Αλγόριθμοι δημόσιου κλειδιού

Αλγόριθμοι δημόσιου κλειδιού

- Η διανομή του κλειδιού είναι ο πιο αδύναμος κρίκος στα περισσότερα κρυπτογραφικά συστήματα
- Diffie και Hellman, 1976 (Stanford Un.) πρότειναν ένα δραματικά διαφορετικό σύστημα κρυπτογράφησης.
- Στο σύστημα αυτό:
  κλειδί κρυπτογράφησης ≠ κλειδί αποκρυπτογράφησης
  και δεν υπάρχει τρόπος το ένα να προκύψει από το άλλο.
- Οι αλγόριθμοι κρυπτογράφησης, E, και αποκρυπτογράφησης, D, θα πρέπει να πληρούν τις:
  - D(E(P))=P
  - Είναι εξαιρετικά δύσκολο να συνάγεις το D από το E.
  - Ο E δεν μπορεί να σπάσει με επίθεση επιλεγμένου κειμένου

Alice και Bob

- Η Αλίκη θέλει να λαμβάνει μυστικά μηνύματα. Πρώτα πρέπει να φτιάξει δύο αλγορίθμους E_A και D_A που να πληρούν τα προηγούμενα κριτήρια.
- Μετά μπορεί να κοινοποιήσει σε οποιονδήποτε τον αλγόριθμο κα το κλειδί κρυπτογράφησης (π.χ να τα βάλει στο site της).
- Αυτός είναι ο λόγος που λέγεται κρυπτογραφία δημόσιου κλειδιού
- Το ίδιο κάνει και ο Μπόμπος. Δημοσιοποιεί το δικό του E_B παραμετροποιημένο με το δημόσιο κλειδί του. Κρατάει όμως μυστικό το D_B.

Επικοινωνία Αλίκης - Μπόμπου

- Η Αλίκη και ο Μπόμπος δεν έχουν επικοινωνήσει ποτέ πριν. Η Αλίκη επιλέγει το κείμενο που θέλει να στείλει, έστω P, και το χρησιμοποιεί τον δημόσιο αλγόριθμο του Μπόμπου για να δημιουργήσει και να στείλει το $E_B(P)$. Ο Μπ. υπολογίζει το $P=D_B(E_B(P))$.
- Κανείς άλλος δεν μπορεί να υπολογίσει το P γιατί κανένας άλλος δεν έχει το D_B και επειδή τα E_B και D_B έχουν τις ιδιότητες που προαναφέραμε.
- Ο Μπ. μπορεί να απαντήσει χρησιμοποιώντας το E_A.

Ορολογία

Public key cryptography
- public key: δημόσιο κλειδί
- private key: ιδιωτικό κλειδί

Symmetric key cryptography — secret key: μυστικό κλειδί

RSA

- Ron Rivest, Adi Shamir, Len Adleman (1978, MIT)
- Έχει αντέξει σε πολλές προσπάθειες σπασίματος
- Κλειδιά μεγέθους > 1024 bits ➔ πολύ αργός σε σύγκριση με τους συμμετρικούς αλγόριθμους
- Ο RSA είναι κώδικας δέσμης (block cipher) στον οποίο το απλό και το κρυπτογραφημένο κείμενο είναι ακέραιοι από 0 έως n-1.

RSA

- Έστω M ένα κομμάτι (block) απλού κειμένου και C ένα κομμάτι (block) κρυπτογραφημένου κειμένου. Η διαδικασία κρυπτογράφησης - αποκρυπτογράφησης είναι η εξής:
  $C = M^e \bmod n$
  $M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

  Το n και το e είναι γνωστά και στον αποστολέα και στον παραλήπτη, άρα αποτελούν το δημόσιο κλειδί KU$\{e, n\}$

RSA

- Το d είναι γνωστό μόνο στον παραλήπτη άρα είναι μέρος του ιδιωτικού κλειδιού KR$\{d, n\}$.
- Για να μπορεί ένας αλγόριθμος να είναι ισχυρός και υλοποιήσιμος πρέπει να ικανοποιεί τις παρακάτω απαιτήσεις:

  1. Πρέπει να βρεθούν οι τιμές των e, d, n ώστε $M = M^{ed} \bmod n$ για όλα τα $M < n$.
  2. Να είναι εύκολο να υπολογίσω τα C και M^e για όλες τις τιμές $M<n$."
  3. Να είναι αδύνατο να υπολογίσεις το d από τα e και n.

- Οι δύο πρώτες απαιτήσεις ικανοποιούνται εύκολα, η τρίτη είναι ισχυρή μόνο για πολύ μεγάλα e και n.

Επιλογή των *n*, *d* και *e*

- Η επιλογή των *n, d, e* βασίζεται σε αρχές της θεωρίας αριθμών. Συνοπτικά η λειτουργία είναι η εξής:

1. Επέλεξε δύο μεγάλους πρώτους αριθμούς, *p* και *q* (τυπικά > 1024 bits)
2. Υπολόγισε το $n = p \times q$
3. Υπολόγισε το $\varphi(n) = (p-1)(q-1)$ (Euler totient του n)
4. Επέλεξε έναν αριθμό d, σχετικά πρώτο του $\varphi(n)$ τέτοιον ώστε $d < \varphi(n)$.
5. Βρες έναν αριθμό *e* για τον οποίο να ισχύει $e \times d = 1 \bmod \varphi(n)$

Παράδειγμα 1

p=7 και q=17 $\Longrightarrow$ n=119, και φ(n)=96

Η παραγοντοποίηση του 96 → $2^5 \times 3^1$. Επομένως, ένας από τους σχετικά πρώτους αριθμούς του 96 είναι ο 5 $\Longrightarrow$ d=5.

d x e = 1 mod 96 $\Longrightarrow$ 5e = 1 mod 96 και e < 96.

Ποιοι αριθμοί διαιρούνται με το 5 και αν διαιρεθούν με το 96 θα δώσουν υπόλοιπο 1;

1 x 96 = 96 + 1 = 97
2 x 96 = 192 + 1 = 193
3 x 96 = 288 + 1 = 289
4 x 96 = 384 + 1 = 285 √

385 / 5 = 77

Άρα 5 x 77 = 385 = 4 x 96 + 1 = 1 mod 96

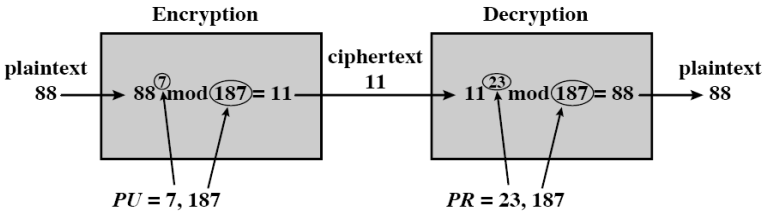
Επομένως e = 77.

public key = {5, 119}

private key = {77, 119}

Παράδειγμα 2

Διαδικασία Κρυπτογράφησης - Αποκρυπτογράφησης



Παράδειγμα 3

P = 3 και q = 11 $\Longrightarrow$ n = 33, και φ(n) = 20

Η παραγοντοποίηση του 20 → $2^2 \times 5^1$. Επομένως, ένας από τους σχετικά πρώτους αριθμούς του 20 είναι ο 3 $\Longrightarrow$ d = 3.

d x e = 1 mod 20 $\Longrightarrow$ 3e = 1 mod 20 και e < 20.

Ποιοι αριθμοί διαιρούνται με το 3 και αν διαιρεθούν με το 20 θα δώσουν υπόλοιπο 1; π.χ. το 21.

Άρα 3 x 7 = 21 = 1 x 20 + 1 = 1 mod 20

Επομένως e = 7.

public key = {3, 33}

private key = {7, 33}

Παράδειγμα 3

Plaintext (P)			Ciphertext (C)		After decryption	
Symbolic	Numeric	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Symbolic
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E
		Sender's computation		Receiver's computation		

Επειδή το n=33 και πρέπει το μέγεθος του block να είναι < 33, μπορώ να κρυπτογραφώ έναν χαρακτήρα τη φορά.
Αν όμως p και q $\approx 2^{512}$ οπότε n $\approx 2^{1024}$ μπορώ να χρησιμοποιώ blocks 1024 bits ή 128 χαρακτήρων σε αντίθεση με τα 8 bytes του DES ή τα 16 του AES

Χρήση RSA

- Ο αλγόριθμος RSA λειτουργεί σαν ECB οπότε χρειάζεται κάποια τεχνική αλύσωσης (chaining). Γενικά είναι πολύ αργός για την κρυπτογράφηση μεγάλου όγκου δεδομένων.
- Σήμερα χρησιμοποιείται κυρίως στη διαδικασία ανταλλαγής των κλειδιών μιας χρήσης στους συμμετρικούς αλγόριθμους όπως ο 3DES.

Άλλοι αλγόριθμοι δημόσιου κλειδιού

- The knapsack algorithm (Merkle και Hellman, 1978)
- Αλγόριθμοι βασισμένοι σε διακριτούς λογαρίθμους (ElGamal, 1985) (Schnorr, 1991)
- Αλγόριθμοι βασισμένοι στις ιδιότητες ελλειπτικών καμπυλών (Menezes και Vanstone, 1993)

Παρεξηγήσεις σχετικά με τις ικανότητες κρυπτογράφησης δημόσιου κλειδιού

1. Η κρυπτογραφία δημόσιου κλειδιού (ΚΔΚ) είναι πιο ισχυρή από τις συμμετρικές μεθόδους (ΚΣΚ):

   Στην πραγματικότητα η ισχύς κάθε συστήματος κρυπτογράφησης εξαρτάται:

   1. Από το μέγεθος του κλειδιού, και
   2. Από τον υπολογιστικό φόρτο για το σπάσιμο του κώδικα

2. Η ΚΔΚ έχει καταστήσει την ΚΣΚ άχρηστη.

   Αντίθετα, λόγω του υπολογιστικού φόρτου που σχετίζεται με την ΚΔΚ δεν φαίνεται να υπάρχει πιθανότητα εγκατάλειψης της ΚΣΚ στο κοντινό μέλλον

3. Υπάρχει η αίσθηση ότι η διανομή του δημόσιου κλειδιού είναι μια πολύ απλή υπόθεση, σε σύγκριση με τη διανομή συμμετρικών κλειδιών.

   Στην πραγματικότητα οι διαδικασίες που απαιτούνται δεν είναι πιο απλές ούτε πιο αποδοτικές από εκείνες της συμβατικής κρυπτογραφίας. Και εδώ απαιτείται η ύπαρξη κατάλληλου πρωτοκόλλου και πράκτορα (agent) διαμοιρασμού κλειδιών

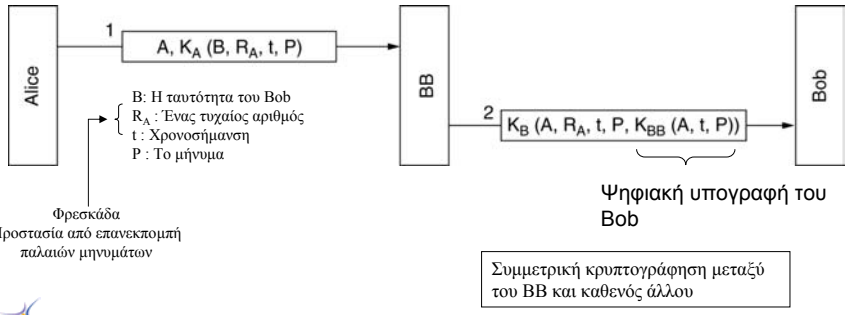
Ψηφιακές υπογραφές

Ψηφιακές υπογραφές

- Υπάρχει ανάγκη αντικατάστασης των χειρόγραφων υπογραφών με ψηφιακές (ΨΥ)
- Αυτές πρέπει να διαθέτουν τα εξής χαρακτηριστικά:
  - Ο παραλήπτης πρέπει να είναι σε θέση να πιστοποιήσει την ταυτότητα του αποστολέα
  - Ο αποστολέας να μην μπορεί να απαρνηθεί το περιεχόμενο του μηνύματος
  - Ο παραλήπτης να μην μπορεί να παραποιήσει το μήνυμα

Υπογραφές συμμετρικού κλειδιού

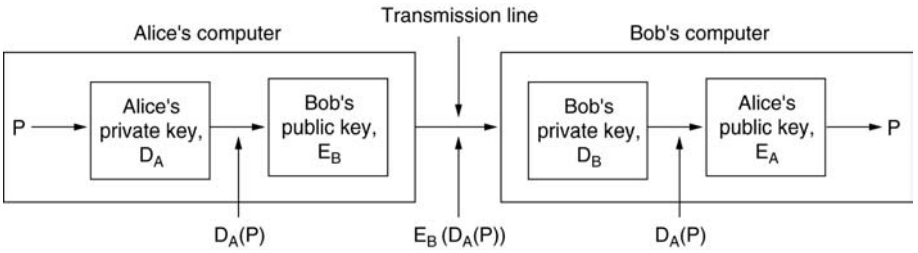
- Μια προσέγγιση στις ΨΥ είναι να υπάρχει μια αρχή που γνωρίζει τους πάντες και την εμπιστεύονται οι πάντες.
  Έστω ότι ονομάζεται BigBrother (BB)



ΨΥ Δημόσιου κλειδιού

- Πρόβλημα στις ΨΥΣΚ: (α) όλοι πρέπει να εμπιστεύονται τον ΒΒ και (β) ο ΒΒ μπορεί να διαβάσει τα μηνύματα όλων
- Εναλλακτικά μπορεί να χρησιμοποιηθεί ΚΔΚ. Προϋπόθεση είναι να υπάρχει αλγόριθμος ΔΚ για τον οποίον εκτός από D(E(P))=P να ισχύει και E(D(P))=P, γεγονός που ισχύει για τον RSA.

ΨΥ Δημόσιου κλειδιού



$P \rightarrow D_A(P) \rightarrow E_B(D_A(P)) \longrightarrow D_B(E_B(D_A(P))) \rightarrow E_A(D_A(P)) \rightarrow P$

μετάδοση

Εξασφαλίζει μη-απάρνηση αν:
1. η Α δεν αλλάξει το δημόσιο κλειδί της
2. ο D_A παραμείνει μυστικός

Digital Signature Standard (DSS)

- Το 1991 το NIST πρότεινε μια παραλλαγή του ElGamal ως DSS. Το πρόβλημα είναι: ότι ο αλγόριθμος που χρησιμοποιείται είναι:
  - Πολύ μυστικός (NSA version)
  - Πολύ αργός (x10 – x40 > RSA)
  - Πολύ νέος (δεν έχει δοκιμαστεί αρκετά)
  - Πολύ ανασφαλής (κλειδιά 512 bit)

Ψηφιακές υπογραφές

Message Digest
(Περίληψη μηνύματος)

Περίληψη μηνύματος (message digest)

- Οι μέθοδοι ΨΥ έχουν δεχθεί κριτική διότι συνήθως μπερδεύουν δύο διακριτές λειτουργίες : την αυθεντικοποίηση και τη μυστικότητα.
- Υπάρχει μια τεχνική που επικεντρώνεται μόνο στην αυθεντικοποίηση.
- Ονομάζεται message digest (MD) και βασίζεται στη χρήση μιας συνάρτησης κοπής (hash function) η οποία παραλαμβάνει ένα απλό κείμενο οσοδήποτε μεγάλο και αυτό παράγει ένα συρμό από bit με συγκεκριμένο μήκος.

Η MD έχει τέσσερις ιδιότητες

1. Με δοσμένο P μπορεί εύκολα να υπολογίσει το MD(P).
2. Με δεδομένο το MD(P) είναι επί της ουσίας αδύνατο να βρεις το P.
3. Με δεδομένο P είναι αδύνατο να βρεθεί P΄ τέτοιο ώστε MD(P΄)=MD(P).
4. Η αλλαγή ακόμα και 1 bit στην είσοδο να παράγει μια πολύ διαφορετική έξοδο.

Message digest

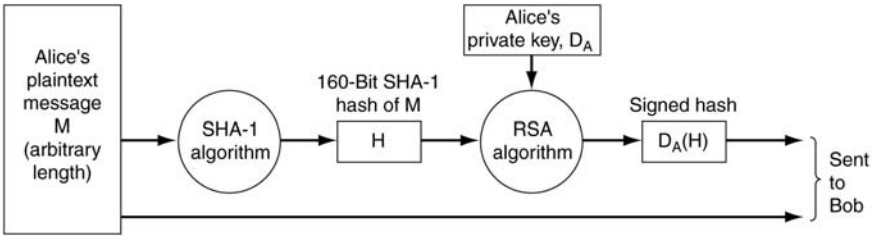
Διαφορές με ΨΥΔΚ και ΨΥΣΚ

- Στην περίπτωση ΨΥΣΚ αντί για το $K_{BB}(A, t, P)$ ο ΒΒ μπορεί να στείλει το $K_{BB}(A, t, MD(P))$ που είναι πιο εύκολο να υπολογιστεί και καταλαμβάνει λιγότερο χώρο.
- Στην περίπτωση ΨΥΔΚ η Α μπορεί να στείλει το $\{P, D_A(MD(P))\}$ ο Β μπορεί να υπολογίσει το MD(P) και να το συγκρίνει με το $E_A(D_A(MD(P)))$.
- Οι συχνότερα χρησιμοποιούμενες συναρτήσεις περίληψης μηνύματος είναι οι MD5, SHA-1 και RIPEMD-160.

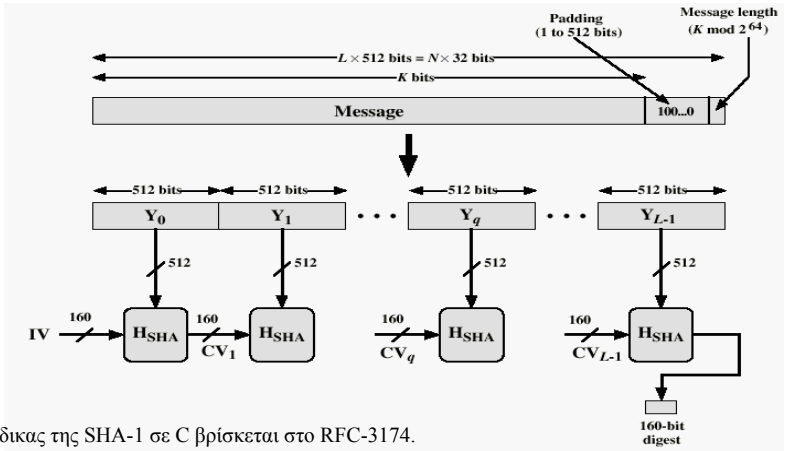
MD5 (RFC 1321)

- Ron Rivest, 1992
- Ο αλγόριθμος επεξεργάζεται το μήνυμα σε κομμάτια των 512 bits και στο τέλος παράγει μια περίληψή του μήκους 128 bits
- Ο MD5 είναι ευαίσθητος στην «επίθεση γενεθλίων» (birthday attack) και τελευταία (2004 και 2005) έχουν δημοσιευθεί τεχνικές για την εύρεση κειμένων που οδηγούν στην ίδια περίληψη του κειμένου
- Έτσι, αν και έχει χρησιμοποιηθεί ευρύτατα στο παρελθόν υπάρχει περίπτωση η τάση να αντικατασταθεί από τεχνικές που παράγουν πιο μεγάλη περίληψη.

SHA-1

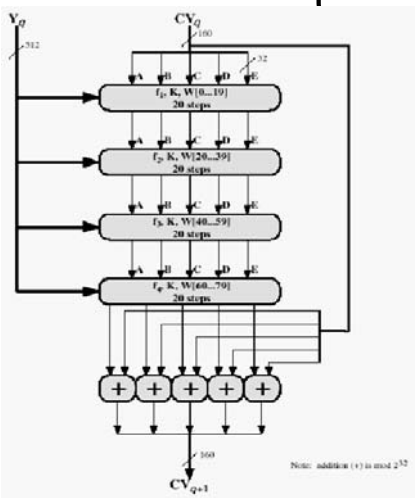


Δημιουργία περίληψης μηνύματος με χρήση της SHA-1



Ο κώδικας της SHA-1 σε C βρίσκεται στο RFC-3174.
Χρησιμοποιείται padding 1000…. ώστε να ολοκληρωθεί το block των 512 bits
Message length K (μέγεθος πριν το padding) 64 bits προστίθονται στο τέλος με OR

Επεξεργασία ενός block 512 bits με την SHA-1



Υπάρχουν 5 μεταβλητές (A, B, C, D, E) 32 bit που ανανεώνονται στη διάρκεια της διαδικασίας και που στο τέλος δημιουργούν το MD μεγέθους 160 bits