ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΚΡΥΠΤΟΓΡΑΦΙΑ

1η Διάλεξη

Κωνσταντίνου Ελισάβετ

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Άδειες Χρήσης

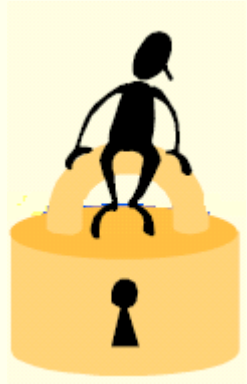
- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αιγαίου**» 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.

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Κρυπτογραφία

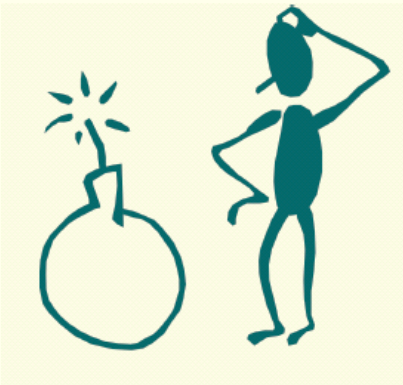


Κωνσταντίνου Ελισάβετ
ekonstantinou@aegean.gr

http://www.icsd.aegean.gr/ekonstantinou

Τι είναι Κρυπτογραφία;

- Επιστήμη που μελετά τρόπους κωδικοποίησης μηνυμάτων.
- Με άλλα λόγια, είναι η μελέτη των ΜΑΘΗΜΑΤΙΚΩΝ ΤΕΧΝΙΚΩΝ που σχετίζονται με έννοιες της ασφάλειας πληροφοριακών συστημάτων όπως η εμπιστευτικότητα, η ακεραιότητα δεδομένων, η πιστοποίηση κτλ.



Τι είναι Θεωρία Αριθμών;

- Κλάδος των μαθηματικών που μελετά τους φυσικούς αριθμούς.
- Περιλαμβάνει για παράδειγμα: μελέτη πρώτων αριθμών, πρόβλημα παραγοντοποίησης ακεραίων, διοφαντικές εξισώσεις κτλ.

Ύλη Μαθήματος

- Εισαγωγικές έννοιες
- Modular αριθμητική, βασικά στοιχεία θεωρίας αριθμών
- Κρυπτογραφικοί αλγόριθμοι δημόσιου κλειδιού (RSA, Rabin, ElGamal)
- Κρυπτογραφικοί αλγόριθμοι τμήματος (Block ciphers)
- Κρυπτογραφικοί αλγόριθμοι ροής (Stream ciphers)
- Ψηφιακές υπογραφές

Βιβλία

Μ. Burmester, Σ. Γκρίτζαλης, Σ. Κάτσικας, Β. Χρυσικόπουλος, Σύγχρονη Κρυπτογραφία: Θεωρία και Εφαρμογές, Εκδόσεις Παπασωτηρίου.

Προτεινόμενο Βιβλίο

Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 2001.

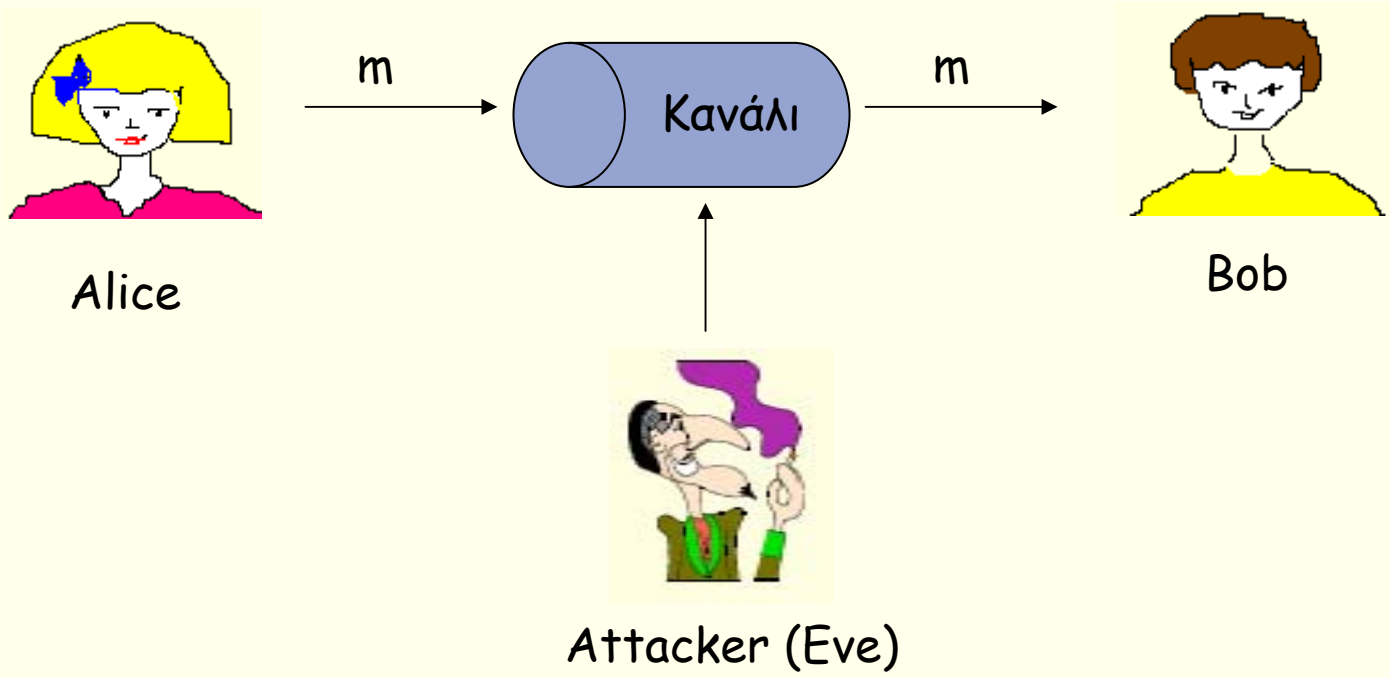
Όλα τα κεφάλαια διαθέσιμα στο:

http://www.cacr.math.uwaterloo.ca/hac

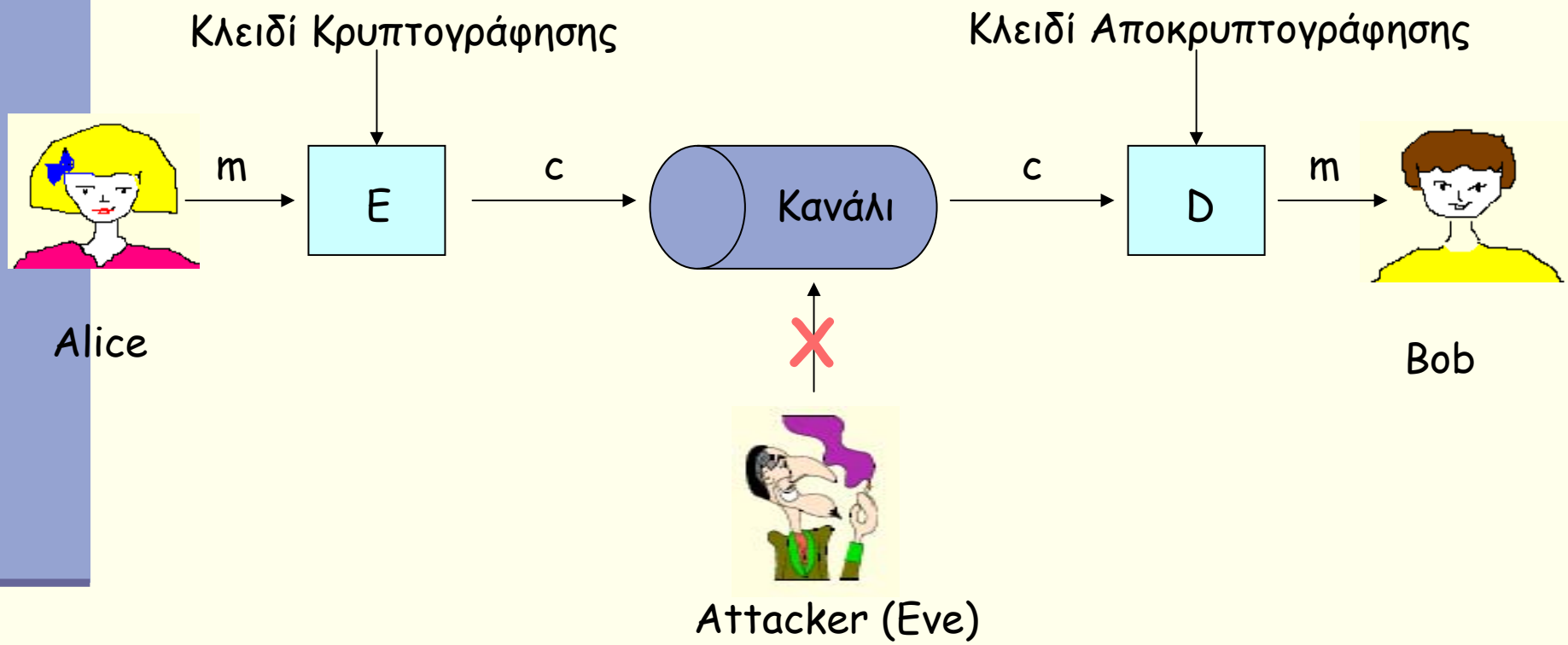
Βαθμολογία Μαθήματος

1) Προγραμματιστική άσκηση σε C (40%).
2) Ασκήσεις (κυρίως) σε προβλήματα θεωρίας αριθμών (30%).
3) Τελική εξέταση (30%).

Σκοπός της Κρυπτογραφίας



Λύση



Kerchoff's principle: Η ασφάλεια ενός κρυπτογραφικού συστήματος πρέπει να βασίζεται στην μυστικότητα του κλειδιού αποκρυπτογράφησης. Υποθέτουμε ότι όλοι οι αλγόριθμοι που χρησιμοποιούνται στο σύστημα είναι γνωστοί.

Λίγη ιστορία...

- 4000 π.Χ. Αρχαία Αίγυπτος
- Αλγόριθμος του Καίσαρα
- Β' Παγκόσμιος Πόλεμος, Enigma, Purple Machine
- Λαθρεμπόριο και Ποτοαπαγόρευση
- Σύγχρονη Εποχή

Λίγη ιστορία...

Polybius Square

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i/j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

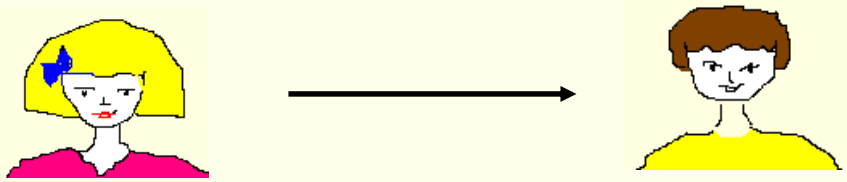
Σκυτάλη (Σπάρτη)

Βασικές Ιδιότητες

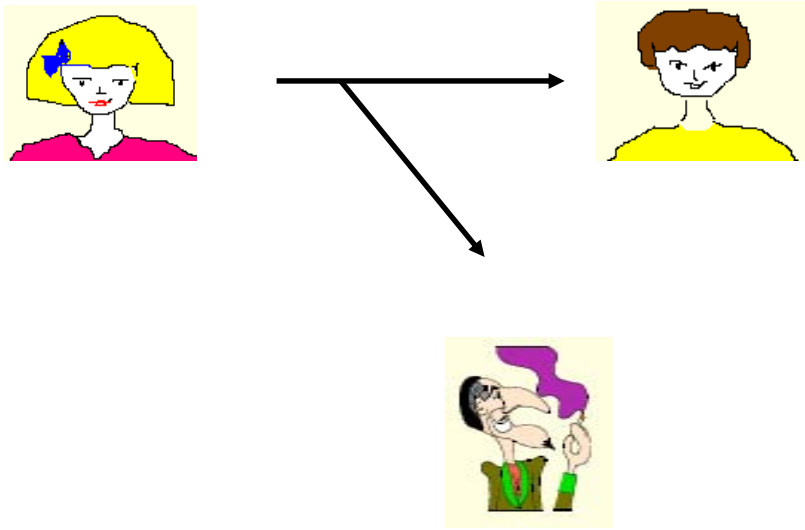
- Εμπιστευτικότητα (Confidentiality or Privacy)
- Πιστοποίηση (Authentication)
  - Πιστοποίηση Οντοτήτων (Entity Auth.)
  - Πιστοποίηση Δεδομένων (Data Auth.)
- Ακεραιότητα (Integrity)
- Μη-αποποίηση (Non-repudiation)
- Διαθεσιμότητα (Availability)

Εμπιστευτικότητα

- Προστασία της μεταδιδόμενης πληροφορίας



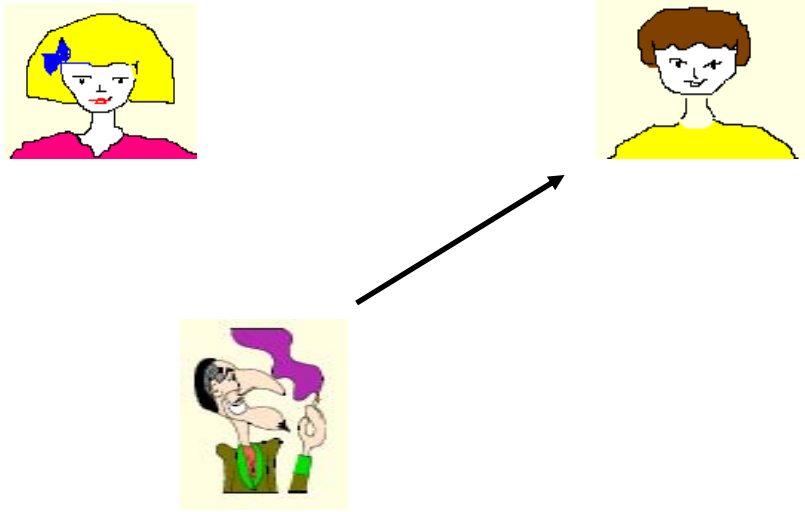
- Υποκλοπή (Interception)



Πιστοποίηση

- Βεβαιότητα ότι το μήνυμα προέρχεται από τη σωστή πηγή.
- Προστασία από πιθανές μεταμφιέσεις τρίτων.
- Πιστοποίηση οντοτήτων και δεδομένων.

- Πλαστογραφία (Fabrication)

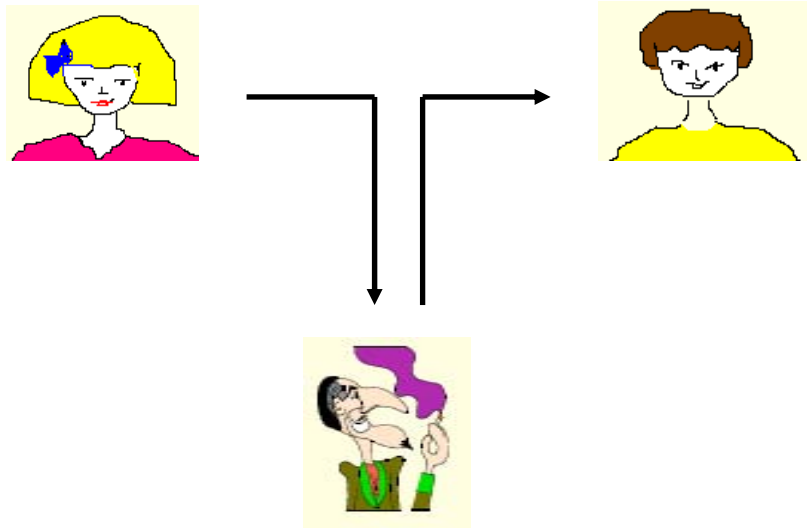


Ακεραιότητα

- Τα μηνύματα παραλαμβάνονται ακριβώς στη μορφή που στέλνονται.

- Σχετίζεται και με περιπτώσεις διαγραφής(deletion), καθυστέρησης στην παραλαβή μηνυμάτων (delay), επανεκπομπής (replay) κ.τ.λ.

- Μετατροπή (Modification)



Μη-αποποίηση

- Αποτρέπει τους χρήστες να αρνηθούν ότι έστειλαν ή έλαβαν κάποιο μήνυμα στο παρελθόν.

- Αποποίηση (Repudiation)

- Η Alice μπορεί να στέλνει πληροφορίες ή κλειδιά και μετά να ισχυριστεί ότι κάποιος τις τα έκλεψε.

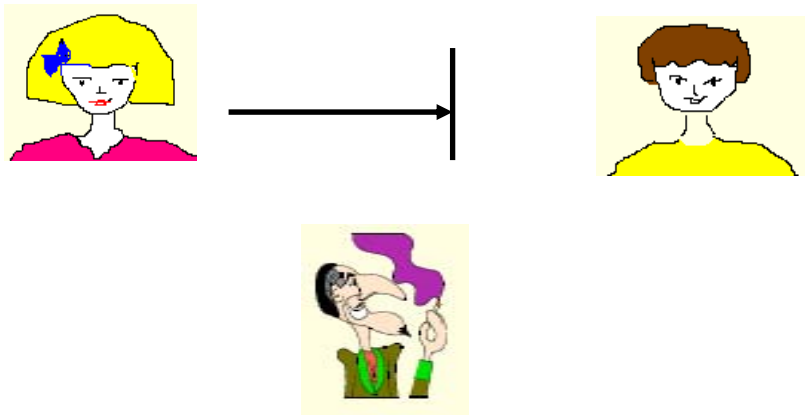
- Μπορεί να κάνει παραγγελία ενός προϊόντος μέσω Internet και μετά να αρνηθεί ότι το παρήγγειλε.

?

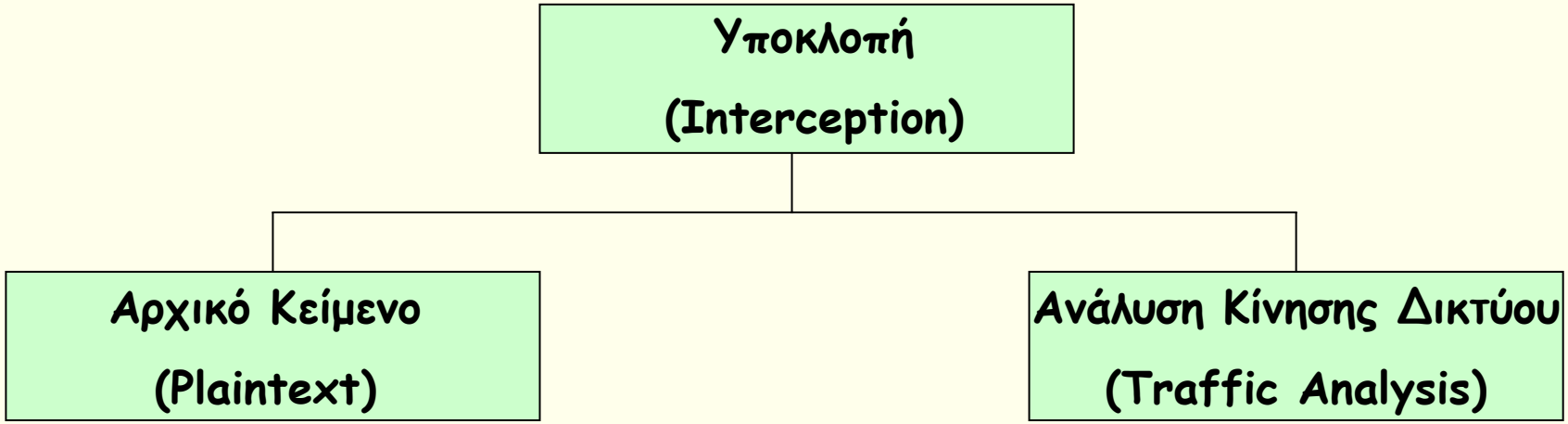
Διαθεσιμότητα

- Η πληροφορία που στέλνεται πρέπει να είναι διαθέσιμη στον δέκτη σε κάθε περίπτωση.

- Διακοπή (Interruption) Επικοινωνίας
- Άρνηση Εξυπηρέτησης (Denial of Service), π.χ. προσθήκη θορύβου στην επικοινωνία

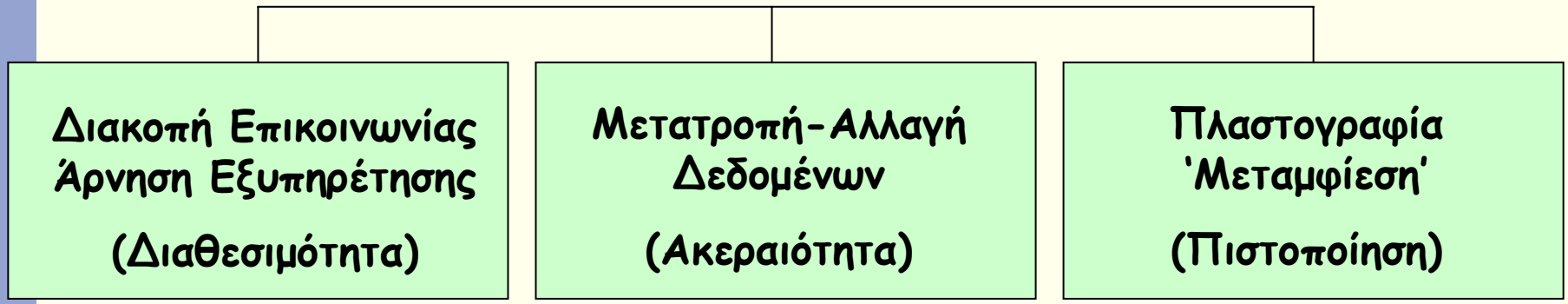


Παθητικές Επιθέσεις



- Ο επιτιθέμενος απλά παρακολουθεί το κανάλι επικοινωνίας (απειλή ως προς την εμπιστευτικότητα)
- Δύσκολο να ανιχνευτούν αυτές οι επιθέσεις -> εύκολο όμως να αποτραπούν

Ενεργές Επιθέσεις



- Περιλαμβάνουν ενεργή συμμετοχή ενός κακόβουλου, τρίτου μέλους σε μια επικοινωνία μεταξύ δύο χρηστών (αλλαγή δεδομένων, διακοπή επικοινωνίας, εισαγωγή νέων μηνυμάτων κ.τ.λ.)
- Δύσκολο να αποτραπούν -> μπορούν όμως να ανιχνευθούν
- Επιθέσεις επανεκπομπής (replay attacks): υποκλέπτονται δεδομένα (παθητική επίθεση) και στη συνέχεια ξαναστέλνονται (ενεργή επίθεση) με σκοπό την κατάρρευση ενός πρωτοκόλλου ή την ανάκτηση πληροφορίας

Κρυπταναλυτικές Τεχνικές

1) Ciphertext-only attack
2) Known-plaintext attack
3) Chosen-plaintext attack
4) Adaptive chosen-plaintext attack
5) Chosen-ciphertext attack
6) Adaptive chosen-ciphertext attack

- **Πρακτική Κρυπτανάλυση**
  - **Κλοπή**
  - **Δωροδοκία**
  - **Εκβιασμός**
  - **Βασανιστήρια**
  - **Ύπνωση**

Κρυπτογραφία + Κρυπτανάλυση = Κρυπτολογία (Cryptology)

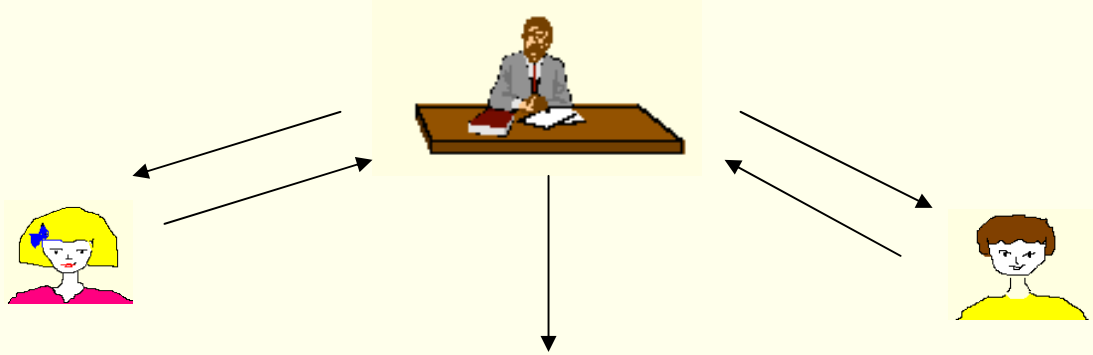
Άλλες Απειλές…

- Man-in-the-middle attack (π.χ. στην ανταλλαγή κλειδιών)

- Επιθέσεις εναντίον υλικού (hardware): από τον χρόνο εκτέλεσης μιας λειτουργίας, την κατανάλωση ενέργειας κ.τ.λ. μιας μικρής συσκευής μπορεί να εξαχθεί πληροφορία για τα bits του κλειδιού

- Κβαντικοί Υπολογιστές

Τι είναι ο TTP?



Trusted Third Party (TTP)

Επιλύει διαφωνίες μεταξύ των χρηστών ή διευκολύνει την επικοινωνία τους (ανταλλαγή κλειδιών, ψηφιακές υπογραφές)

Άνευ όρων έμπιστο (unconditionally trusted TTP): μπορεί να γνωρίζει και τα μυστικά κλειδιά των χρηστών

Λειτουργικά έμπιστο (functionally trusted TTP): επιλύει διαφωνίες, αλλά δεν γνωρίζει μυστικά κλειδιά

Κρυπτογράφηση

Αρχικό κείμενο (m)

Hello world

Αλγόριθμος Κρυπτογράφησης E

c = E(m)

Κρυπτογραφημένο κείμενο (c)

jkies9l[io

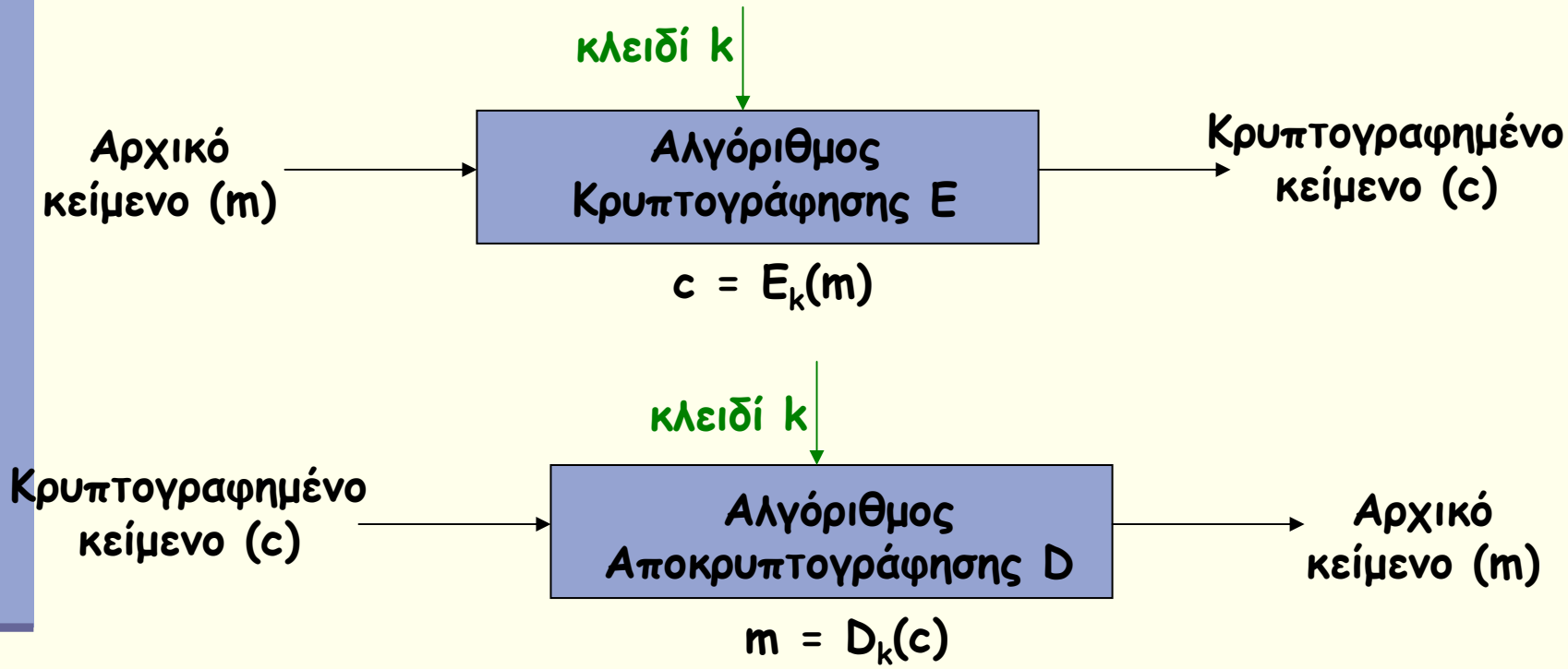
Κρυπτογραφημένο κείμενο (c)

Αλγόριθμος Αποκρυπτογράφησης D

m = D(c)

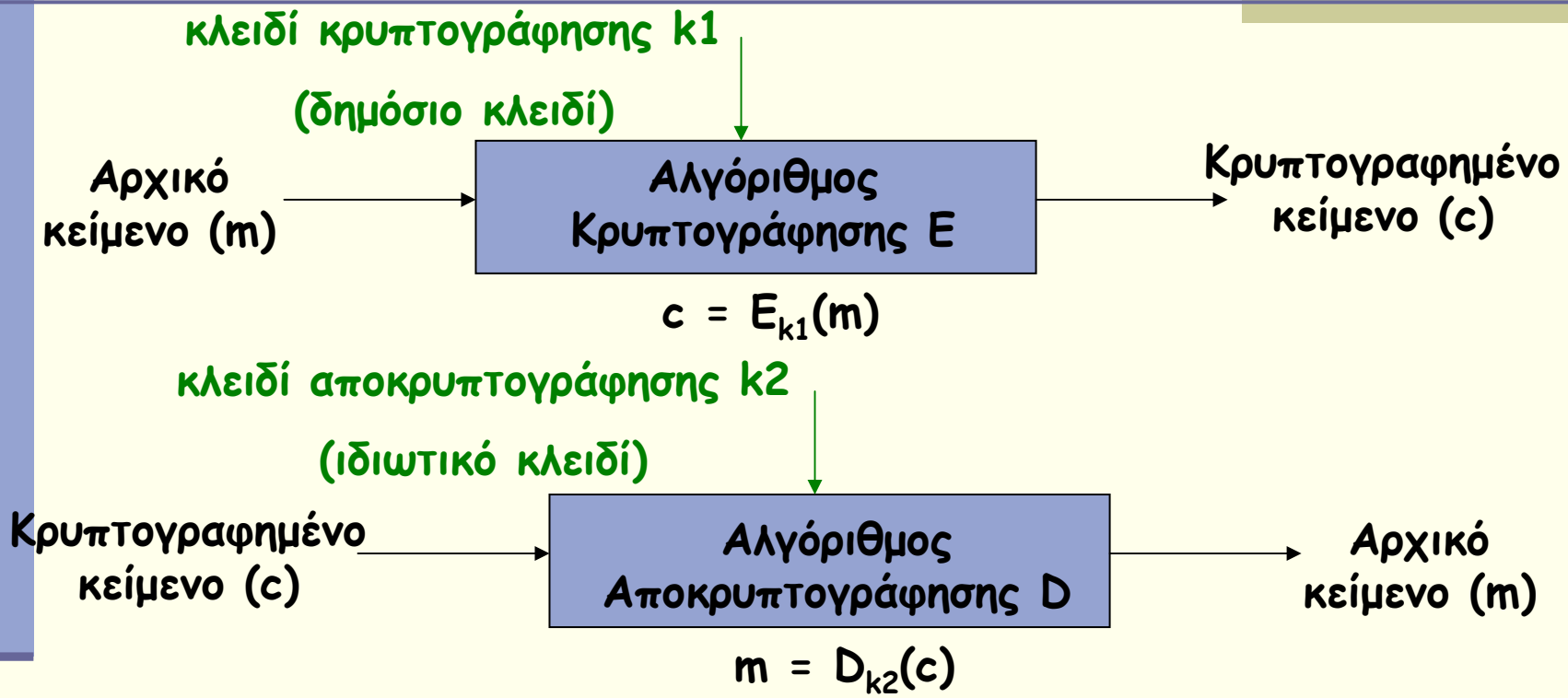
Αρχικό κείμενο (m)

Συμμετρικά Κρυπτοσυστήματα



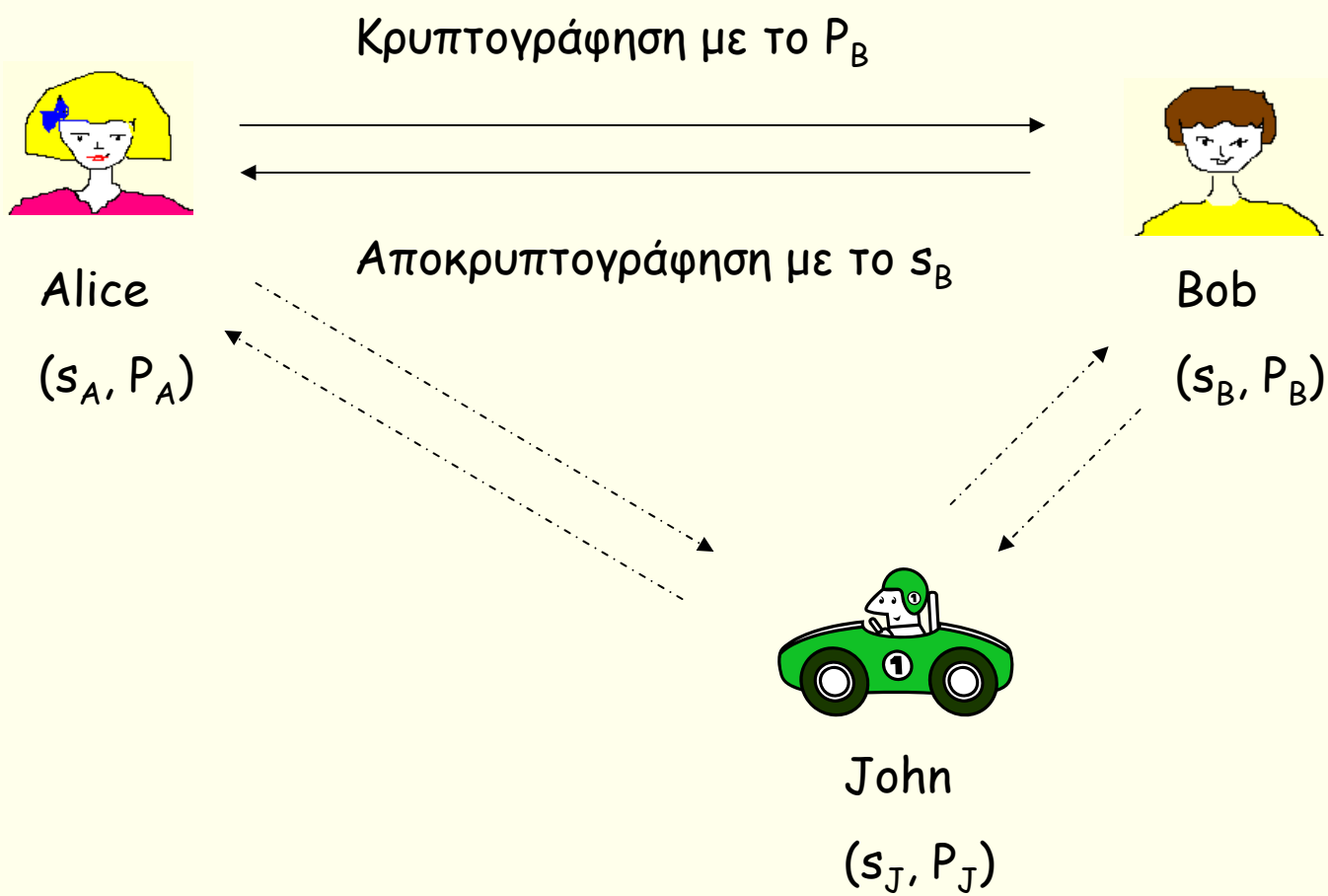
Το κλειδί αποκρυπτογράφησης μπορεί να βρεθεί εύκολα από το αντίστοιχο κλειδί κρυπτογράφησης. Στις περισσότερες περιπτώσεις είναι ακριβώς τα ίδια.

Ασύμμετρα Κρυπτοσυστήματα



Το κλειδί αποκρυπτογράφησης βρίσκεται δύσκολα από το αντίστοιχο κλειδί κρυπτογράφησης. Η δυσκολία βασίζεται σε κάποιο μαθηματικό πρόβλημα.

Ασύμμετρα Κρυπτοσυστήματα



Μια απλή επίθεση...

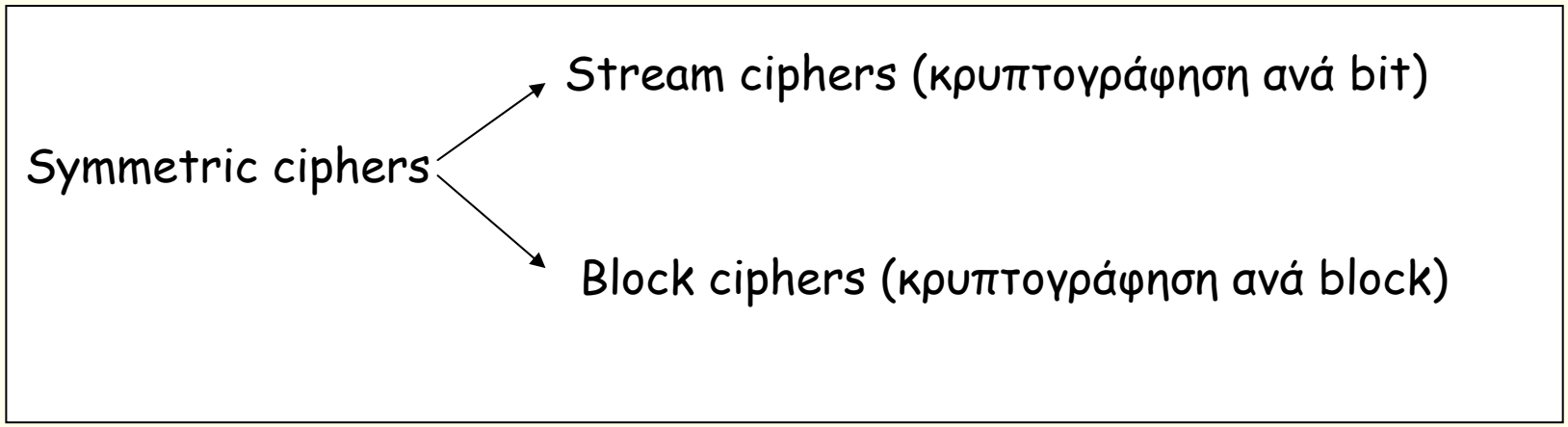
- **Man-in-the-middle attack**

Ανακτά το αρχικό μήνυμα m

Αναγκαία η πιστοποίηση οντοτήτων!

Συμμετρικά Κρυπτοσυστήματα

- Τα συμμετρικά συστήματα προϋπήρχαν των συστημάτων δημόσιου κλειδιού (τα οποία εμφανίστηκαν το 1976 με την εργασία των Diffie-Hellman).
- Βασίζονται στη μυστικότητα του κλειδιού αποκρυπτογράφησης-κρυπτογράφησης, οπότε θα πρέπει να υπάρχει ένας ασφαλής δίαυλος επικοινωνίας μεταξύ των δύο χρηστών για την εγκατάσταση του κλειδιού.
- Κάτι τέτοιο δεν χρειάζεται στα συστήματα δημόσιου κλειδιού.



One-time Pad

- Το αρχικό κείμενο (plaintext) συνδυάζεται με ένα τυχαίο κλειδί (ή 'pad') που έχει μήκος όσο και το αρχικό κείμενο.
- Και τα δύο μέλη της επικοινωνίας πρέπει να διαθέτουν το ίδιο κλειδί.
- Το κλειδί θα πρέπει να καταστρέφεται μετά την χρήση του και να μην ξαναχρησιμοποιείται.
- Προσφέρει τέλεια μυστικότητα (perfect secrecy).
- Μειονεκτήματα?

Παραδείγματα:

K: 01011100101….

P: 11011101100….

C: 10000001001….

K: 321424….
P: crypto….
C: ftzsvt….

Συμμετρικά Κρυπτοσυστήματα

Πλεονεκτήματα:

1) Πολύ γρήγορη κρυπτογράφηση.
2) Μέγεθος κλειδιών μικρό (συσκευές περιορισμένων πόρων).
3) Δημιουργία γεννητριών τυχαίων αριθμών και συναρτήσεων κατακερματισμού.
4) Συνδυασμοί τους παράγουν ισχυρότερους αλγορίθμους.
5) Είναι αρκετά δοκιμασμένα στην πράξη.

Μειονεκτήματα:

1) Απαιτείται ασφαλής δίαυλος επικοινωνίας για την ανταλλαγή κλειδιών.
2) Πολλά κλειδιά (n(n-1)/2).
3) Ύπαρξη άνευ όρων έμπιστου TTP (διαχείριση κλειδιών).
4) Συχνή αλλαγή κλειδιών.
5) Ψηφιακές υπογραφές απαιτούν μεγάλα κλειδιά ή την ύπαρξη TTP.

Ασύμμετρα Κρυπτοσυστήματα

Πλεονεκτήματα:

1) Δεν απαιτείται ασφαλής δίαυλος επικοινωνίας.
2) Τα κλειδιά δεν αλλάζουν συχνά.
3) Αλγόριθμοι ψηφιακών υπογραφών πολύ πιο αποδοτικοί.
4) Πλήθος κλειδιών σε δίκτυο n χρηστών μικρός (2n).
5) Για τη διαχείριση των κλειδιών απαιτείται ένα λειτουργικά έμπιστο TTP.

Μειονεκτήματα:

1) Ταχύτητα κρυπτογράφησης – αποκρυπτογράφησης πιο αργή.
2) Κλειδιά σχετικά μεγάλα.
3) Δεν έχουν δοκιμαστεί στην πράξη όσο τα συμμετρικά (?).
4) Βασίζονται σε προβλήματα Θεωρίας αριθμών, των οποίων η δυσκολία δεν έχει αποδειχθεί θεωρητικά.

Κρυπτογραφική Ισχύς

- Άνευ όρων ασφαλές (Unconditionally secure)

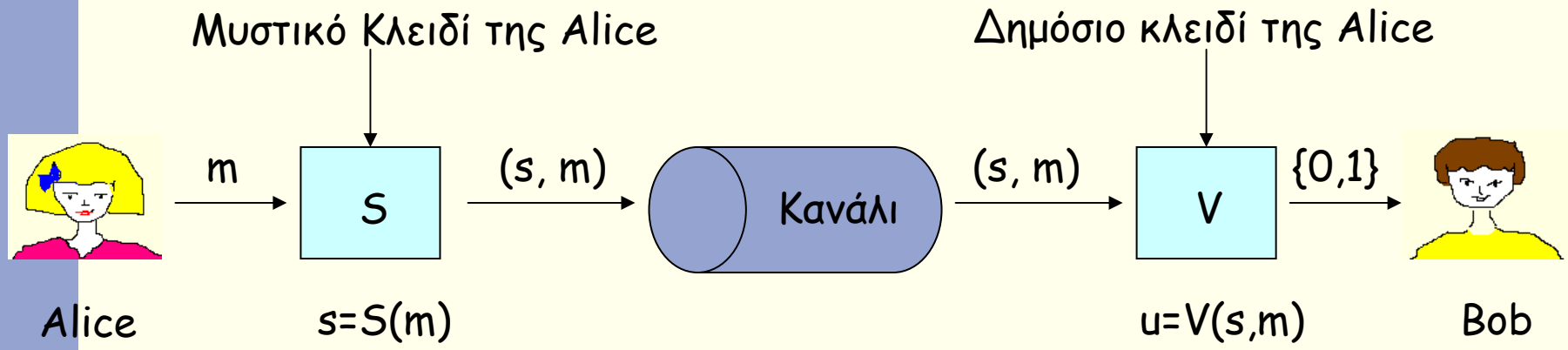
  Ανεξάρτητα από το πλήθος των κρυπτοκειμένων που γνωρίζουμε, δεν μπορούμε να εξάγουμε πληροφορία για το αρχικό κείμενο. Μόνο τα ONE-TIME PADS συστήματα είναι άνευ όρων ασφαλή. Ιδιότητα γνωστή και ως perfect secrecy.
- Αποδεδειγμένα ασφαλές (Provably secure)

  Το κρυπτογραφικό σύστημα είναι τόσο δύσκολο να σπάσει όσο και ο υπολογισμός της λύσης ενός δύσκολου αριθμο-θεωρητικού προβλήματος, π.χ. παραγοντοποίηση μεγάλων ακεραίων.
- Πρακτικά ασφαλές (Computationally infeasible - Practically secure)

  Πεποίθηση ότι το κρυπτοσύστημα δεν μπορεί να σπάσει με συγκεκριμένη υπολογιστική ισχύ.

Ψηφιακές Υπογραφές

- Συνδέουν μια οντότητα με μια πληροφορία.
- Άρρηκτα συνδεδεμένες με τις έννοιες της πιστοποίησης και της μη-αποποίησης.



1) Μια ψηφιακή υπογραφή είναι έγκυρη μόνο αν ο αλγόριθμος επαλήθευσης επιστρέψει την τιμή 1.

2) Θα πρέπει να είναι υπολογιστικά αδύνατο για οποιονδήποτε χρήστη εκτός του υπογράφοντος να δημιουργήσει μια έγκυρη υπογραφή.

Συναρτήσεις Κατακερματισμού

Ορισμός: Μια συνάρτηση $h: \{0,1\}^* \rightarrow \{0,1\}^k$ που μπορεί να υπολογιστεί αποδοτικά, καλείται συνάρτηση κατακερματισμού (hash function). Συνήθως k=128 ή k=160.

Χρησιμοποιούνται σε σχήματα ψηφιακών υπογραφών και για να διασφαλίσουμε την ακεραιότητα των δεδομένων.

Για χρήση σε κρυπτογραφικές εφαρμογές Θα πρέπει:

1) να είναι υπολογιστικά αδύνατο να βρεις την είσοδο x της συνάρτησης κατακερματισμού αν είναι γνωστή η έξοδος y=h(x).

2) να είναι υπολογιστικά αδύνατη η εύρεση δύο τιμών x_1 και x_2 τέτοιων ώστε $h(x_1) = h(x_2)$

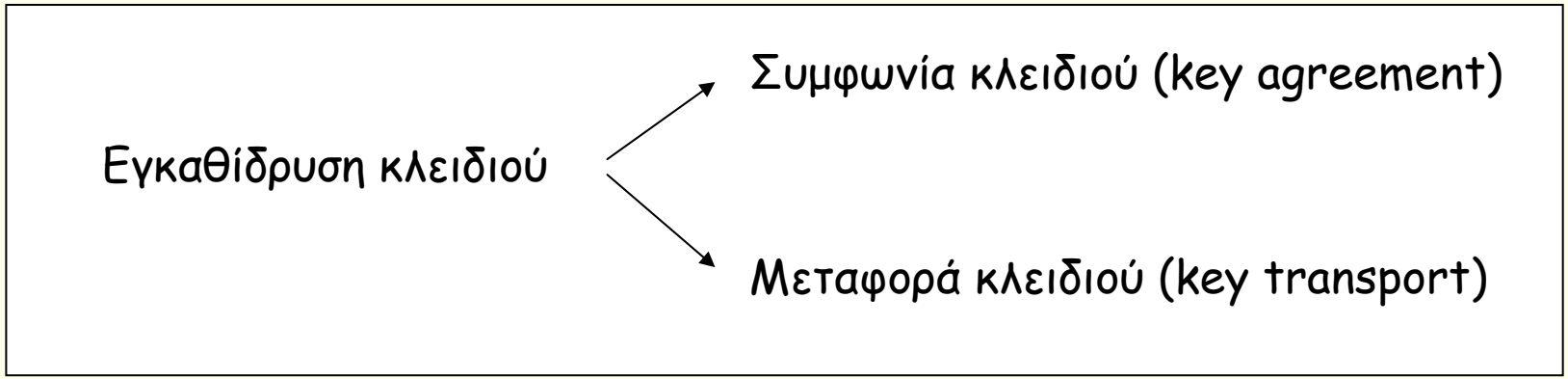
Ψευδοτυχαίες Γεννήτριες

- Τυχαίοι αριθμοί χρειάζονται σε όλα τα κρυπτογραφικά πρωτόκολλα…
- Γεννήτριες πραγματικά τυχαίων (truly random) αριθμών προέρχονται από φυσικές πηγές -> δαπανηρές ή αργές.
- Με κάποιο ντετερμινιστικό τρόπο (deterministic) κατασκευάζονται ψευδοτυχαίες γεννήτριες (pseudorandom). Θα πρέπει να περνάνε όλους τους στατιστικούς ελέγχους.

Διαχείριση Κλειδιών

Ορισμός: Εγκαθίδρυση κλειδιού (key establishment) είναι η διαδικασία κατά την οποία ένα μυστικό κλειδί διαμοιράζεται σε δύο ή περισσότερους χρήστες.

Ορισμός: Διαχείριση κλειδιού (key management) είναι το σύνολο των μηχανισμών που υποστηρίζουν την εγκατάσταση, διατήρηση ή αντικατάσταση των κλειδιών.



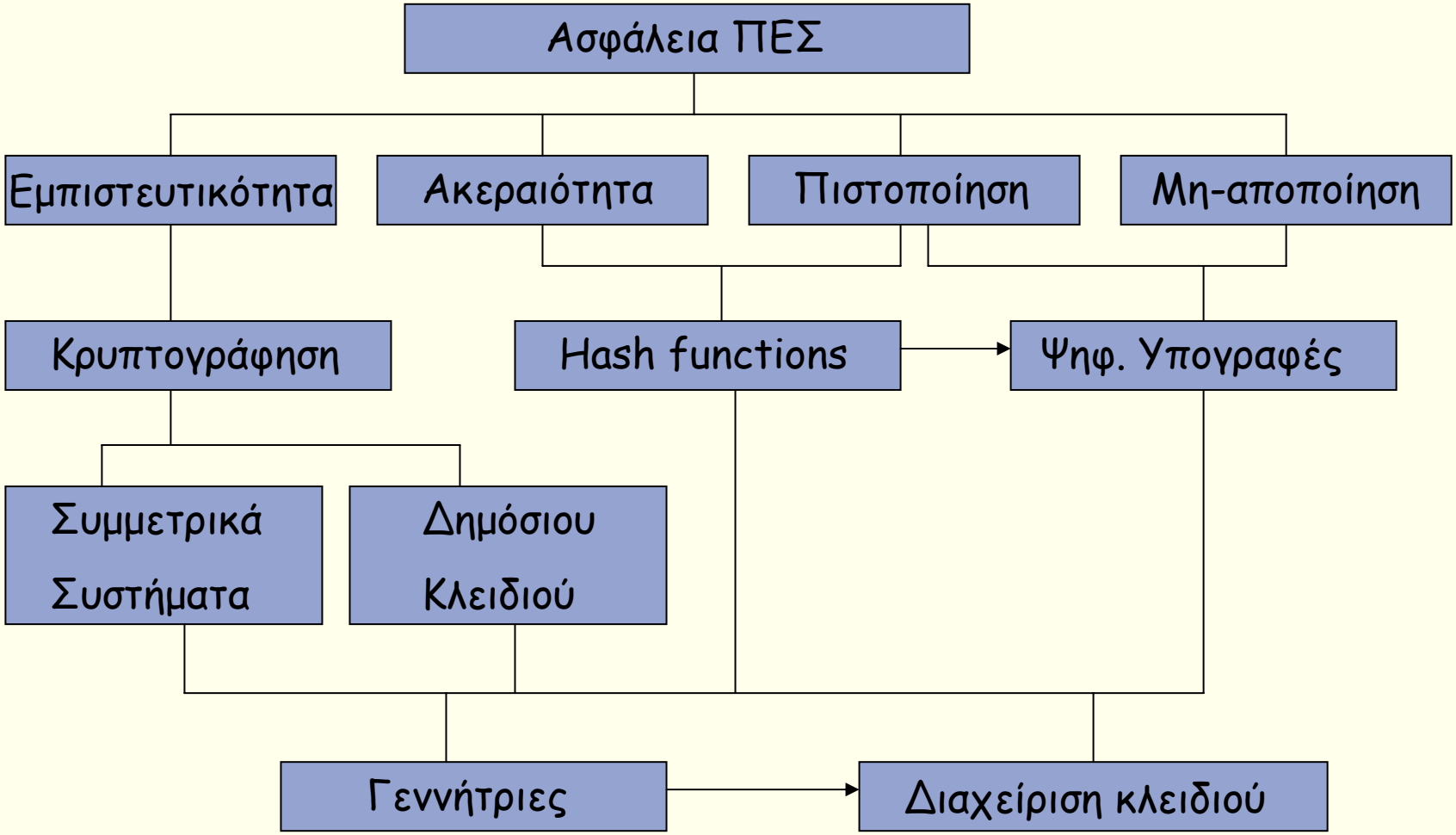
Στεγανογραφία = Κρυπτογραφία?

- Η πληροφορία 'κρύβεται' μέσα σε κείμενα ή εικόνες. Για παράδειγμα, μπορεί να είναι το λιγότερο σημαντικό bit των pixels μιας εικόνας.
- Αν αποκαλυφθεί ο συγκεκριμένος μηχανισμός, αποκαλύπτεται και η πληροφορία.
- Βασίζει την ασφάλεια του στην άγνοια ύπαρξης μιας πληροφορίας σε μια εικόνα ή κείμενο που φαίνεται «αθώο».

Σκοπός και των δύο είναι η αποστολή μιας πληροφορίας με μυστικό τρόπο. Ξεκάθαρα όμως είναι δύο τελείως διαφορετικές έννοιες.

Στεγανογραφία ≠ Κρυπτογραφία

Συνοψίζοντας…



Ασκήσεις για την επόμενη εβδομάδα

- Γράψτε 1-2 σελίδες για τις σημαντικότερες εφαρμογές της κρυπτογραφίας στα σύγχρονα πληροφοριακά/επικοινωνιακά συστήματα.
- Παρουσίαση στην τάξη των ευρημάτων σας!

Καλή Αρχή!