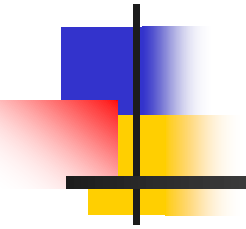
Πανεπιστήμιο Αθηνών
Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Εργαστήριο Ηλεκτρονικής Διακυβέρνησης

Πρόγραμμα Μεταπτυχιακών Σπουδών
Ασφάλεια Πληροφοριακών
Συστημάτων



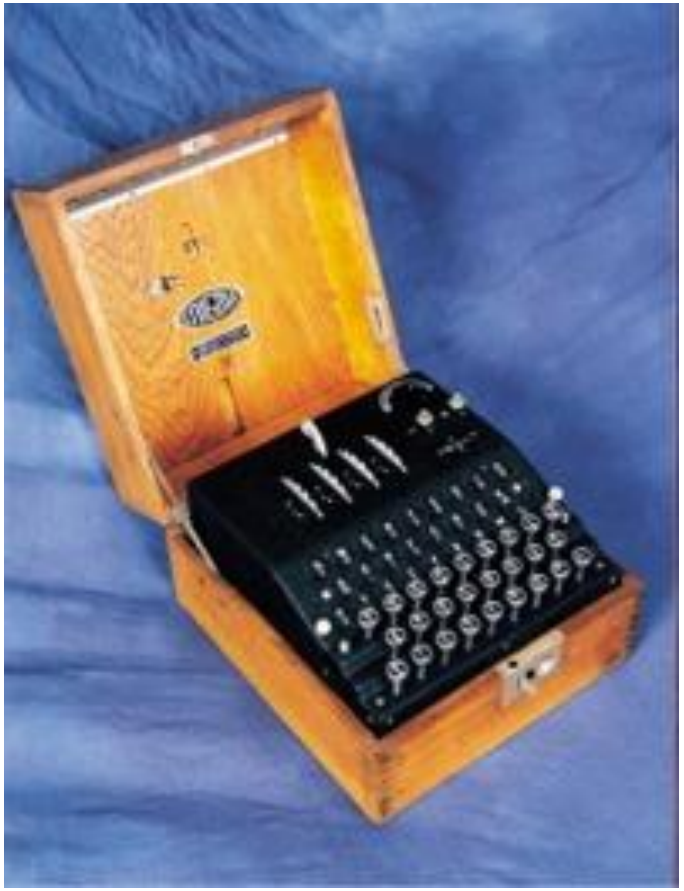
# Κρυπτογραφία

Δρ. Κωνσταντίνος Παπαπαναγιώτου
conpap@di.uoa.gr

# Ιστορία


- 1586 - Queen Mary of the Scots
  - Συνωμοτούσε εναντίον της βασίλισσας Ελισάβετ
  - Κρυπτογραφούσε τα μηνύματά της με απλή αντικατάσταση
  - Ο Tomas Phelippes κατάφερε να τα αποκωδικοποιήσει

# Β’ Παγκόσμιος Πόλεμος

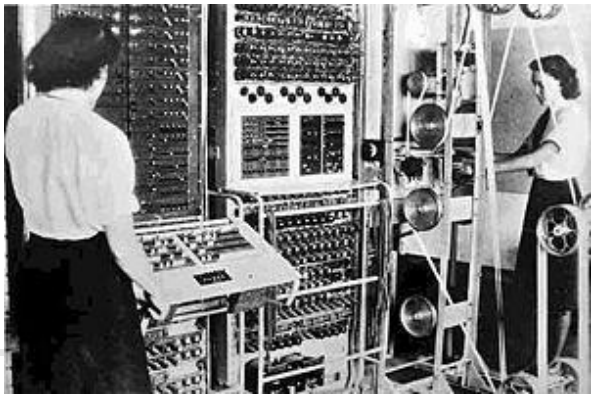


*… "Κάποιος ρώτησε γιατί, αν υποθέσουμε ότι αποκωδικοποιήσαμε το Enigma, δεν κερδίσαμε νωρίτερα τον πόλεμο. Και κάποιος άλλος ρώτησε αν θα μπορούσαμε να τον είχαμε κερδίσει ποτέ αν πρώτα δεν το αποκωδικοποιήσαμε" ….*

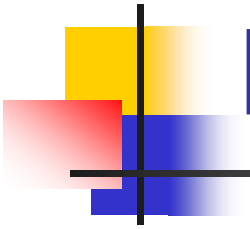
Enigma

- κώδικας αντικατάστασης
- ασφάλεια μέσω rotor machine
- http://www.bletchleypark.org.uk/content/enigmasim.rhtm

# Σταθμοί



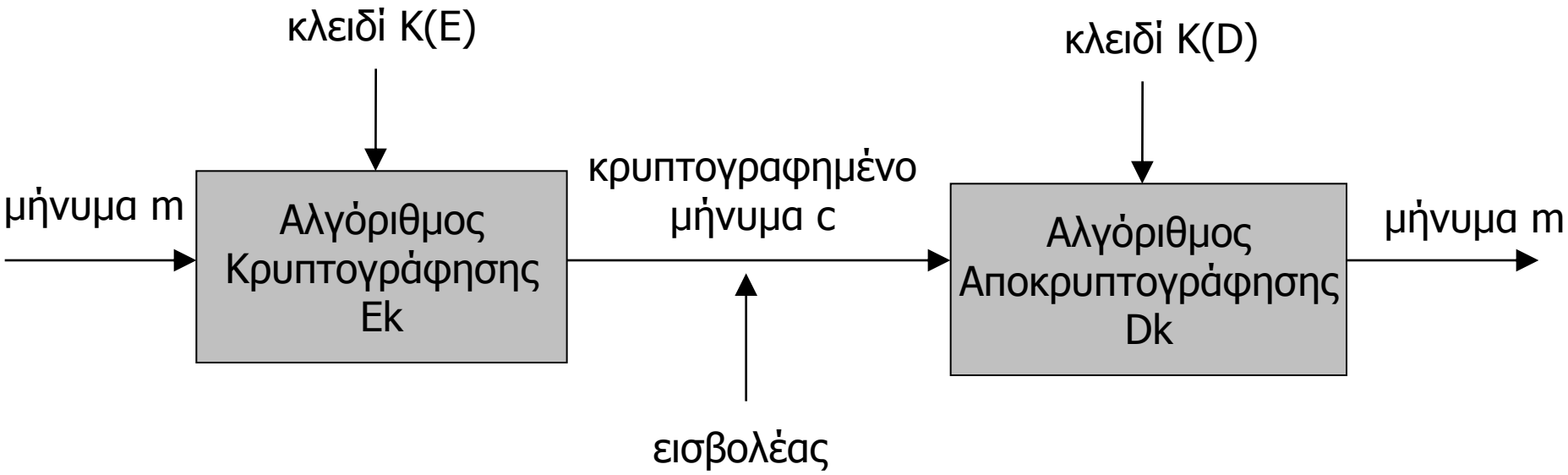
- 1883: Auguste Kerckhoffs, "La Cryptographie militaire"
- 1943: Colossus
- 1949: Claude Shannon, "Communication Theory of Secrecy Systems"
- 1964: David Kahn, "The Codebreakers"
- 1976: DES – Diffie-Hellman, "New Directions in Cryptography"
- 1977: Rivest-Shamir-Adleman, RSA
- 1985: Hugo Cornwall, "Hacker's Handbook": οδηγίες και διαγράμματα για Phreaking
- 1988: Δημιουργία CERT (Computer Emergency Response Team): http://www.cert.org/
- 1989: Clifford Stoll, "Cuckoo's Egg": πρώτη υπόθεση στρατιωτικής κατασκοπίας
- 1997 – Phil Zimmermann, PGP
- 2001 - AES



# Κρυπτογραφία

- Η επιστήμη και η μελέτη της τήρησης μυστικών
- Κρυπτογράφηση: μέθοδος μετασχηματισμού απλού-μη κρυπτογραφημένου κειμένου (plaintext) σε κρυπτογραφημένο κείμενο (cipher text)
- Ο μετασχηματισμός ορίζεται μέσω ενός *κλειδιού*

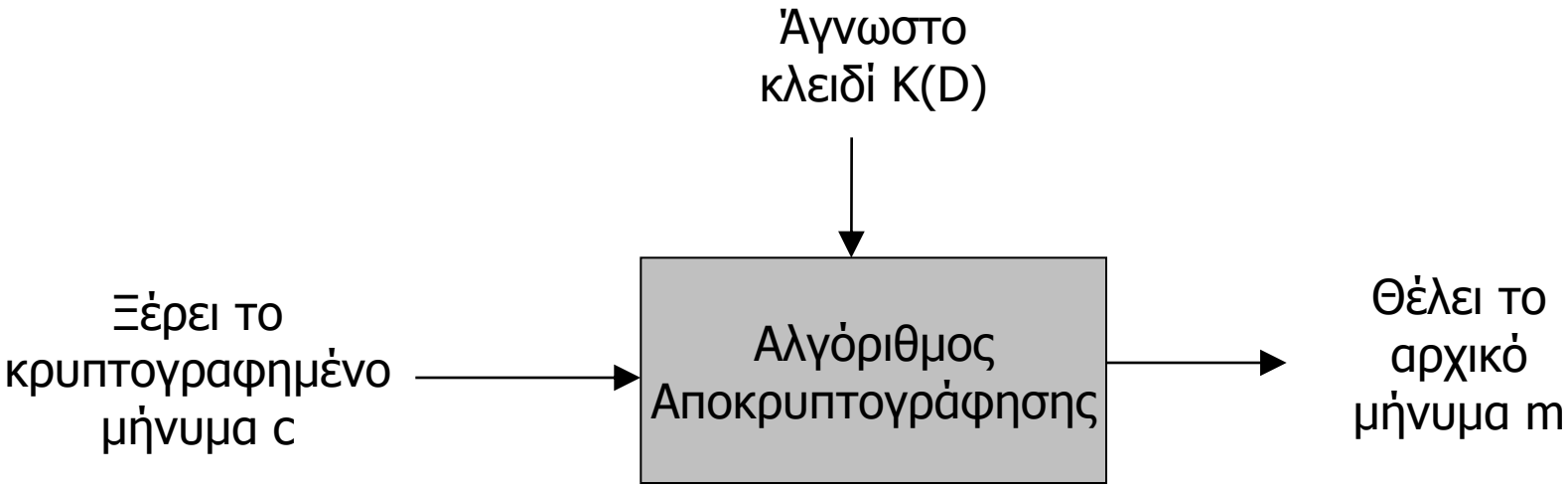
# Σύστημα Κρυπτογραφίας

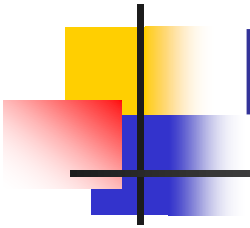


# Στόχοι Κρυπτογραφίας

- Εμπιστευτικότητα
  - Πρέπει να είναι ανέφικτος ο υπολογισμός του m από ένα c
  - Πρέπει να είναι ανέφικτο να υπολογιστεί το Dk από το c, ακόμη και αν είναι γνωστό το m
- Ακεραιότητα
- Αυθεντικότητα
  - Πρέπει να είναι υπολογιστικά ανέφικτο να προσδιοριστεί το Ek από το c, ακόμη και αν είναι γνωστό το m
  - Πρέπει να είναι υπολογιστικά ανέφικτο να βρεθεί ένα c', τέτοιο ώστε το Dk(c') να είναι το ίδιο μη κρυπτογραφημένο μήνυμα
- Μη αποποίηση
- Μελλοντικά: Μυστικότητα, Ανωνυμία

# Η άποψη του εισβολέα

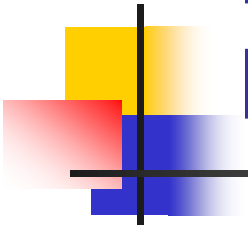




# Κρυπτανάλυση

- Κρυπτανάλυση: καταστρέφω τους στόχους της κρυπτογραφίας
  - Παραβίαση εχεμύθειας: διαβάζω το κείμενο χωρίς να έχω εξουσιοδότηση
  - Παραβίαση αυθεντικότητας: δημιουργώ μήνυμα που φαίνεται να προέρχεται από άλλον αποστολέα
- Μέθοδοι:
  - Έλεγχος όλων των πιθανών κλειδιών
  - Στατιστική ανάλυση
  - Επίθεση στον αλγόριθμο
  - Κακή διαχείριση κλειδιών
  - κλπ

# Κατηγορίες Συστημάτων Κρυπτογραφίας



- Συμμετρική Κρυπτογραφία
  - Ένα κλειδί
  - k(D) υπολογίζεται εύκολα από το k(E)
- Ασύμμετρη Κρυπτογραφία
  - Δύο διαφορετικά κλειδιά
  - Υπολογιστικά αδύνατο να υπολογιστεί το k(D) από το k(E)

# Κρυπτογράφηση με Αντικατάσταση

- Κάθε χαρακτήρας του μη κρυπτογραφημένου κειμένου αντικαθίσταται από έναν διαφορετικό χαρακτήρα στο κρυπτογραφημένο κείμενο
  - Απλή αντικατάσταση
  - Πολυαλφαβητική αντικατάσταση
  - Αντικατάσταση τρέχοντος κλειδιού
  - Μέθοδος Vernam

# Απλή Αντικατάσταση

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

ΑΣΠΡΗ ΠΕΤΡΑ ΞΕΞΑΣΠΡΗ
ΔΘΒΧΩ ΒΥΝΧΔ ΜΥΜΔΘΒΧΩ

- Αλγόριθμος του Καίσαρα

ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ

CAT
FDW

- Ευάλωτοι σε Στατιστική ανάλυση

# Πολυαλφαβητική Αντικατάσταση

- Απαιτείται ένα κλειδί
- Χρησιμοποιούμε έναν δισδιάστατο πίνακα απεικόνισης, οι γραμμές του οποίου αντιστοιχούν σε χαρακτήρες του κλειδιού και οι στήλες σε χαρακτήρες του μηνύματος
- Αν $M_i$ είναι ο υπ' αριθμόν $i$ χαρακτήρας του μη κρυπτογραφημένου μηνύματος και $K_i$ ο υπ' αριθμόν $i$ χαρακτήρας του κλειδιού, ο υπ' αριθμόν $i$ χαρακτήρας του κρυπτογραφημένου μηνύματος είναι η καταχώρηση στη θέση ($K_i$, $M_i$) του πίνακα

# Πολυαλφαβητική Αντικατάσταση

- Παράδειγμα:

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

- Κλειδί κρυπτογράφησης: ΑΒΒΑ

  ΑΣΠΡΗ ΠΕΤΡΑ ΞΕΞΑΣΠΡΗ ← Plaintext

  ΑΒΒΑΑ ΒΒΑΑΒ ΒΑΑΒΒΑΑΒ ← Κλειδί

  ΔΒΧΧΩ ΧΔΝΧΗ ΙΘΜΗΒΒΧΚ ← Ciphertext

# Αντικατάσταση Τρέχοντος Κλειδιού

- Όμοια με την πολυαλφαβητική αντικατάσταση αλλά το κλειδί απλά δεν τελειώνει ποτέ
  - Κείμενο βιβλίου
  - τυχαία δεδομένα που δημιουργούνται αλγοριθμικά (π.χ. περιστροφικές μηχανές)
  - Προτιμάται η χρήση τυχαίων δεδομένων καθώς δεν είναι ευάλωτη σε στατιστικές αναλύσεις
- Χρησιμοποιήθηκε από τους Γερμανούς στον Β' Παγκόσμιο Πόλεμο, ο κώδικας έσπασε από την ομάδα του Alan Turing

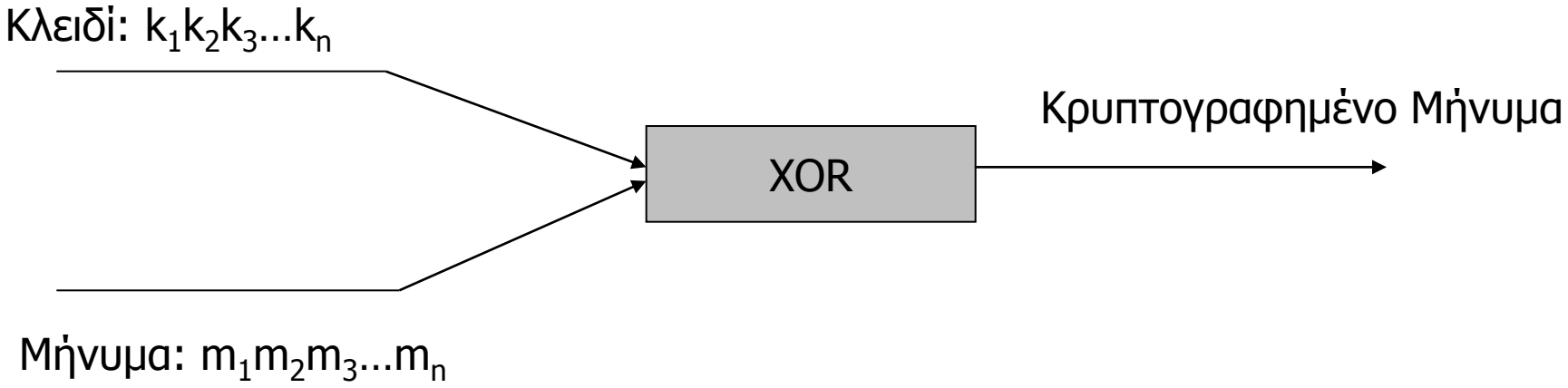
# Άριστο Σύστημα Κρυπτογράφησης

- Δύο Πιθανά Μηνύματα:

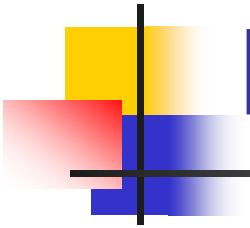
  ΠΟΥΛΑ ή ΑΓΟΡΑΣΕ

- 50% Πιθανότητα «Μαντέματος»
- Κακή πρακτική: Απλή Αντικατάσταση
- Καλύτερη δυνατή πρακτική:
  - Κλειδί k1  E(k1)(ΠΟΥΛΑ)=0  E(k1)(ΑΓΟΡΑΣΕ)=1
  - Κλειδί k2  E(k2)(ΠΟΥΛΑ)=1  E(k2)(ΑΓΟΡΑΣΕ)=0
- Λέμε ότι έχουμε ένα άριστο σύστημα, αν βλέποντας ένας εισβολέας το κρυπτογραφημένο μήνυμα δε μπορεί να εξάγει από αυτό **καμία** πληροφορία για το αρχικό μήνυμα.
- Ο εισβολέας εξαναγκάζεται να μαντέψει.

# Μέθοδος Vernam (One Time Pad)

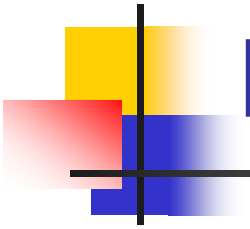



- Τα κλειδιά ανταλλάσσονται εκ των προτέρων εξωσυστημικά
- Το κλειδί χρησιμοποιείται μόνο μία φορά (ιδανικά είναι μια τυχαία ακολουθία)
- Το κλειδί έχει μήκος τουλάχιστον ίσο με το μήκος του μηνύματος



# Πρακτικά…

- Ένα σύστημα κρυπτογραφίας που είναι ασφαλές στη θεωρία, μπορεί να μην είναι ασφαλές στην πράξη
- Ένα σύστημα κρυπτογραφίας που μπορεί να μην είναι ασφαλές στη θεωρία, μπορεί να είναι ασφαλές στην πράξη
- Αυτό που μας ενδιαφέρει κυρίως είναι ο **χρόνος κάλυψης**, ο χρόνος για τον οποίο το μήνυμα πρέπει να μείνει κρυφό.
  - Ο χρόνος κάλυψης για ένα ημερήσιο password είναι 24 ώρες
  - Ο χρόνος κάλυψης για το password του taxisnet είναι πολλά χρόνια
- Τα συστήματα σχεδιάζονται έτσι, ώστε να απαιτείται περισσότερος χρόνος για να σπάσουν, από το χρόνο κάλυψης



# Κρυπτογράφηση με μεταθέσεις

- Βασική ιδέα: αλλαγή της θέσης bits ή bytes εντός του μηνύματος
  - Απλή μετάθεση
  - «Συρματόπλεγμα»
  - Μετάθεση κατά στήλες

# Απλή Μετάθεση

- Το μήνυμα *m* κατατμείται σε μπλοκ και κάθε μπλοκ αναδιατάσσεται βάσει κάποιου σχήματος
- Παράδειγμα
  - Κλειδί = (25413)

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| m | Μ | Υ | Σ | Τ | Ι | Κ | Ο | | Μ | Η | Ν | Υ | Μ | Α | ∅ |
| c | Υ | Ι | Τ | Μ | Σ | Ο | Η | Μ | Κ | | Υ | ∅ | Α | Ν | Μ |

# «Συρματόπλεγμα»

| Μ | Υ | Σ | Τ | Ι | Κ | Ο |  | Μ | Η | Ν | Υ | Μ | Α |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Μ | | | | Ι | | | | Μ | | | | Μ | | (1) |
| | Υ | | Τ | | Κ | | | | Η | | Υ | | Α | (2) |
| | | Σ | | | | Ο | | | | Ν | | | | (3) |

| Μ | Ι | Μ | Μ | Υ | Τ | Κ |  | Η | Υ | Α | Σ | Ο | Ν |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

# Μετάθεση κατά στήλες

- Κλειδί: μία λέξη, της οποίας τα γράμματα αντιστοιχίζονται σε αριθμούς, ανάλογα με τη σειρά εμφάνισής τους στο αλφάβητο

| Π | Ο | Λ | Υ | Μ | Ε | Ρ | Ε | Σ |
|---|---|---|---|---|---|---|---|---|
| 6 | 5 | 3 | 9 | 4 | 1 | 7 | 2 | 8 |

Το μη κρυπτογραφημένο κείμενο γράφεται σε έναν πίνακα που έχει τόσες στήλες όσες τα γράμματα του κλειδιού

# Μετάθεση κατά στήλες

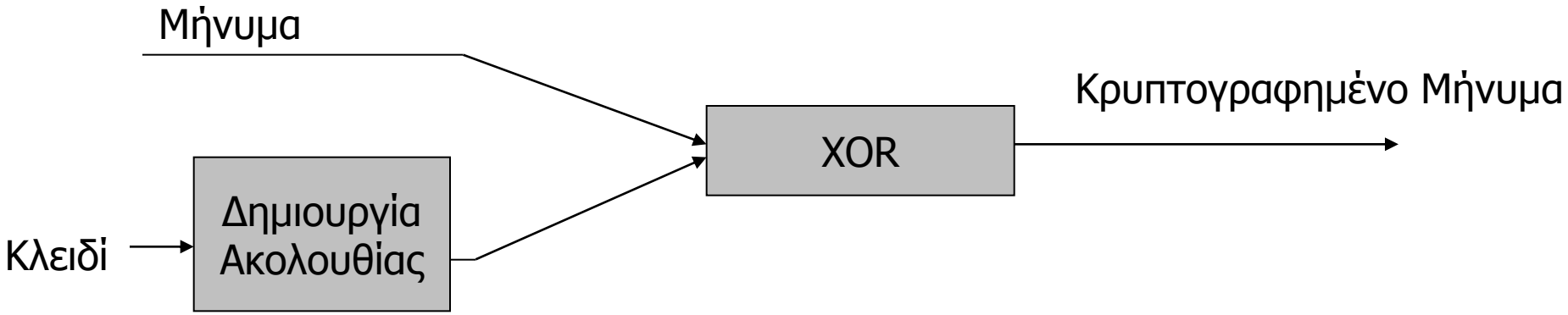
- ΑΣΠΡΗ ΠΕΤΡΑ ΞΕΞΑΣΠΡΗ

| Π | Ο | Λ | Υ | Μ | Ε | Ρ | Ε | Σ |
|---|---|---|---|---|---|---|---|---|
| 6 | 5 | 3 | 9 | 4 | 1 | 7 | 2 | 8 |
| Α | Σ | Π | Ρ | Η | | Π | Ε | Τ |
| Ρ | Α | | Ξ | Ε | Ξ | Α | Σ | Π |
| Ρ | Η | ∅ | ∅ | ∅ | ∅ | ∅ | ∅ | ∅ |

–Το κρυπτογραφημένο κείμενο παράγεται με ανάγνωση του πίνακα κατά στήλες, με τη σειρά που ορίζεται από την απεικόνιση του κλειδιού

| | Ξ | ∅ | Ε | Σ | ∅ | Π | | ∅ | Η | Ε | ∅ | Σ | Α | Η | Α | Ρ | Ρ | Π | ... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

# Κρυπτογραφία ροής



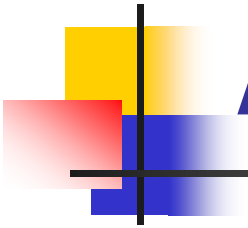

- Κρυπτογραφεί bit προς bit
- Προσπαθεί να εκμεταλλευτεί κάποια χαρακτηριστικά του one time pad
- Πλεονεκτήματα:
  - Ταχύτητα
  - Ευκολία Υλοποίησης
- Μειονέκτήματα:
  - Ακολουθία κλειδιού

# Κρυπτογράφηση κατά μπλοκ

- Το μήνυμα Μ διασπάται σε διαδοχικά μπλοκ Μ1, Μ2, ...
- Το κάθε μπλοκ κρυπτογραφείται με το ίδιο κλειδί Κ
- Τελικό μήνυμα: $E_k(M1)E_k(M2)...$
- Πλεονεκτήματα:
  - Μόνο μία εκτέλεση του κρυπταλγόριθμου ανά μπλοκ
  - Σφάλματα στο ένα μπλοκ δεν επηρεάζουν τα άλλα
- Μειονεκτήματα
  - Πιο ευάλωτα σε αναλύσεις κρυπτογραφίας
  - Όμοια τμήματα plaintext γεννούν το ίδιο ciphertext

# Αλυσιδωτά μπλοκ

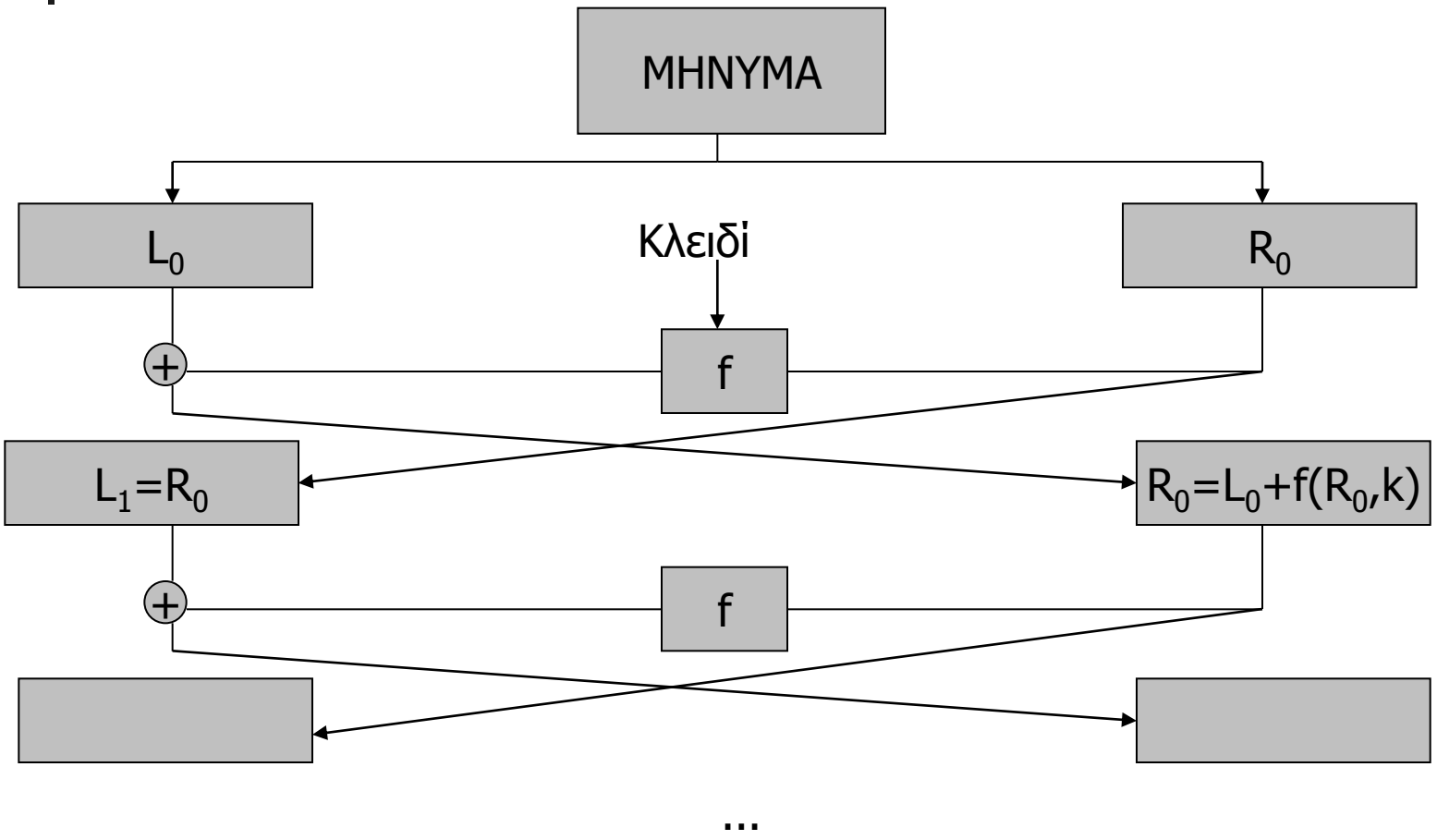
- Το κάθε μπλοκ δεν είναι αυτόνομο, αλλά περιλαμβάνει bits από τα προηγούμενα (κρυπτογραφημένα ή μη)
  - Μειώνονται οι διαθέσιμες θέσεις πληροφορίας σε κάθε μπλοκ
  - Αναιρείται το πλεονέκτημα της ανοχής σε σφάλματα
  - Αυξάνεται όμως η ασφάλεια
- Παράδειγμα:
  - $C_i = E_k(M_i \text{ XOR } C_{i-1})$
  - Το $C_i$ πρακτικά εξαρτάται από όλα τα $C_k$ με $i < k$
  - Ιδιαίτερα χρήσιμο για ψηφιακές υπογραφές

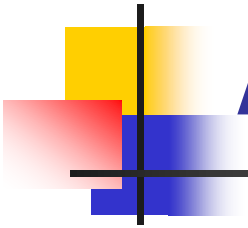


# Αλγόριθμος DES

- Μπλοκ 64 bit
- Κλειδί 56 bit
- 16 επαναλήψεις του αλγορίθμου Feistel
- Έγινε στάνταρ το 1977

# Αλγόριθμος Feistel (~1974)



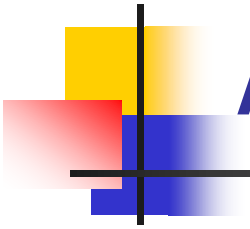


# Ασφάλεια του DES

- Εξουθενωτική Αναζήτηση Κλειδιών:
  - $2^{56}$ κλειδιά
  - 1977: Diffie & Hellman: 20 ώρες σε μηχανή $20.000.000
- 1997: Αναζήτηση κλειδιού στο Internet
  - 10.000 υπολογιστές
  - 140 μέρες
- 1998: EFF DES Cracker
  - Μηχανή $200.000
  - 56 ώρες για το κλειδί
  - 220 ώρες για αναζήτηση όλων των κλειδιών

# Παραλλαγές του DES

- Διπλός DES
  - k=(k1,k2)
  - Ek(m)=Ek1(Ek2(m))
  - Ασθενή κλειδιά: Ek(Ek(m))=m
  - Ημιασθενή κλειδιά: Ek1(Ek2(m))=m
  - Ευάλωτος σε επιθέσεις «συνάντησης στη μέση»
- Τριπλός DES
  - Ek(m)=Ek1(Dk2(Ek1(m)))
  - Με 3 κλειδιά:
    - Ek(m)=Ek1(Dk2(Ek3(m)))



# Αλγόριθμος AES

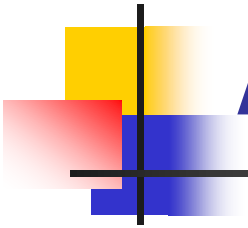
- Advanced Encryption Standard
- 1998: Διάδοχος του DES.

  5 υποψήφιοι
- 2000: Τελικός νικητής: Rijndael
  - Μπλοκ 128 bit
  - Κλειδία 128, 192, 256 bit
  - Ταχύτερος από τον τριπλό DES

# Επιθυμητές ιδιότητες συστημάτων κρυπτογραφίας

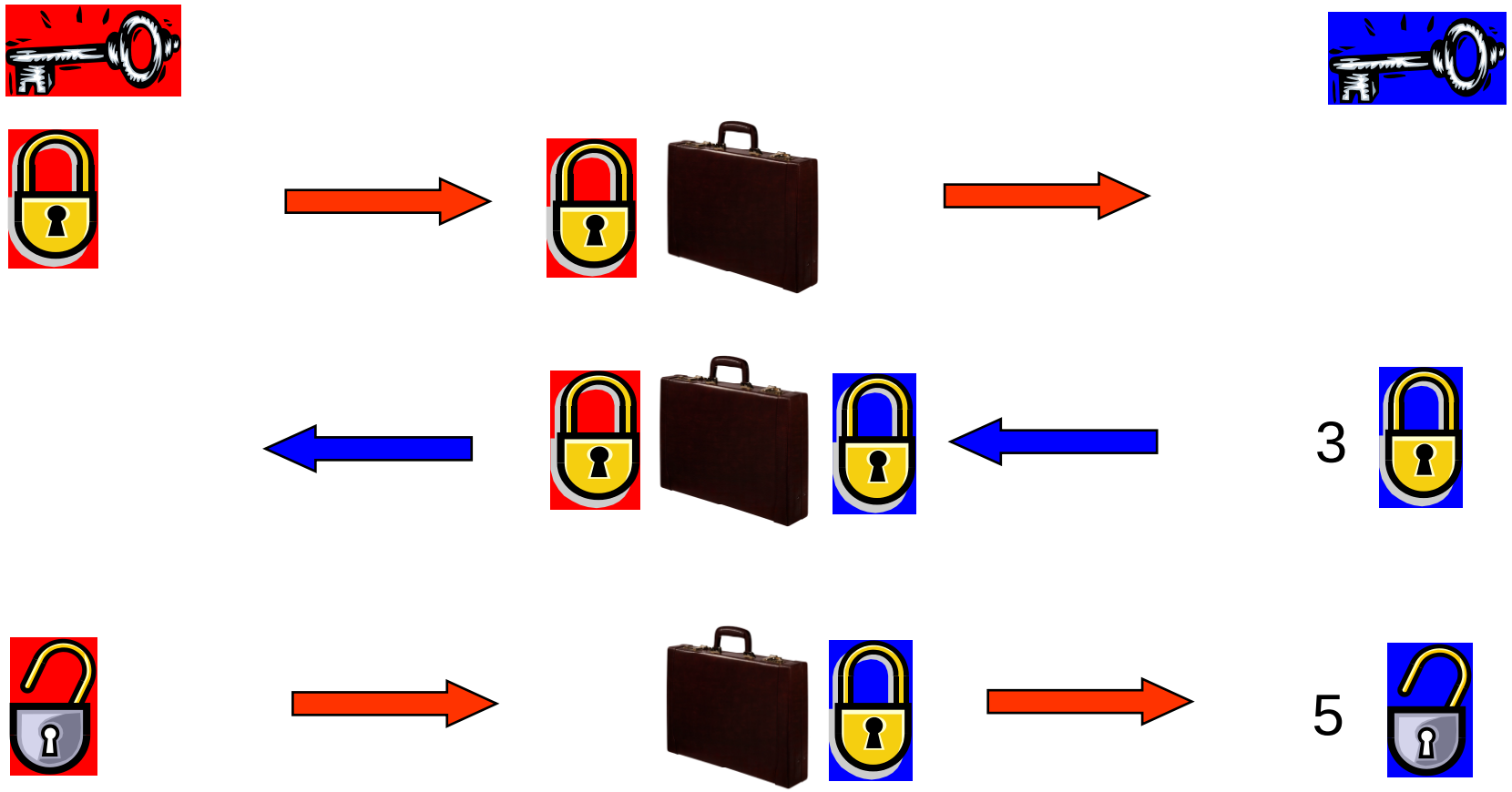
- Πρέπει να υπάρχουν αποδοτικοί αλγόριθμοι για τις λειτουργίες της κωδικοποίησης και της αποκωδικοποίησης
- Εύχρηστο σύστημα
- Η προστασία που παρέχει το σύστημα πρέπει να προϋποθέτει μόνο τη μυστικότητα των κλειδιών, όχι του αλγόριθμου

# Ασύμμετρη Κρυπτογραφία



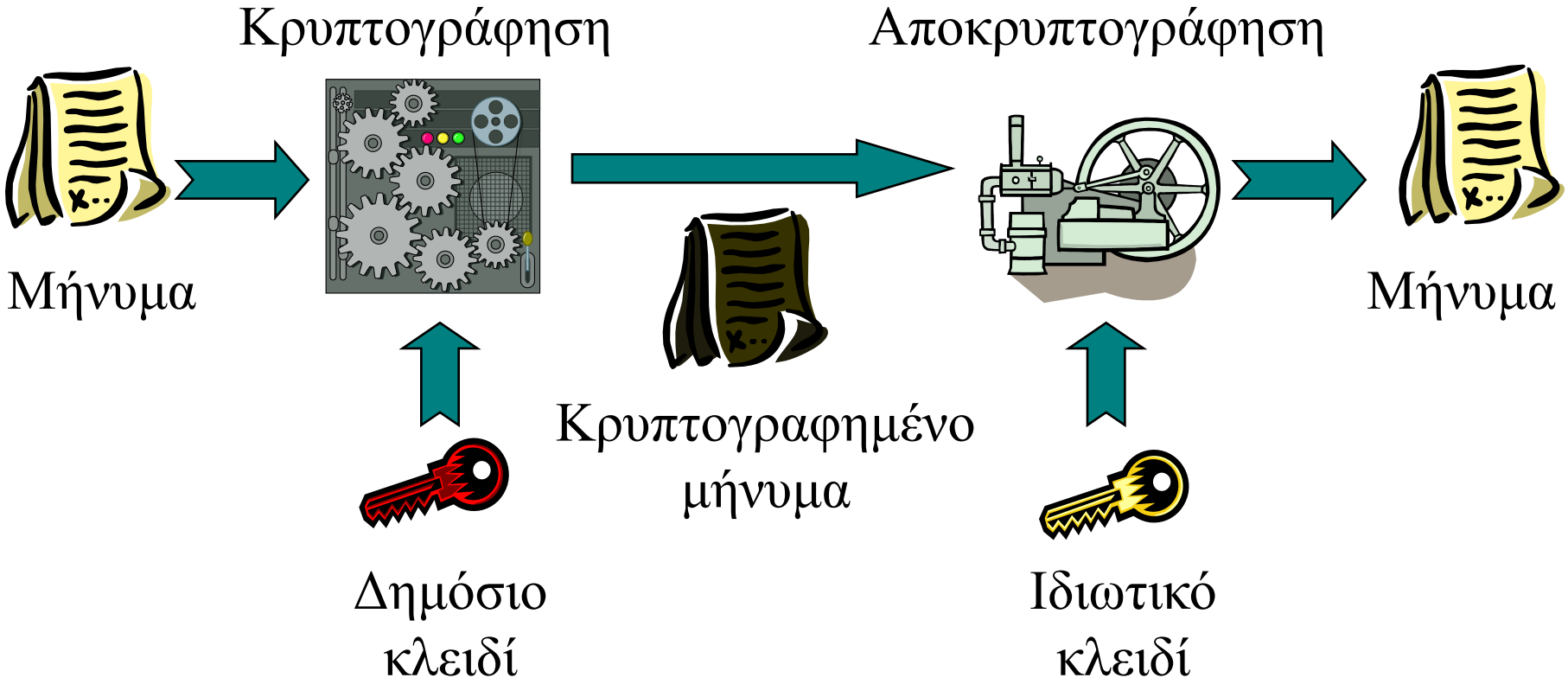
- Στόχοι: Εχεμύθεια και αυθεντικότητα
- Δύο κλειδιά, *δημόσιο* (public) και *ιδιωτικό* (private)
- Το ιδιωτικό είναι διαθέσιμο μόνο στον κάτοχο, το δημόσιο σε όλους τους χρήστες
- Ανέφικτο να υπολογιστεί το ένα κλειδί από το άλλο
- Για να επικοινωνήσουν δύο μέρη, αρκεί ο ένας να γνωρίζει το δημόσιο κλειδί του άλλου

# Ασύμμετρη Κρυπτογραφία



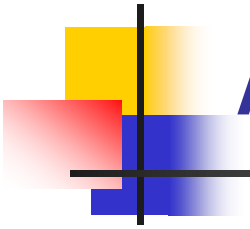
# Αποστολή Μηνύματος

- Στόχος: Εμπιστευτικότητα
- Κρυπτογραφούμε με δημόσιο κλειδί, αποκρυπτογραφούμε με το ιδιωτικό



# Συναρτήσεις «μονής» κατεύθυνσης

- Για ένα ασύμμετρο κρυπτοσύστημα, η κρυπτογράφηση πρέπει να είναι μία συνάρτηση μονής κατεύθυνσης
- Υπάρχει μία έξοδος διαφυγής που αποκρυπτογραφεί το μήνυμα και τη γνωρίζει μόνο ο παραλήπτης
- Συναρτήσεις που πραγματοποιούνται εύκολα αλλά είναι αδύνατο να αντιστραφούν:
  - Σπάσιμο του αυγού
  - Αναζήτηση στον τηλεφωνικό κατάλογο
  - Πολλαπλασιασμός 2 μεγάλων πρώτων αριθμών



# Αλγόριθμος RSA

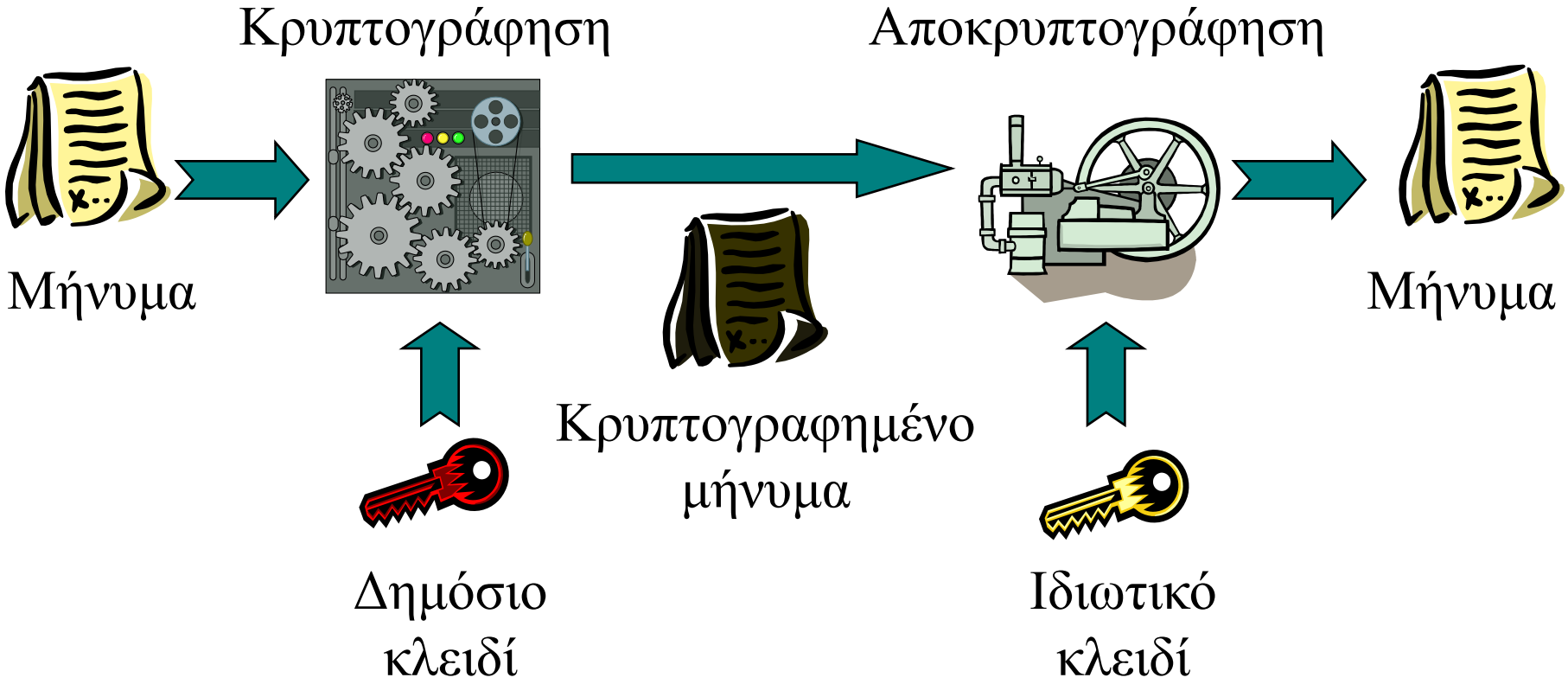
- Για την παραγωγή κλειδιών χρησιμοποιείται ο πολλαπλασιασμός πρώτων αριθμών
- Η εχεμύθεια βασίζεται στη δυσκολία παραγοντοποίησης μεγάλων ακεραίων

# Αλγόριθμος Diffie-Hellman

- Χρήση δημόσιου συστήματος για ανταλλαγή μυστικής πληροφορίας
- Επιλογή ενός μεγάλου πρώτου p και ενός ακεραίου a
- Ο χρήστης A διαλέγει τυχαία έναν ακέραιο $r_A$ και στέλνει στον B τον αριθμό: $a^{r_A}(\text{mod}p)$
- Ομοίως ο χρήστης B διαλέγει τυχαία έναν αριθμό $r_B$ και στέλνει στον A: $a^{r_B}(\text{mod}p)$
- Και οι δύο χρήστες υπολογίζουν το μυστικό κλειδί: $a^{r_A r_B}(\text{mod}p) = (a^{r_A})^{r_B}(\text{mod}p) = (a^{r_B})^{r_A}(\text{mod}p)$
- Επίθεση ενδιάμεσου ανθρώπου (man in the middle attack)

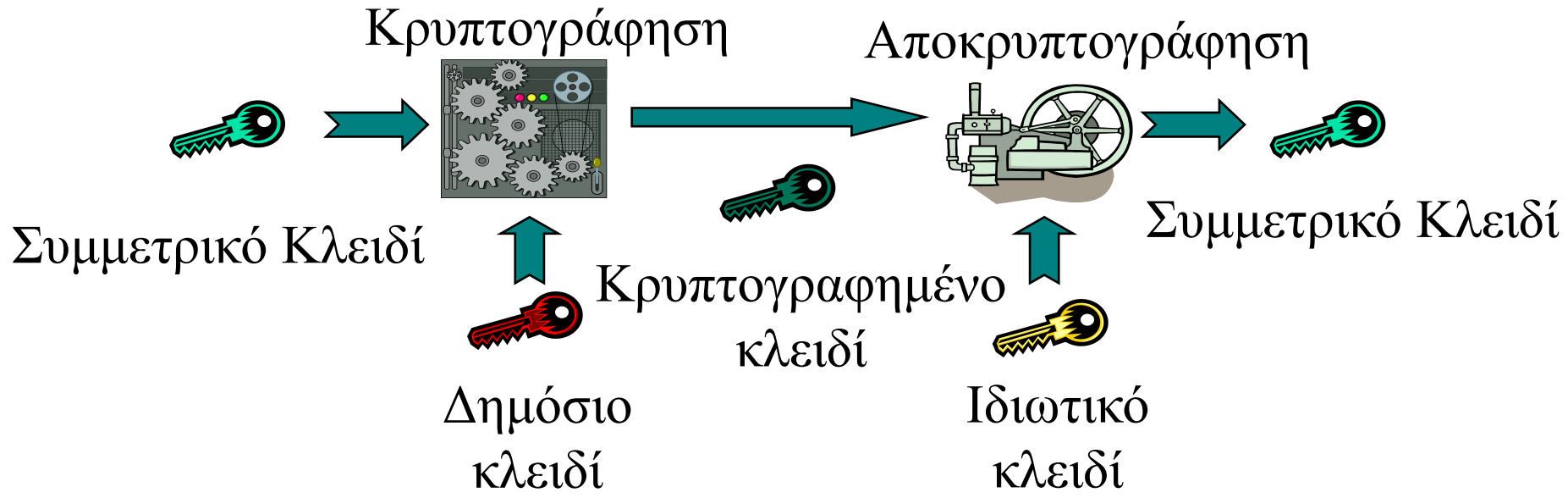
# Αποστολή Μηνύματος

- Στόχος: Εμπιστευτικότητα
- Κρυπτογραφούμε με δημόσιο κλειδί, αποκρυπτογραφούμε με το ιδιωτικό



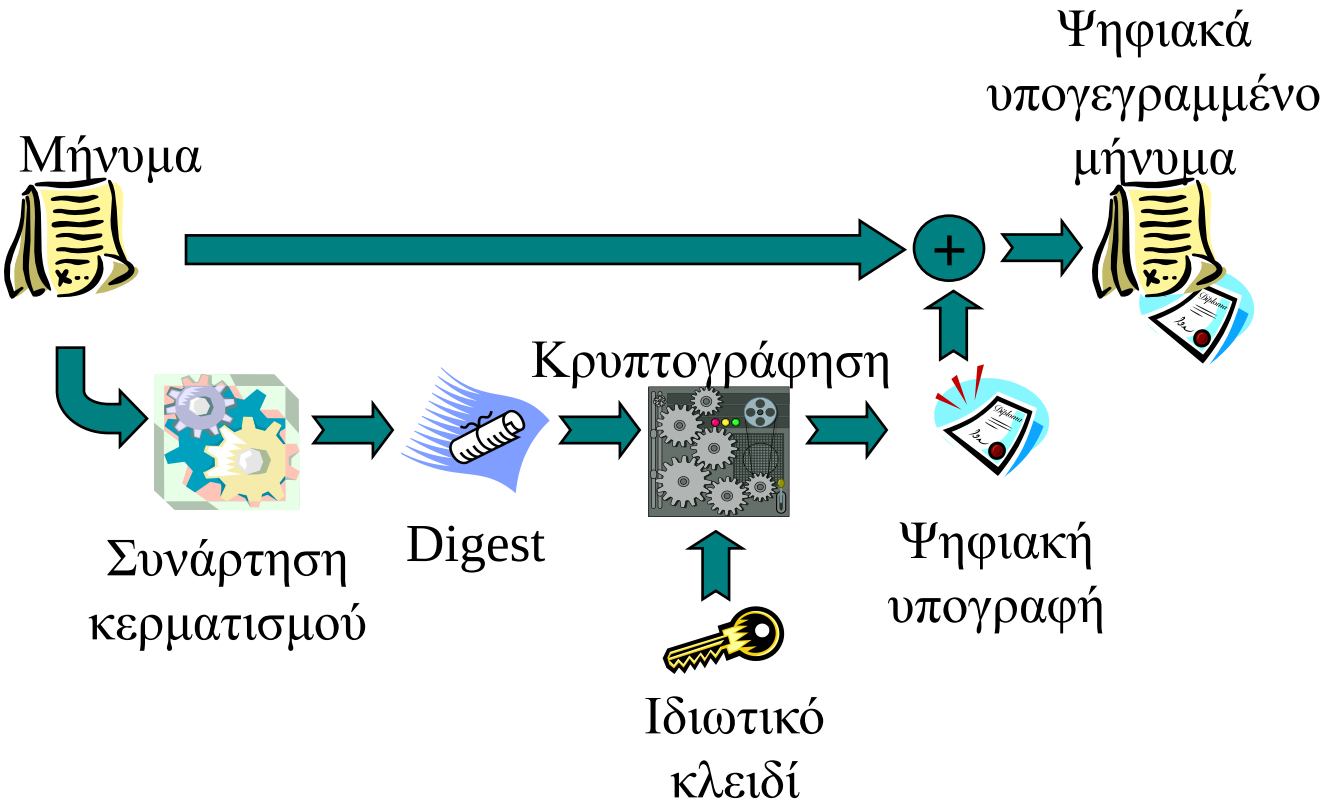
# Ασύμμετρη εναντίον Συμμετρικής

- Πλεονέκτημα: Δεν απαιτείται ανταλλαγή μυστικού κλειδιού
- Μειονέκτημα: Πιο αργή
- Υβριδική λύση

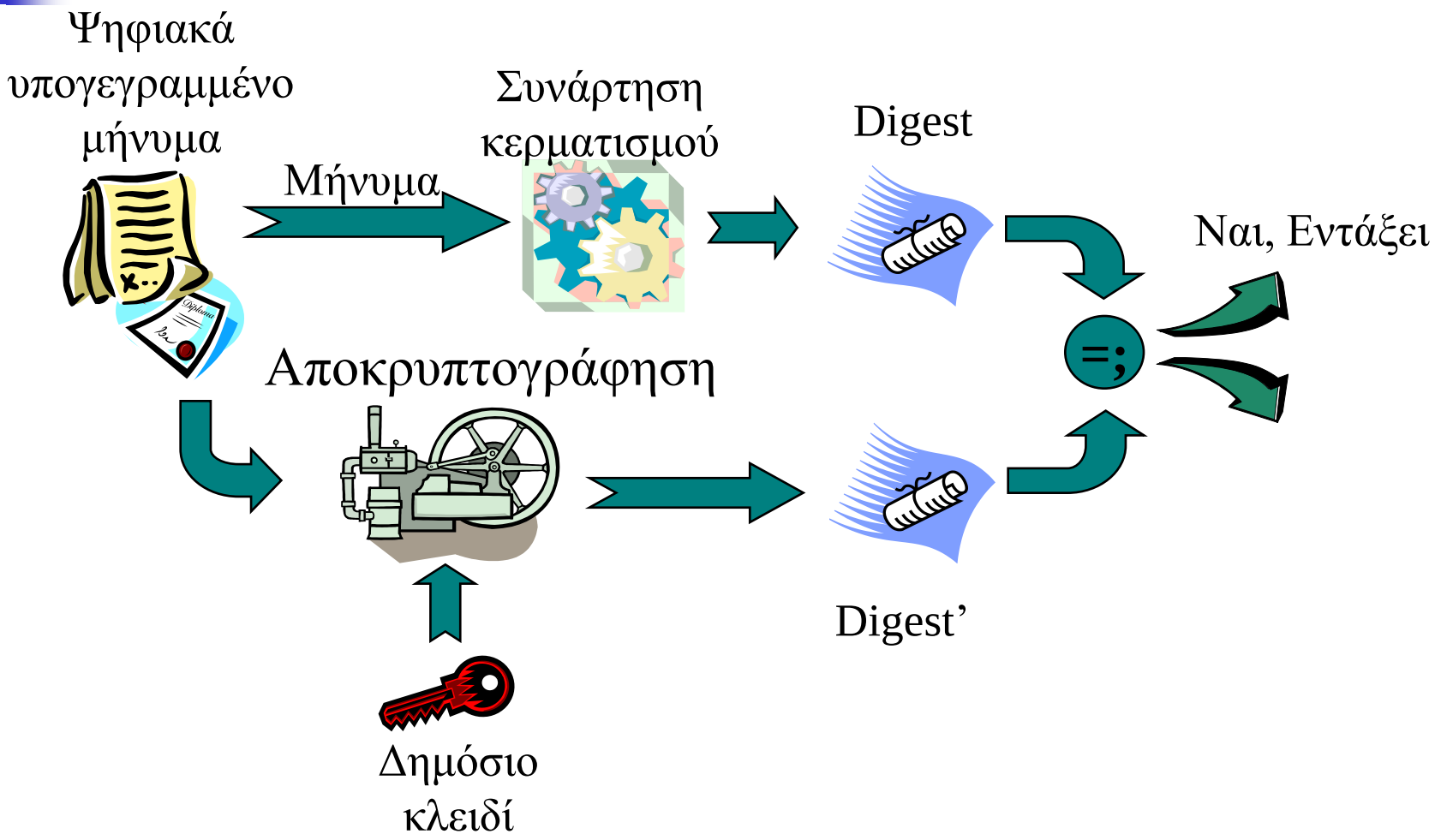


# Ψηφιακές Υπογραφές - Αποστολή

- Στόχος: Αυθεντικότητα και Ακεραιότητα



# Ψηφιακές Υπογραφές - Παραλαβή

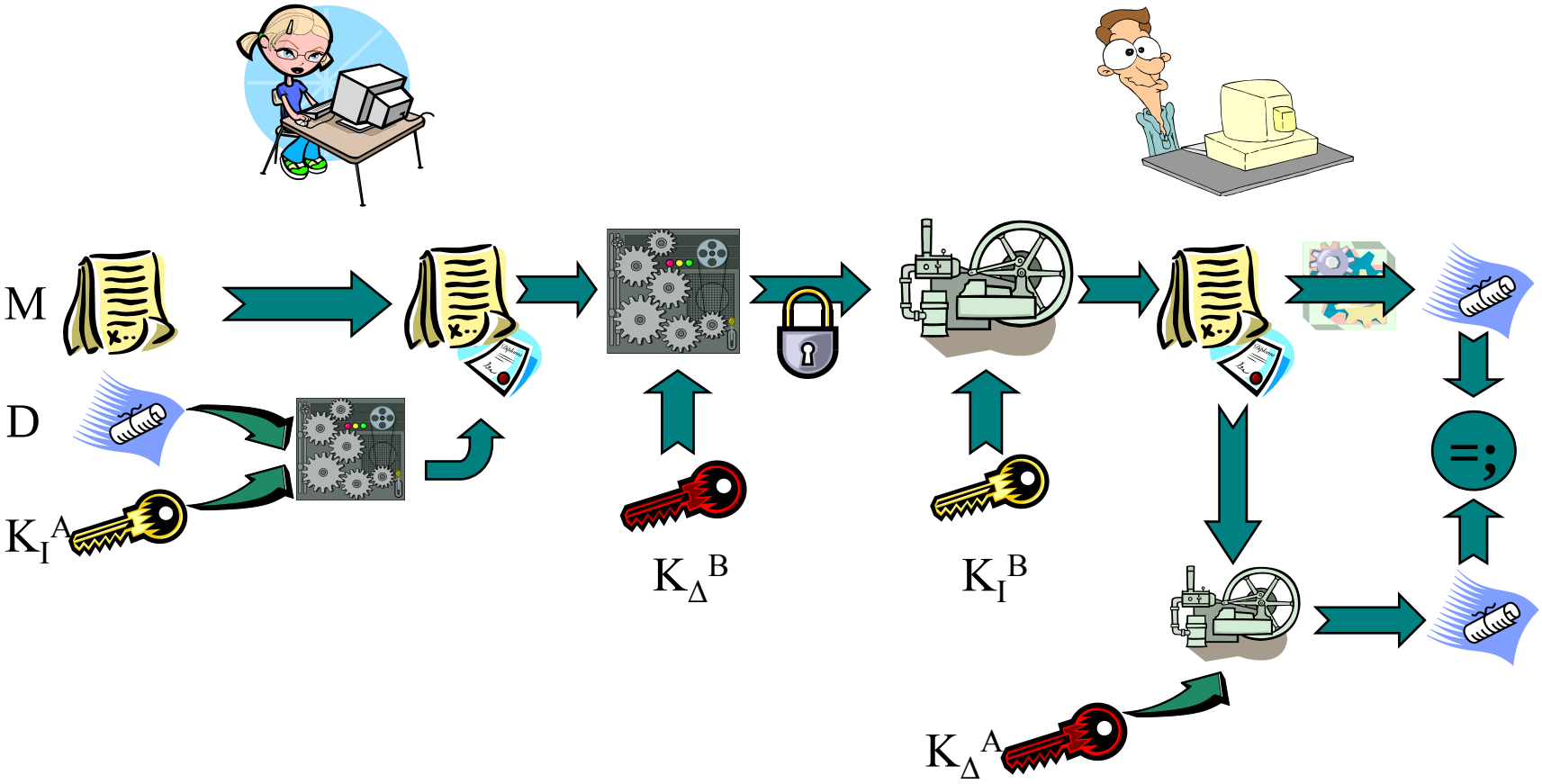


# Ψηφιακές Υπογραφές

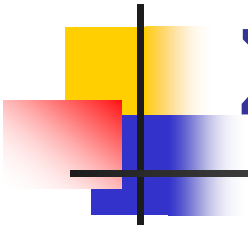
- Είναι ένα σύνολο από bits που προσθέτει ο αποστολέας ενός εγγράφου σ' αυτό και έχουν τις ακόλουθες ιδιότητες:
  - Ο παραλήπτης μπορεί να επαληθεύσει ότι η υπογραφή είναι του αποστολέα
  - Θα πρέπει να είναι αδύνατο για οποιονδήποτε, συμπεριλαμβανομένου του παραλήπτη, να πλαστογραφήσει την υπογραφή του Α
  - Θα πρέπει να είναι δυνατόν για κάποιον τρίτο (π.χ. δικαστική αρχή) να διευθετήσει κάποια διαφωνία μεταξύ αποστολέα και παραλήπτη
  - Εξασφαλίζει την ακεραιότητα των δεδομένων

# Ψηφιακές Υπογραφές

- Στόχος: Εμπιστευτικότητα, Αυθεντικότητα και Ακεραιότητα



# Συναρτήσεις κερματισμού

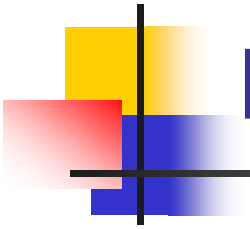


- ή συναρτήσεις σύνοψης (hash functions)
- Λαμβάνει στην είσοδο μία ακολουθία δεδομένων απροσδιόριστου μήκους και παράγει μία ακολουθία σταθερού μήκους
- Είναι μονόδρομες συναρτήσεις
- Είναι δύσκολο να βρεθούν 2 διαφορετικές είσοδοι που να δίνουν την ίδια έξοδο.
  - Κάτι τέτοιο φυσικά είναι αδύνατο
  - Μας ενδιαφέρει όμως να είναι υπολογιστικά δύσκολο να συμβεί

# Πραγματικές Υπογραφές

- Πραγματική Υπογραφή:
  - «Ιδιαίτερη» για τον καθένα (μοναδική)
  - Ίδια σε κάθε κείμενο
  - Φυσική τοποθέτηση στο κείμενο
  - Πλαστογραφείται εύκολα;
  - Είναι πάντα ίδια;
- Ψηφιακή Υπογραφή
  - Εξαρτάται από το κείμενο
  - Βασίζεται σε ένα μυστικό

# Επιθέσεις στις Ψηφιακές Υπογραφές



- Κλοπή Ταυτότητας (Identity Theft)
  - Ο καθένας «είναι» το ιδιωτικό του κλειδί
  - Οποιοσδήποτε μπορεί να δημιουργήσει ένα ζεύγος κλειδιών και να ισχυριστεί ότι είναι κάποιος (κλοπή ιδιωτικού κλειδιού)
  - Εάν ο παραλήπτης δεν έχει το δημόσιο κλειδί του αποστολέα, μπορεί να εξαπατηθεί (αντικατάσταση δημόσιου κλειδιού)
- Ασφάλεια συναρτήσεων κερματισμού

# Αρχή Διαχείρισης Πιστοποιητικών

- Certification Authority - CA
- Έμπιστη Τρίτη Οντότητα που εγγυάται την αυθεντικότητα των δημόσιων κλειδιών
- Υπογράφει ένα πιστοποιητικό που περιέχει την ταυτότητα του χρήστη και το δημόσιο κλειδί του.
- Για την υπογραφή των πιστοποιητικών χρησιμοποιεί το ιδιωτικό της κλειδί. Συνεπώς όλοι οι χρήστες πρέπει να κατέχουν το δημόσιό της κλειδί

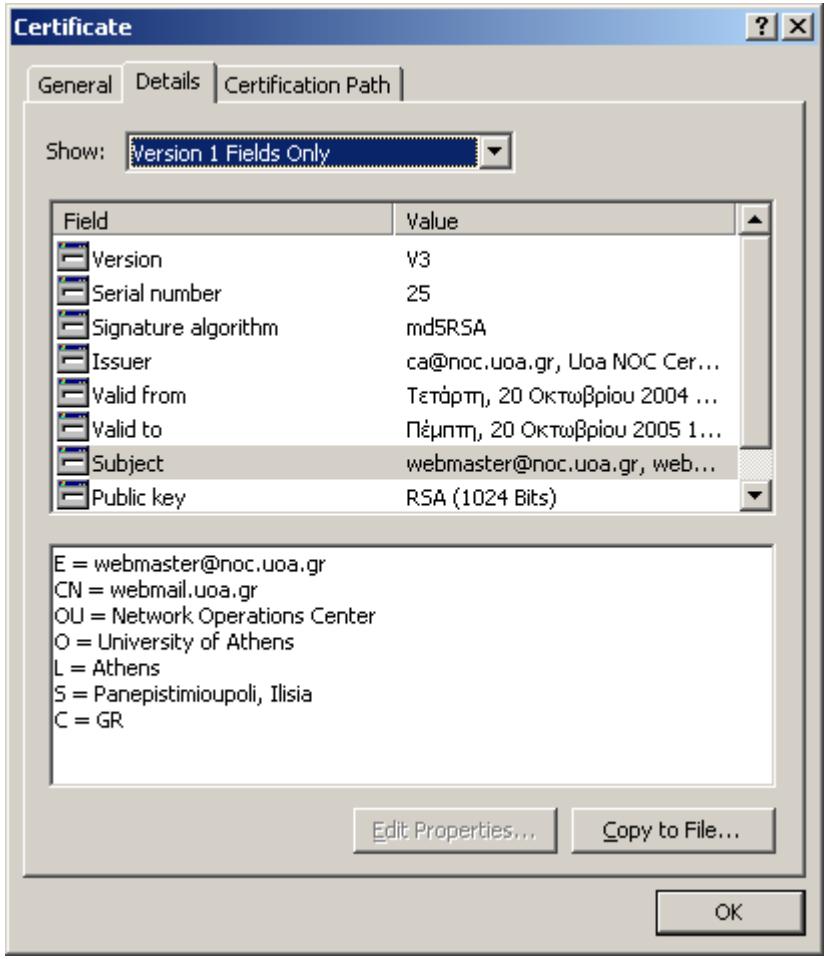
# Διαδικασία Πιστοποίησης

- Δημιουργείται το ζεύγος κλειδιών της ΑΔΠ
- Δημιουργείται το ζεύγος κλειδιών του χρήστη
- Ζητείται ένα πιστοποιητικό για τον χρήστη
- Η ταυτότητα του χρήστη ελέγχεται
- Επικυρώνεται το ζεύγος κλειδιών του χρήστη
- Εκδίδεται ένα πιστοποιητικό για το χρήστη
- Ο χρήστης ελέγχει την ορθότητα του πιστοποιητικού

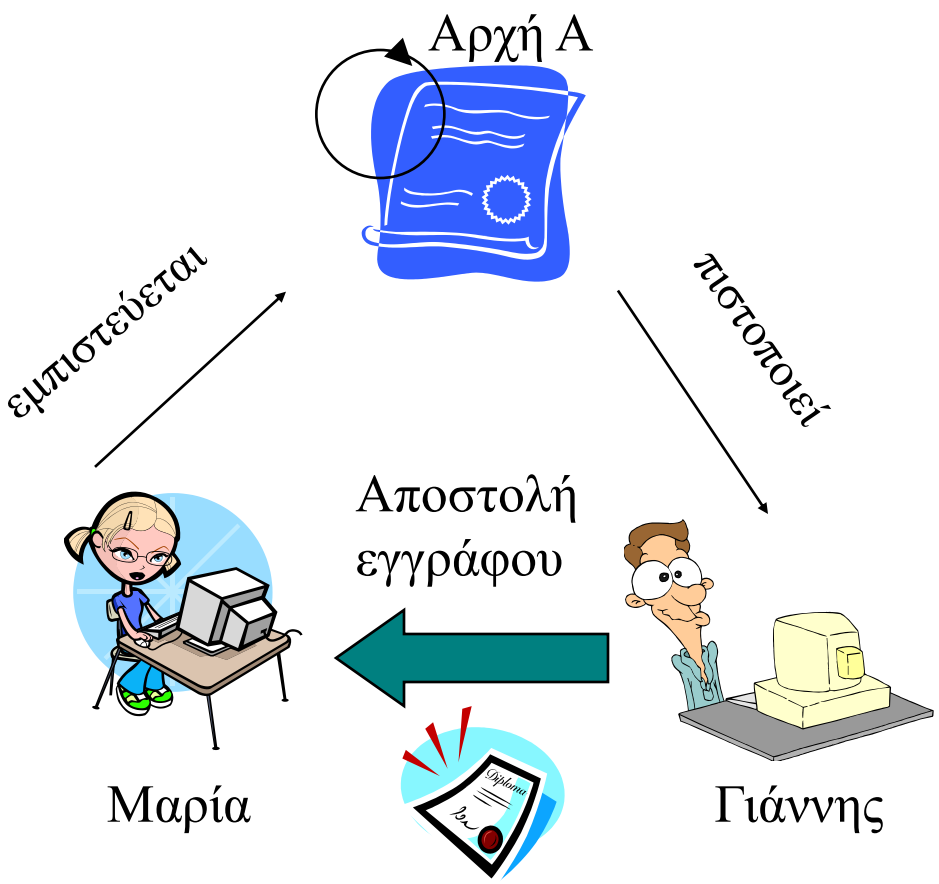
# Ψηφιακά Πιστοποιητικά

- Το *πιστοποιητικό* είναι μία δομή δεδομένων που περιέχει:
  - Έκδοση και αριθμό σειράς
  - Το όνομα του εκδότη
  - Το όνομα του υποκειμένου και άλλες τυχόν επεκτάσεις (διεύθυνση οικίας, εργασίας, αριθμό ταυτότητας κ.λπ.)
  - Το σκοπό του πιστοποιητικού
  - Το δημόσιο κλειδί του υποκειμένου
  - Την περίοδο εγκυρότητας του πιστοποιητικού
  - Την υπογραφή της αρχής διαχείρισης πιστοποιητικών
- Αυτοϋπογεγραμμένα πιστοποιητικά: Μία αρχή πιστοποίησης (ή οποιοσδήποτε!) μπορεί να φτιάξει ένα αυτοϋπογεγραμμένο πιστοποιητικό

# Πιστοποιητικό X.509v3

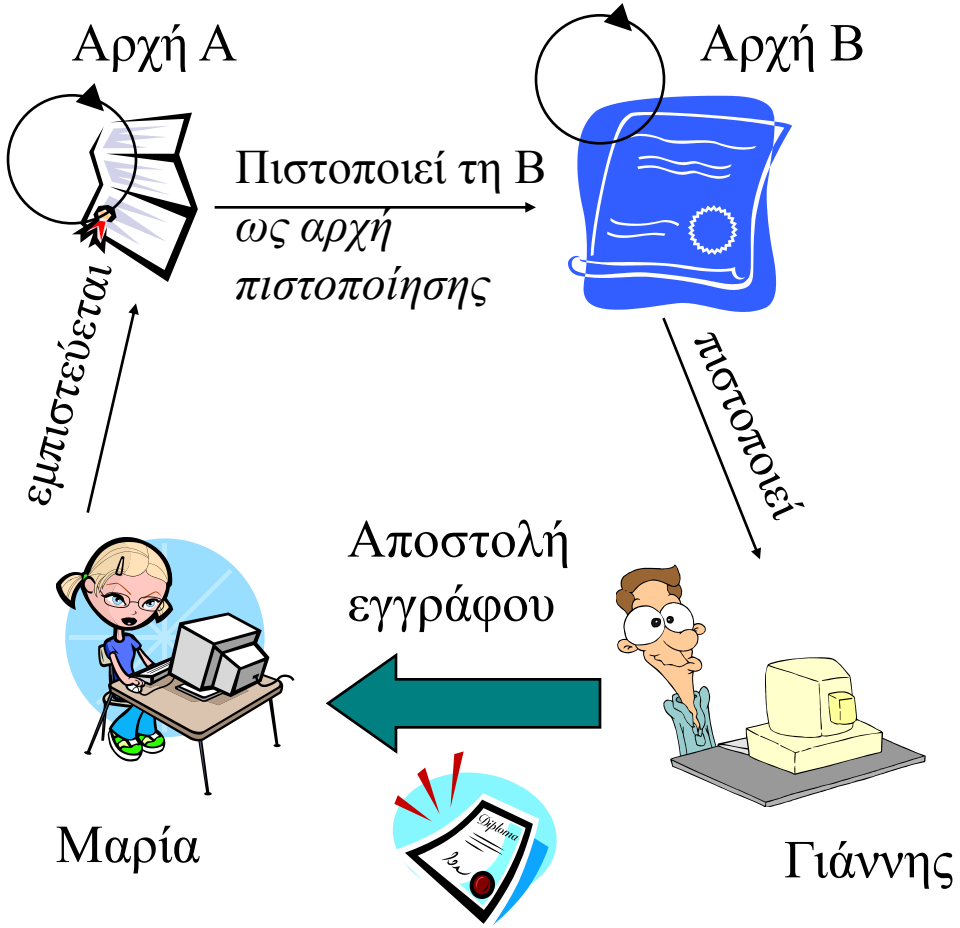
# Αποστολή Μηνύματος



# Ομότιμη διασταυρούμενη πιστοποίηση

- Cross certification
- Οι αρχές πιστοποίησης εγκαθιστούν μεταξύ τους μονόδρομες ή αμφίδρομες σχέσεις εμπιστοσύνης σε ομότιμη βάση
  - Η αρχή Α πιστοποιεί την αρχή Β ως έγκυρη αρχή πιστοποίησης
- Οι χρήστες εμπιστεύονται τις επί μέρους αρχές πιστοποίησης
- Για τη διακρίβωση των πιστοποιητικών αξιοποιούνται οι σχέσεις εμπιστοσύνης μεταξύ των αρχών πιστοποίησης

# Ομότιμη διασταυρούμενη πιστοποίηση

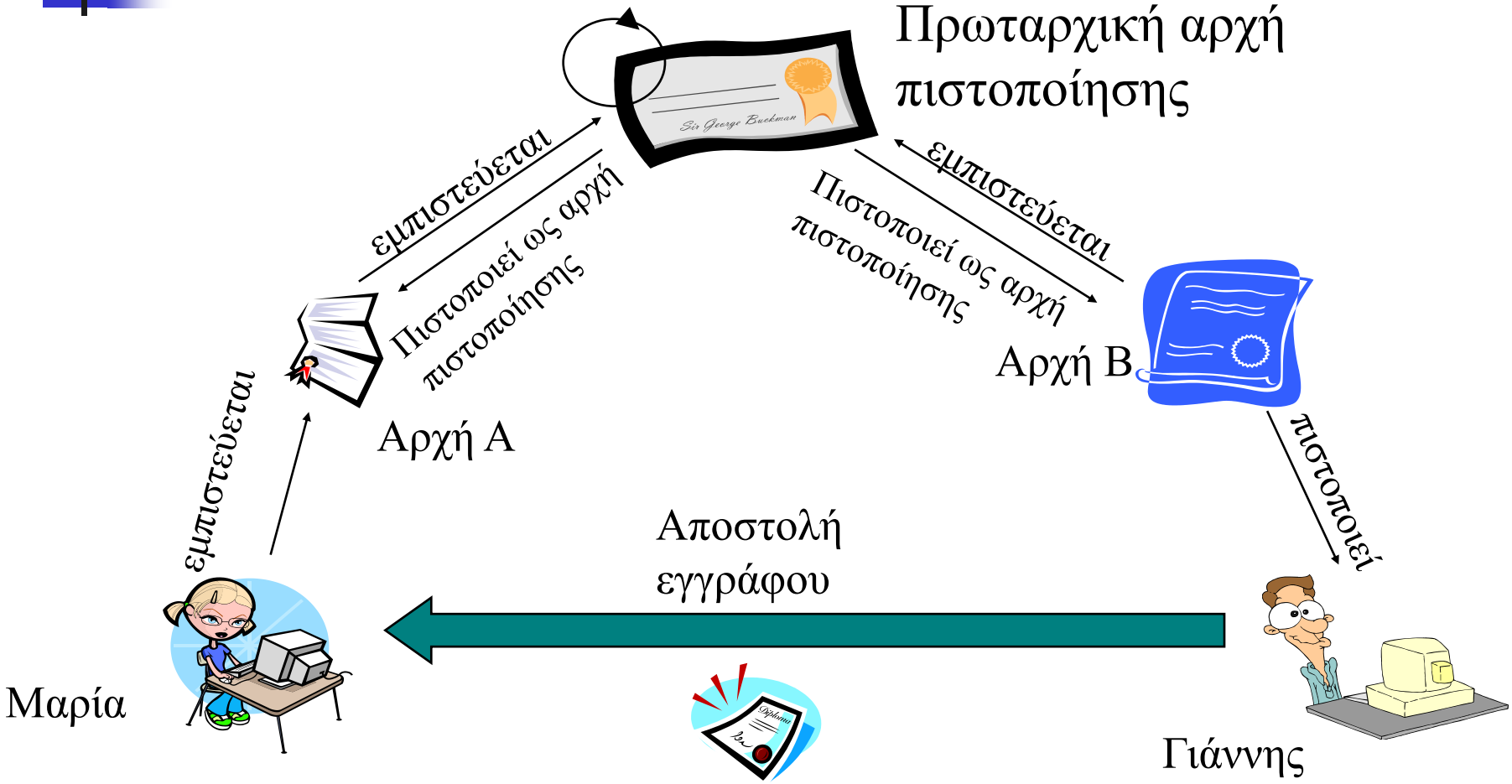



*Αλυσίδα εμπιστοσύνης: Μαρία → Αρχή Α → Αρχή Β → Γιάννης*

# Ιεραρχική διασταυρούμενη πιστοποίηση

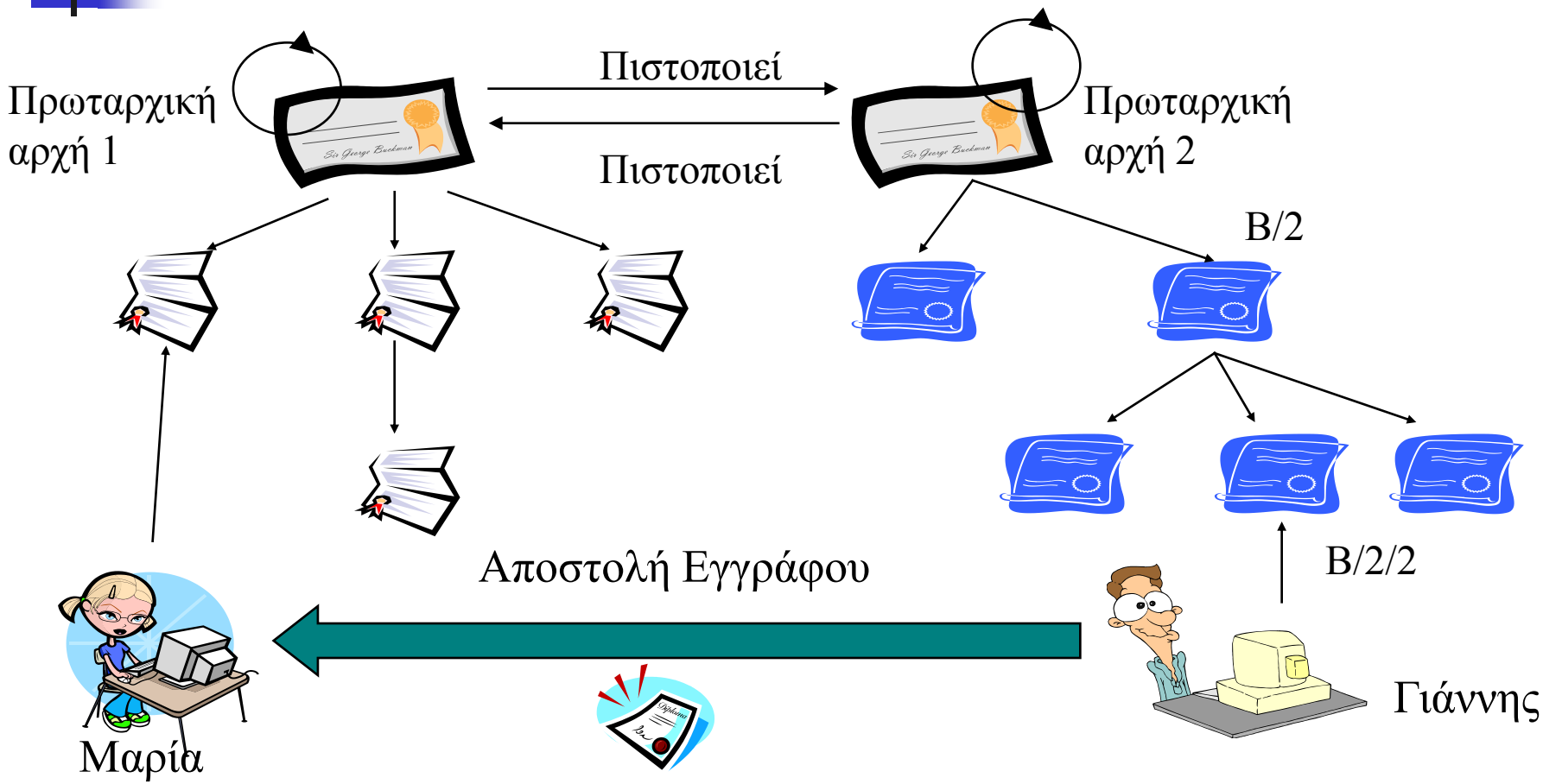
- Οι αρχές πιστοποίησης οργανώνονται σε ιεραρχίες, με κάθε μία να πιστοποιεί τις υφιστάμενές της ως αρχές πιστοποίησης
- Εδώ κάθε χρήστης εμπιστεύεται την *πρωταρχική αρχή πιστοποίησης,* στη ρίζα της ιεραρχίας
  - τα πιστοποιητικά εκδίδονται από τις αρχές χαμηλότερα στην ιεραρχία
  - Οι χρήστες εμπιστεύονται την έκδοση των πιστοποιητικών τους στις αρχές διότι «εγγυάται» γι' αυτές η πρωταρχική αρχή πιστοποίησης
  - Για τη διακρίβωση των πιστοποιητικών προσπαθούμε να φτάσουμε στη ρίζα διασχίζοντας αντίστροφα σχέσεις τύπου «πιστοποιεί»

# Ιεραρχική διασταυρούμενη πιστοποίηση




*Αλυσίδα εμπιστοσύνης: Μαρία → Αρχή Α → Πρωτ. Αρχή → Αρχή Β → Γιάννης*

# Υβριδικό μοντέλο




*Αλυσίδα εμπιστοσύνης: Μαρία → Πρωτ. Αρχή 1 → Πρωτ. Αρχή 2 → Β/2 → Β/2/2 → Γιάννης*

# Νέα Προβλήματα

- Ο καθένας πλέον «είναι» 2 αριθμοί:
  - Το ιδιωτικό του κλειδί
  - Το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο που αναγράφεται στο πιστοποιητικό του
- Ποιος δημιουργεί τα κλειδιά;
- Πώς επιβεβαιώνεται η πραγματική ταυτότητα των χρηστών;
- Πώς ακυρώνονται πιστοποιητικά;

# Υποδομές Δημόσιου Κλειδιού

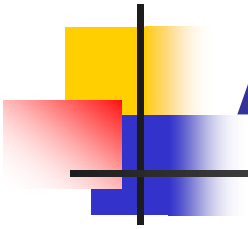
- Public Key Infrastructure (PKI)
- Διευκολύνει τη χρήση της ασύμμετρης κρυπτογραφίας

# Δημιουργία Κλειδιών

- Εάν εμπιστεύεσαι κάποιον για να δημιουργήσει το ιδιωτικό σου κλειδί, γιατί να μην τον εμπιστεύεσαι και για να υπογράφει εκ μέρους σου;
- Το ιδιωτικό κλειδί πρέπει να παραμένει στον τόπο δημιουργίας του.

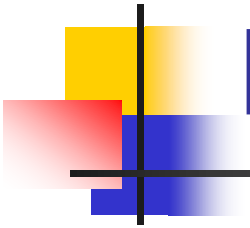
# Εξακρίβωση Ταυτότητας

- Το γεγονός ότι κάποιος έχει στην κατοχή του ένα πιστοποιητικό, δε σημαίνει τίποτα για την ταυτότητά του
- Ο πραγματικός κάτοχος του πιστοποιητικού γνωρίζει το ιδιωτικό κλειδί
- Εξαιρετικά Σημαντική Διαδικασία
- Χειροκίνητη διαδικασία (για συστήματα υψηλής ασφάλειας)
- Αρχή Εγγραφής – Registration Authority (RA)
- Ασφαλής Διασύνδεση μεταξύ RA και CA



# Διανομή Πιστοποιητικών

- Τα πιστοποιητικά αποστέλλονται προς τους χρήστες (Pushing)
- Τα πιστοποιητικά ζητούνται από τους χρήστες (Pulling)
  - Κατάλογοι Πιστοποιητικών (X.500, LDAP, Active Directory, κλπ.)



# Εγκυρότητα πιστοποιητικών

- Δυνατότητα ανάκλησης πιστοποιητικών
  - Κλοπή ιδιωτικού κλειδιού
  - Παραβίαση συμφωνίας
- Λίστες Ανάκλησης Πιστοποιητικών (CRLs – Certificate Revocation Lists)
  - Εκδίδεται ανά τακτά χρονικά διαστήματα
  - Περιλαμβάνει λίστα με όσα πιστοποιητικά έχουν ανακληθεί ως τότε
  - Υπογράφεται από την ΑΔΠ

# Εγκυρότητα πιστοποιητικών

- Προβλήματα ΛΑΠ
  - Περιοδικότητα
  - Μέγεθος
  - Δημοσιοποίηση
- OCSP – Online Certificate Status Protocol
  - Πρωτόκολλο Ερώτησης – Απάντησης
  - Δυνατότητα άμεσου ελέγχου ενός ή περισσότερων πιστοποιητικών

# Αποδοχή Πιστοποιητικών

- Έλεγχος Ονόματος Χρήστη
- Έλεγχος Ονόματος Εκδούσας ΑΔΠ
- Έλεγχος Δημ. Κλειδιού και Πιστοποιητικού Εκδούσας ΑΔΠ
- Έλεγχος Εγκυρότητας Πιστοποιητικού

- Εμπιστοσύνη (Trust)

# Επιλογή ΑΔΠ

- Δήλωση Πολιτικής
- Δήλωση Πρακτικής

- Ευρωπαϊκή Οδηγία (2001)
- Ελληνική Νομοθεσία (ΕΕΤΤ)

# Είναι όλα εντάξει;

- Microsoft Security Bulletin MS01-017

  Η Verisign ενημέρωσε τη Microsoft ότι στις 29 και 30 Ιανουαρίου 2001 εξέδωσε δύο πιστοποιητικά υψηλού επιπέδου σε κάποιο πρόσωπο που κακόβουλα δήλωσε πως είναι υπάλληλος της Microsoft.

# Βιβλιογραφία


- Simon Singh, “The Code Book: The Secret History of Codes and Code-breaking”
- Fred Piper and Sean Murphy, “Cryptography: A Very Short Introduction”
- Bruce Schneier, “Applied Cryptography”
- David Kahn, “The Codebreakers”