

Ε Κ Δ Ο Σ Ε Ι Σ Κ Λ Ε Ι Δ Α Ρ Ι Θ Μ Ο Σ

ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ

ΑΡΧΕΣ ΚΑΙ ΠΡΑΚΤΙΚΕΣ

3η αμερικανική έκδοση



William Stallings • Lawrie Brown



Κεφάλαιο 2

Κρυπτογραφικά εργαλεία

Συμμετρική κρυπτογράφηση

- Καθολικά αποδεκτή τεχνική που χρησιμοποιείται για τη διαφύλαξη της εμπιστευτικότητας δεδομένων τα οποία μεταδίδονται ή αποθηκεύονται
- Γνωστή και ως συμβατική κρυπτογράφηση ή κρυπτογράφηση ενός κλειδιού
- Δύο απαιτήσεις για την ασφαλή χρήση της:
 - Χρειαζόμαστε έναν ισχυρό αλγόριθμο κρυπτογράφησης
 - Ο αποστολέας και ο παραλήπτης πρέπει να έχουν παραλάβει αντίγραφα του μυστικού κλειδιού με ασφαλή τρόπο και να το προστατεύουν συνεχώς

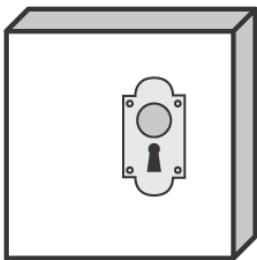


Κοινόχρηστο μυστικό κλειδί
για αποστολέα και παραλήπτη

Κοινόχρηστο μυστικό κλειδί
για αποστολέα και παραλήπτη



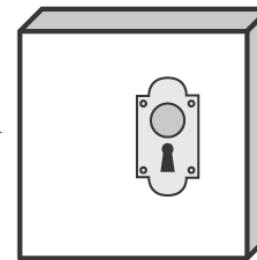
X



Απλό κείμενο
εισόδου

Αλγόριθμος κρυπτογράφησης
(π.χ. DES)

Μεταδιδόμενο
κρυπτοείμενο
 $Y = E[K, X]$



$X = D[K, Y]$



Απλό κείμενο
εξόδου

Εικόνα 2.1 Απλουστευμένο μοντέλο συμμετρικής κρυπτογράφησης

Προσβολή σχήματος συμμετρικής κρυπτογράφησης

Κρυπταναλυτικές επιθέσεις

- Βασίζονται στα εξής:
 - Φύση του αλγορίθμου
 - Κάποια γνώση των γενικών χαρακτηριστικών του απλού κειμένου
 - Κάποια δειγματοληπτικά ζεύγη απλού κειμένου-κρυπτοκειμένου
- Εκμεταλλεύονται τα χαρακτηριστικά του αλγορίθμου με στόχο να συνάγουν ένα συγκεκριμένο απλό κείμενο ή το μυστικό κλειδί που χρησιμοποιείται
 - Αν η έκβαση είναι επιτυχής, όλα τα προηγούμενα και τα μελλοντικά μηνύματα, των οποίων η κρυπτογράφηση βασίζεται στο συγκεκριμένο το κλειδί, είναι εκτεθειμένα

Επίθεση ωμής βίας

- Δοκιμή κάθε πιθανού κλειδιού σε κάποιο κρυπτοκειμένου κρυπτοκείμενο μέχρι να εξαχθεί μια κατανοητή «μετάφραση» σε απλό κείμενο
 - Κατά μέσο όρο απαιτείται η δοκιμή των μισών από όλα τα πιθανά κλειδιά μέχρι να έχουμε επιτυχές αποτέλεσμα



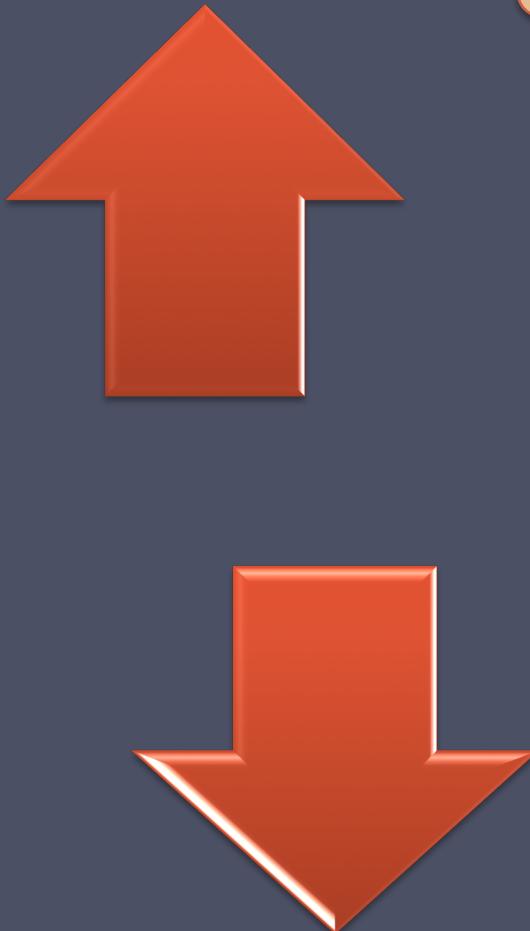
Πίνακας 2.1

Σύγκριση τριών διαδεδομένων αλγορίθμων συμμετρικής κρυπτογράφησης

	DES	Τριπλό DES	AES
Μέγεθος τμήματος απλού κειμένου (σε bit)	64	64	128
Μέγεθος τμήματος κρυπτοκειμένου (σε bit)	64	64	128
Μέγεθος κλειδιού (σε bit)	56	112 ή 168	128, 192, ή 256

DES = Πρότυπο Κρυπτογράφησης Δεδομένων
AES = Προηγμένο Πρότυπο Κρυπτογράφησης

Πρότυπο Κρυπτογράφησης Δεδομένων (DES)



- Το πιο διαδεδομένο σχήμα κρυπτογράφησης
- FIPS PUB 46
- Ένωστό ως Αλγόριθμος Κρυπτογράφησης Δεδομένων (Data Encryption Algorithm, DEA)
- Χρησιμοποιεί ένα τμήμα απλού κειμένου μήκους 64 bit και ένα κλειδί μήκους 56 bit για να παραγάγει ένα τμήμα κρυπτοκειμένου μήκους 64 bit
- Οι ανησυχίες για την ισχύ του αφορούν
 - Όντων ίδιο τον αλγόριθμο
 - Έχει μελετηθεί περισσότερο από όλους τους υπάρχοντες αλγορίθμους κρυπτογράφησης
 - Ότη χρήση του κλειδιού των 56 bit
 - Τον Ιούλιο του 1998 Το Ίδρυμα για τα Ηλεκτρονικά Σύνορα (Electronic Frontier Foundation, EFF) ανακοίνωσε ότι κατάφερε να «σπάσει» μια κρυπτογράφηση DES

Πίνακας 2.2

Μέσος απαιτούμενος χρόνος για εξαντλητική αναζήτηση κλειδιών

Μέγεθος κλειδιού (bit)	Κρυπτογράφημα	Πλήθος εναλλακτικών κλειδιών	Απαιτούμενος χρόνος με ρυθμό 10^9 αποκρυπτογραφήσεις/μs	Απαιτούμενος χρόνος με ρυθμό 10^{13} αποκρυπτογραφήσεις/μs
56	DES	$2^{56} \approx 7,2 \times 10^{16}$	$2^{55} \mu\text{s} = 1,125$ έτη	1 ώρα
128	AES	$2^{128} \approx 3,4 \times 10^{38}$	$2^{127} \mu\text{s} = 5,3 \times 10^{21}$ έτη	$5,3 \times 10^{17}$ έτη
168	Τριπλό DES	$2^{168} \approx 3,7 \times 10^{50}$	$2^{167} \mu\text{s} = 5,8 \times 10^{33}$ έτη	$5,8 \times 10^{29}$ έτη
192	AES	$2^{192} \approx 6,3 \times 10^{57}$	$2^{191} \mu\text{s} = 9,8 \times 10^{40}$ έτη	$9,8 \times 10^{36}$ έτη
256	AES	$2^{256} \approx 1,2 \times 10^{77}$	$2^{255} \mu\text{s} = 1,8 \times 10^{60}$ έτη	$1,8 \times 10^{56}$ έτη

Τριπλό DES (3DES)

- Επανάληψη του βασικού αλγορίθμου του DES τρεις φορές, χρησιμοποιώντας είτε δύο είτε τρία μοναδικά κλειδιά
- Προτυποποιήθηκε για πρώτη φορά το 1985 στα πλαίσια του προτύπου ANSI X9.17 με σκοπό τη χρήση του σε χρηματοοικονομικές εφαρμογές
- Πλεονεκτήματα:
 - Το κλειδί μήκους 168 bit υπερνικά την αδυναμία του DES να ανταπεξέλθει σε επιθέσεις ωμής βίας
 - Ο υποκείμενος αλγόριθμος κρυπτογράφησης είναι ίδιος με τον αλγόριθμο του DES
- Μειονεκτήματα:
 - Σχετικά αργός σε υλοποιήσεις λογισμικού
 - Χρησιμοποιεί τμήματα με μέγεθος 64 bit



Προηγμένο Πρότυπο Κρυπτογράφησης (AES)

Ανάγκη
αντικατάστασης
του 3DES

Το 3DES δεν ήταν
κατάλληλο για
μακροχρόνια
χρήση

Το 1997 το NIST
εξέδωσε πρόσκληση
υποβολής προτάσεων
για ένα νέο AES

Θα έπρεπε να παρέχει
ίση ή μεγαλύτερη
ασφάλεια από το 3DES

Σημαντικά βελτιωμένη
απόδοση

Συμμετρικό
κρυπτογράφημα
τμημάτων

Τμήματα 128 bit και
κλειδιά με μήκος
128/192/256 bit

Τον Νοέμβριο του 2001
επέλεξε τον αλγόριθμο
Rijndael

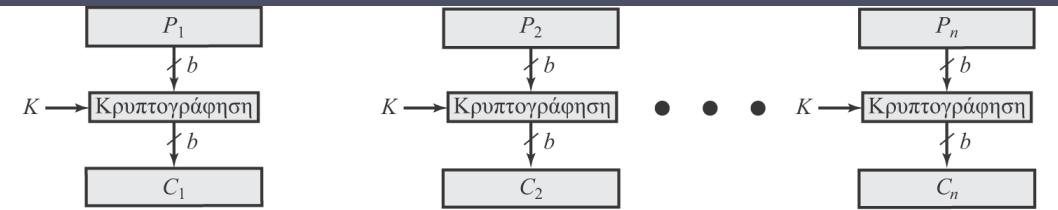
Πρότυπο
FIPS 197

Πρακτικά ζητήματα ασφαλείας

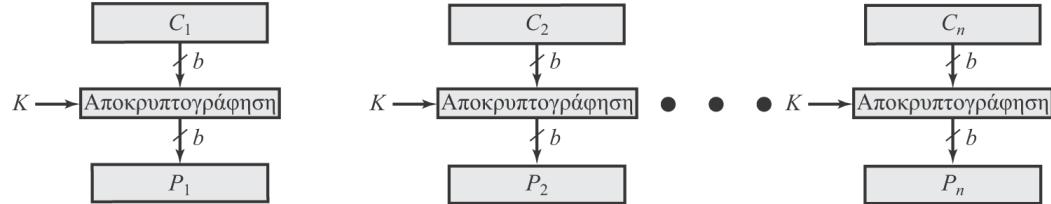
- Συμμετρική κρυπτογράφηση εφαρμόζεται συνήθως σε μονάδες δεδομένων μεγαλύτερες από ένα μεμονωμένο τμήμα 64 ή 128 bit
- Η κατάσταση λειτουργίας ηλεκτρονικού βιβλίου κωδικών (electronic codebook mode, ECB mode) είναι η πιο απλή μέθοδος για την κρυπτογράφηση πολλών τμημάτων
 - Κάθε τμήμα απλού κειμένου κρυπτογραφείται με το ίδιο κλειδί
 - Ο κρυπταναλυτής ενδέχεται να είναι σε θέση να εκμεταλλευθεί κανονικότητες του απλού κειμένου
- Καταστάσεις λειτουργίας
 - Εναλλακτικές μέθοδοι με τις οποίες ενισχύεται η ασφάλεια της κρυπτογράφησης συμμετρικών τμημάτων για μεγάλες ακολουθίες δεδομένων
 - Εξαλείφουν τις αδυναμίες της ECB



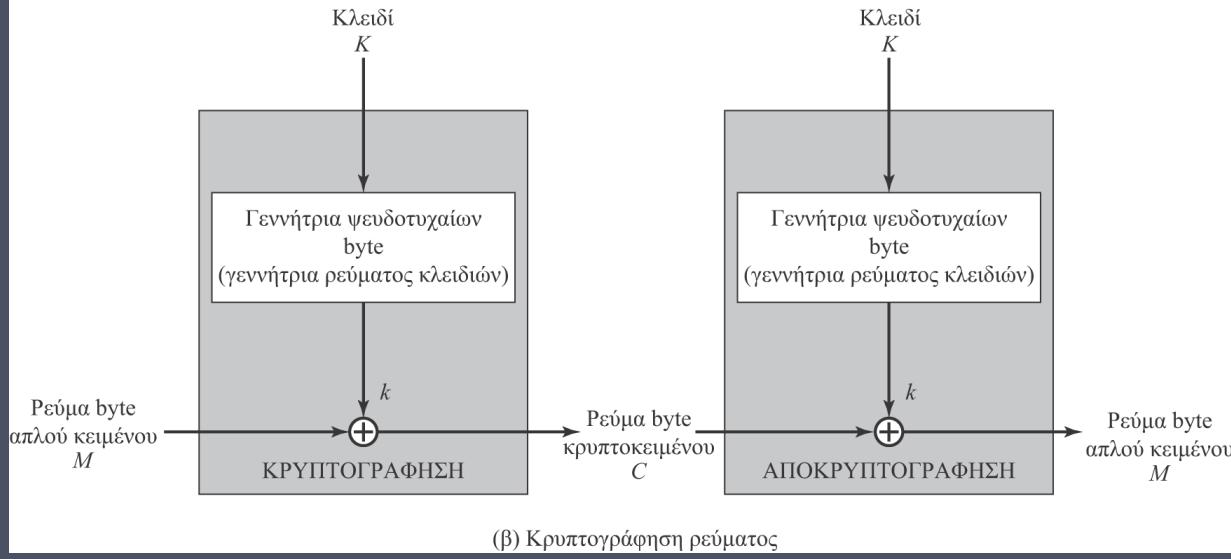
Κρυπτογράφηση



Αποκρυπτογράφηση



(α) Κρυπτογράφηση με κρυπτογράφημα τμημάτων (κατάσταση λειτουργίας ηλεκτρονικού βιβλίου κωδικών)



(β) Κρυπτογράφηση ρεύματος



Εικόνα 2.2 Τύποι συμμετρικής κρυπτογράφησης



Κρυπτογραφήματα τμημάτων και ρεύματος

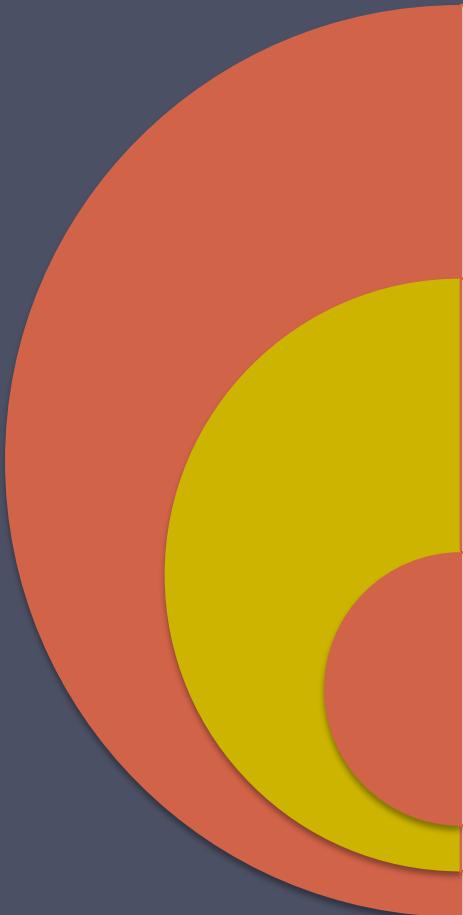
Κρυπτογράφημα τμημάτων

- Επεξεργάζεται την είσοδο ενός τμήματος στοιχείων κάθε φορά
- Παράγει ένα τμήμα εξόδου για κάθε τμήμα εισόδου
- Μπορεί να επαναχρησιμοποιεί τα ίδια κλειδιά
- Πιο διαδεδομένο

Κρυπτογράφημα ρεύματος

- Επεξεργάζεται τα στοιχεία εισόδου με συνεχή τρόπο
- Παράγει ένα στοιχείο εξόδου κάθε φορά
- Το κυριότερο πλεονέκτημά του είναι ότι είναι σχεδόν πάντα ταχύτερο και χρησιμοποιεί πολύ μικρότερο κώδικα
- Κρυπτογραφεί κάθε byte του απλού κειμένου ξεχωριστά
- Ένα ψευδοτυχαίο ρεύμα δεν μπορεί να προβλεφθεί χωρίς γνώση του κλειδιού που χρησιμοποιήθηκε στην είσοδο

Πιστοποίηση ταυτότητας μηνυμάτων



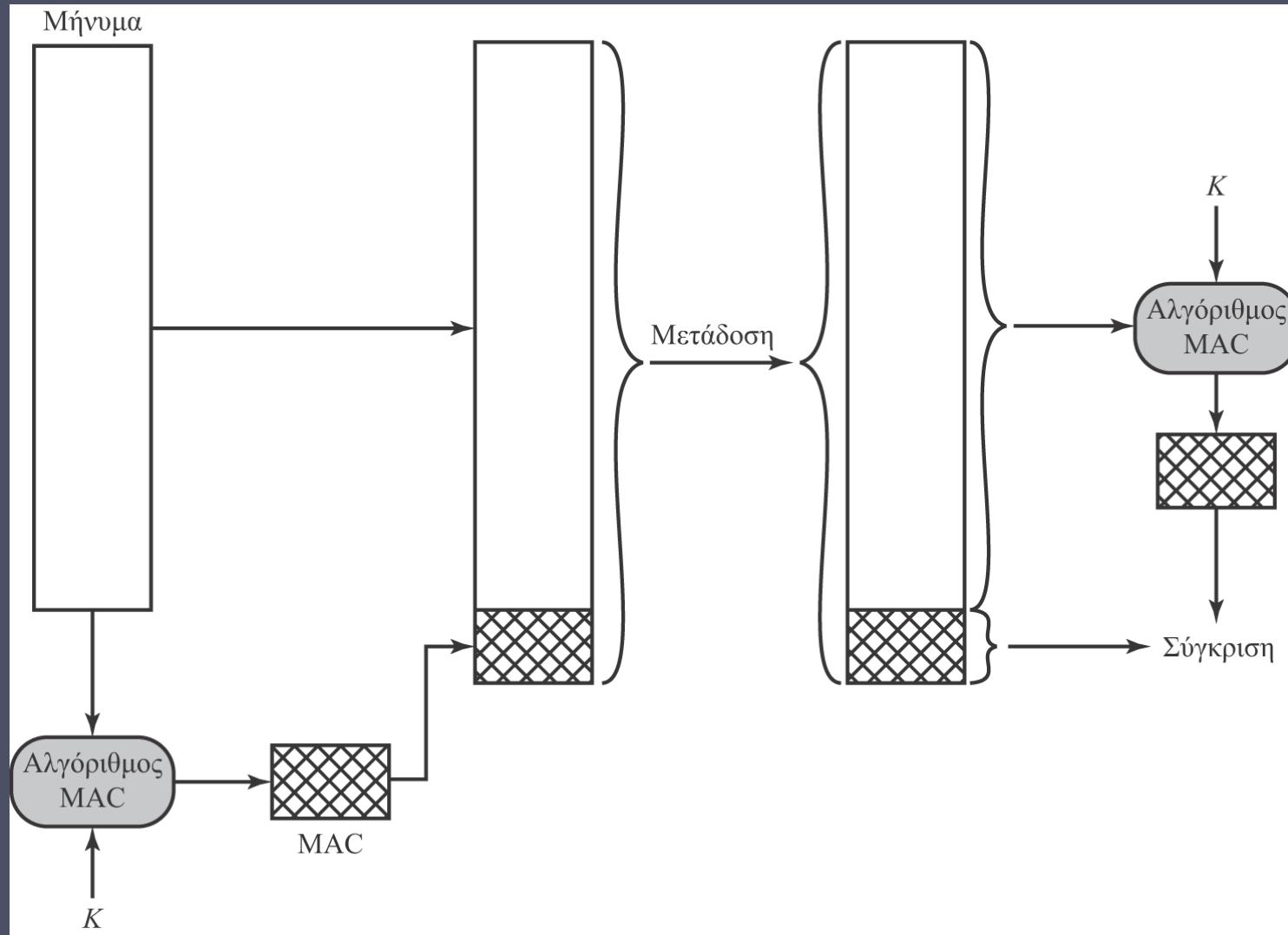
Παρέχει προστασία
από ενεργητικές
επιθέσεις

Επαληθεύει
την αυθεντικότητα
του παραληφθέντος
μηνύματος

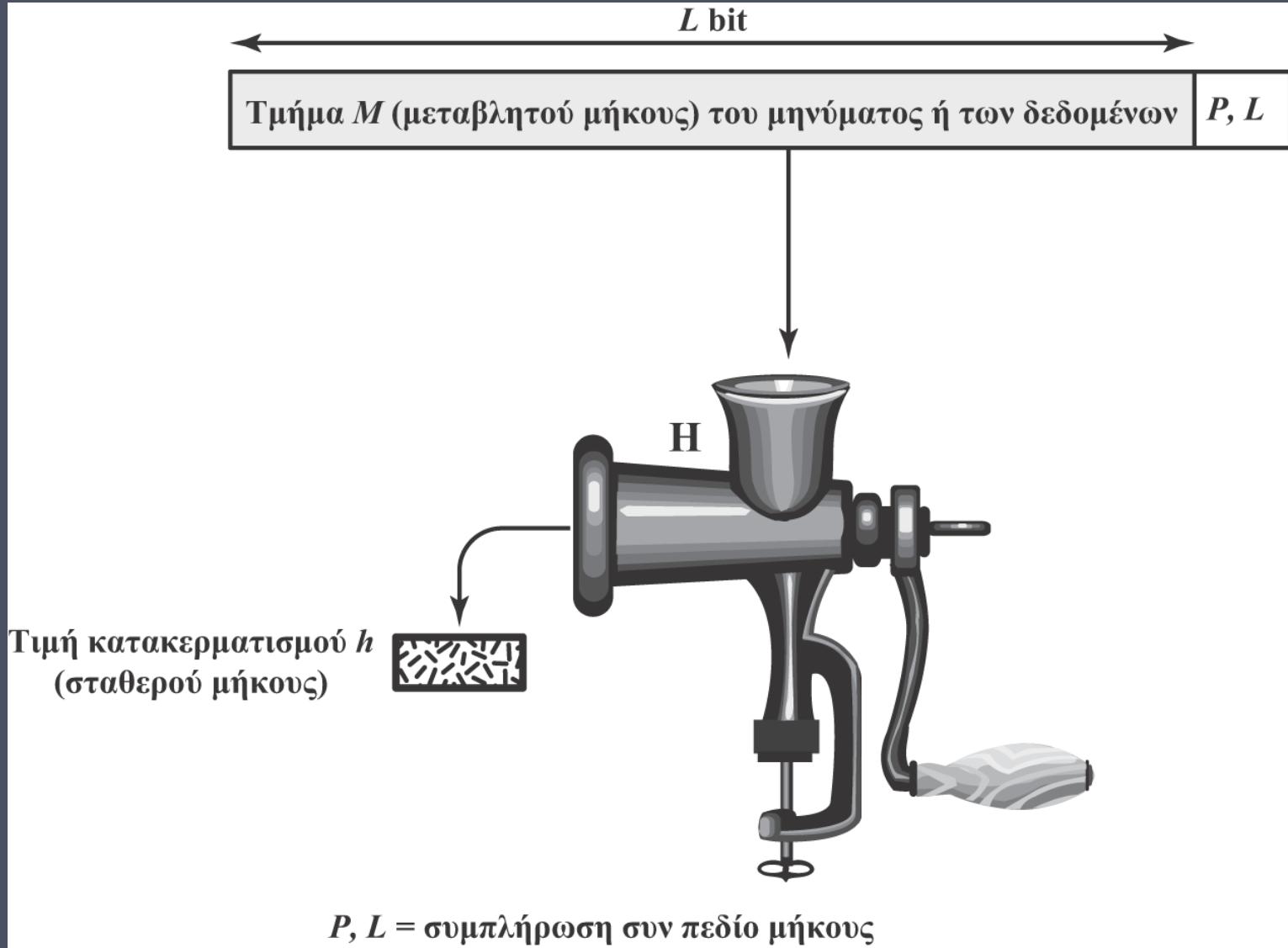
Μπορεί
να χρησιμοποιεί
συμβατική
κρυπτογράφηση

- Τα περιεχόμενα δεν έχουν τροποποιηθεί
- Η προέλευση είναι αυθεντική
- Είναι επίκαιρο και έφτασε με τη σωστή σειρά

- Αποστολέας και παραλήπτης είναι οι μόνοι που μοιράζονται το κλειδί

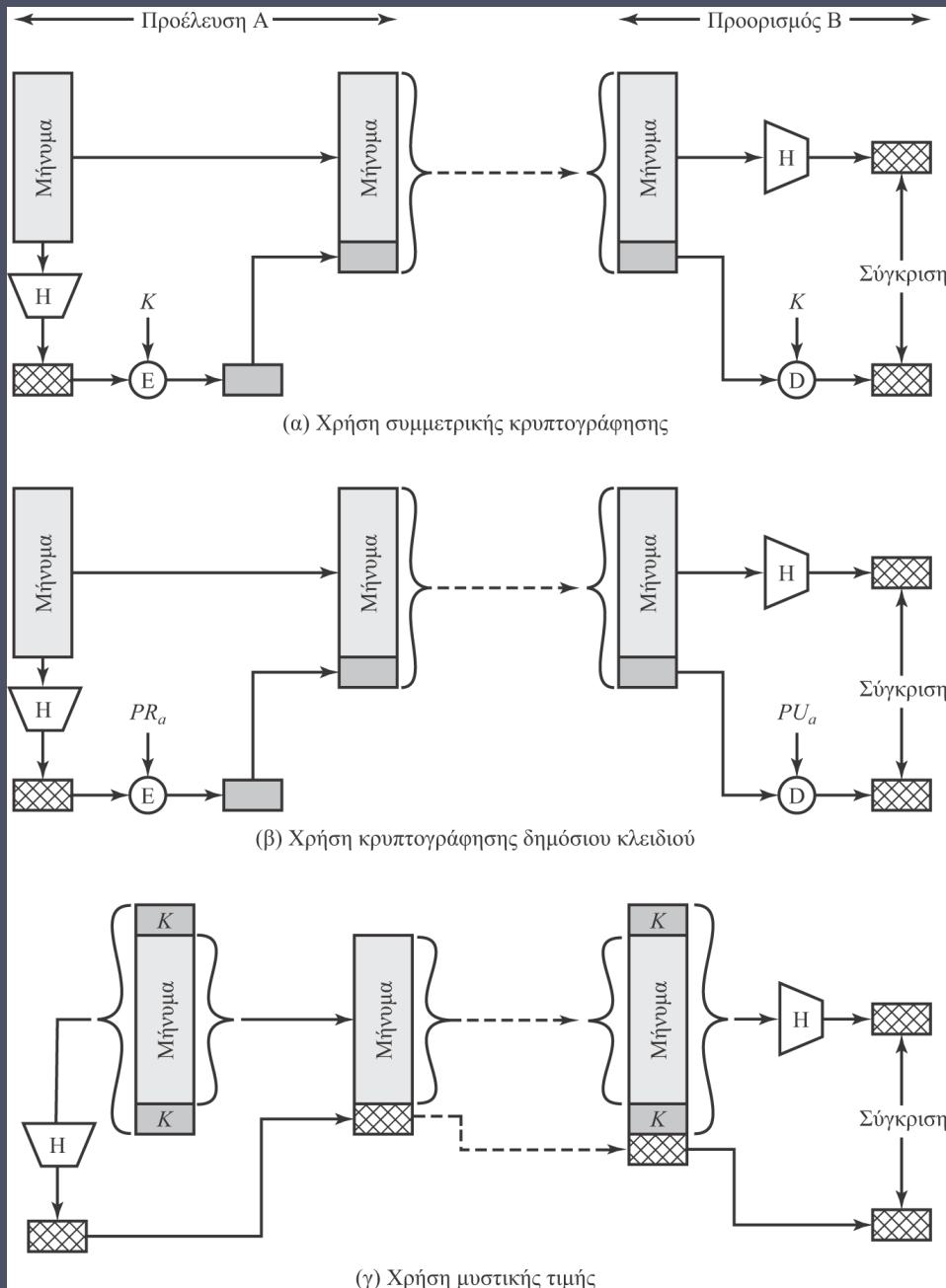


Εικόνα 2.3 Πιστοποίηση ταυτότητας μηνυμάτων με χρήση κωδικού πιστοποίησης ταυτότητας μηνύματος (MAC)



Εικόνα 2.4 Κρυπτογραφική συνάρτηση κατακερματισμού $h = H(M)$.

Εικόνα 2.5 Πιστοποίηση ταυτότητας μηνυμάτων με χρήση μονόδρομης συνάρτησης κατακερματισμού



Απαιτήσεις συναρτήσεων κατακερματισμού

Να μπορεί να εφαρμόζεται σε τμήματα δεδομένων οποιουδήποτε μεγέθους

Να παράγει έξοδο σταθερού μήκους

Να είναι σχετικά εύκολη στον υπολογισμό για οποιοδήποτε δεδομένο x

Να είναι μονόδομη ή ανθεκτική σε προεικόνες (pre-image resistant)

- Να είναι υπολογιστικά ανέφικτη η εύρεση μιας τιμής x τέτοιας ώστε να ισχύει $H(x) = h$

Να είναι υπολογιστικά ανέφικτη η εύρεση μιας τιμής $y \neq x$ τέτοιας ώστε να ισχύει $H(y) = H(x)$

Να είναι ανθεκτική σε συγκρούσεις ή να εμφανίζει ισχυρή ανθεκτικότητα σε συγκρούσεις

- Να είναι υπολογιστικά ανέφικτη η εύρεση οποιουδήποτε ζεύγους τιμών (x, y) τέτοιου ώστε να ισχύει $H(x) = H(y)$

Ασφάλεια συναρτήσεων κατακερματισμού

Υπάρχουν δύο τρόποι επίθεσης εναντίον μιας ασφαλούς συναρτησης κατακερματισμού:

Κρυπτανάλυση

- Εκμετάλλευση των αδυναμιών του αλγορίθμου σε λογικό επίπεδο

Επίθεση ωμής βίας

- Η ανθεκτικότητα μιας συνάρτησης κατακερματισμού εξαρτάται αποκλειστικά από το μήκος του κωδικού κατακερματισμού που παράγει ο αλγόριθμος

SHA: Ο αλγόριθμος κατακερματισμού που χρησιμοποιείται περισσότερο

Άλλες εφαρμογές των συναρτήσεων κατακερματισμού:

Κωδικοί πρόσβασης

- Το λειτουργικό σύστημα αποθηκεύει μια τιμή κατακερματισμού ενός κωδικού πρόσβασης

Ανίχνευση εισβολών

- Για κάθε αρχείο ενός συστήματος αποθηκεύονται οι τιμές $H(F)$. Οι τιμές κατακερματισμού φυλάσσονται με ασφάλεια.

Δομή της κρυπτογράφησης δημόσιου κλειδιού

Προτάθηκε
για πρώτη
φορά
δημόσια το
1976 από
τους Diffie
και Hellman

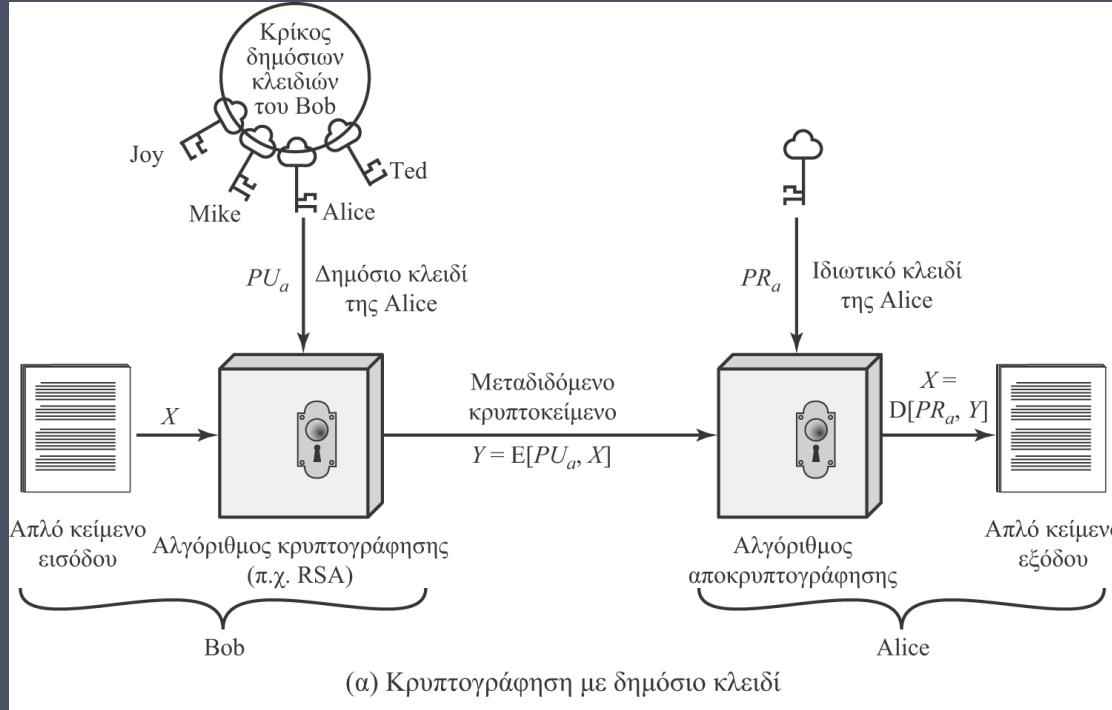
Βασίζεται σε
μαθηματικές
συναρτήσεις

Ασύμμετρη

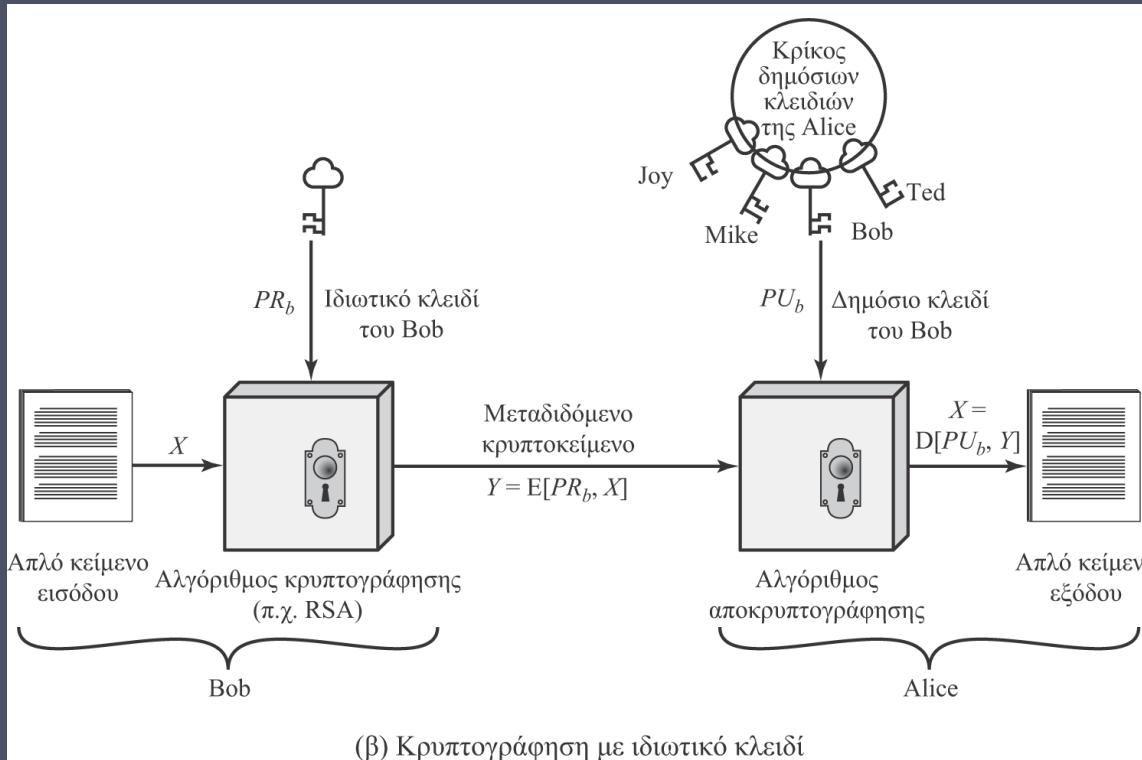
- Χρήση δύο κλειδιών
- Δημόσιο και ιδιωτικό κλειδί
- Το δημόσιο κλειδί κοινοποιείται ώστε να το χρησιμοποιούν και άλλοι

Απαιτείται
κάποια
μορφή
πρωτοκόλλου





- **Απλό κείμενο (plaintext)**
 - Το μήνυμα (ή τα δεδομένα) σε αναγνώσιμη μορφή το οποίο παρέχεται στον αλγόριθμο ως είσοδος
- **Αλγόριθμος κρυπτογράφησης**
 - Εκτελεί διάφορους μετασχηματισμούς στο απλό κείμενο
- **Δημόσιο και ιδιωτικό κλειδί**
 - Ζεύγος κλειδιών, το ένα για την κρυπτογράφηση και το άλλο για την αποκρυπτογράφηση
- **Κρυπτοκείμενο**
 - Κρυπτογραφημένο μήνυμα που παράγεται ως έξοδος
- **Αλγόριθμος αποκρυπτογράφησης**
 - Παράγει ως έξοδο το αρχικό απλό κείμενο



- Κάθε χρήστης κρυπτογραφεί δεδομένα χρησιμοποιώντας το δικό του ιδιωτικό κλειδί
- Οποιοσδήποτε γνωρίζει το αντίστοιχο δημόσιο κλειδί θα είναι σε θέση να αποκρυπτογραφήσει το μήνυμα

Πίνακας 2.3

Εφαρμογές των κρυπτοσυστημάτων δημόσιου κλειδιού

Αλγόριθμος	Ψηφιακή υπογραφή	Διανομή συμμετρικών κλειδιών	Κρυπτογράφηση μυστικών κλειδιών
RSA	Ναι	Ναι	Ναι
Diffie-Hellman	Όχι	Ναι	Όχι
DSS	Ναι	Όχι	Όχι
Ελλειπτικής καμπύλης	Ναι	Ναι	Ναι

Απαιτήσεις για κρυπτοσυστήματα δημόσιου κλειδιού

Είναι υπολογιστικά εύκολο
να παραχθούν
ζεύγη κλειδιών

Χρήσιμα αν οποιοδήποτε από
τα δύο κλειδιά μπορεί να
χρησιμοποιηθεί για κάθε ρόλο

Είναι υπολογιστικά
ανέφικτο για κάποιον
αντίπαλο να ανακτήσει το
αρχικό μήνυμα



Είναι υπολογιστικά ανέφικτο
για κάποιον αντίπαλο,
ο οποίος γνωρίζει
το δημόσιο κλειδί, να βρει το
ιδιωτικό κλειδί

Είναι υπολογιστικά εύκολο για
τον αποστολέα, ο οποίος γνωρίζει
το δημόσιο κλειδί, να κρυπτογραφεί
μηνύματα

Είναι υπολογιστικά εύκολο για
τον παραλήπτη, ο οποίος
γνωρίζει το ιδιωτικό κλειδί,
να αποκρυπτογραφεί κρυπτοκείμενο

Αλγόριθμοι ασύμμετρης κρυπτογράφησης

RSA (Rivest,
Shamir,
Adleman)

Αναπτύχθηκε το 1977

Η πιο ευρέως αποδεκτή,
εφαρμοσμένη
προσέγγιση
κρυπτογράφησης
δημόσιου κλειδιού

Κρυπτογράφημα τμημάτων
στο οποίο το απλό κείμενο
και το κρυπτοκείμενο είναι
ακέραιοι αριθμοί μεταξύ 0
και $n - 1$, για κάποια τιμή
του n .

Αλγόριθμος
ανταλλαγής
κλειδιών
Diffie-Hellman

Δύο χρήστες φτάνουν
σε συμφωνία για ένα κοινό
μυστικό στοιχείο το οποίο
θα χρησιμοποιούν ως
μυστικό κλειδί
για τη μελλοντική συμμετρική
κρυπτογράφηση μηνυμάτων

Περιορίζεται
στην ανταλλαγή
των κλειδιών

Πρότυπο
Ψηφιακής
Υπογραφής
(DSS)

Παρέχει μόνο
μια συνάρτηση
ψηφιακής
υπογραφής
με τον SHA-1

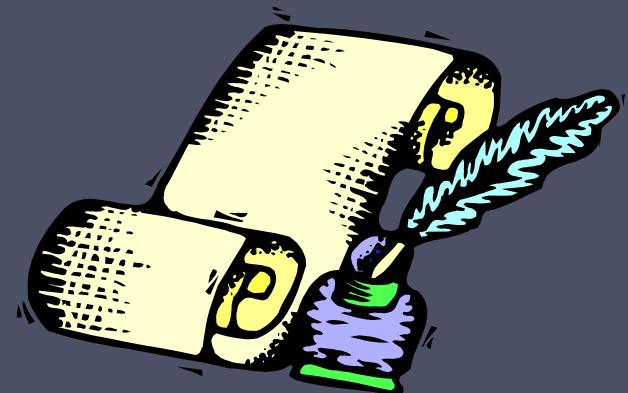
Δεν μπορεί να
χρησιμοποιηθεί για
κρυπτογράφηση ή
ανταλλαγή κλειδιών

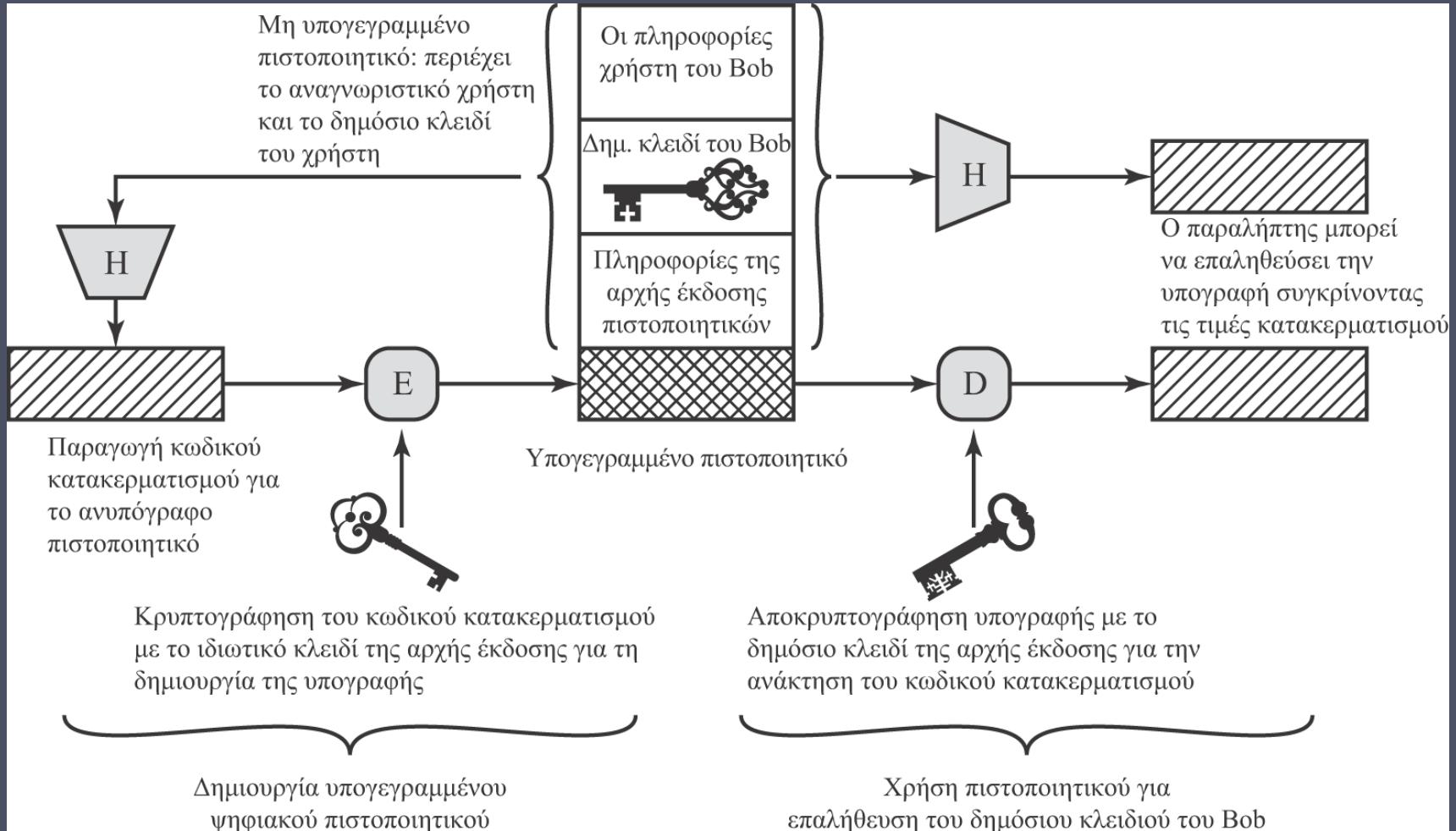
Κρυπτογραφία
ελλειπτικής
καμπύλης
(ECC)

Προσφέρει την ίδια
ασφάλεια με το RSA
χρησιμοποιώντας
πολύ μικρότερα
κλειδιά

Ψηφιακές υπογραφές

- Χρησιμοποιούνται για πιστοποίηση και της προέλευσης και της ακεραιότητας των δεδομένων
- Δημιουργούνται μέσω της κρυπτογράφησης του κωδικού κατακερματισμού με το ιδιωτικό κλειδί
- Δεν διασφαλίζουν την εμπιστευτικότητα
 - Ακόμα και στην περίπτωση της κρυπτογράφησης ολόκληρου του μηνύματος
 - Το μήνυμα είναι προστατευμένο από την τροποποίηση, αλλά όχι και από την υποκλοπή

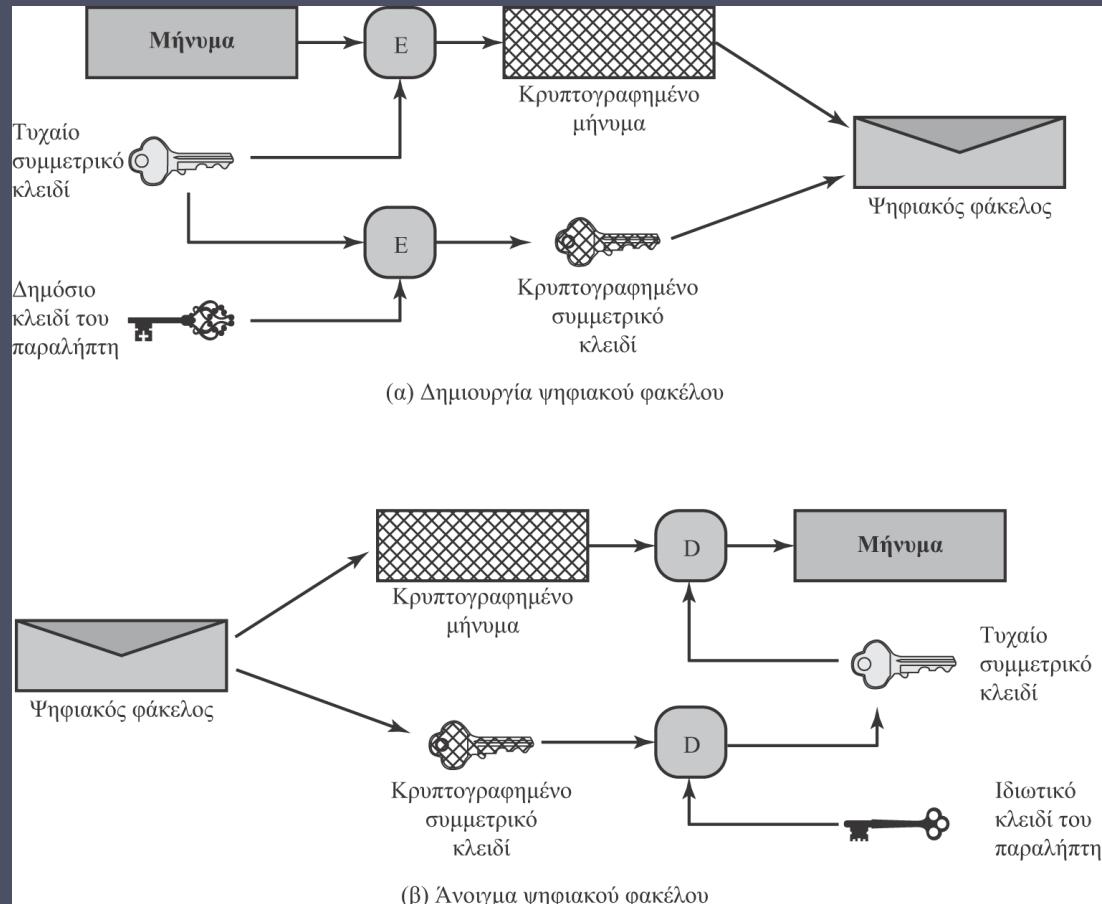




Εικόνα 2.7 Χρήση πιστοποιητικού δημόσιου κλειδιού

Ψηφιακοί φάκελοι

- Προστατεύουν μηνύματα χωρίς να είναι απαραίτητο ο αποστολέας και ο παραλήπτης να έχουν διευθετήσει το ζήτημα της κατοχής του ίδιου μυστικού κλειδιού
- Αποτελεί το αντίστοιχο ενός σφραγισμένου φακέλου που περιέχει μια ανυπόγραφη επιστολή



Εικόνα 2.8 Ψηφιακοί φάκελοι

Τυχαίοι αριθμοί



Χρήσεις:

- Παραγωγή κλειδιών για αλγορίθμους δημόσιου κλειδιού
- Παραγωγή κλειδιού ρεύματος για συμμετρικά κρυπτογραφήματα ρεύματος
- Παραγωγή συμμετρικού κλειδιού το οποίο θα χρησιμοποιηθεί ως προσωρινό κλειδί συνόδου (session key) ή για τη δημιουργία ψηφιακού φακέλου
- «Χειραψία» για την αποτροπή επιθέσεων αναπαραγωγής
- Παραγωγή κλειδιών συνόδου

Απαιτήσεις τυχαίων αριθμών

Τυχαιότητα

- Κριτήρια:

- Ομοιόμορφη κατανομή
 - Η συχνότητα εμφάνισης κάθε αριθμού είναι κατά προσέγγιση η ίδια
- Ανεξαρτησία
 - Καμία τιμή της ακολουθίας δεν μπορεί να εξαχθεί συμπερασματικά από τις υπόλοιπες

Αδυναμία πρόβλεψης

- Κάθε αριθμός είναι στατιστικά ανεξάρτητος από τους υπόλοιπους αριθμούς της ακολουθίας
- Οι αντίπαλοι δεν είναι σε θέση να προβλέπουν επόμενα στοιχεία της ακολουθίας βασιζόμενοι σε προηγούμενα στοιχεία της

Σύγκριση τυχαίων και ψευδοτυχαίων αριθμών

Οι κρυπτογραφικές εφαρμογές συνήθως χρησιμοποιούν
αλγόριθμικές τεχνικές για την παραγωγή τυχαίων αριθμών

- Οι αλγόριθμοι είναι αιτιοκρατικοί, οπότε παράγουν ακολουθίες αριθμών
που δεν είναι στατιστικά τυχαίοι

Ψευδοτυχαίοι αριθμοί

- Παραγόμενες ακολουθίες που περνούν με επιτυχία πολλές
στατιστικές δοκιμές τυχαιότητας
- Πιθανόν να μπορούν να προβλεφθούν

Γεννήτρια πραγματικά τυχαίων αριθμών (TRNG):

- Χρησιμοποιεί μη αιτιοκρατική πηγή για τη δημιουργία της τυχαιότητας
- Οι περισσότερες λειτουργούν με βάση μετρήσεις απόδρασης φυσικών
διεργασιών
- π.χ. ακτινοβολία, έκλυση αερίων, πυκνωτές με διαρροή ηλεκτρικού φορτίου
- Ενσωματώνεται σε ολοένα και περισσότερους σύγχρονους επεξεργαστές

Πρακτική εφαρμογή:

Κρυπτογράφηση αποθηκευμένων δεδομένων

Η κρυπτογράφηση μεταδιδόμενων δεδομένων αποτελεί συνήθη τακτική

Δεν ισχύει το ίδιο για τα αποθηκευμένα δεδομένα



Συχνά δεν παρέχεται προστασία πέραν της πιστοποίησης ταυτότητας περιοχής (domain authentication), και των μηχανισμών ελέγχου πρόσβασης του λεπτομερικού συστήματος

Τα δεδομένα αρχειοθετούνται για αδιευκρίνιστες χρονικές περιόδους

Ακόμα και όταν διαγράφονται δεδομένα από τον σκληρό δίσκο, είναι ανακτήσιμα μέχρι να επαναχρησιμοποιηθούν οι αντίστοιχοι τομείς του δίσκου

Προσεγγίσεις κρυπτογράφησης αποθηκευμένων δεδομένων:

Χρήση ενός εμπορικά διαθέσιμου πακέτου κρυπτογράφησης

Συσκευή οπισθοφυλακής

Κρυπτογράφηση μαγνητοταινιών βιβλιοθήκης

Κρυπτογράφηση δεδομένων σε προσωπικούς ή φορητούς υπολογιστές στο παρασκήνιο

Σύνοψη

- Εμπιστευτικότητα με συμμετρική κρυπτογράφηση
 - Συμμετρική κρυπτογράφηση
 - Αλγόριθμοι συμμετρικής κρυπτογράφησης τμημάτων
 - Κρυπτογραφήματα ρεύματος
- Πιστοποίηση ταυτότητας μηνυμάτων και συναρτήσεις κατακερματισμού
 - Πιστοποίηση ταυτότητας με χρήση συμμετρικής κρυπτογράφησης
 - Πιστοποίηση ταυτότητας μηνυμάτων χωρίς κρυπτογράφηση
 - Ασφαλείς συναρτήσεις κατακερματισμού
 - Άλλες εφαρμογές των συναρτήσεων κατακερματισμού
- Τυχαίοι και ψευδοτυχαίοι αριθμοί
 - Χρήση τυχαίων αριθμών
 - Σύγκριση τυχαίων και ψευδοτυχαίων αριθμών
- Κρυπτογράφηση δημόσιου κλειδιού
 - Δομή
 - Εφαρμογές των κρυπτοσυστημάτων δημόσιου κλειδιού
 - Απαιτήσεις της κρυπτογραφίας δημόσιου κλειδιού
 - Αλγόριθμοι ασύμμετρης κρυπτογράφησης
- Ψηφιακές υπογραφές και διαχείριση κλειδιών
 - Ψηφιακή υπογραφή
 - Πιστοποιητικά δημόσιου κλειδιού
 - Ανταλλαγή συμμετρικών κλειδιών με χρήση κρυπτογράφησης δημόσιου κλειδιού
 - Ψηφιακοί φάκελοι

