



Κρυπτογραφία

Υπ. Δρ. Κωνσταντίνος Παπαπαναγιώτου
conpap@di.uoa.gr

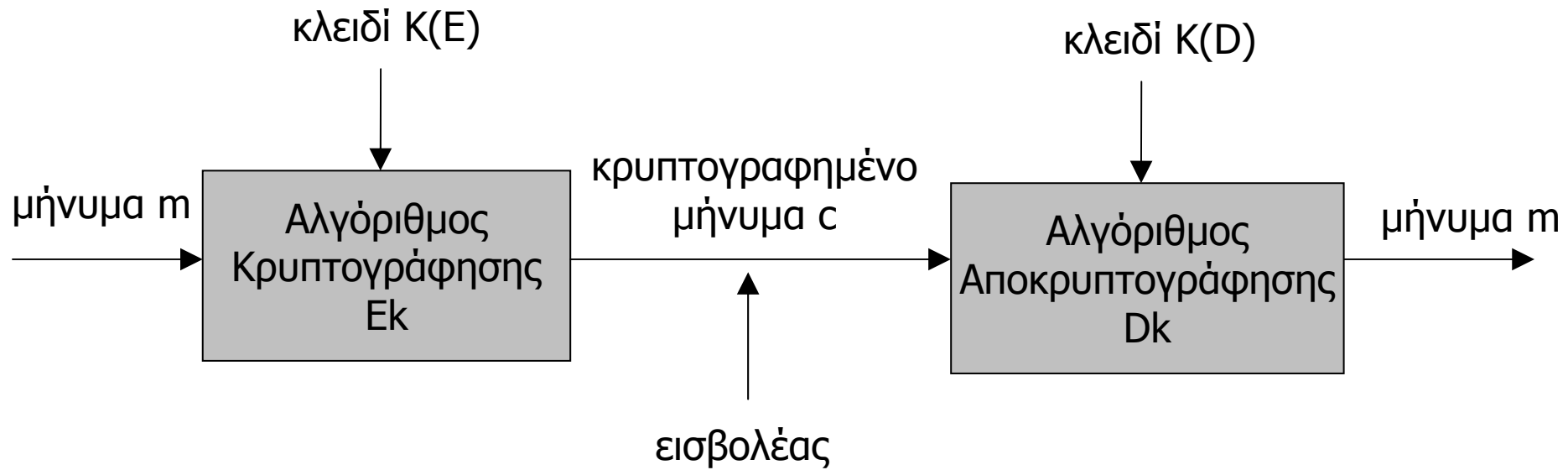


Κρυπτογραφία

- 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 D_k από το c , ακόμη και αν είναι γνωστό το m
- Ακεραιότητα
- Αυθεντικότητα
 - Πρέπει να είναι υπολογιστικά ανέφικτο να προσδιοριστεί το E_k από το c , ακόμη και αν είναι γνωστό το m
 - Πρέπει να είναι υπολογιστικά ανέφικτο να βρεθεί ένα c' , τέτοιο ώστε το $D_k(c')$ να είναι το ίδιο μη κρυπτογραφημένο μήνυμα
- Μη αποποίηση
- Μελλοντικά: Μυστικότητα, Ανωνυμία

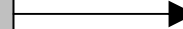
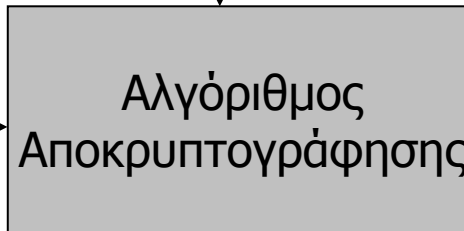
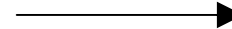


Η άποψη του εισβολέα

Άγνωστο
κλειδί $K(D)$



Ξέρει το
κρυπτογραφημένο
μήνυμα c



Θέλει το
αρχικό
μήνυμα m



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



Κρυπτανάλυση – Είδη επιθέσεων

- Μόνο βάσει κρυπτογραφημένου κειμένου
 - Ο επιτιθέμενος γνωρίζει μόνο το κρυπτογραφημένο κείμενο και προσπαθεί να βρει το μη κρυπτογραφημένο, χωρίς να έχει καμία πρότερη γνώση του τελευταίου. Η αντοχή ενός κρυπτογραφικού κώδικα σε αυτόν τον τύπο επίθεσης είναι το βασικότερο χαρακτηριστικό της ποιότητάς του
- Βάσει γνωστού μη κρυπτογραφημένου κειμένου
 - Ο επιτιθέμενος γνωρίζει το μη κρυπτογραφημένο κείμενο καθώς και το αντίστοιχο κρυπτογραφημένο (Το συγκεκριμένο μήνυμα θεωρείται ότι έχει «σπάσει»)
 - Σε μερικά συστήματα, η γνώση ενός και μόνου ζεύγους (*μη κρυπτογραφημένο κείμενο, κρυπτογραφημένο κείμενο*) επαρκεί για να απωλεσθεί όλη η ασφάλεια του συστήματος (ανεπιθύμητο)
 - Σημείο εκκίνησης όταν η μηχανή κρυπτογράφησης είναι διαθέσιμη στον επιτιθέμενο



Κρυπτανάλυση – Είδη επιθέσεων

- *Επιλεγμένο μη κρυπτογραφημένο κείμενο.*
 - Στην επίθεση αυτή ο επιτιθέμενος μπορεί να βρει το κρυπτογραφημένο κείμενο που αντιστοιχεί σε ένα μη κρυπτογραφημένο κείμενο που αυτός επιλέγει
- *Επιλεγμένο κρυπτογραφημένο κείμενο*
 - Ο επιτιθέμενος μπορεί να επιλέξει όποιο κρυπτογραφημένο κείμενο επιθυμεί και να υπολογίσει το αντίστοιχο μη κρυπτογραφημένο κείμενο. Ο τύπος αυτός επίθεσης μπορεί να απαντηθεί σε συστήματα δημόσιου κλειδιού όπου μπορεί να αποκαλυφθεί το ιδιωτικό κλειδί
- *Προσαρμοζόμενο επιλεγμένο μη κρυπτογραφημένο κείμενο*
 - Ο επιτιθέμενος μπορεί να προσδιορίσει το κρυπτογραφημένο κείμενο για επιλεγμένα μη κρυπτογραφημένα κείμενα σε μία επαναληπτική διαδικασία, βάσει των προηγούμενων αποτελεσμάτων



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 ΞΞΞΑΣΠΡΗ
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_j ο υπ' αριθμόν j χαρακτήρας του κλειδιού, ο υπ' αριθμόν i χαρακτήρας του κρυπτογραφημένου μηνύματος είναι η καταχώρηση στη θέση (K_j, M_i) του πίνακα



Πολυαλφαβητική Αντικατάσταση

- Παράδειγμα:

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

ΑΣΠΡΗ ΠΕΤΡΑ ΞΞΑΣΠΡΗ ← Plaintext

ABBA ABBA ABBA ← 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

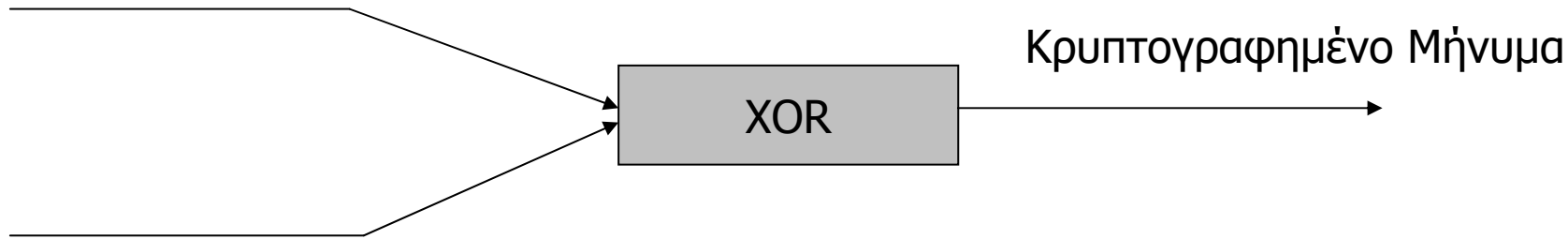
- Δύο Πιθανά Μηνύματα:

ΠΟΥΛΑ ή ΑΓΟΡΑΣΕ

- 50% Πιθανότητα «Μαντέματος»
- Κακή πρακτική: Απλή Αντικατάσταση
- Καλύτερη δυνατή πρακτική:
 - Κλειδί k_1 $E(k_1)(\text{ΠΟΥΛΑ})=0$ $E(k_1)(\text{ΑΓΟΡΑΣΕ})=1$
 - Κλειδί k_2 $E(k_2)(\text{ΠΟΥΛΑ})=1$ $E(k_2)(\text{ΑΓΟΡΑΣΕ})=0$

Μέθοδος Vernam (One Time Pad)

Κλειδί: $k_1k_2k_3\dots k_n$



Μήνυμα: $m_1m_2m_3\dots m_n$

- 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



Κρυπτογράφηση με μεταθέσεις

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



Απλή Μετάθεση

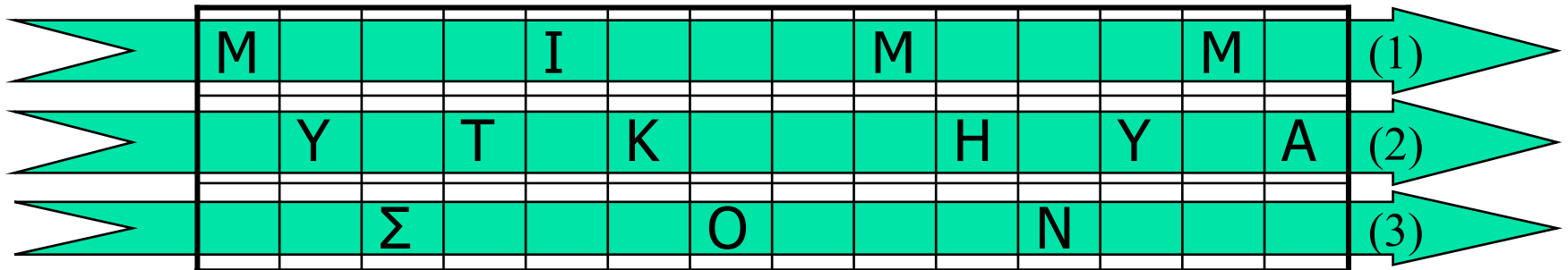
- Το μήνυμα m κατατμείται σε μπλοκ και κάθε μπλοκ αναδιατάσσεται βάσει κάποιου σχήματος
- Παράδειγμα
 - Κλειδί = (25413)

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

«Συρματοπλέγμα»



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



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

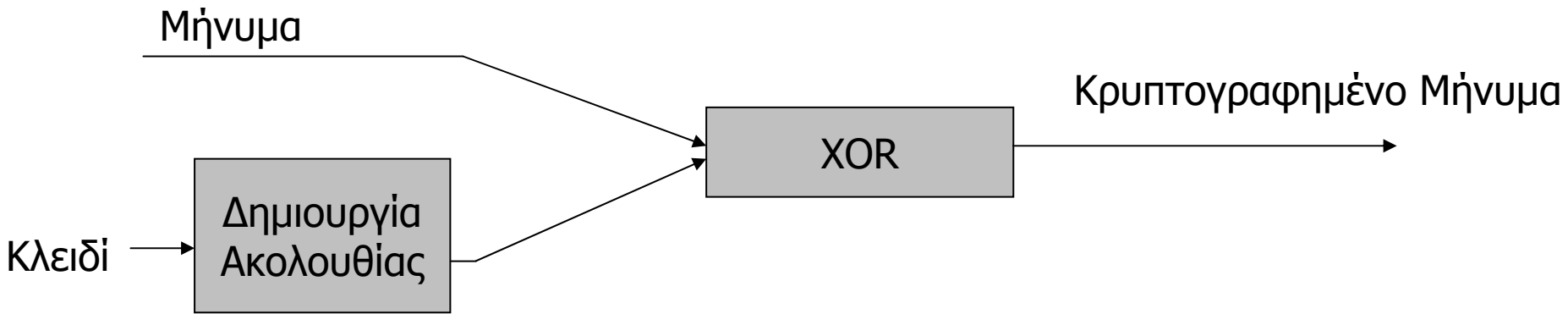
- ΑΣΠΡΗ ΠΕΤΡΑ ΞΕΞΑΣΠΡΗ

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
- Πλεονεκτήματα:
 - Ταχύτητα
 - Ευκολία Υλοποίησης
- Μειονεκτήματα:
 - Ακολουθία κλειδιού



Κρυπτογράφηση κατά μπλοκ

- Το μήνυμα M διασπάται σε διαδοχικά μπλοκ M_1, M_2, \dots
- Το κάθε μπλοκ κρυπτογραφείται με το ίδιο κλειδί K
- Τελικό μήνυμα: $E_k(M_1)E_k(M_2)\dots$
- 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

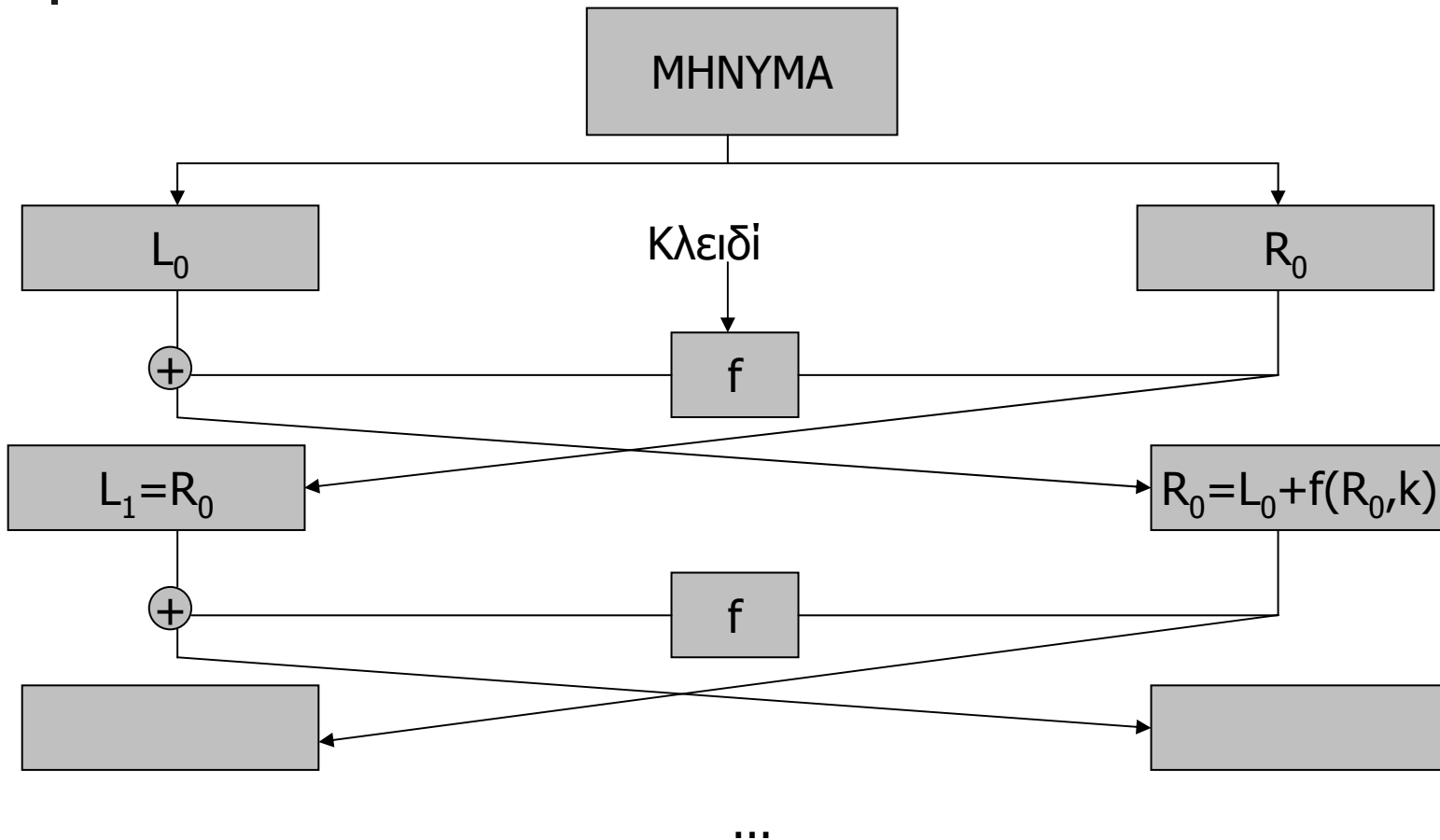
- Το κάθε μπλοκ δεν είναι αυτόνομο, αλλά περιλαμβάνει bits από τα προηγούμενα (κρυπτογραφημένα ή μη)
 - Μειώνονται οι διαθέσιμες θέσεις πληροφορίας σε κάθε μπλοκ
 - Αναιρείται το πλεονέκτημα της ανοχής σε σφάλματα
 - Αυξάνεται όμως η ασφάλεια
- Παράδειγμα:
 - $C_i = E_k(M_i \text{ XOR } C_{i-1})$
 -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





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
 - $k=(k_1,k_2)$
 - $E_k(m)=E_{k_1}(E_{k_2}(m))$
 - Ασθενή κλειδιά: $E_k(E_k(m))=m$
 - Ημιασθενή κλειδιά: $E_{k_1}(E_{k_2}(m))=m$
 - Ευάλωτος σε επιθέσεις «συνάντησης στη μέση»
- Τριπλός DES
 - $E_k(m)=E_{k_1}(D_{k_2}(E_{k_1}(m)))$
 - Με 3 κλειδιά:
 - $E_k(m)=E_{k_1}(D_{k_2}(E_{k_3}(m)))$



Αλγόριθμος AES

- Advanced Encryption Standard
- 1998: Διάδοχος του DES.
5 υποψήφιοι
- 2000: Τελικός νικητής: Rijndael
 - Μπλοκ 128 bit
 - Κλειδιά 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

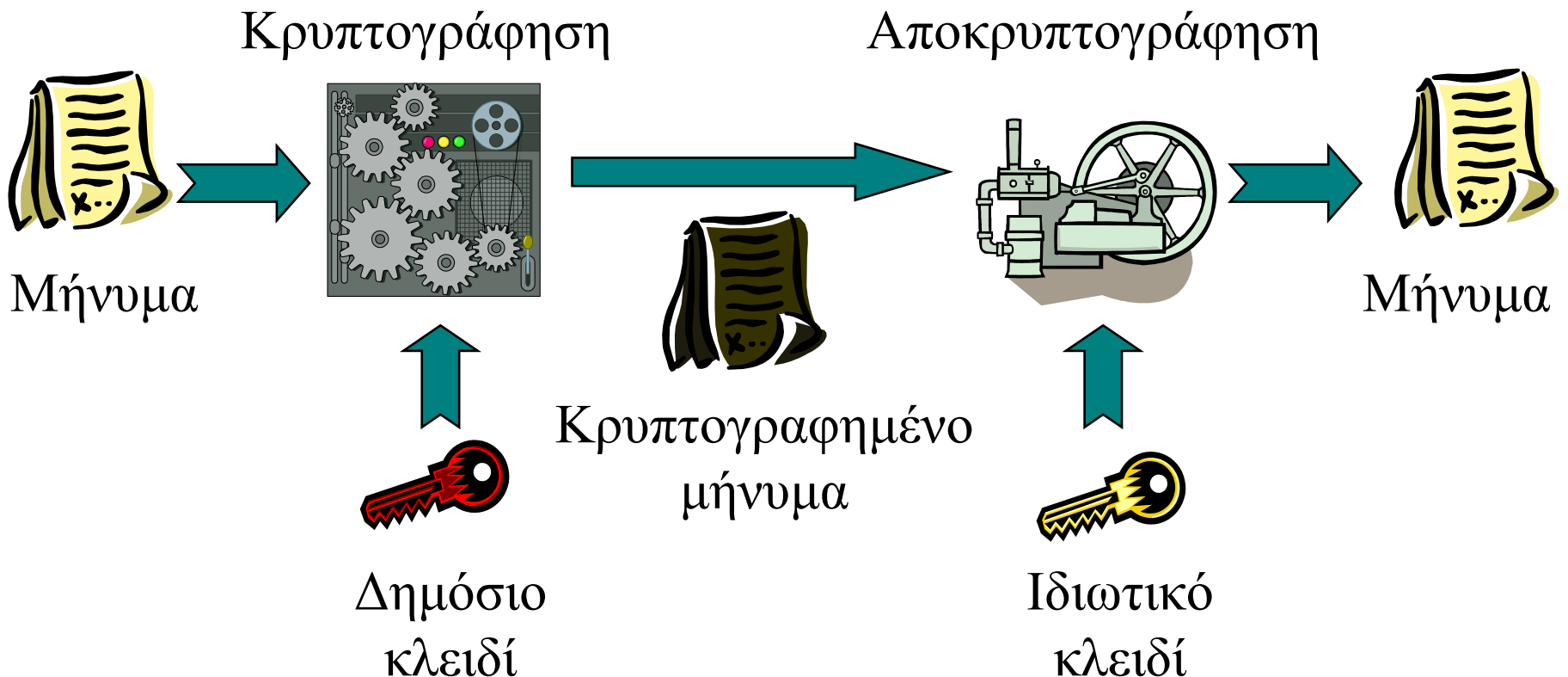


Ασύμμετρη Κρυπτογραφία

- Τοποθετώ ένα μήνυμα σε μια βαλίτσα
- Κλειδώνω τη βαλίτσα με ένα λουκέτο και κρατάω το κλειδί
- Στέλνω τη βαλίτσα σε κάποιον
- Αυτός βάζει ένα δεύτερο δικό του λουκέτο, το κλειδώνει, κρατάει το κλειδί και μου επιστρέφει τη βαλίτσα
- Ξεκλειδώνω το δικό μου λουκέτο και ξαναστέλνω πίσω τη βαλίτσα
- Ξεκλειδώνει το δικό του λουκέτο και διαβάζει το μήνυμα

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



RSA: Επιλογή Κλειδιών

- Επιλέγουμε δύο μεγάλους πρώτους αριθμούς p και q
- Υπολογίζουμε το $n = p * q$
- Υπολογίζουμε το $\varphi(n) = (p - 1) * (q - 1)$
- Επιλέγουμε έναν ακέραιο e με $3 \leq e \leq \varphi(n)$ τέτοιο ώστε να μην έχει κοινό παράγοντα με το $\varphi(n)$
- Αν M το αρχικό μήνυμα κρυπτογράφηση σύμφωνα με την εξίσωση $C = M^e \bmod n$
- Οι αριθμοί p και q παραμένουν κρυφοί



Αλγόριθμος RSA

- Εφόσον e και $\varphi(n)$ πρώτοι μεταξύ τους, θα υπάρχει ακέραιος d τέτοιος, ώστε: $d * e = 1 \pmod{\varphi(n)}$
- Είναι αδύνατο να υπολογίσουμε τον d αν δεν ξέρουμε τα p και q
- Για να αποκρυπτογραφήσουμε χρησιμοποιούμε την εξίσωση: $M = C^d \pmod{n}$
- Δημόσιο κλειδί: (e,n) , Ιδιωτικό κλειδί: (d,n)

- Παράδειγμα:
 - $p = 251, q = 269, n = p * q = 67519, \varphi(n) = 67000$
 - $e = 50253, d = \text{inv}(e) \pmod{67000} = 27917$
 - Με $n = 67619$ μπορούμε να κωδικοποιήσουμε αριθμούς από 0 έως 67618

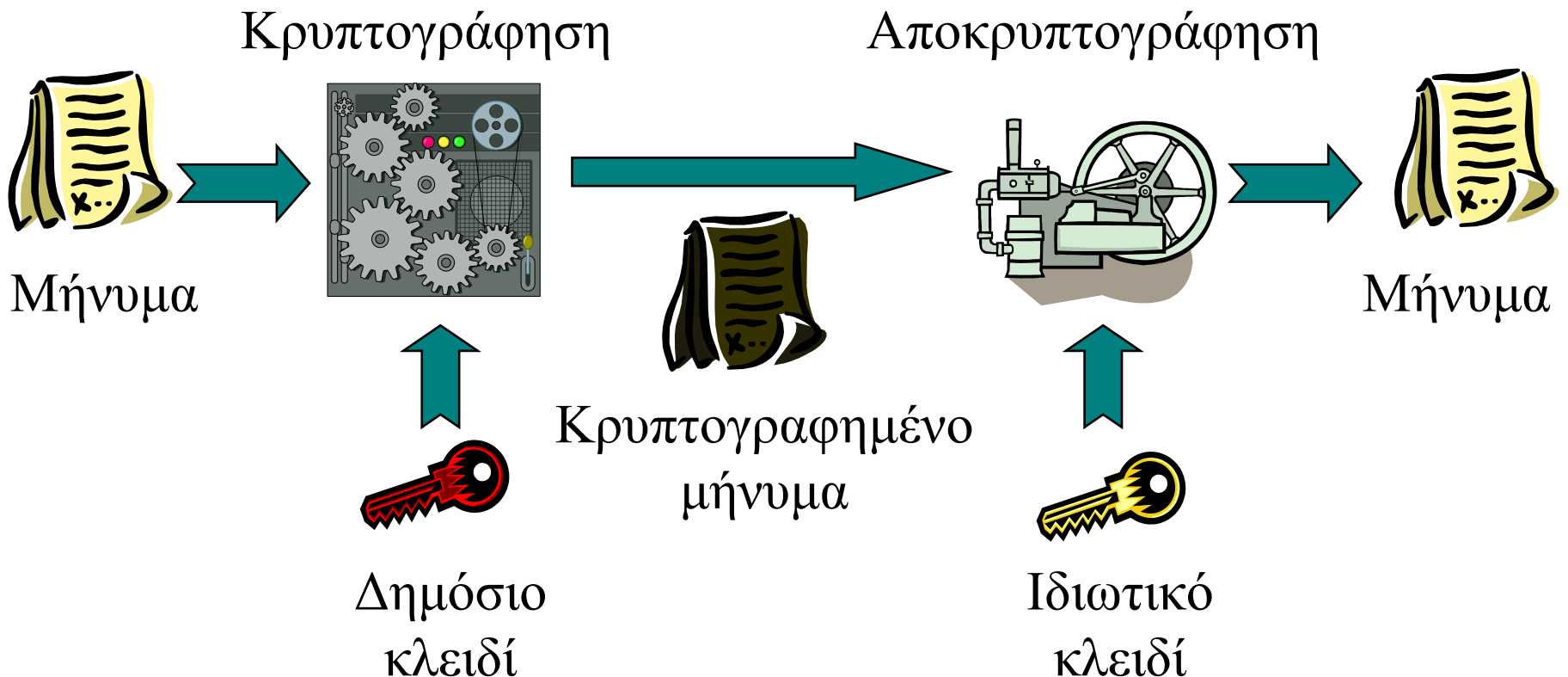


Αλγόριθμος Diffie-Hellman

- 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: $a^{r_A} \pmod{p}$
- Ομοίως ο χρήστης B διαλέγει τυχαία έναν αριθμό r_B και στέλνει στον A : $a^{r_B} \pmod{p}$
- Και οι δύο χρήστες υπολογίζουν το μυστικό κλειδί: $a^{r_A r_B} \pmod{p}$
- Επίθεση ενδιάμεσου ανθρώπου (man in the middle attack)

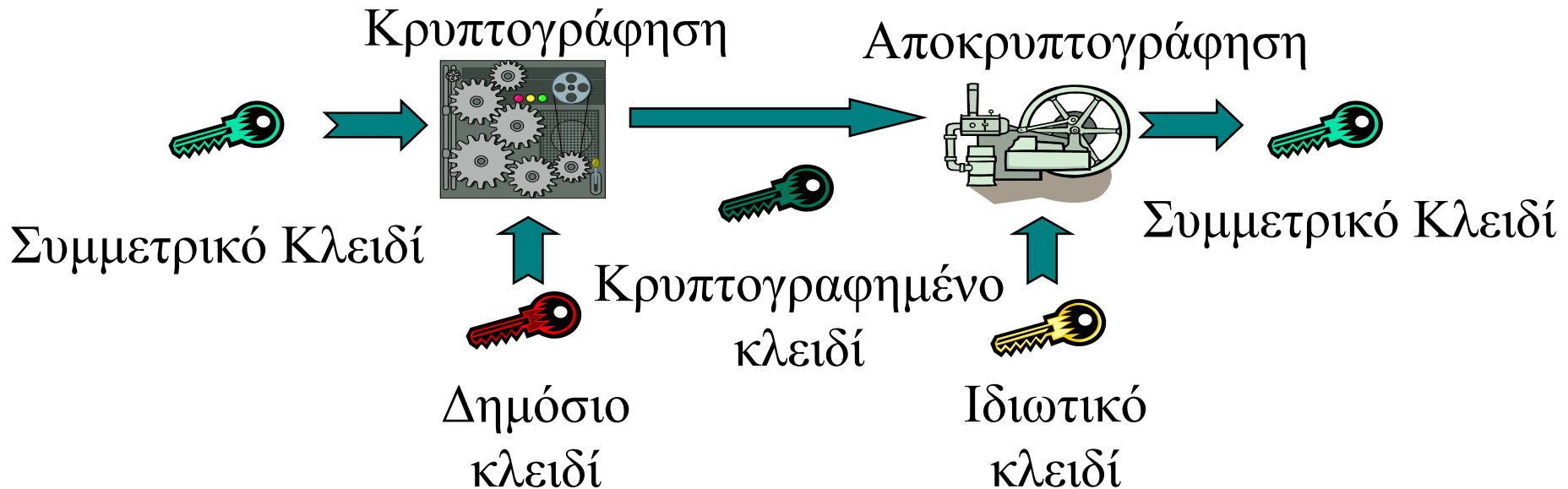
Αποστολή Μηνύματος

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



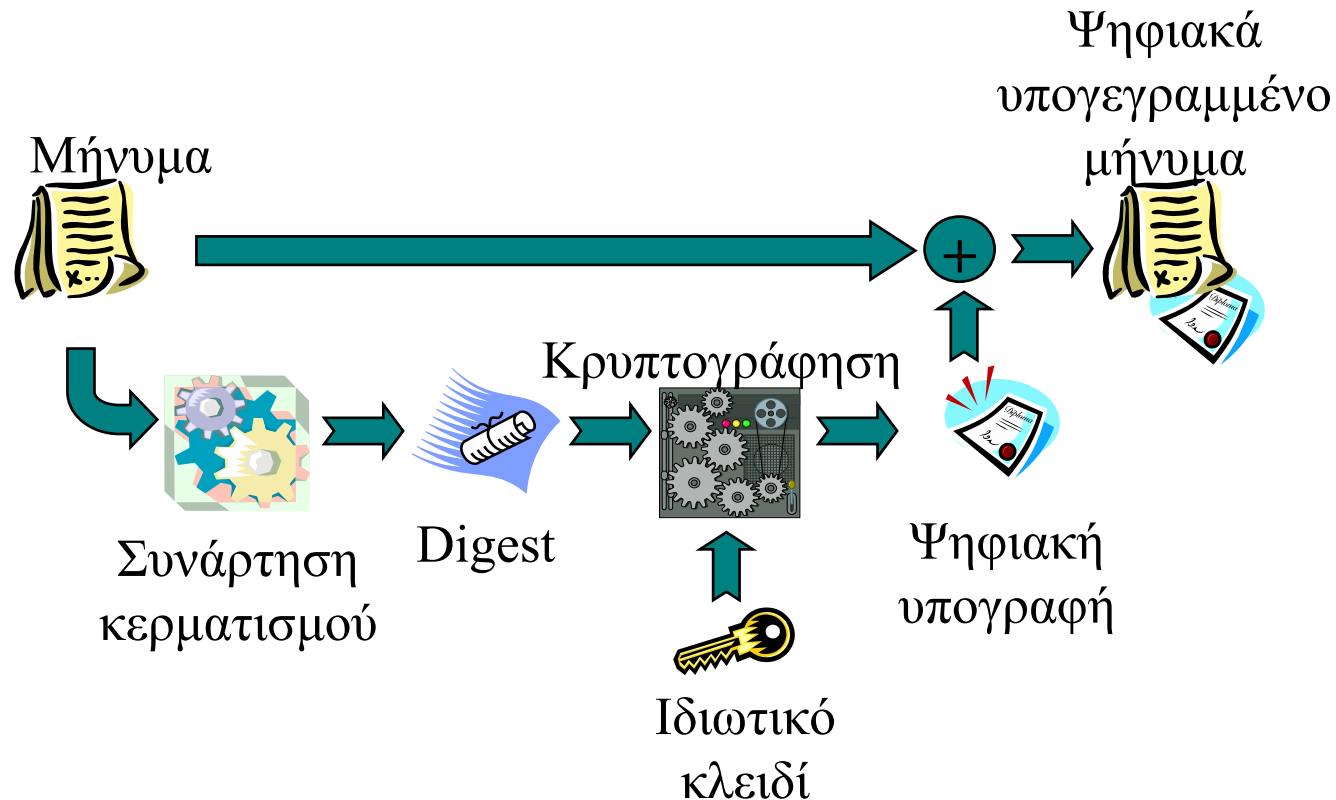
Ασύμμετρη εναντίον Συμμετρικής

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



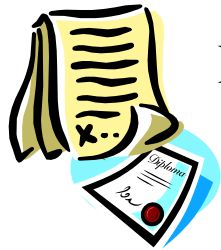
Ψηφιακές Υπογραφές - Αποστολή

- Στόχος: Αυθεντικότητα και Ακεραιότητα



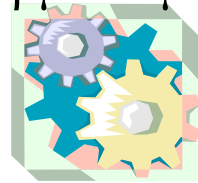
Ψηφιακές Υπογραφές - Παραλαβή

Ψηφιακά
υπογεγραμμένο
μήνυμα



Μήνυμα

Συνάρτηση
κερματισμού

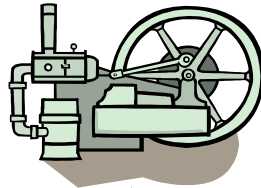


Digest



Ναι, Εντάξει

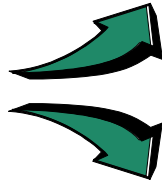
Αποκρυπτογράφηση



Digest'



Δημόσιο
κλειδί



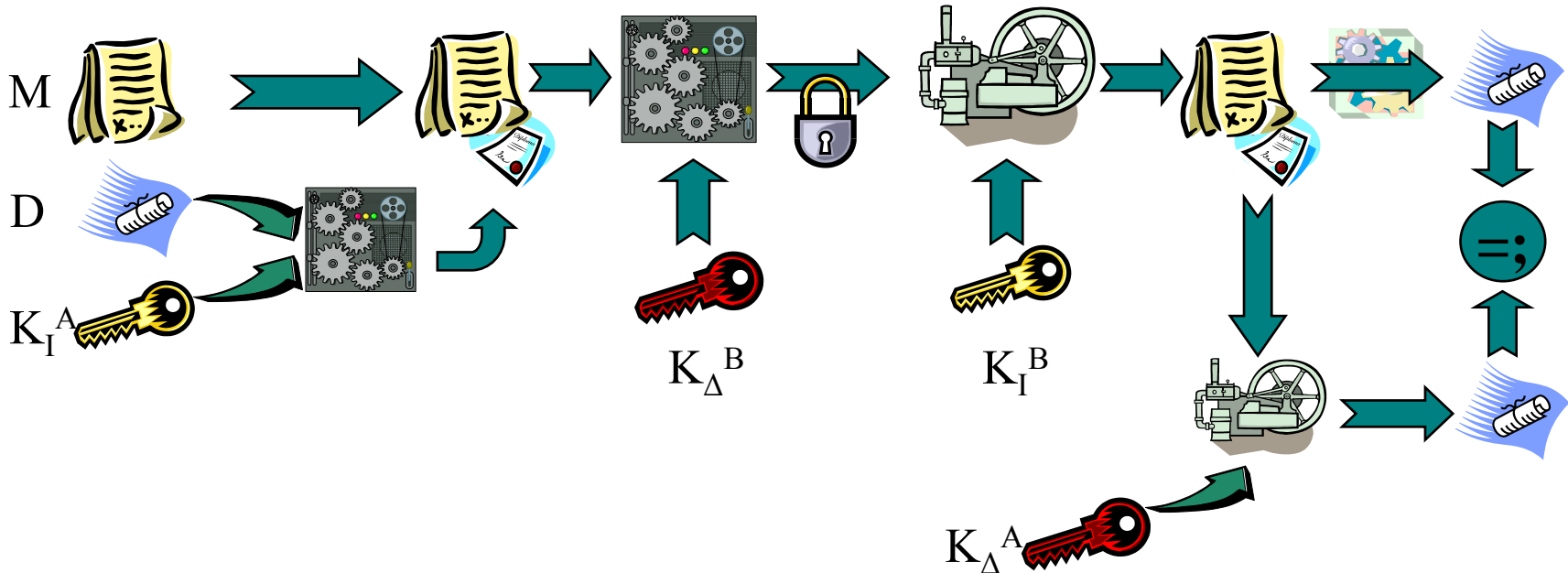
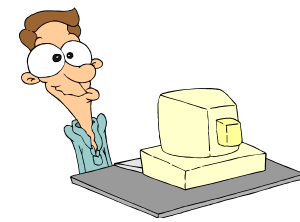


Ψηφιακές Υπογραφές

- 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 A
 - 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





Πραγματικές Υπογραφές

- Πραγματική Υπογραφή:
 - «Ιδιαίτερη» για τον καθένα (μοναδική)
 - Ίδια σε κάθε κείμενο
 - Φυσική τοποθέτηση στο κείμενο
 - Πλαστογραφείται εύκολα;
- 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)



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 δημόσιο της κλειδί



Διασικασία Πιστοποίησης

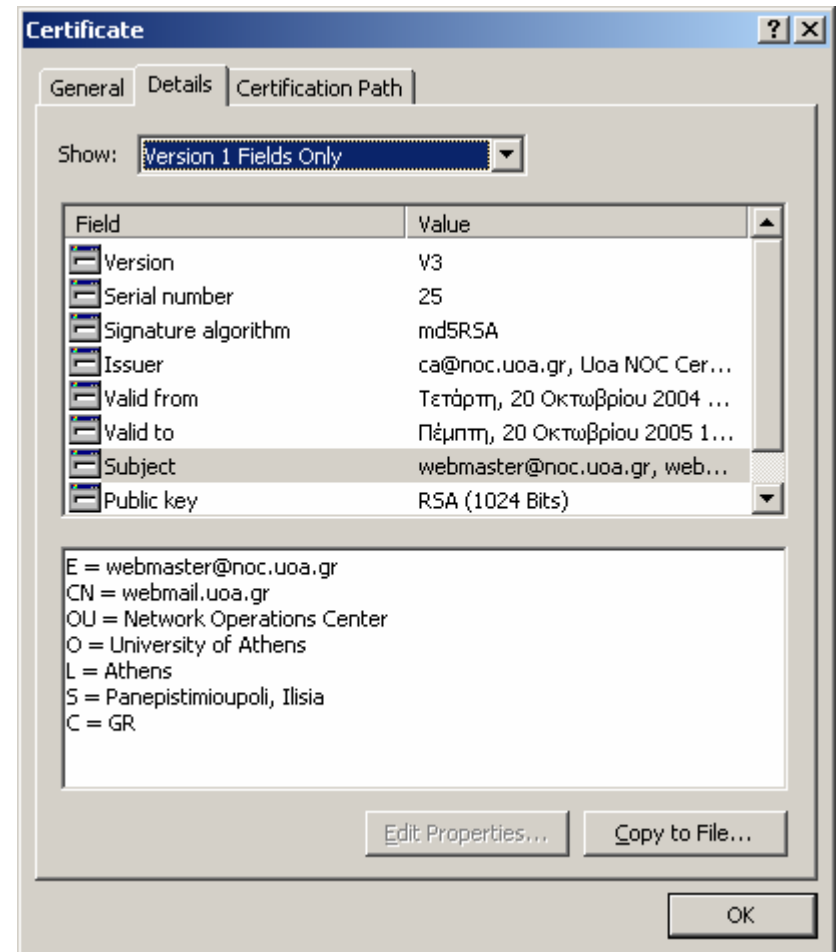
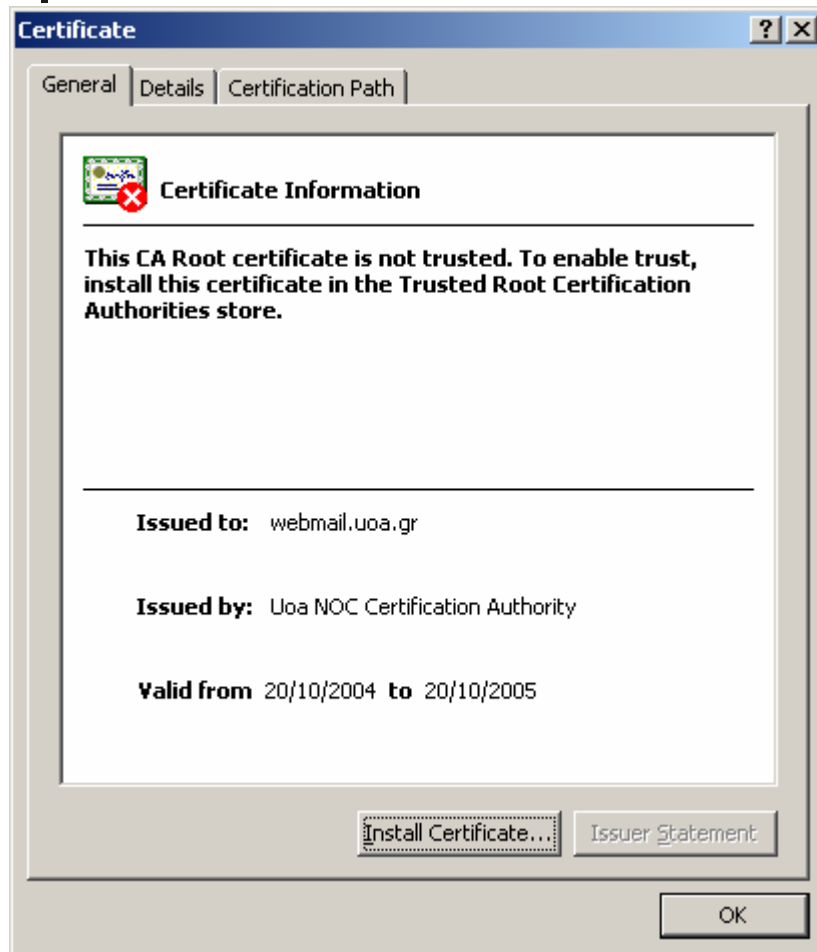
- Δημιουργείται το ζεύγος κλειδιών της ΑΔΠ
- Δημιουργείται το ζεύγος κλειδιών του χρήστη
- Ζητείται ένα πιστοποιητικό για τον χρήστη
- Η ταυτότητα του χρήστη ελέγχεται
- Επικυρώνεται το ζεύγος κλειδιών του χρήστη
- Εκδίδεται ένα πιστοποιητικό για το χρήστη
- Ο χρήστης ελέγχει την ορθότητα του πιστοποιητικού



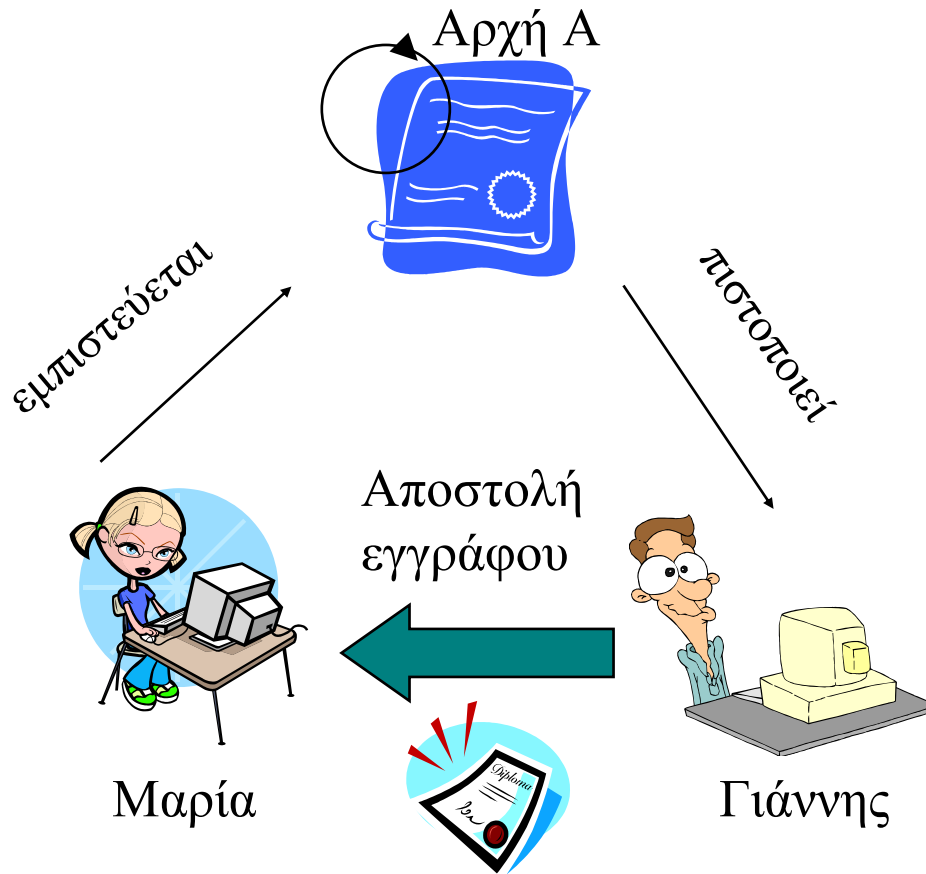
Ψηφιακά Πιστοποιητικά

- 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, εργασία, 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

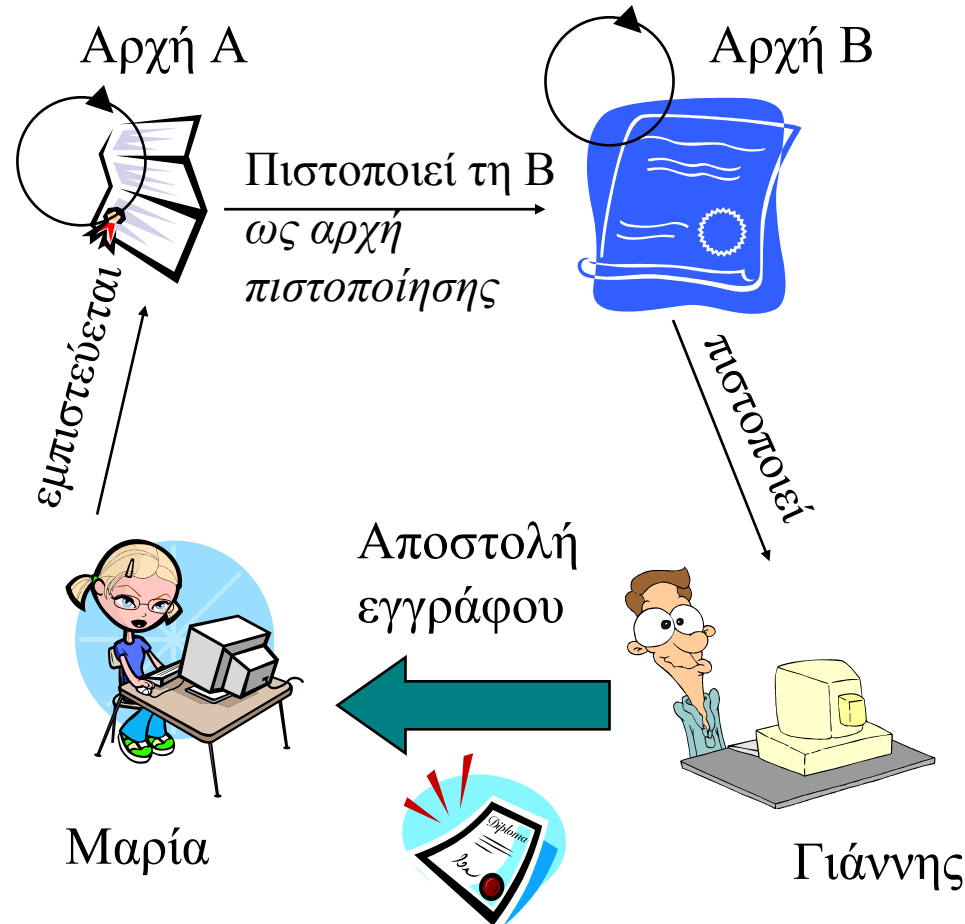




Ομότιμη διασταυρούμενη πιστοποίηση

- Οι αρχές πιστοποίησης εγκαθιστούν μεταξύ τους μονόδρομες ή αμφίδρομες σχέσεις εμπιστοσύνης σε ομότιμη βάση
 - Η αρχή A πιστοποιεί την αρχή B 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



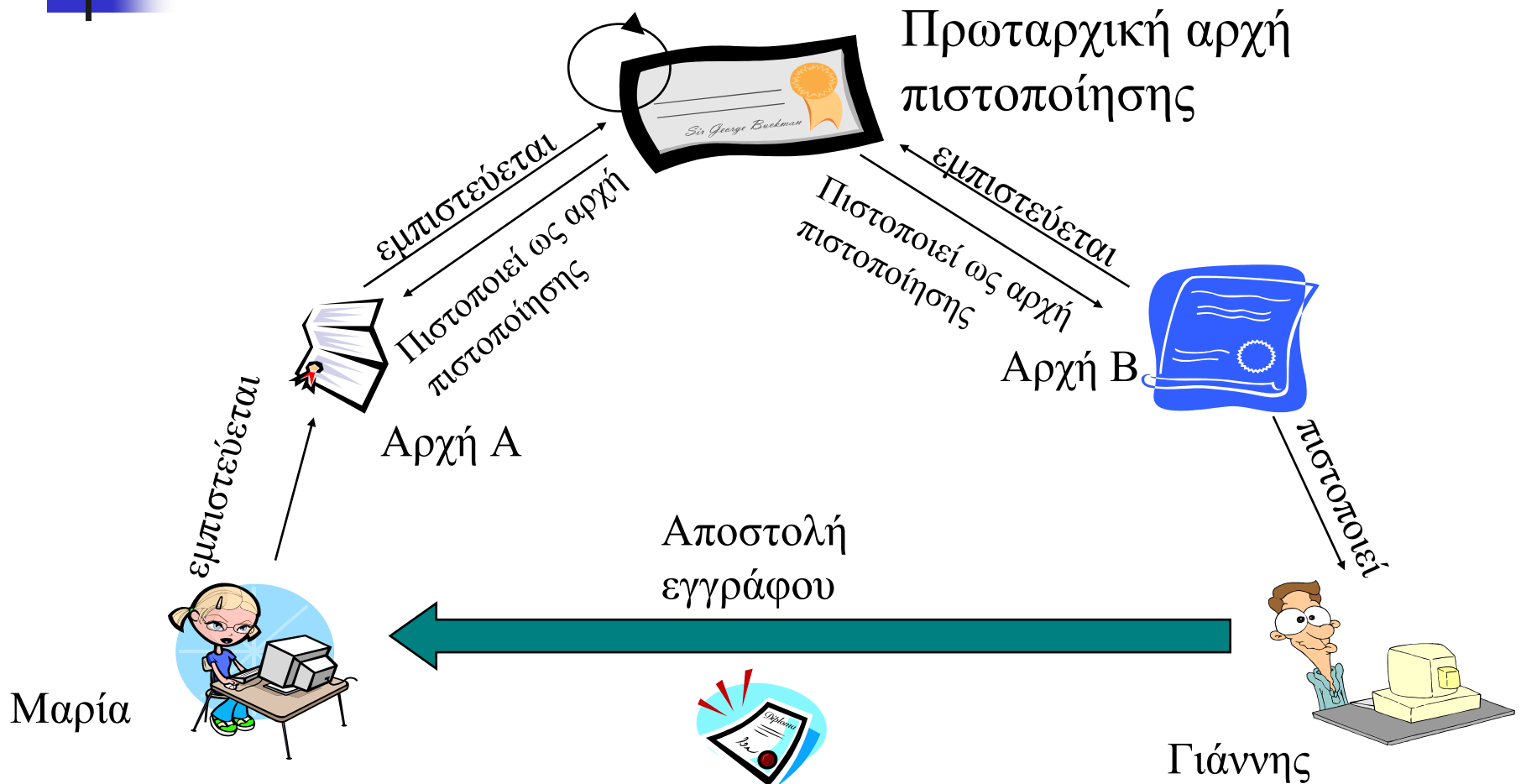
Αλυσίδα εμπιστοσύνης: Μαρία → Αρχή Α → Αρχή Β → Γιάννης



Ιεραρχική διασταυρούμενη πιστοποίηση

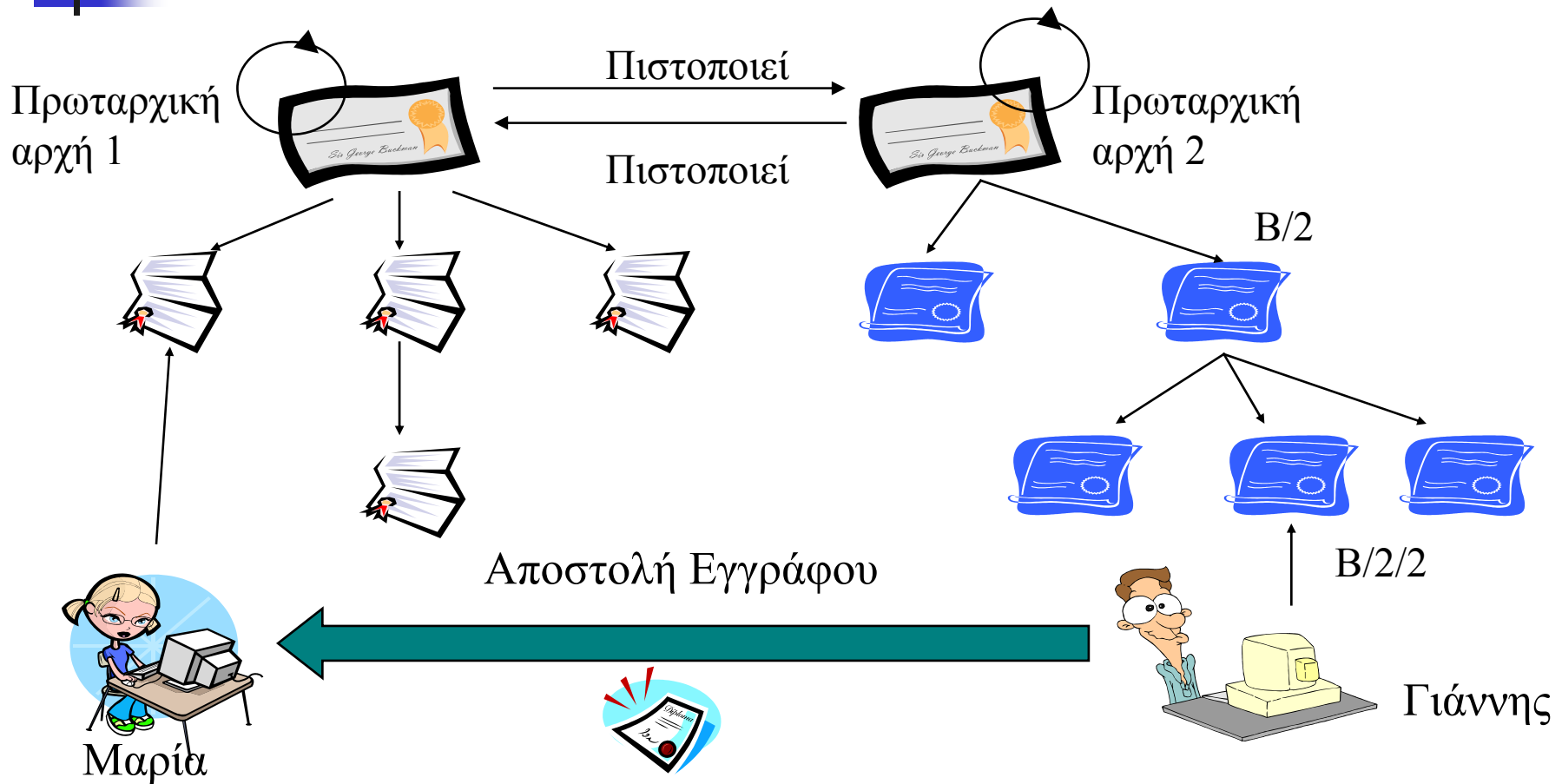
- Οι αρχές πιστοποίησης οργανώνονται σε ιεραρχίες, με κάθε μία να πιστοποιεί τις υφιστάμενές της ως αρχές πιστοποίησης
- Εδώ κάθε χρήστης εμπιστεύεται την *πρωταρχική αρχή πιστοποίησης*, στη ρίζα της ιεραρχίας
 - τα πιστοποιητικά εκδίδονται από τις αρχές χαμηλότερα στην ιεραρχία
 - Οι χρήστες εμπιστεύονται 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 A → Πρωτ. Αρχή → Αρχή B → Γιάννης

Υβριδικό μοντέλο



Αλυσίδα εμπιστοσύνης: Μαρία → Πρωτ. Αρχή 1 → Πρωτ. Αρχή 2 → B/2 → B/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 υπογράψει 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.



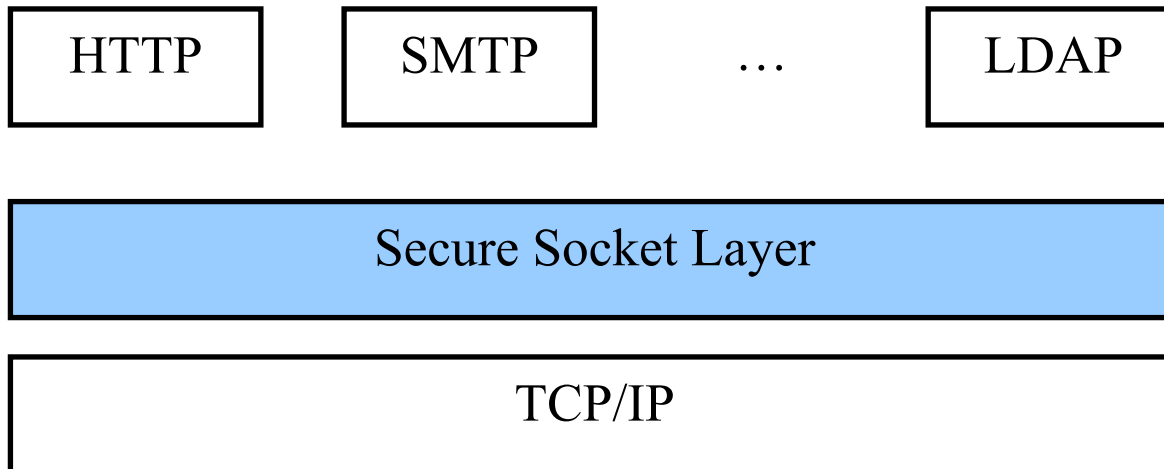
SSL/TLS

- SSL = Secure Sockets Layer
 - v1: δεν εκδόθηκε
 - v2: χρήσιμη αλλά με λάθη
 - v3
- TLS = Transport Layer Security
 - TLS 1.0 = SSL 3.0 με μικρές διορθώσεις
 - RFC 2246
 - <http://www.openssl.org>
- Χρησιμοποιείται ευρύτατα στους φυλλομετρητές για εφαρμογές ηλεκτρονικού εμπορίου



Πρωτόκολλο SSL/TLS

- Το πρωτόκολλο SSL παρεμβάλλεται μεταξύ του TCP/IP και του επιπέδου εφαρμογής προκειμένου να:
 - πιστοποιεί τον εξυπηρέτη στον εξυπηρετούμενο
 - πιστοποιεί τον εξυπηρετούμενο στον εξυπηρέτη
 - κρυπτογραφεί την επικοινωνία

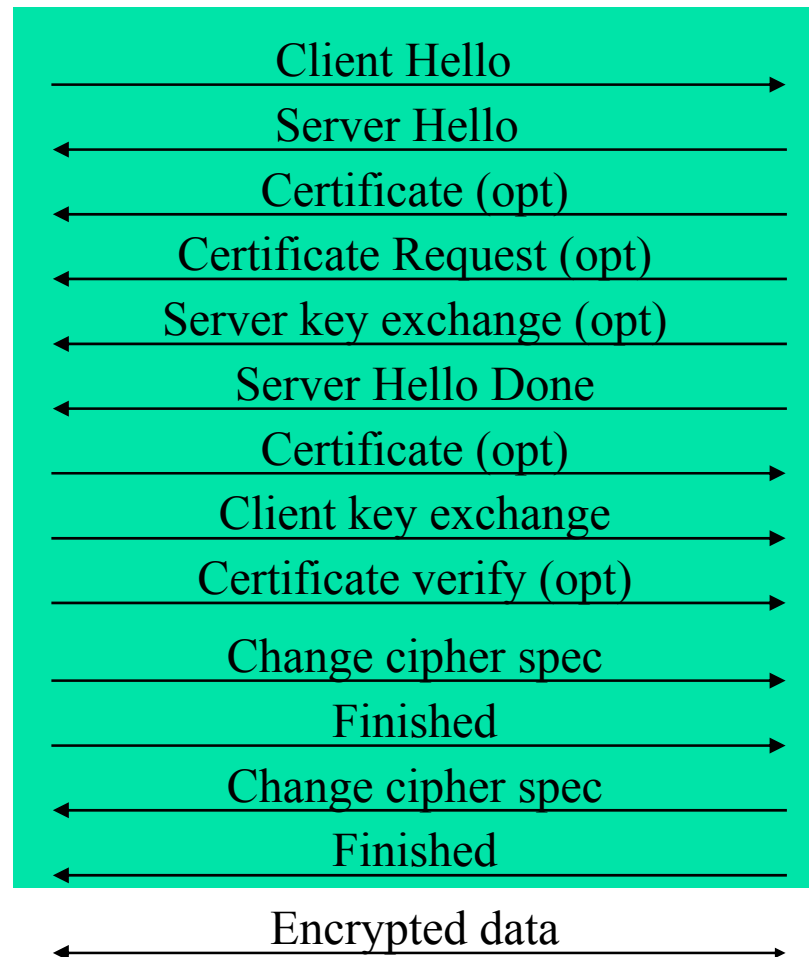




Ανατομία του πρωτοκόλλου SSL

- Δύο επί μέρους πρωτόκολλα
 - χειραψία SSL
 - ανταλλαγή δεδομένων SSL
- Στόχοι χειραψίας
 - Να πιστοποιηθεί ο εξυπηρέτης στον εξυπηρετούμενο
 - Συμφωνία πάνω στους αλγόριθμους κρυπτογραφίας που θα χρησιμοποιηθούν για την επικοινωνία
 - Προαιρετικά, πιστοποίηση εξυπηρετούμενου στον εξυπηρέτη
 - Δημιουργία «διαμοιραζόμενων μυστικών» μέσω τεχνικών κρυπτογραφίας δημόσιου κλειδιού για την κρυπτογράφηση της επικοινωνίας
 - Εγκαθίδρυση του κρυπτογραφημένου διαύλου επικοινωνίας

Χειραψία πρωτοκόλλου SSL





Βήματα Χειραψίας SSL (1)

- *Client Hello* – αποστέλλονται στον εξυπηρέτη:
 - αριθμός έκδοσης SSL του εξυπηρετούμενου
 - λίστα υποστηριζόμενων αλγόριθμων κρυπτογράφησης και αντιστοιχών μεγεθών κλειδιών
 - ταυτότητα της συνόδου κ.τ.λ.
- *Server Hello* – αποστέλλονται στον εξυπηρετούμενο
 - αριθμός έκδοσης SSL του εξυπηρέτη
 - ο πιο κατάλληλος αλγόριθμος κρυπτογράφησης
 - το επιλεγμένο μήκος κλειδιών



Βήματα Χειραψίας SSL (2)

- *Certificate* - (προαιρετικό, αν απαιτείται πιστοποίηση του εξυπηρέτη)
 - ο εξυπηρέτης αποστέλλει το πιστοποιητικό του στον εξυπηρετούμενο. Το πιστοποιητικό περιέχει το δημόσιο κλειδί του εξυπηρέτη. Ο εξυπηρετούμενος διακριβώνει την ταυτότητα του εξυπηρέτη.
- *Certificate request* - (προαιρετικό, αν απαιτείται πιστοποίηση του εξυπηρετούμενου)
 - ο εξυπηρέτης αποστέλλει ένα μήνυμα με το οποίο ζητά το πιστοποιητικό του εξυπηρετούμενου.



Βήματα Χειραψίας SSL (3)

- *Server key exchange* - (προαιρετικό, αν το πιστοποιητικό του εξυπηρέτη δεν είναι επαρκές για την ανταλλαγή κλειδιών που θα ακολουθήσει)
- *Server Hello Done*
 - Ο εξυπηρέτης υποδεικνύει ότι έχει τελειώσει την προκαταρκτική φάση εγκαθίδρυσης της συνόδου
- *Certificate* (προαιρετικό, αν ο εξυπηρέτης έχει αποστείλει μήνυμα certificate request)
 - ο εξυπηρετούμενος αποστέλλει το πιστοποιητικό του, ο εξυπηρέτης το επαληθεύει



Βήματα Χειραψίας SSL (4)

- *Client key exchange*
 - ο εξυπηρετούμενος δημιουργεί το προκαταρκτικό μυστικό (premaster secret) για τη συγκεκριμένη σύνοδο, το κρυπτογραφεί με το δημόσιο κλειδί του εξυπηρέτη και το αποστέλλει σ' αυτόν.
- *Certificate verify* (προαιρετικό, αν ο εξυπηρέτης έχει ζητήσει το πιστοποιητικό του εξυπηρετούμενου)
 - το μήνυμα αυτό επιτρέπει στον εξυπηρέτη να ολοκληρώσει τη διαδικασία επαλήθευσης του πιστοποιητικού



Βήματα Χειραψίας SSL (5)

- *Change cipher spec*
 - Ο εξυπηρετούμενος είναι έτοιμος να μεταβεί σε ασφαλή επικοινωνία
- *Finished*
 - Ο εξυπηρετούμενος τελείωσε το δικό του τμήμα της χειραψίας
- *Change cipher spec*
 - Ο εξυπηρέτης είναι έτοιμος να μεταβεί σε ασφαλή επικοινωνία
- *Finished*
 - Ο εξυπηρέτης έχει τελειώσει το δικό του τμήμα της χειραψίας



Ανταλλαγή δεδομένων στο SSL

- Με συμμετρικό αλγόριθμο κρυπτογραφίας
- Το κλειδί παράγεται με βάση το *προκαταρκτικό μυστικό*
- Ο αλγόριθμος παραγωγής εξαρτάται από τον συμμετρικό αλγόριθμο κρυπτογραφίας που θα χρησιμοποιηθεί και το μήκος των κλειδιών

SessionKey = genKey(premasterSecret, cipher, keyLen)



Σε ποιο σημείο κρυπτογραφούμε;

- Κρυπτογράφηση από άκρο σε άκρο
 - Απαραίτητο κλειδί για κάθε επικοινωνιακό εταίρο
 - Πιθανή επίθεση με ανάλυση κυκλοφορίας
- Κρυπτογράφηση σε επικοινωνιακό κανάλι
 - Κάθε κόμβος ξέρει μόνο τους γείτονές του
 - Η πληροφορία είναι εκτεθειμένη σε κάθε ενδιάμεσο επικοινωνιακό κόμβο
 - Απαιτείται πρόσβαση σε όλα τα ενδιάμεσα κανάλια
- Συνδυασμός των δύο κρυπτογραφήσεων