

ΕΚΔΟΣΕΙΣ ΚΛΕΙΔΑΡΙΘΜΟΣ

ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ

ΑΡΧΕΣ ΚΑΙ ΠΡΑΚΤΙΚΕΣ

3η αμερικανική έκδοση



William Stallings • Lawrie Brown



Κεφάλαιο 21

Κρυπτογραφία δημόσιου κλειδιού και
πιστοποίηση ταυτότητας μηνυμάτων

	Bit 1	Bit 2	...	Bit <i>n</i>
Τμήμα 1	b_{11}	b_{21}		b_{n1}
Τμήμα 2	b_{12}	b_{22}		b_{n2}

Τμήμα <i>m</i>	b_{1m}	b_{2m}		b_{nm}
Κωδικός κατακερματισμού	C_1	C_2		C_n

Εικόνα 21.1 Απλή συνάρτηση κατακερματισμού με χρήση XOR σε επίπεδο bit

Ασφαλής Αλγόριθμος Κατακερματισμού (SHA)

- Αναπτύχθηκε αρχικά από το NIST
- Το 1993 δημοσιεύθηκε ως πρότυπο (FIPS 180)
- Το 1995 κυκλοφόρησε μια αναθεωρημένη έκδοσή του (SHA-1)
 - Παράγει τιμές κατακερματισμού των 160 bit
- Το 2002 το NIST προχώρησε στην αναθεώρηση του προτύπου (FIPS 180-2)
 - Προσθέτει τρεις νέες εκδόσεις του SHA
 - SHA-256, SHA-384, SHA-512
 - Τιμές κατακερματισμού των 256/384/512 bit
 - Ήδια βασική δομή με την έκδοση SHA-1· αυξημένη ασφάλεια
- Το 2005 το NIST ανακοίνωσε την πρόθεσή του να αποσύρει σταδιακά την έγκριση της έκδοσης SHA-1 και να στηρίξει τις άλλες εκδόσεις του SHA έως το 2010

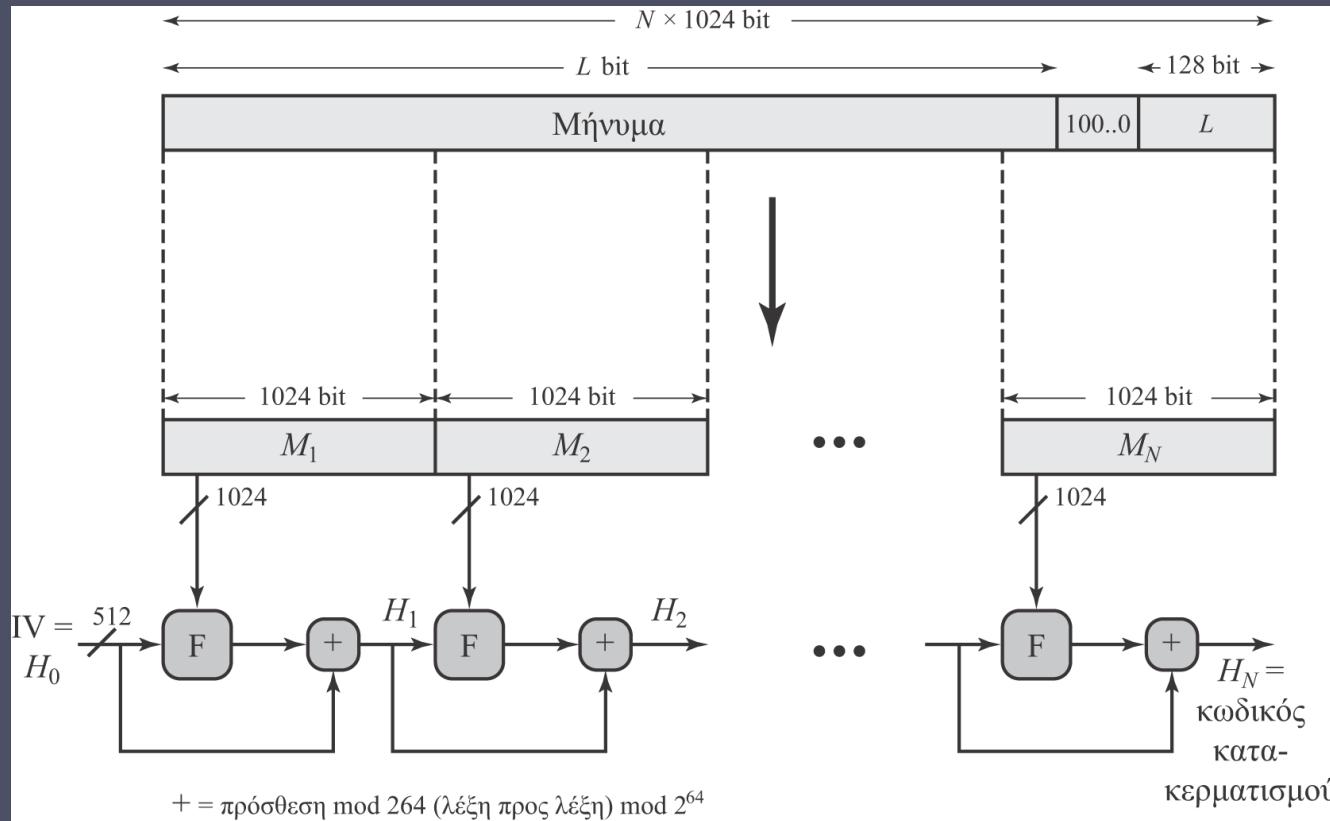
Πίνακας 21.1

Σύγκριση παραμέτρων SHA

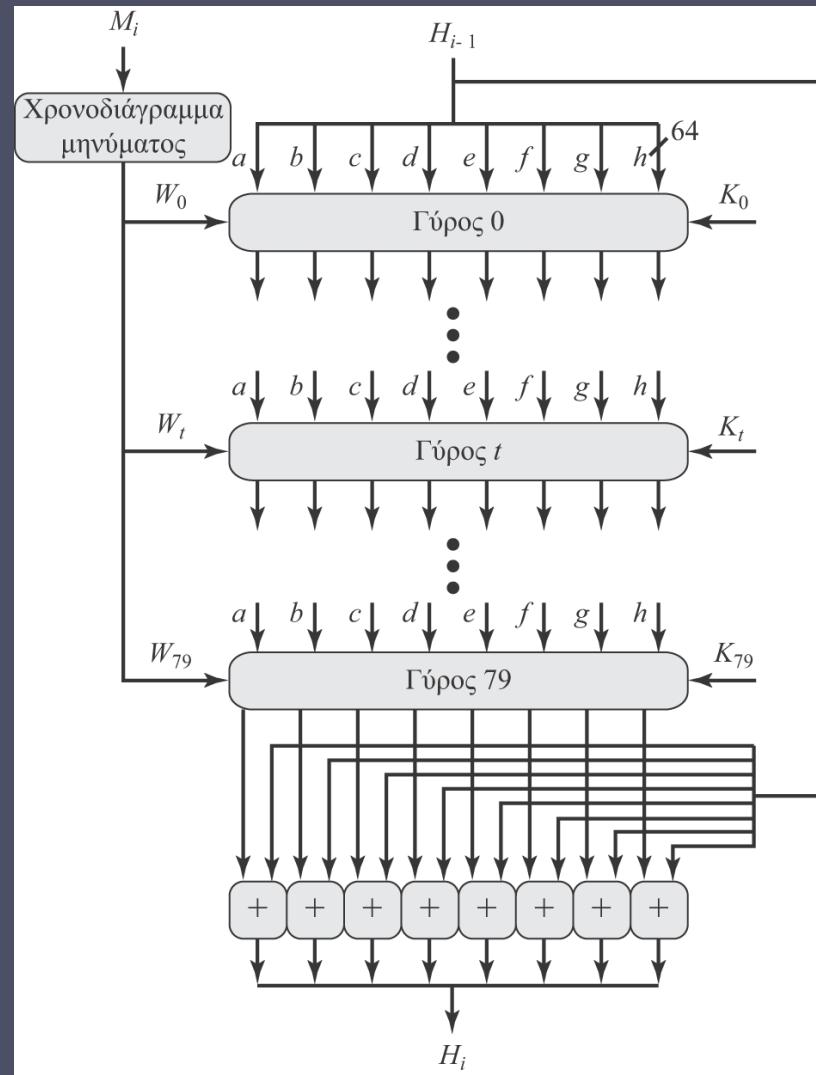
	SHA-1	SHA-256	SHA-384	SHA-512
Μέγεθος σύνοψης μηνύματος	160	256	384	512
Μέγεθος μηνύματος	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Μέγεθος τμήματος	512	512	1024	1024
Μέγεθος λέξης	32	32	64	64
Πλήθος βημάτων	80	64	80	80
Ασφάλεια	80	128	192	256

Σημειώσεις:

1. Όλα τα μεγέθη μετριούνται σε bit.
2. Η ασφάλεια αναφέρεται στο γεγονός ότι μια «επίθεση γενεθλίων» (birthday attack) εναντίον μιας σύνοψης μηνύματος (message digest) μεγέθους n παράγει μια σύγκρουση με συντελεστή εργασίας (work factor) κατά προσέγγιση ίσο με $2^{n/2}$.



Εικόνα 21.2 Παραγωγή σύνοψης μηνύματος με χρήση της έκδοσης SHA-512



Εικόνα 21.3 Επεξεργασία ενός τμήματος 1024 bit στην έκδοση SHA-512

SHA-3

- Ο αλγόριθμος SHA-2 έχει την ίδια δομή και στηρίζεται στις ίδιες μαθηματικές πράξεις με τους προκατόχους του, και αυτό εγείρει ανησυχίες
- Λόγω του χρόνου που θα χρειαζόταν για την αντικατάσταση του SHA-2 στην περίπτωση που εντοπιζόταν κάποια αδυναμία του, το 2007 το NIST ανακοίνωσε τη διεξαγωγή διαγωνισμού για τη δημιουργία της επόμενης γενιάς (SHA-3)

Απαιτήσεις:

- Πρέπει να υποστηρίζει τιμές κατακερματισμού με μήκος 224, 256, 384 και 512 bit
- Ο αλγόριθμος πρέπει να επεξεργάζεται σχετικά μικρά τμήματα τη φορά αντί να απαιτεί την προσωρινή αποθήκευση ολόκληρου του μηνύματος στη μνήμη προτού το επεξεργαστεί



HMAC



- Έχει αυξηθεί το ενδιαφέρον για την ανάπτυξη ενός κωδικού MAC ο οποίος θα προκύπτει από κάποιον κρυπτογραφικό κωδικό κατακερματισμού
 - Γενικά, οι κρυπτογραφικές συναρτήσεις κατακερματισμού εκτελούνται πιο γρήγορα
 - Υπάρχει ευρέως διαθέσιμος κώδικας βιβλιοθηκών
 - Η συνάρτηση SHA-1 δεν έχει σχεδιαστεί για χρήση ως κωδικός MAC επειδή δεν στηρίζεται σε μυστικό κλειδί
- Δημοσιεύθηκε στο έγγραφο RFC 2044
- Έχει επιλεχθεί ως υποχρεωτικός κωδικός MAC για όλες τις υλοποιήσεις της Ασφάλειας IP (IPSec)
 - Χρησιμοποιείται και σε άλλα πρωτόκολλα Διαδικτύου, όπως η Ασφάλεια Επιπέδου Μεταφοράς (Transport Layer Security, TLS) και η Ασφαλής Ηλεκτρονική Συναλλαγή (Secure Electronic Transaction, SET)

Αντικειμενικοί στόχοι σχεδιασμού του ΗΜΑC

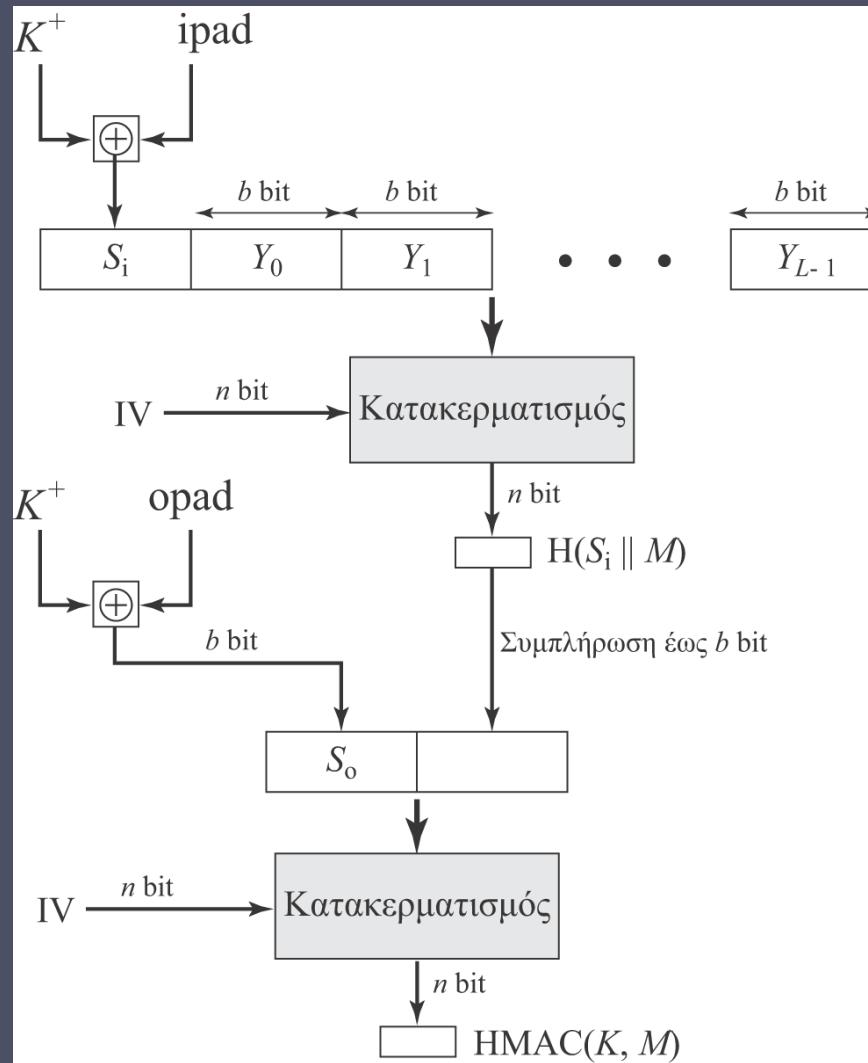
Να χρησιμοποιεί, χωρίς
τροποποιήσεις, διαθέσιμες
συνάρτησεις κατακερματισμού

Να διατηρεί την αρχική απόδοση
της συνάρτησης
κατακερματισμού χωρίς να
επιφέρει σημαντική μείωση

Να παρέχει δυνατότητα εύκολης
αντικατάστασης της
ενσωματωμένης συνάρτησης
κατακερματισμού σε περίπτωση
που ανακαλυφθούν ή
απαιτηθούν πιο γρήγορες ή
ασφαλείς συνάρτησεις
κατακερματισμού

Να χρησιμοποιεί και να
χειρίζεται κλειδιά με απλό τρόπο

Να διαθέτει μια πλήρως
κατανοητή κρυπτογραφική
ανάλυση της ισχύος του
μηχανισμού πιστοποίησης
ταυτότητας με βάση λογικές
υποθέσεις για την
ενσωματωμένη συνάρτηση
κατακερματισμού



Εικόνα 21.4 Δομή του HMAC

Ασφάλεια του HMAC

- Η ασφάλεια εξαρτάται από την κρυπτογραφική ισχύ της υποκείμενης συνάρτησης κατακερματισμού
- Για δεδομένο επίπεδο προσπάθειας με μηνύματα που παράγονται από κάποιον έγκυρο χρήστη και παρατηρούνται από τον επιτιθέμενο, η πιθανότητα εκδήλωσης επιτυχούς επίθεσης εναντίον του HMAC είναι ισοδύναμη με την πιθανότητα των παρακάτω επιθέσεων εναντίον της ενσωματωμένης συνάρτησης κατακερματισμού :
 - Ο επιτιθέμενος είναι σε θέση να υπολογίσει μια έξοδο ακόμα και με ένα διάνυσμα **IV** το οποίο είναι τυχαίο και μυστικό
 - Επίθεση ωμής βίας εναντίον του κλειδιού $O(2^n)$, ή επίθεση των γενεθλίων
 - Ο επιτιθέμενος εντοπίζει συγκρούσεις στη συνάρτηση κατακερματισμού ακόμη και όταν το διάνυσμα **IV** είναι τυχαίο και μυστικό
 - Δηλαδή, εύρεση μηνυμάτων M και M' τέτοιων ώστε $H(M) = H(M')$
 - Επίθεση των γενεθλίων $O(2^{n/2})$
 - Η συνάρτηση MD5 είναι ασφαλής στον HMAC επειδή ο επιτιθέμενος μόνο παρατηρεί



Κρυπτογράφηση δημόσιου κλειδιού RSA

- Αναπτύχθηκε το 1977 από τους Rivest, Shamir και Adleman στο MIT
- Ο πιο γνωστός και ευρέως χρησιμοποιούμενος αλγόριθμος δημόσιου κλειδιού
- Χρησιμοποιεί πράξεις ύψωσης ακεραίων σε δύναμη modulo έναν πρώτο αριθμό
- Κρυπτογράφηση: $C = M^e \text{ mod } n$
- Αποκρυπτογράφηση: $M = C^d \text{ mod } n = (M^e)^d \text{ mod } n = M^{ed} \text{ mod } n$
- Αποστολέας και παραλήπτης γνωρίζουν τις τιμές των n και e
- Μόνο ο παραλήπτης γνωρίζει την τιμή του d
- Αλγόριθμος κρυπτογράφησης δημόσιου κλειδιού με δημόσιο κλειδί $PU = \{e, n\}$ και ιδιωτικό κλειδί $PR = \{d, n\}$

Παραγωγή κλειδιών

Επιλογή των p, q

Οι p και q είναι πρώτοι αριθμοί, $p \neq q$

Υπολογισμός του $n = p \times q$

Υπολογισμός του $\varphi(n) = (p - 1)(q - 1)$

Επιλογή ακεραίου e

$\text{MKΔ}(\varphi(n), e) = 1, 1 < e < \varphi(n)$

Υπολογισμός του d

$de \bmod \varphi(n) = 1$

Δημόσιο κλειδί

$KU = \{e, n\}$

Ιδιωτικό κλειδί

$KR = \{d, n\}$

Κρυπτογράφηση

Απλό κείμενο:

$M < n$

Κρυπτοκείμενο:

$C = M^e \pmod{n}$

Αποκρυπτογράφηση

Κρυπτοκείμενο:

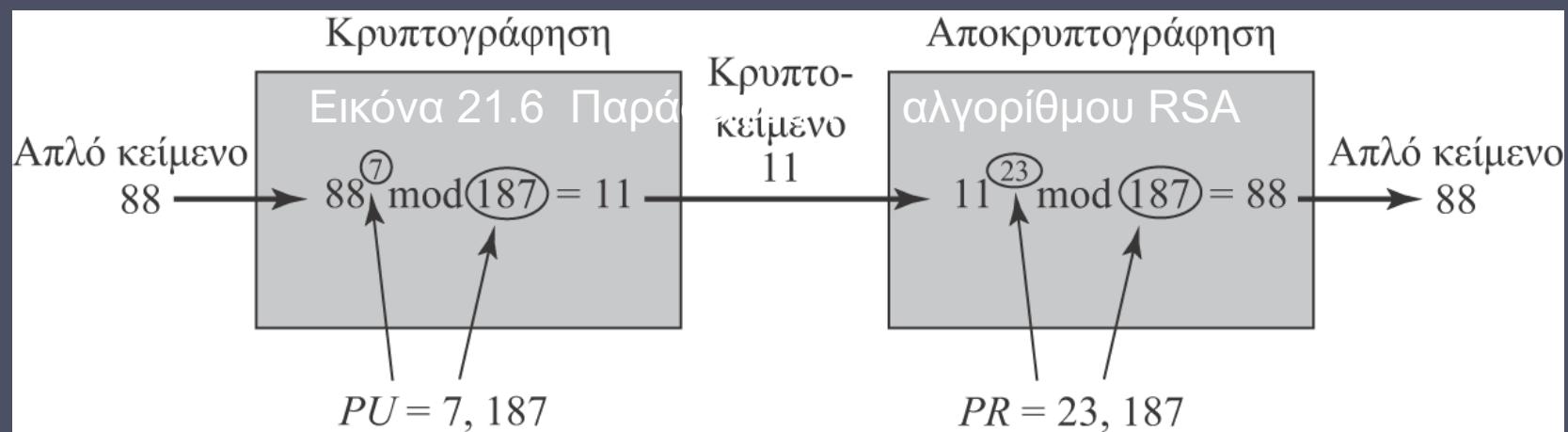
C

Απλό κείμενο:

$M = C^d \pmod{n}$

1. Επιλογή δύο πρώτων αριθμών, $p = 17$ και $q = 11$.
2. Υπολογισμός του $n = pq = 17 \times 11 = 187$.
3. Υπολογισμός του $\varphi(n) = (p - 1)(q - 1) = 16 \times 10 = 160$.
4. Επιλογή του ακεραίου e έτσι ώστε να είναι πρώτος σε σχέση με το $\varphi(n) = 160$ και μικρότερος από το $\varphi(n)$. επιλέγουμε $e = 7$.
5. Υπολογισμός του d έτσι ώστε να ισχύει $de \text{ mod } 160 = 1$ και $d < 160$. Η σωστή τιμή είναι $d = 23$ επειδή $23 \times 7 = 161 = (1 \times 160) + 1$.

Δημόσιο κλειδί $PU = \{7, 187\}$, ιδιωτικό κλειδί $PR = \{23, 187\}$.



Ασφάλεια του RSA



Ωμή βία

- Περιλαμβάνει τη δοκιμή όλων των πιθανών ιδιωτικών κλειδιών

Μαθηματικές επιθέσεις

- Υπάρχουν αρκετές προσεγγίσεις, οι οποίες επιχειρούν να αναλύσουν το γινόμενο δύο πρώτων αριθμών σε παράγοντες

Επιθέσεις χρονομέτρησης

- Εξαρτώνται από τον χρόνο εκτέλεσης του αλγορίθμου αποκρυπτογράφησης

Επιθέσεις επιλεγμένου κρυπτοκειμένου

- Αυτός ο τύπος επίθεσης εκμεταλλεύεται ιδιότητες του αλγορίθμου RSA

Πίνακας 21.2

Η πρόοδος της ανάλυσης σε παράγοντες

Πλήθος δεικαδικών ψηφίων	Πλήθος σε bit (κατά προσέγγιση)	Ημερομηνία επίτευξης	MIPS-έτη
100	332	Απρίλιος 1991	7
110	365	Απρίλιος 1992	75
120	398	Ιούνιος 1993	830
129	428	Απρίλιος 1994	5000
130	431	Απρίλιος 1996	1000
140	465	Φεβρουάριος 1999	2000
155	512	Αύγουστος 1999	8000
160	530	Απρίλιος 2003	–
174	576	Δεκέμβριος 2003	–
200	663	Μάιος 2005	–

Ανταλλαγή κλειδιών Diffie-Hellman

- Πρώτος δημοσιευμένος αλγόριθμος δημόσιου κλειδιού
- Δημοσιεύθηκε το 1976 από τους Diffie και Hellman, οι οποίοι όρισαν ουσιαστικά την κρυπτογραφία δημόσιου κλειδιού
- Χρησιμοποιείται σε αρκετά εμπορικά προϊόντα
- Πρακτική μέθοδος που επιτρέπει σε δύο χρήστες να ανταλλάξουν με ασφαλή τρόπο ένα μυστικό κλειδί το οποίο μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση μελλοντικών μηνυμάτων
- Η ασφάλεια επιτυγχάνεται λόγω της δυσκολίας υπολογισμού των διακριτών λογαρίθμων



Καθολικά, δημόσια στοιχεία

q

α

Πρώτος αριθμός

$a < q$ και a πρωτοβάθμια ρίζα του q

Παραγωγή κλειδιών του χρήστη Α

Επιλογή ιδιωτικού X_A

$X_A < q$

Υπολογισμός δημόσιου Y_A

$Y_A = a^{X_A} \text{mod } q$

Παραγωγή κλειδιών του χρήστη Β

Επιλογή ιδιωτικού X_B

$X_B < q$

Υπολογισμός δημόσιου Y_B

$Y_B = a^{X_B} \text{mod } q$

Παραγωγή μυστικού κλειδιού από τον χρήστη Α

$K = (Y_B)^{X_A} \text{mod } q$

Παραγωγή μυστικού κλειδιού από τον χρήστη Β

$K = (Y_A)^{X_B} \text{mod } q$

Εικόνα 21.7 Ο αλγόριθμος ανταλλαγής κλειδιών Diffie-Hellman

Παράδειγμα ανταλλαγής Diffie-Hellman

Δεδομένα

- Πρώτος αριθμός $q = 353$
- Πρωτοβάθμια ρίζα $\alpha = 3$

Οι Α και Β υπολογίζουν το δημόσιο κλειδί τους

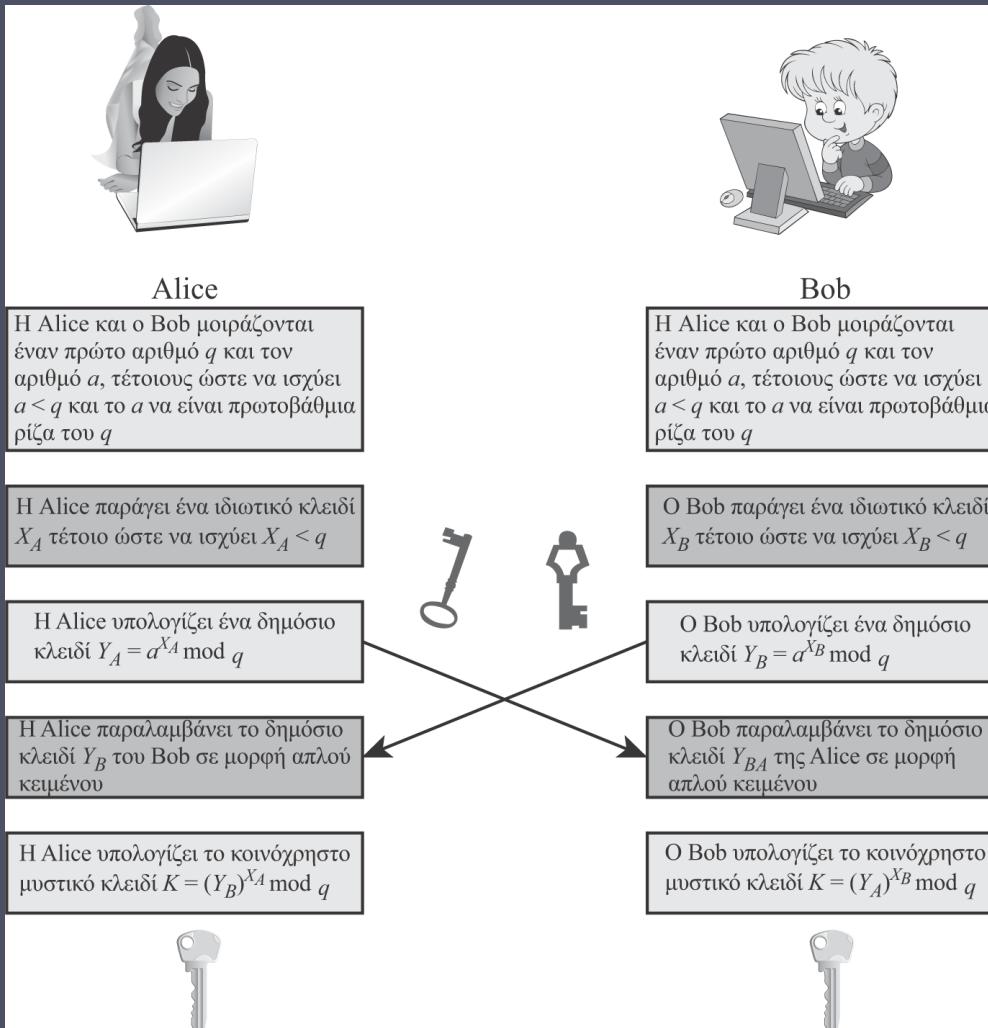
- Ο Α υπολογίζει το $Y_A = 3^{97} \text{ mod } 353 = 40$
- Ο Β υπολογίζει το $Y_B = 3^{233} \text{ mod } 353 = 248$

Ανταλλάσσουν και υπολογίζουν το μυστικό κλειδί:

- Για τον Α: $K = (Y_B)^{X_A} \text{ mod } 353 = 248^{97} \text{ mod } 353 = 160$
- Για τον Β: $K = (Y_A)^{X_B} \text{ mod } 353 = 40^{233} \text{ mod } 353 = 160$

Ο επιτιθέμενος πρέπει να λύσει την εξίσωση

- $3^x \text{ mod } 353 = 40$, το οποίο είναι δύσκολο
- Η ζητούμενη απάντηση είναι το 97· έπειτα υπολογίζει το κλειδί όπως ο Β



Εικόνα 21.8 Ανταλλαγή κλειδιών Diffie-Hellman

Επίθεση μεσάζοντα

- Η επίθεση εξελίσσεται ως εξής :
 1. Ο Darth παράγει τα ιδιωτικά κλειδιά X_{D1} και X_{D2} , και κατόπιν υπολογίζει τα αντίστοιχα δημόσια κλειδιά Y_{D1} και Y_{D2}
 2. Η Alice μεταδίδει το Y_A στον Bob
 3. Ο Darth υποκλέπτει το Y_A και μεταδίδει το Y_{D1} στον Bob. Επίσης ο Darth υπολογίζει το K2
 4. Ο Bob παραλαμβάνει το Y_{D1} και υπολογίζει το K1
 5. Ο Bob μεταδίδει το X_A στην Alice
 6. Ο Darth υποκλέπτει το X_A και μεταδίδει το Y_{D2} στην Alice. Επίσης ο Darth υπολογίζει το K1
 7. Η Alice παραλαμβάνει το Y_{D2} και υπολογίζει το K2
- Όλη η μελλοντική επικοινωνία έχει παραβιαστεί

Άλλοι αλγόριθμοι δημόσιου κλειδιού

Πρότυπο Ψηφιακής Υπογραφής (DSS)

- FIPS PUB 186
- Χρησιμοποιεί τον αλγόριθμο SHA-1 και τον Αλγόριθμο Ψηφιακής Υπογραφής (Digital Signature Algorithm, DSA)
- Προτάθηκε αρχικά το 1991 και αναθεωρήθηκε το 1993 λόγω ανησυχιών για την ασφάλεια. το 1996 πραγματοποιήθηκε μια ακόμα μικρή αναθεώρηση
- Δεν μπορεί να χρησιμοποιηθεί για κρυπτογράφηση ή ανταλλαγή κλειδιών
- Χρησιμοποιεί έναν αλγόριθμο σχεδιασμένο να παρέχει μόνο τη συνάρτηση ψηφιακής υπογραφής

Κρυπτογραφία Ελλειπτικής Καμπύλης (ECC)

- Προσφέρει την ίδια ασφάλεια με τον αλγόριθμο RSA για πολύ μικρότερο πλήθος bit
- Εμφανίζεται σε πρότυπα όπως το P1363 του IEEE
- Το επίπεδο εμπιστοσύνης δεν είναι τόσο υψηλό όσο το αντίστοιχο επίπεδο στον αλγόριθμο RSA
- Βασίζεται σε μια μαθηματική δομή που είναι γνωστή ως ελλειπτική καμπύλη



Σύνοψη

- Ασφαλείς συναρτήσεις κατακερματισμού
 - Απλές συναρτήσεις κατακερματισμού
 - Η ασφαλής συνάρτηση κατακερματισμού SHA
 - SHA-3
- Ο αλγόριθμος Diffie-Hellman και άλλοι ασύμμετροι αλγόριθμοι
 - Ανταλλαγή κλειδιών Diffie-Hellman
 - Άλλοι αλγόριθμοι κρυπτογραφίας δημόσιου κλειδιού



- Ο αλγόριθμος κρυπτογράφησης δημόσιου κλειδιού RSA
 - Περιγραφή του αλγορίθμου
 - Η ασφάλεια του RSA
- ΗMAC
 - Αντικειμενικοί στόχοι σχεδιασμού του ΗMAC
 - Αλγόριθμος ΗMAC
 - Ασφάλεια του ΗMAC