ΤΕΙ ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΑΝΟΙΚΤΑ ΑΚΑΔΗΜΑΙΚΑ ΜΑΘΗΜΑΤΑ

ΑΣΦΑΛΕΙΑ & ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ(Θ)

Ενότητα 6: ΑΣΦΑΛΕΙΑ & ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ

ΔΙΔΑΣΚΩΝ: ΚΩΝΣΤΑΝΤΙΝΟΣ ΧΕΙΛΑΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΤΕ

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

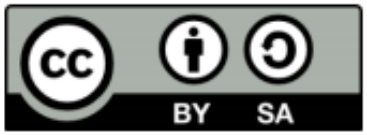
ΕΣΠΑ 2007-2013
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.

- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.



Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «Ανοικτά Ακαδημαϊκά Μαθήματα στο ΤΕΙ Κεντρικής Μακεδονίας» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Ενότητα 6

ΑΣΦΑΛΕΙΑ & ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ

Χειλάς Κωνσταντίνος
Διδάκτορας Φυσικής

Περιεχόμενα ενότητας

1. Ψηφιακές υπογραφές
2. Υπογραφές συμμετρικού κλειδιού
3. ΨΥ Δημόσιου κλειδιού
4. Digital Signature Standard (DSS)
5. Ψηφιακές υπογραφές
    1. Message Digest(Περίληψη μηνύματος)
6. Η MD έχει τέσσερις ιδιότητες
7. Διαφορές με ΨΥΔΚ και ΨΥΣΚ
8. MD5 (RFC 1321)
9. Δημιουργία περίληψης μηνύματος με χρήση της SHA-1
10. Επεξεργασία ενός block 512 bits με την SHA-1
11. Διαδικασία ψηφιακής υπογραφής με χρήση SHA-1 και RSA
12. Διαχείριση δημόσιων κλειδιών
    1. Διαχείριση ψηφ. Υπογραφών
    2. Προβλήματα με ΨΥΔΚ
    3. PKI
    4. Πιστοποιητικά
    5. X.509 (τα βασικά πεδία ενός πιστοποιητικού)

Σκοποί ενότητας

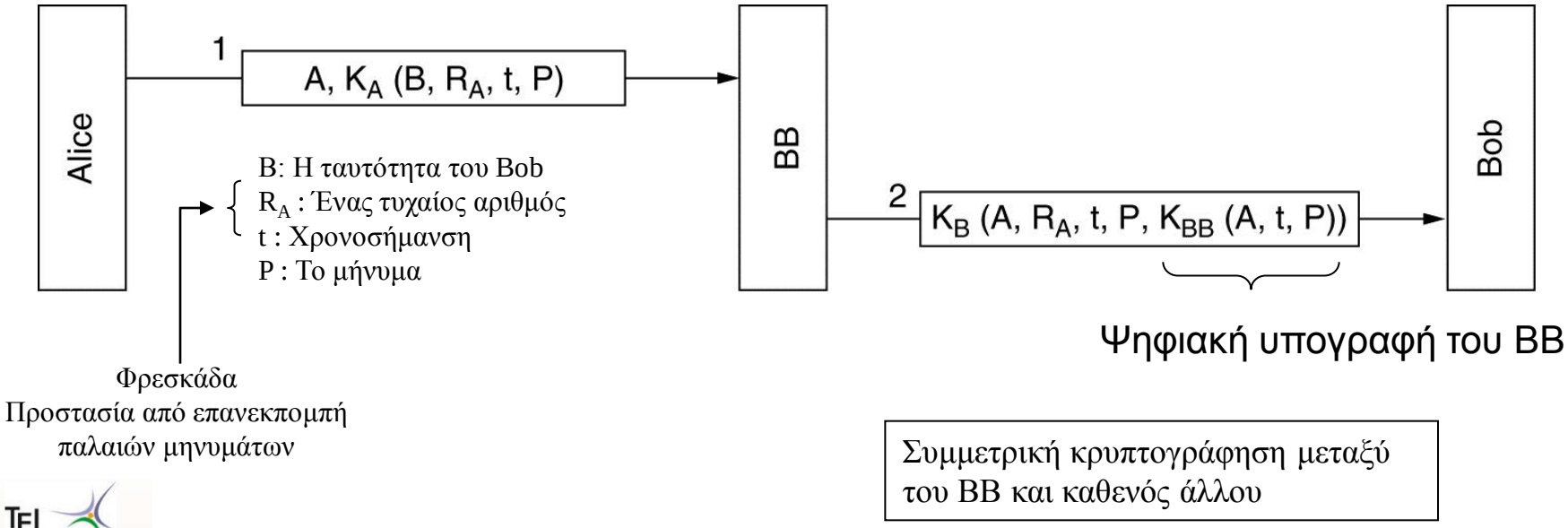
Ψηφιακές υπογραφές

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

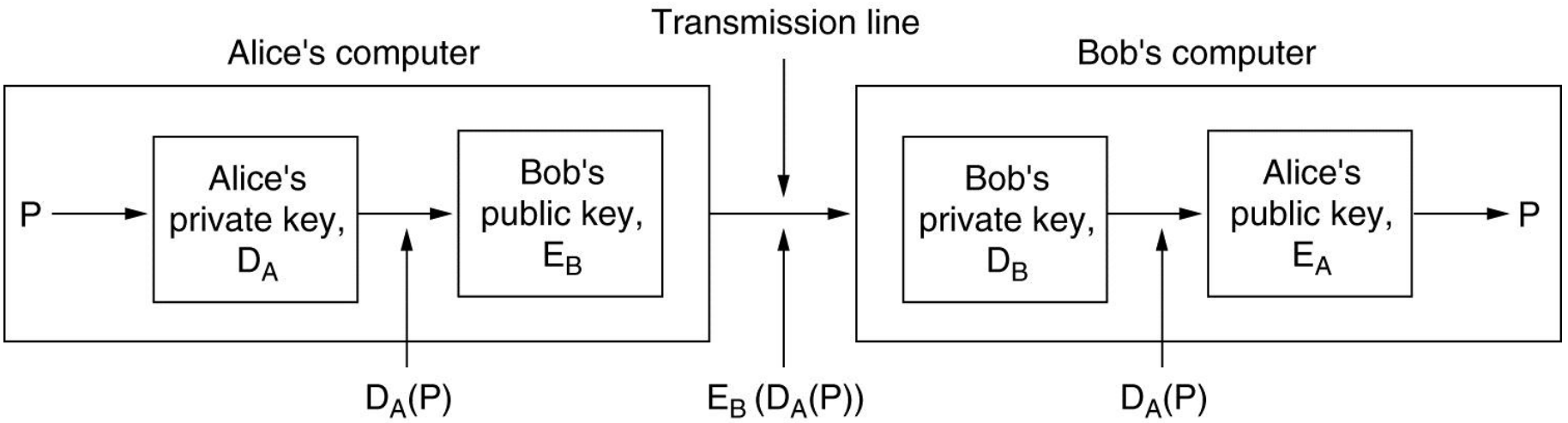
- Μια προσέγγιση στις ΨΥ είναι να υπάρχει μια αρχή που γνωρίζει τους πάντες και την εμπιστεύονται οι πάντες.
  Έστω ότι ονομάζεται BigBrother (BB)



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

Message digest

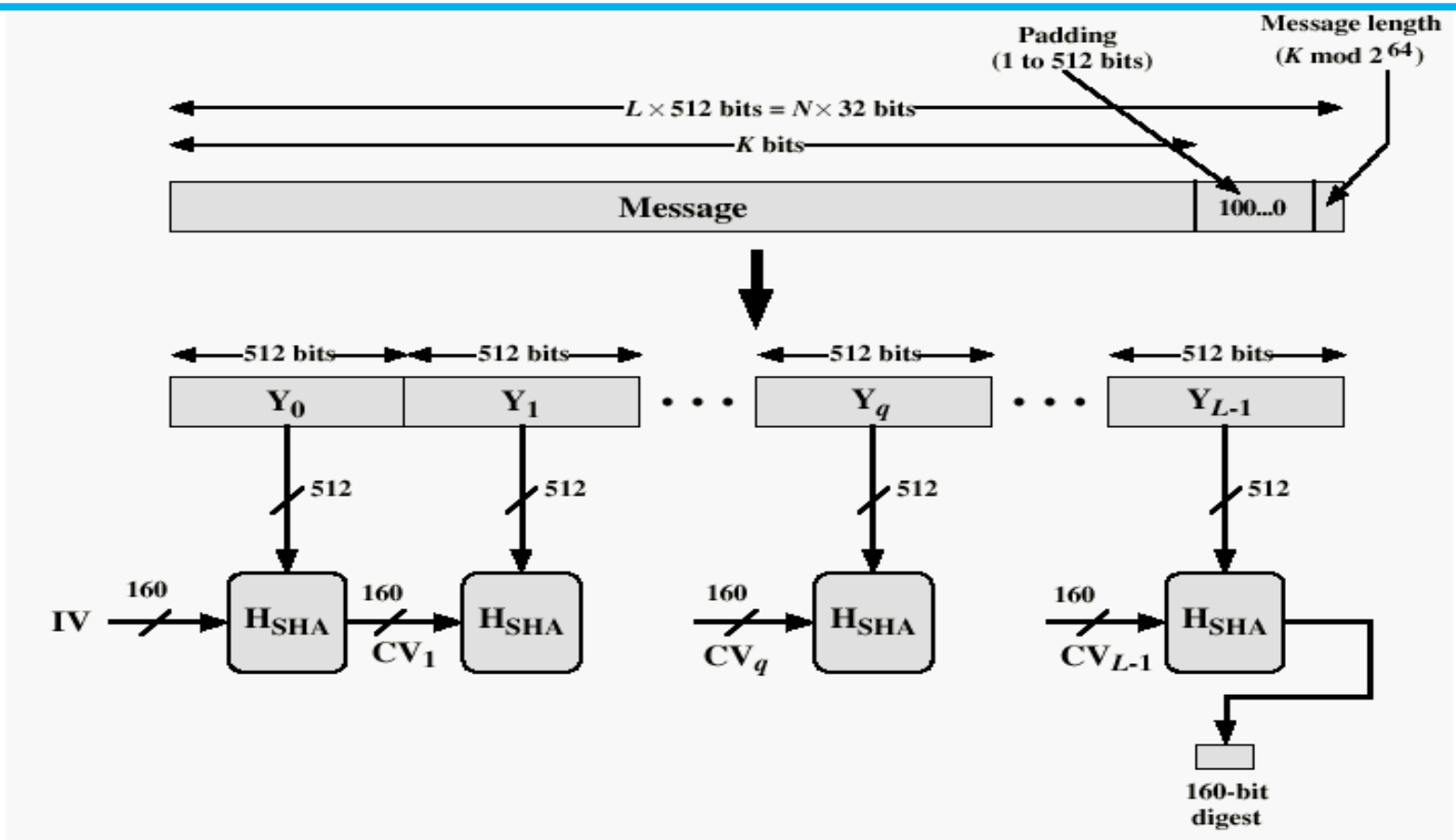
Διαφορές με ΨΥΔΚ και ΨΥΣΚ

- Στην περίπτωση ΨΥΣΚ αντί για το $K_{BB}(A, t, P)$ ο BB 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)

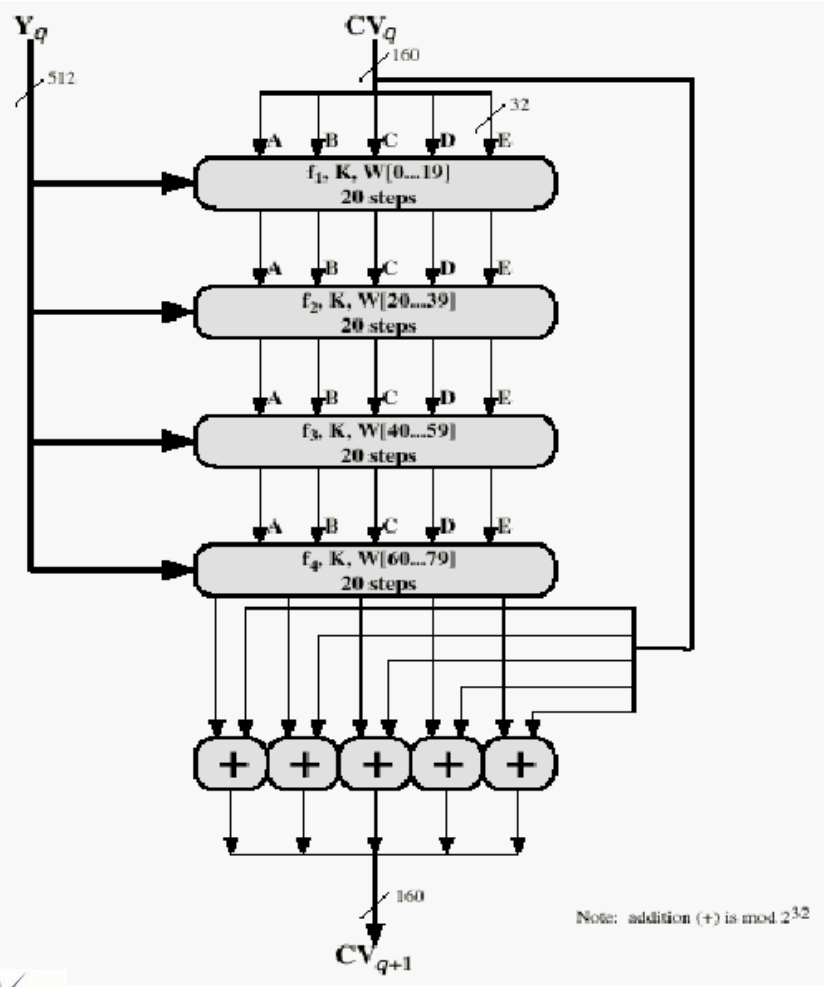
- Ron Rivest, 1992
- Ο αλγόριθμος επεξεργάζεται το μήνυμα σε κομμάτια των 512 bits και στο τέλος παράγει μια περίληψή του μήκους 128 bits
- Ο MD5 είναι ευαίσθητος στην «επίθεση γενεθλίων» (birthday attack) και τελευταία (2004, 2005, 2008) έχουν δημοσιευθεί τεχνικές για την εύρεση κειμένων που οδηγούν στην ίδια περίληψη του κειμένου.
  - Marc Stevens, Arjen Lenstra and Benne de Weger, "Chosen-prefix Collisions for MD5 and Applications", 25th Annual Chaos Communication Congress, Berlin, December 2008.
- Έτσι, αν και έχει χρησιμοποιηθεί ευρύτατα στο παρελθόν υπάρχει η τάση να αντικατασταθεί από τεχνικές που παράγουν πιο μεγάλη περίληψη όπως, για παράδειγμα, ο SHA-2.

Δημιουργία περίληψης μηνύματος με χρήση της SHA-1



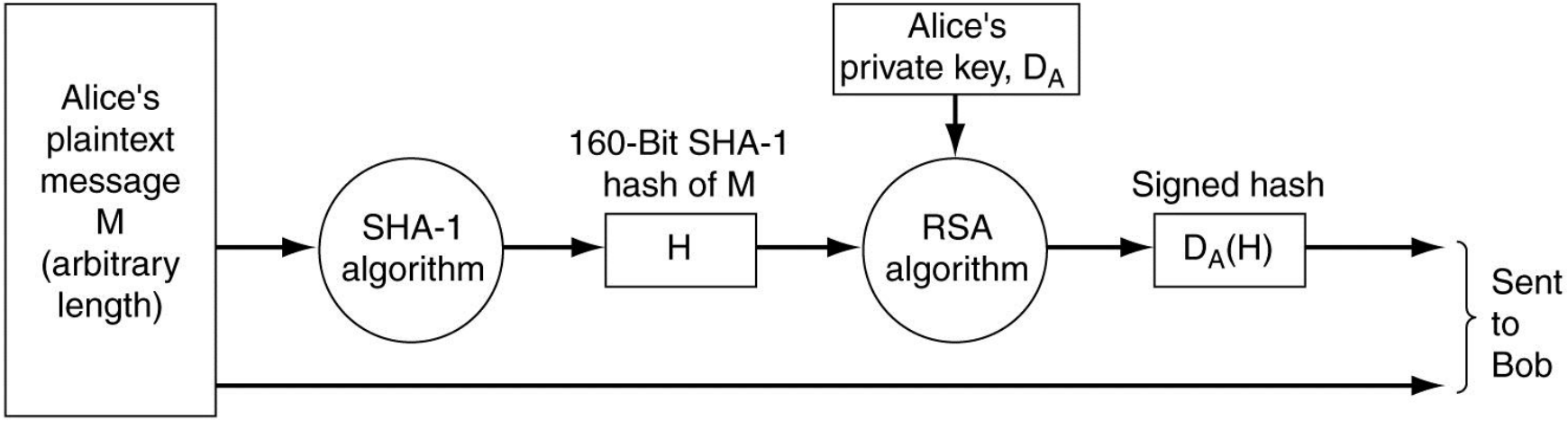
Ο κώδικας της SHA-1 σε C βρίσκεται στο RFC-3174.
Χρησιμοποιείται padding 1000…. ώστε να ολοκληρωθεί το block των 512 bits
Message length K (μέγεθος πριν το padding) 64 bits προστίθενται στο τέλος με OR

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

Διαδικασία ψηφιακής υπογραφής με χρήση SHA-1 και RSA

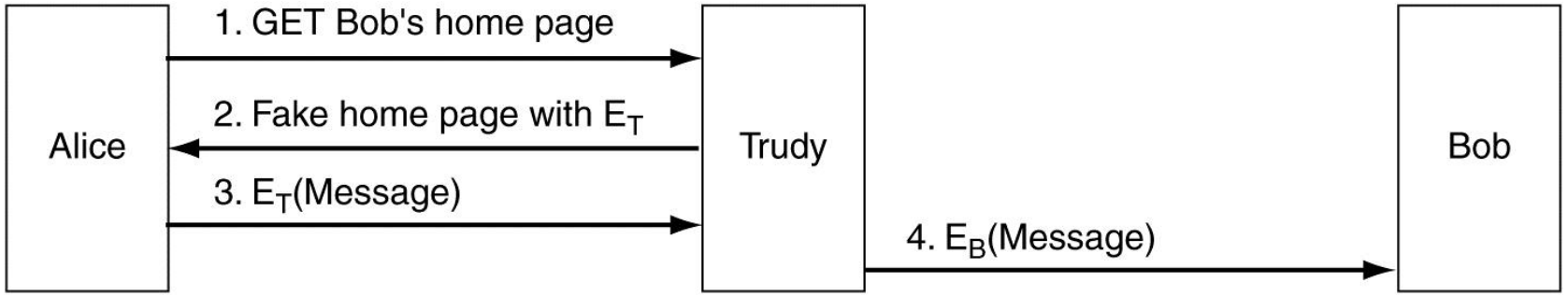


Διαχείριση δημόσιων κλειδιών

Διαχείριση ψηφ. υπογραφών

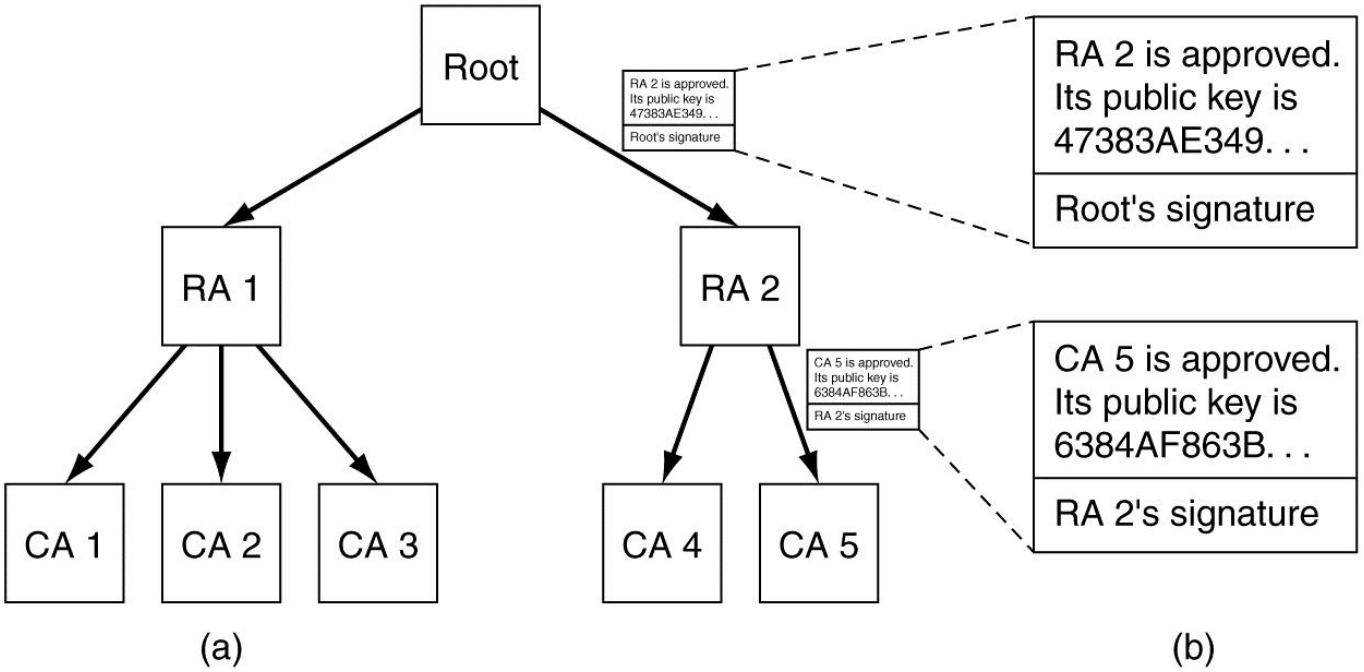
- Certificates
- X.509
- Public Key Infrastructures

Προβλήματα με ΨΥΔΚ



- Αν ο Bob και η Alice δεν γνωρίζονται, πώς παίρνει ο ένας το δημόσιο κλειδί του άλλου;
- Η Trudy μπορεί να παρεμβληθεί και να παρουσιάσει μια ιστοσελίδα ως του Bob, παρέχοντας όμως το δικό της δημόσιο κλειδί (?)

PKI



(a) μια ιεραρχική δομή PKI.

(b) Ένα δέντρο (αλυσίδα) πιστοποιητικών.

Πιστοποιητικά

I hereby certify that the public key
19836A8B03030CF83737E3837837FC3s87092827262643FFA82710382828282A
belongs to
Robert John Smith
12345 University Avenue
Berkeley, CA 94702
Birthday: July 4, 1958
Email: bob@superdupernet.com

SHA-1 hash of the above certificate signed with the CA's private key

Ένα πιθανό πιστοποιητικό υπογεγραμμένο με το ιδιωτικό κλειδί μιας CA (Verisign, COMODO, HARICA, …).

X.509
(τα βασικά πεδία ενός πιστοποιητικού)

Field	Meaning
Version	Which version of X.509
Serial number	This number plus the CA's name uniquely identifies the certificate
Signature algorithm	The algorithm used to sign the certificate
Issuer	X.500 name of the CA
Validity period	The starting and ending times of the validity period
Subject name	The entity whose key is being certified
Public key	The subject's public key and the ID of the algorithm using it
Issuer ID	An optional ID uniquely identifying the certificate's issuer
Subject ID	An optional ID uniquely identifying the certificate's subject
Extensions	Many extensions have been defined
Signature	The certificate's signature (signed by the CA's private key)

Τέλος Ενότητας