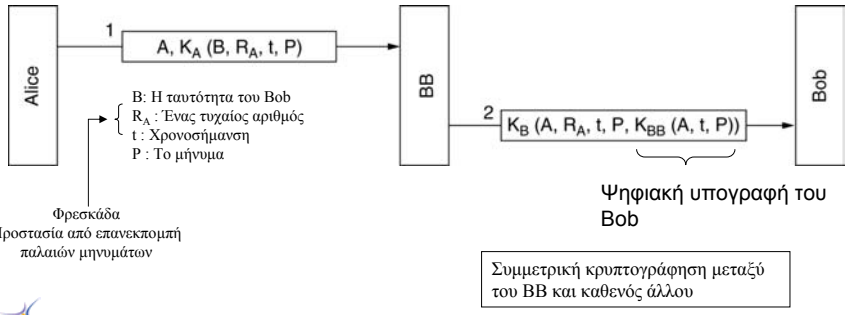
Ψηφιακές υπογραφές

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

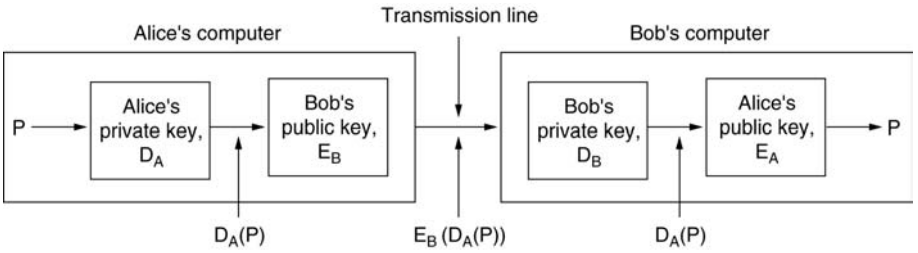
- Μια προσέγγιση στις ΨΥ είναι να υπάρχει μια αρχή που γνωρίζει τους πάντες και την εμπιστεύονται οι πάντες.
  Έστω ότι ονομάζεται BigBrother (BB)



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

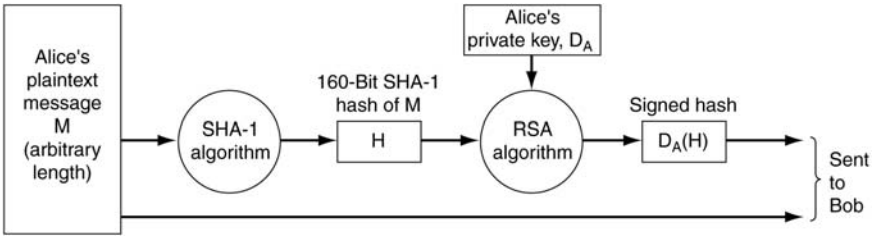
Διαφορές με ΨΥΔΚ και ΨΥΣΚ

- 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.

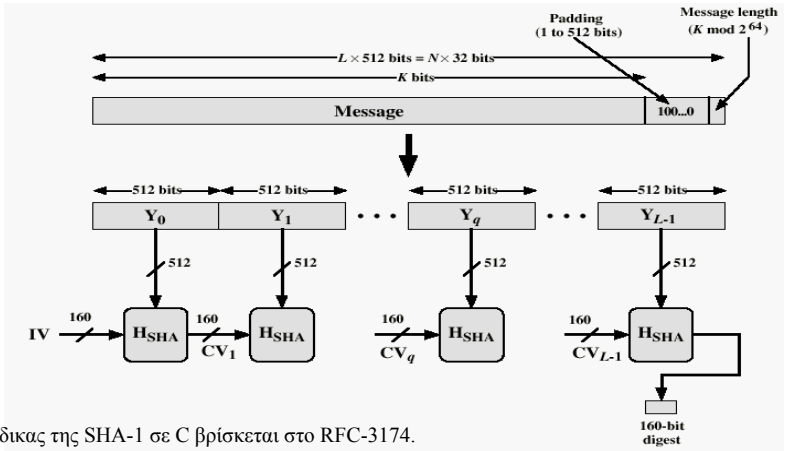
MD5 (RFC 1321)

- 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

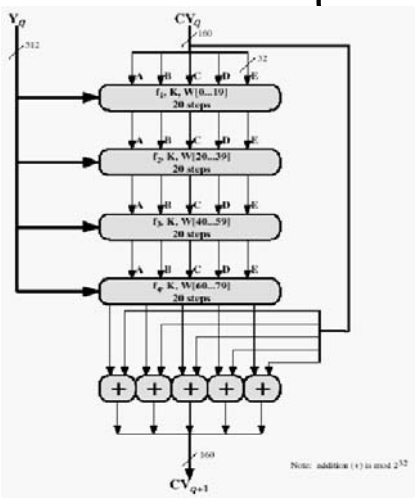


Δημιουργία περίληψης μηνύματος με χρήση της SHA-1



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