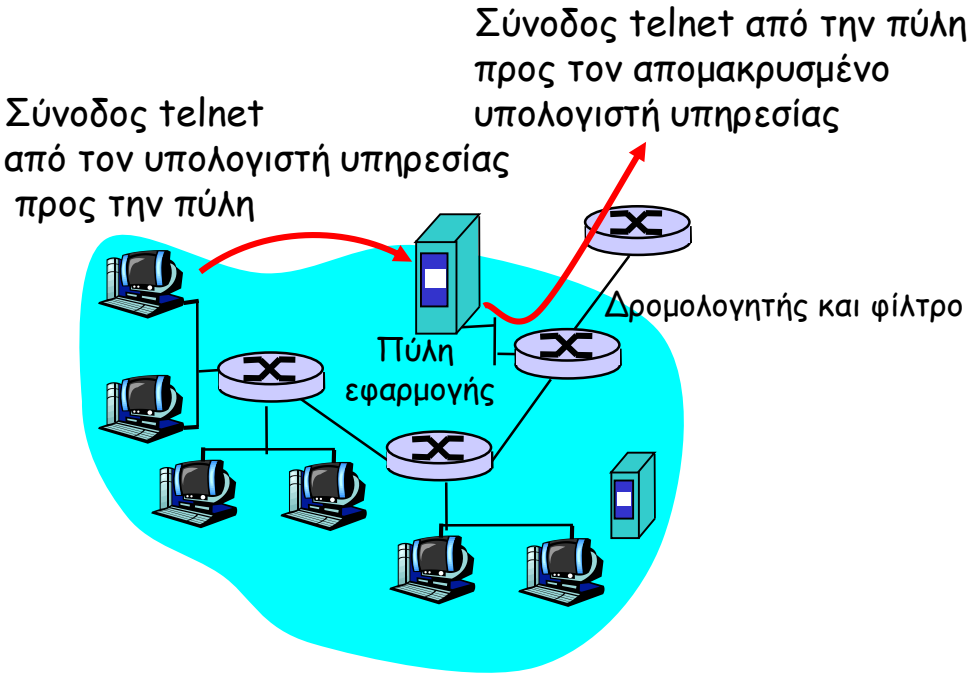
Φιλτράρισμα πακέτων (Stateful)

- Αναβαθμισμένη ACL που επιτρέπει τον έλεγχο της κατάστασης μιας σύνδεσης πριν την αποδοχή ενός πακέτου

Ενεργεία	Διεύθυνση αποστολέα	Διεύθυνση παραλήπτη	πρωτόκολλο	Θύρα αποστολέα	Θύρα παραλήπτη	flag bit	Έλεγχος σύνδεσης
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	✗
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	✗
deny	all	all	all	all	all	all	

Πύλες εφαρμογής

- Φιλτράρει πακέτα σε δεδομένα της εφαρμογής και σε IP/TCP/UDP πεδία.
- Παράδειγμα: δυνατότητα για επιλογή των χρηστών που θα επιτρέπονται να πραγματοποιούν συνδέσεις telnet.



1. Απαιτεί από όλους τους χρήστες telnet να κάνουν συνδέσεις telnet μέσω της πύλης εφαρμογής.
2. Για εξουσιοδοτημένους χρήστες, ο δρομολογητής πύλης εγκαθιστά συνδέσεις telnet στον απομακρυσμένο υπολογιστή υπηρεσίας. Η πύλη μεταγει δεδομένα μεταξύ δύο συνδέσεων
3. Ένας δρομολογητής φιλτράρει όλες τις συνδέσεις telnet που δεν προέρχονται από την πύλη.

Περιορισμοί των firewalls

- Παραπλάνηση IP: οι δρομολογητές δεν μπορούν να γνωρίζουν αν τα δεδομένα προέρχονται από την πηγή που επικαλείται ότι τα έστειλε.
- Αν διαφορετικές εφαρμογές απαιτούν ξεχωριστή αντιπετώπιση, τότε θα πρέπει να έχει η κάθε μια εφαρμογή την δική της πύλη εφαρμογής.
- Το λογισμικό του πελάτη πρέπει να γνωρίζει πώς να επικοινωνήσει με την πύλη.
  - π.χ., πρέπει να καθορίσει την IP διεύθυνση ενός μεσολαβητή στο πρόγραμμα περιήγησης.διαδικτύου
- trade-off: βαθμός επικοινωνίας με εξωτερικά δίκτυα, επίπεδο ασφαλείας.
- Πολλές προστατευμένες με firewall υπηρεσίες δέχονται ακόμα επιθέσεις.

Συστήματα εντοπισμού παρεισφρήσεων

IDS: intrusion detection system

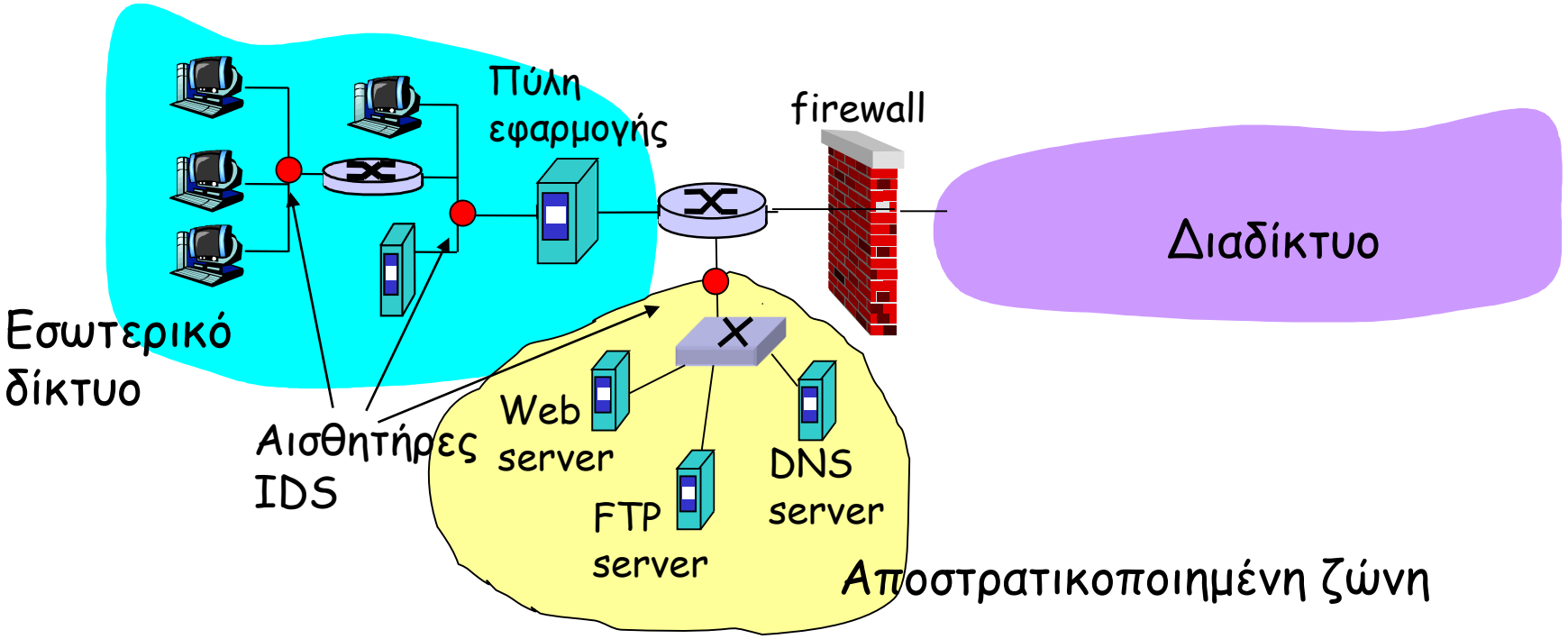
Έλεγχος πακέτων: Εξέταση περιεχομένων των πακέτων (π.χ., αντιστοίχηση σειράς χαρακτήρων εντός πακέτου με βάση δεδομένων για γνωστούς ιούς)

Έλεγχος συσχετισμών μεταξύ πολλαπλών πακέτων

- Σάρωση θυρών
- Χαρτογράφηση δικτύου
- Επιθέσεις άρνησης υπηρεσιών

Συστήματα εντοπισμού παρεισφρήσεων

Πολλαπλά IDSs: διαφορετικοί τύποι ελέγχου σε διαφορετικά σημεία



Ασφάλεια Δικτύων (περίληψη)

- Βασικές τεχνικές...
  - κρυπτογράφηση (συμμετρική και δημόσιου κλειδιού)
  - ακεραιότητα μηνύματος
  - αυθεντικοποίηση

.... Χρησιμοποιούνται σε διάφορα σενάρια

  - ασφάλεια στην ηλεκτρονική αλληλογραφία
  - ασφάλεια σε επίπεδο μεταφοράς-SSL
  - ασφάλεια σε επίπεδο δικτύου-IP sec
  - ασφάλεια σε επίπεδο ζεύξης-802.11

firewalls και IDS

Τέλος Ενότητας

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Άδεια Χρήσης

Σημείωμα Αναφοράς

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Μαθήματα στο Πανεπιστήμιο Αθηνών**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.