ΚΡΥΠΤΟΓΡΑΦΙΑ

- Η επιστήμη και η μελέτη της τήρησης μυστικών
- Κρυπτογράφηση: μέθοδος μετασχηματισμού απλού-μη κρυπτογραφημένου κειμένου (plaintext) σε κρυπτογραφημένο κείμενο (cipher text)
- Ο μετασχηματισμός ορίζεται μέσω ενός *κλειδιού*

Συστήματα κρυπτογραφίας

- Ενός κλειδιού
- Δύο κλειδιών
- Δημόσιου κλειδιού
- Ψηφιακές υπογραφές
- Συστατικά
  - Ο χώρος μη κρυπτογραφημένων μηνυμάτων M
  - Ο χώρος κρυπτογραφημένων μηνυμάτων C
  - Ο χώρος κλειδιών K
  - Μία οικογένεια μετασχηματισμών κρυπτογράφησης Ek: M → C
  - Μία οικογένεια μετασχηματισμών αποκρυπτογράφησης Dk: C → M

Στόχοι κρυπτογραφίας

- Εχεμύθεια
  - Πρέπει να είναι ανέφικτο να υπολογιστεί το Dk από το c, ακόμη και αν είναι γνωστό το m
  - Πρέπει να είναι ανέφικτος ο υπολογισμός του m από ένα c
- Αυθεντικότητα
  - Πρέπει να είναι υπολογιστικά ανέφικτο να προσδιοριστεί το Ek από το c, ακόμη και αν είναι γνωστό το m
  - Πρέπει να είναι υπολογιστικά ανέφικτο να βρεθεί ένα c', τέτοιο ώστε το Dk(c') να είναι παραδεκτό μη κρυπτογραφημένο μήνυμα του συνόλου M

Επιθυμητές ιδιότητες συστημάτων κρυπτογραφίας

- Πρέπει να υπάρχουν αποδοτικοί αλγόριθμοι για τις λειτουργίες της κωδικοποίησης και της αποκωδικοποίησης
- Εύχρηστο σύστημα
- Η προστασία που παρέχει το σύστημα πρέπει να προϋποθέτει μόνο τη μυστικότητα των κλειδιών, όχι του αλγόριθμου

Η κρυπτογραφία δεν είναι απρόσβλητη - Κρυπτανάλυση

- Κρυπτανάλυση: καταστρέφω τους στόχους της κρυπτογραφίας
  - Παραβίαση εχεμύθειας: διαβάζω το κείμενο χωρίς να έχω εξουσιοδότηση
  - Παραβίαση αυθεντικότητας: δημιουργώ μήνυμα που φαίνεται να προέρχεται από άλλον αποστολέα
- Παραδοσιακές μέθοδοι κρυπτανάλυσης: αναλυτική σκέψη, εφαρμογή μαθηματικών εργαλείων, αναγνώριση προτύπων, υπομονή , αποφασιστικότητα και τύχη
- Σύγχρονες μέθοδοι: μαθηματικές έννοιες, όπως η παραγοντοποίηση ακεραίων και η εύρεση διακριτών λογαρίθμων

Κρυπτανάλυση – Είδη επιθέσεων

- Μόνο βάσει κρυπτογραφημένου κειμένου
  - Ο επιτιθέμενος γνωρίζει μόνο το κρυπτογραφημένο κείμενο και προσπαθεί μα βρει το μη κρυπτογραφημένο, χωρίς να έχει καμία πρότερη γνώση του τελευταίου. Η αντοχή ενός κρυπτογραφικού κώδικα σε αυτόν τον τύπο επίθεσης είναι το βασικότερο χαρακτηριστικό της ποιότητάς του
- Βάσει γνωστού μη κρυπτογραφημένου κειμένου
  - Ο επιτιθέμενος γνωρίζει το μη κρυπτογραφημένο κείμενο καθώς και το αντίστοιχο κρυπτογραφημένο (Το συγκεκριμένο μήνυμα θεωρείται ότι έχει «σπάσει»)
  - Σε μερικά συστήματα, η γνώση ενός και μόνου ζεύγους *(μη κρυπτογραφημένο κείμενο, κρυπτογραφημένο κείμενο)* επαρκεί για να απωλεσθεί όλη η ασφάλεια του συστήματος (ανεπιθύμητο)
  - Σημείο εκκίνησης όταν η μηχανή κρυπτογράφησης είναι διαθέσιμη στον επιτιθέμενο

Κρυπτανάλυση – Είδη επιθέσεων

- *Επιλεγμένο μη κρυπτογραφημένο κείμενο.*
  - Στην επίθεση αυτή ο επιτιθέμενος μπορεί να βρει το κρυπτογραφημένο κείμενο που αντιστοιχεί σε ένα μη κρυπτογραφημένο κείμενο που αυτός επιλέγει
- *Επιλεγμένο κρυπτογραφημένο κείμενο*
  - Ο επιτιθέμενος μπορεί να επιλέξει όποιο κρυπτογραφημένο κείμενο επιθυμεί και να υπολογίσει το αντίστοιχο μη κρυπτογραφημένο κείμενο. Ο τύπος αυτός επίθεσης μπορεί να απαντηθεί σε συστήματα δημόσιου κλειδιού όπου μπορεί να αποκαλυφθεί το ιδιωτικό κλειδί
- *Προσαρμοζόμενο επιλεγμένο μη κρυπτογραφημένο κείμενο*
  - Ο επιτιθέμενος μπορεί να προσδιορίσει το κρυπτογραφημένο κείμενο για επιλεγμένα μη κρυπτογραφημένα κείμενα σε μία επαναληπτική διαδικασία, βάσει των προηγούμενων αποτελεσμάτων

Κρυπτογράφηση με μεταθέσεις

- Βασική ιδέα: αλλαγή της θέσης bits ή bytes εντός του μηνύματος
- Χαρακτηριστικοί εκπρόσωποι:
  - Απλή μετάθεση
  - «Συρματόπλεγμα»
  - Μετάθεση κατά στήλες

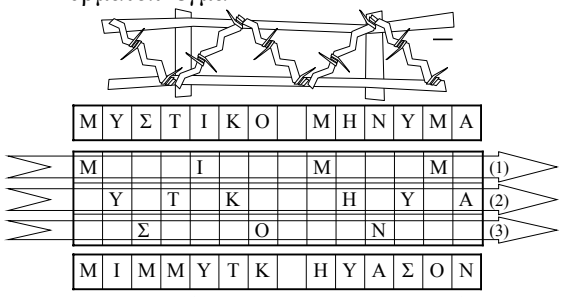
Κρυπτογράφηση με μεταθέσεις

- Απλή μετάθεση
  - Το μήνυμα *m* κατατμείται σε μπλοκ και κάθε μπλοκ αναδιατάσσεται βάσει κάποιου σχήματος
  - Παράδειγμα
    - » Κλειδί = (25413)

m	Μ	Υ	Σ	Τ	Ι	Κ	Ο		Μ	Η	Ν	Υ	Μ	Α	∅
c	Υ	Ι	Τ	Μ	Σ	Ο	Η	Μ	Κ		Υ	∅	Α	Ν	Μ

Κρυπτογράφηση με μεταθέσεις

- «Συρματόπλεγμα»



- Παράμετροι: (ύψος, μετατόπιση αρχής)

Κρυπτογράφηση με μεταθέσεις

- Μετάθεση κατά στήλες
  - Κλειδί: μία λέξη, της οποίας τα γράμματα αντιστοιχίζονται σε αριθμούς, ανάλογα με τη σειρά εμφάνισής τους στο αλφάβητο

Π	Ο	Λ	Υ	Μ	Ε	Ρ	Ε	Σ
6	5	3	9	4	1	7	2	8

  - Το μη κρυπτογραφημένο κείμενο γράφεται σε έναν πίνακα που έχει τόσες στήλες όσες τα γράμματα του κλειδιού

συνέχεια >>

Κρυπτογράφηση με μεταθέσεις

- Μετάθεση κατά στήλες
  - ΑΣΠΡΗ ΠΕΤΡΑ ΞΕΞΑΣΠΡΗ

Π	Ο	Λ	Υ	Μ	Ε	Ρ	Ε	Σ
6	5	3	9	4	1	7	2	8
Α	Σ	Π	Ρ	Η		Π	Ε	Τ
Ρ	Α		Ξ	Ε	Ξ	Α	Σ	Π
Ρ	Η	∅	∅	∅	∅	∅	∅	∅

  - Το κρυπτογραφημένο κείμενο παράγεται με ανάγνωση του πίνακα κατά στήλες, με τη σειρά που ορίζεται από την απεικόνιση του κλειδιού

	Ξ	∅	Ε	Σ	∅	Π		∅	Η	Ε	∅	Σ	Α	Η	Α	Ρ	Ρ	Π	...

Κρυπτογράφηση με αντικατάσταση

- Βασική ιδέα: Κάθε χαρακτήρας του μη κρυπτογραφημένου κειμένου αντικαθίσταται από έναν διαφορετικό χαρακτήρα στο κρυπτογραφημένο κείμενο
  - Απλή αντικατάσταση
  - Πολυαλφαβητική αντικατάσταση
  - Αντικατάσταση τρέχοντος κλειδιού
  - Μέθοδος Vernam

Κρυπτογράφηση με αντικατάσταση

- Απλή αντικατάσταση
  - Για κάθε γράμμα του αλφάβητου των μηνυμάτων ορίζουμε την απεικόνισή του.

Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω
Δ	Κ	Ρ	Ο	Υ	Λ	Ω	Ε	Π	Η	Α	Φ	Ζ	Μ	Τ	Β	Χ	Θ	Ν	Ψ	Γ	Ι	Σ	Ξ

ΑΣΠΡΗ ΠΕΤΡΑ ΞΕΞΑΣΠΡΗ

ΔΘΒΧΩ ΒΥΝΧΔ ΜΥΜΔΘΒΧΩ

- Ιδιαίτερα ευάλωτη προσέγγιση σε στατιστικές αναλύσεις εμφάνισης μεμονωμένων χαρακτήρων, ζευγών, τριάδων, κ.λπ.

Κρυπτογράφηση με αντικατάσταση

- Πολυαλφαβητική αντικατάσταση
  - Απαιτείται ένα κλειδί
  - Χρησιμοποιούμε έναν δισδιάστατο πίνακα απεικόνισης, οι γραμμές του οποίου αντιστοιχούν σε χαρακτήρες του κλειδιού και οι στήλες σε χαρακτήρες του μηνύματος
  - Αν M_i είναι ο υπ' αριθμόν i χαρακτήρας του μη κρυπτογραφημένου μηνύματος και K_i ο υπ' αριθμόν i χαρακτήρας του κλειδιού, ο υπ' αριθμόν i χαρακτήρας του κρυπτογραφημένου μηνύματος είναι η καταχώρηση στη θέση (K_i, M_i) του πίνακα

Κρυπτογράφηση με αντικατάσταση

- Πολυαλφαβητική αντικατάσταση - παράδειγμα

	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω
Α	Δ	Κ	Ρ	Ο	Υ	Λ	Ω	Ε	Π	Η	Α	Φ	Ζ	Μ	Τ	Β	Χ	Θ	Ν	Ψ	Γ	Ι	Σ	Ξ
Β	Η	Λ	Θ	Ρ	Δ	Ξ	Κ	Α	Φ	Ο	Γ	Ψ	Π	Ι	Υ	Χ	Μ	Β	Σ	Ω	Ε	Ν	Ζ	Τ

- Κλειδί κρυπτογράφησης: ΑΒΒΑ

ΑΣΠΡΗ ΠΕΤΡΑ ΞΕΞΑΣΠΡΗ ← Plaintext

ΑΒΒΑΑ ΒΒΑΑΒ ΒΑΑΒΒΑΑΒ ← Κλειδί

ΔΒΧΧΩ ΧΔΝΧΗ ΙΘΜΗΒΒΧΚ ← Ciphertext

Κρυπτογράφηση με αντικατάσταση

- Πολυαλφαβητική αντικατάσταση – επιλογές
  - Αν το κλειδί τελειώσει τότε:
    - » Ξαναχρησιμοποιείται εξ αρχής
      ΑΒΒΑ → ΑΒΒΑΑΒΒΑΑΒΒΑΑΒΒΑ
    - » Ξαναχρησιμοποιείται μετασχηματισμένο
      HAL → HALIBMJCN…
    - » Χρησιμοποιούμε ως κλειδί το ίδιο το μήνυμα
      ΑΒΒΑ → ΑΒΒΑΑΣΠΡΗΠΕΤΡΑΞΕΞΑΣΠΡΗ
- Αν ο κακός μπορεί να μαντέψει μέρος του μηνύματος, βρίσκει και το κλειδί

Κρυπτογράφηση με αντικατάσταση

- Κρυπτογράφηση τρέχοντος κλειδιού
  - Όμοια με την πολυαλφαβητική αντικατάσταση αλλά το κλειδί απλά δεν τελειώνει ποτέ
    - » Κείμενο βιβλίου
    - » τυχαία δεδομένα που δημιουργούνται αλγοριθμικά (π.χ. περιστροφικές μηχανές)
    - » Προτιμάται η χρήση τυχαίων δεδομένων καθώς δεν είναι ευάλωτη σε στατιστικές αναλύσεις
  - Χρησιμοποιήθηκε από τους Γερμανούς στον Β' Παγκόσμιο Πόλεμο, ο κώδικας έσπασε από την ομάδα του Alan Turing

Κρυπτογράφηση με αντικατάσταση

- Μέθοδος Vernam
  - Εξαιρετικά ασφαλής
  - Μήνυμα και κλειδί θεωρούνται ακολουθίες bits

Κλειδί \ Μήνυμα	0	1
0	0	1
1	1	0

- Τα κλειδιά ανταλλάσσονται εκ των προτέρων εξωσυστημικά
- Το κλειδί χρησιμοποιείται μόνο μία φορά
- Το κλειδί έχει μήκος τουλάχιστον ίσο με το μήκος του μηνύματος

Είδη κρυπτοσυστημάτων

- Συμβατικά (ή συμμετρικά)
  - Ένα κλειδί
  - Κρυπτογράφηση και αποκρυπτογράφηση με τον ίδιο τρόπο
- Ασύμμετρα κρυπτοσυστήματα
  - Δύο διαφορετικά κλειδιά
  - Διαφορετικοί τρόποι κρυπτογράφησης και αποκρυπτογράφησης
  - Υπολογιστικά ανέφικτος ο συμπερασμός του ενός κλειδιού από το άλλο

Κρυπτογράφηση κατά μπλοκ

- Το μήνυμα Μ διασπάται σε διαδοχικά μπλοκ M1, M2, ...
- Το κάθε μπλοκ κρυπτογραφείται με το ίδιο κλειδί Κ
- Τελικό μήνυμα: $E_k(M1)E_k(M2)$
- Πλεονεκτήματα:
  - Μόνο μία εκτέλεση του κρυπταλγόριθμου ανά μπλοκ
  - Σφάλματα στο ένα μπλοκ δεν επηρεάζουν τα άλλα
- Μειονεκτήματα
  - Πιο ευάλωτα σε αναλύσεις κρυπτογραφίας
  - Όμοια τμήματα plaintext γεννούν το ίδιο ciphertext

Αλυσιδωτά μπλοκ

- Το κάθε μπλοκ δεν είναι αυτόνομο, αλλά περιλαμβάνει bits από τα προηγούμενα (κρυπτογραφημένα ή μη)
  - Μειώνονται οι διαθέσιμες θέσεις πληροφορίας σε κάθε μπλοκ
  - Αναιρείται το πλεονέκτημα της ανοχής σε σφάλματα
  - Αυξάνεται όμως η ασφάλεια
- Παράδειγμα:
  - $C_i = E_k(M_i \text{ XOR } C_{i-1})$
  - Το C_i πρακτικά εξαρτάται από όλα τα C_k με $i < k$
  - Ιδιαίτερα χρήσιμο για ψηφιακές υπογραφές

Αλγόριθμος DES

- Η κρυπτογράφηση γίνεται σε μπλοκ των 64 bit
- Το κλειδί είναι μήκους 56 bits
  - Εκτελούνται 19 επαναλήψεις του υπολογισμού:
    - » $L_i = R_{i-1}$ and $R_i = L_{i-1}$ AND $f(R_{i-1}, K_i)$ *όπου*
    - » το K_i υπολογίζεται χωρίζοντας το κλειδί των 56 bit σε δύο τμήματα των 28 και ολισθαίνοντας προς τα αριστερά το κάθε τμήμα ένα πλήθος θέσεων, ανάλογα με το *i*
    - » το $f(R_{i-1}, K_i)$ υπολογίζεται ως ακολούθως:
      - Το R_{i-1} επεκτείνεται στα 48 bits και καλείται *E*
      - TMP = E XOR K_i
      - CHUNKS[1..8] = Split(TMP, 6)
      - SUBSTCHUNKS[1..8] = MAP(CHUNKS[1..8])
      - Τα τελικά τμήματα των 4 bits αναδιατάσσονται

Διπλός DES

- Στη βασική του διαμόρφωση ο DES είναι ανασφαλής – σε διαγωνισμό του ’98 ο κώδικας έσπασε σε 56 ώρες από μηχανή που κόστισε λιγότερο από 300.000 €
- Διπλός DES:
  - $E(E(M, K_1), K_2)$
  - *Είναι όμως καλύτερος;*
    - » Υπάρχουν τέσσερα *ασθενή κλειδιά*, τέτοια ώστε E(E(M, K), K) = M
    - » Υπάρχουν τέσσερα *ημιασθενή ζεύγη κλειδιών,* τέτοια ώστε $E(E(M, K_1), K_2) = M$
    - » *Ακόμη χειρότερα...*
      - Είναι ευάλωτος σε επιθέσεις τύπου *«συνάντησης στο μέσον»*, όπου η πολυπλοκότητα του αλγορίθμου της αποκρυπτογράφησης είναι ίση με αυτή του απλού αλγόριθμου

Τριπλός DES

- $C = E(D(E(M, K_1), K_2), K_3)$ (DES-EDE) ή
- $C = E(E(E(M, K_1), K_2), K_3)$ (DES-EEE)

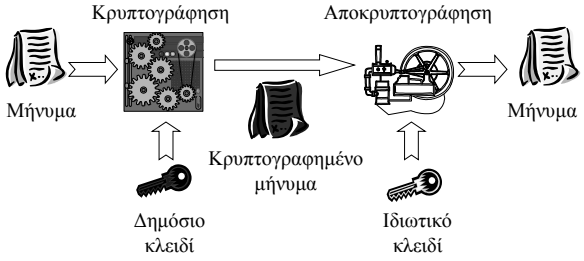
Κρυπτογραφήσεις	Κλειδιά	Υπολογισμός	Αποθήκευση	Είδος επίθεσης
1	1	2^{56}	-	Known plaintext
1	1	2^{38}	2^{38}	Chosen plaintext
1	1	-	2^{56}	Known plaintext
2	2	2^{212}	-	Chosen plaintext
2	2	2^{56}	2^{56}	Known plaintext
2	2	-	2^{112}	Chosen plaintext
3	2	2^{212}	-	Known plaintext
3	2	2^{56}	2^{56}	Chosen plaintext
3	2	2^{120-t}	2^{t}	Known plaintext
3	2	-	2^{56}	Chosen plaintext
3	3	2^{112}	2^{56}	Known plaintext
3	3	2^{56}	2^{112}	Chosen plaintext

Ασύμμετρα κρυπτοσυστήματα

- Στόχοι: Εχεμύθεια και αυθεντικότητα
- Δύο κλειδιά, *δημόσιο* (public) και *ιδιωτικό* (private)
- Το ιδιωτικό είναι διαθέσιμο μόνο στον κάτοχο, το δημόσιο σε όλους τους χρήστες
- Ανέφικτο να υπολογιστεί το ένα κλειδί από το άλλο
- Χρησιμοποιούνται αλγόριθμοι κρυπτογράφησης-αποκρυπτογράφησης (E, D) τέτοιοι ώστε:
  - D(E(M, Pub), Priv) = M
  - D(E(M, Priv), Pub) = M
- Για να επικοινωνήσουν δύο μέρη, αρκεί ο ένας να γνωρίζει το δημόσιο κλειδί του άλλου

Ασύμμετρα κρυπτοσυστήματα

- Εχεμύθεια: Κρυπτογραφούμε με δημόσιο κλειδί, αποκρυπτογραφούμε με το ιδιωτικό



Ασύμμετρα κρυπτοσυστήματα

- Αυθεντικότητα: *Ψηφιακές υπογραφές*
- Είναι ένα σύνολο από bits που προσθέτει ο αποστολέας ενός εγγράφου σ' αυτό και έχουν τις ακόλουθες ιδιότητες:
  - Ο παραλήπτης μπορεί να επαληθεύσει ότι η υπογραφή είναι του αποστολέα
  - Θα πρέπει να είναι αδύνατο για οποιονδήποτε, συμπεριλαμβανομένου του παραλήπτη, να πλαστογραφήσει την υπογραφή του Α
  - Θα πρέπει να είναι δυνατόν για κάποιον τρίτο (π.χ. δικαστική αρχή) να διευθετήσει κάποια διαφωνία μεταξύ αποστολέα και παραλήπτη

Ο αλγόριθμος RSA

- Για την παραγωγή κλειδιών χρησιμοποιείται ο πολλαπλασιασμός πρώτων αριθμών
- Η εχεμύθεια βασίζεται στη δυσκολία παραγοντοποίησης μεγάλων ακεραίων

Ο αλγόριθμος RSA – Επιλογή κλειδιών

- Επιλέγουμε δύο μεγάλους πρώτους αριθμούς p και q
- Υπολογίζουμε το $n = p * q$
- Υπολογίζουμε το $\varphi(n) = (p - 1) * (q - 1)$
- Επιλέγουμε έναν ακέραιο e με $3 \le e \le \varphi(n)$ τέτοιο ώστε να μην έχει κοινό παράγοντα με το $\varphi(n)$
- Επιλέγουμε έναν ακέραιο d τέτοιο ώστε $d * e \bmod \varphi(n) = 1$
- Τα e, n δημοσιοποιούνται
- Τα p, q, d, $\varphi(n)$ φυλάσσονται μυστικά

Αλγόριθμος RSA

- Κρυπτογράφηση:
  - $C = M^e \bmod n$
- Αποκρυπτογράφηση:
  - $M = C^d \bmod n$
- Παράδειγμα:
  - p = 251, q = 269, n = p * q = 67519, φ(n) = 67000
  - e = 50253, d = inv(e) $\bmod_{67000}$ = 27917
  - Με n = 67619 μπορούμε να κωδικοποιήσουμε αριθμούς από 0 έως 67618

ASCII	*Bytes*	*256 * b_1 + b_2*	*C = M^e mod n*	*bytes*	*ASCII*
"RS"	82 83	21075	48469	189 85	"½U"
"A "	65 32	16672	14579	56 243	"8ó"
"wo"	119 111	30575	26195	102 83	"fS"
"rk"	114 107	29291	58005	226 149	"â~"
"s!"	115 33	29473	30141	117 189	"u½"

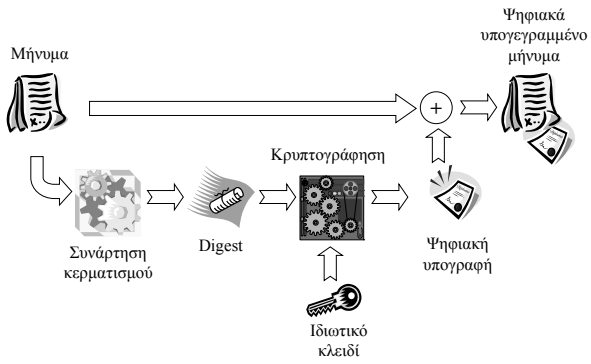
Advanced Encryption Standard

- Πέντε υποψήφιοι
  - MARS
    - » Πολύπλοκος, όχι εύκολος να αναλυθεί, αργός
  - RC6
    - » Ταχύς σε λογισμικό, απαιτεί πολύ μνήμη, μέτριες επιδόσεις σε υλικό
  - Serpent
    - » Ιδιαίτερα ασφαλής, πολύ αργός σε λογισμικό, πολύ καλός σε υλικό
  - Twofish
    - » Πρωτοποριακός, καθώς το μισό κλειδί καθορίζει τον τρόπο λειτουργίας, δύσκολο να αναλυθεί, μέτρια ταχύτητα
  - Rijndael
    - » Ταχύς, απλός και συμπαγής, με ελαφρώς μικρότερη ασφάλεια από τους συνυποψήφιους, εξαιρετικός για έξυπνες κάρτες και υλοποίηση σε επίπεδο υλικού, αρκετή εγγενής παραλληλία

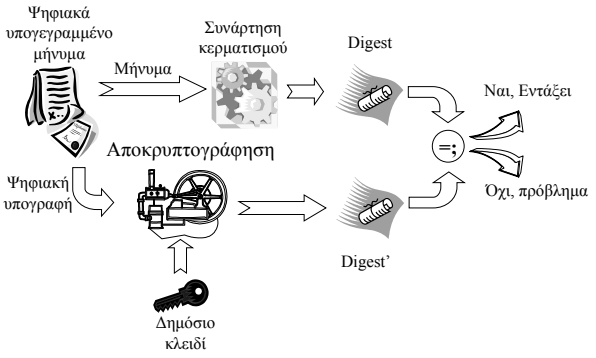
Advanced Encryption Standard

- Τελικός νικητής – Rijndael
  - Κλειδιά μεγέθους 128, 192 και 256 bits
  - Μπλοκ δεδομένων μεγέθους 128, 192 και 256 bits
  - Δυνατός ο συνδυασμός όλων των μεγεθών κλειδιών και μπλοκ δεδομένων
  - Με εξειδικευμένες μηχανές που δοκιμάζουν 2^{55} κλειδιά ανά δευτερόλεπτο απαιτούνται 149 τρισεκατομμύρια έτη για να σπάσει ένα κλειδί των 128 bits
  - Εκτιμάται ότι θα «κρατήσει» για 20 χρόνια

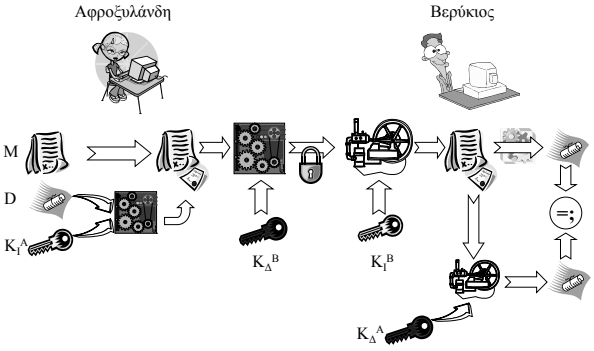
Ψηφιακές υπογραφές - Αποστολή



Ψηφιακές υπογραφές - Παραλαβή



Εχεμύθεια + Αυθεντικότητα



Προσπάθειες Εξαπάτησης

- Ο Νταβέλης δημιουργεί ένα ζεύγος κλειδιών με το όνομα της Αφροξυλάνδης, υπογράφει ψηφιακά ένα έγγραφο με τα κλειδιά αυτά και το στέλνει στον Βερύκιο

- Αν ο Βερύκιος δεν έχει ήδη το δημόσιο κλειδί της Αφροξυλάνδης μπορεί να εξαπατηθεί
- *Λύση: εισαγωγή μιας τρίτης οντότητας, της Αρχής Διαχείρισης Πιστοποιητικών* (certificate authority)

Αρχή Διαχείρισης Πιστοποιητικών

- Εκδίδει ψηφιακώς υπογεγραμμένα *πιστοποιητικά*, αφού διαπιστώσει εξωσυστημικά την ταυτότητα του υποκειμένου.
- Το *πιστοποιητικό* είναι ένα έγγραφο που περιέχει:
  - Έκδοση και αριθμό σειράς
  - Το όνομα του εκδότη
  - Το όνομα του υποκειμένου και άλλες τυχόν επεκτάσεις (διεύθυνση οικίας, εργασίας, αριθμό ταυτότητας κ.λπ.)
  - Το σκοπό του πιστοποιητικού (αν το υποκείμενο δρα και ως αρχή πιστοποίησης)
  - Το δημόσιο κλειδί του υποκειμένου
  - Την περίοδο εγκυρότητας του πιστοποιητικού
  - Την υπογραφή της αρχής διαχείρισης πιστοποιητικών

Αρχή Διαχείρισης Πιστοποιητικών

- Η αρχή διαχείρισης πιστοποιητικών υποστηρίζει:
  - *Κατάλογος* (directory). Περιέχει όλες τις πληροφορίες που είναι απαραίτητες για την υποδομή δημόσιου κλειδιού, όπως τα πιστοποιητικά δημόσιου κλειδιού, λίστες ανάκλησης κλειδιών, λίστες ανάκλησης αρχών, πιστοποιητικά αρχών κ.λπ. Απαιτείται υψηλή διαθεσιμότητα
  - *Λίστες ανακλήσεων.* Αν η ασφάλεια κάποιου πιστοποιητικού έχει διακυβευτεί, οι ενδιαφερόμενοι που *έχουν ήδη λάβει* το κλειδί πρέπει να γνωρίζουν ότι έχει καταστεί άκυρο. Οι λίστες ανακλήσεως πιστοποιητικών (CRLs) παρέχουν αυτή τη δυνατότητα. Υπάρχουν και λίστες ανακλήσεως αρχών (ARLs) που ακυρώνουν όλα τα πιστοποιητικά που υπογράφονται από τη συγκεκριμένη αρχή
  - *Αυτοϋπογεγραμμένο πιστοποιητικό*. Μία αρχή πιστοποίησης μπορεί να εκδίδει για τον εαυτό της ένα *αυτοϋπογεγραμμένο πιστοποιητικό* που οι χρήστες μπορούν να *επιλέγουν να εμπιστεύονται*

Διασταυρούμενη πιστοποίηση

- Αν το υποκείμενο Χ πιστοποιείται από και εμπιστεύεται για πιστοποίηση την αρχή Α και το υποκείμενο Υ πιστοποιείται από και εμπιστεύεται για πιστοποίηση την αρχή Β, ποια αξία έχουν για τον Υ τα πιστοποιητικά του Α; (και όλα τα έγγραφα που βασίζονται σ' αυτά)
  - Λύση 1: Κάθε υποκείμενο πρέπει να δηλώνει ρητώς ποιες αρχές πιστοποίησης εμπιστεύεται (μη διαχειρίσιμο λόγω μεγάλου πλήθους και ανεπάρκειας γνώσεων των χρηστών)

Ομότιμη διασταυρούμενη πιστοποίηση

- Οι αρχές πιστοποίησης εγκαθιστούν μεταξύ τους μονόδρομες ή αμφίδρομες σχέσεις εμπιστοσύνης σε ομότιμη βάση
  - Η αρχή Α πιστοποιεί την αρχή Β ως έγκυρη αρχή πιστοποίησης
- Οι χρήστες εμπιστεύονται τις επί μέρους αρχές πιστοποίησης
- Για τη διακρίβωση των πιστοποιητικών αξιοποιούνται οι σχέσεις εμπιστοσύνης μεταξύ των αρχών πιστοποίησης

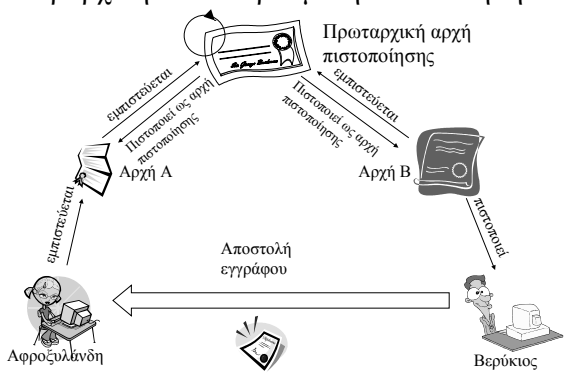
Ομότιμη διασταυρούμενη πιστοποίηση

Αλυσίδα εμπιστοσύνης: Αφροξυλάνδη → Αρχή Α → Αρχή Β →Βερύκιος

Ιεραρχική διασταυρούμενη πιστοποίηση

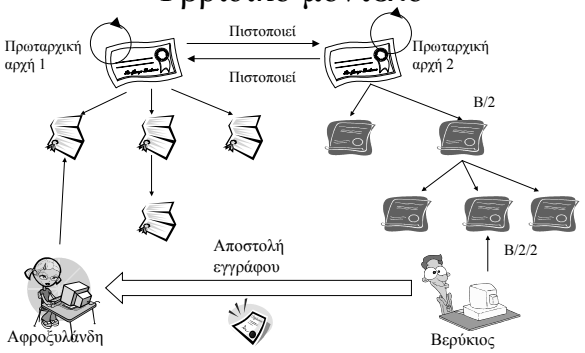
- Οι αρχές πιστοποίησης οργανώνονται σε ιεραρχίες, με κάθε μία να πιστοποιεί τις υφιστάμενές της ως αρχές πιστοποίησης
- Εδώ κάθε χρήστης εμπιστεύεται την *πρωταρχική αρχή πιστοποίησης,* στη ρίζα της ιεραρχίας
  - τα πιστοποιητικά εκδίδονται από τις αρχές χαμηλότερα στην ιεραρχία
  - Οι χρήστες εμπιστεύονται την έκδοση των πιστοποιητικών τους στις αρχές διότι «εγγυάται» γι' αυτές η πρωταρχική αρχή πιστοποίησης
  - Για τη διακρίβωση των πιστοποιητικών προσπαθούμε να φτάσουμε στη ρίζα διασχίζοντας αντίστροφα σχέσεις τύπου «πιστοποιεί»

Ιεραρχική διασταυρούμενη πιστοποίηση



Αλυσίδα εμπιστοσύνης: Αφροξυλάνδη → Πρωτ. Αρχή → Αρχή Β →Βερύκιος

Υβριδικό μοντέλο



Αλυσίδα εμπιστοσύνης: Αφροξυλάνδη → Πρωτ. Αρχή 1 → Πρωτ. Αρχή 2 → Β/2 → Β/2/2 → Βερύκιος

Ψηφιακό πιστοποιητικό

Υποκείμενο:	Αφροξυλάνδη Ψαξεβρέστου 2
Πληροφορίες πιστοποιητικού:	
	Έγκυρο κατά: [02/2002, 05/2002]
	Αριθμός σειράς: A32B540XX
	Δημόσιο κλειδί: ΜΙΑ ΠΑΠΙΑ ΜΑ ΠΟΙΑ ΠΑΠΙΑ ΜΙΑ ΠΑΠΙΑ ΜΕ ΠΑΠΙΑ
Αρχή πιστοποίησης:	CLOPYSOFT SA

Ψηφιακό πιστοποιητικό - παράδειγμα

Version: 1 (0x0)
Serial Number: 04:60:00:00:02
Signature Algorithm: md2WithRSAEncryption
Issuer: C=US, O=CREN/Corp for Research and Educational Networking, OU=Education and Research Client CA
Validity
Not Before: Nov 17 00:00:00 1999 GM
Not After : Nov 17 00:00:00 2003 GMT
Subject: C=US, O=CREN/Corp for Research and Educational Networking, OU=Education and Research Client CA
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit): (πολλά δυαδικά δεδομένα)
Signature Algorithm: md2WithRSAEncryption (και άλλα δυαδικά δεδομένα)
Certificate: (ακόμη περισσότερα δυαδικά δεδομένα)

Αυτοϋπογεγραμμένα πιστοποιητικά

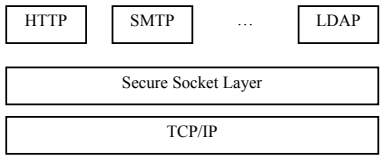
- Μία αρχή πιστοποίησης (ή οποιοσδήποτε!) μπορεί να φτιάξει ένα αυτοϋπογεγραμμένο πιστοποιητικό
  - Χωρίς την «αλυσίδα εμπιστοσύνης» ένα αυτοϋπογεγραμμένο πιστοποιητικό είναι χρήσιμο για *κρυπτογράφηση μόνο* όχι για διακρίβωση ταυτότητας (εκτός αν διανεμηθεί εξωσυστημικά)

Δημιουργία αυτοϋπογεγραμμένου πιστοποιητικά

```
# Δημιουργία προστατευμένου ιδιωτικού κλειδιού
openssl genrsa 1024 > host.key
chmod 400 host.key
# Δημιουργία δημόσιου πιστοποιητικού – Το host.cert περιέχει
# "δυαδικά" δεδομένα. Ζητάται η ακόλουθη πληροφορία
openssl req -new -x509 -nodes -sha1 -days 365 \
   -key host.key > host.cert
Country Name (2 letter code) [AU]:GR
State or Province Name (full name) [Some-State]:Attica
Locality Name (eg, city) []:Athens
Organization Name (eg, company) [SomeComp]:ClopySoft
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []: www.clopysoft.gr
Email Address []: info@clopysoft.gr
# Προαιρετικό – Δημιουργία "αναγνώσιμου από άνθρωπο" αρχείου
# μεταδεδομένων
openssl x509 -noout -fingerprint -text < host.cert > host.info
# Προαιρετικό – Συνδυασμός πιστοποιητικού και μεταδεδομένων
cat host.cert host.key > host.pem
# Προστατεύεται γιατί έχει το ιδιωτικό κλειδί
chmod 400 host.pem
```

Το πρωτόκολλο SSL

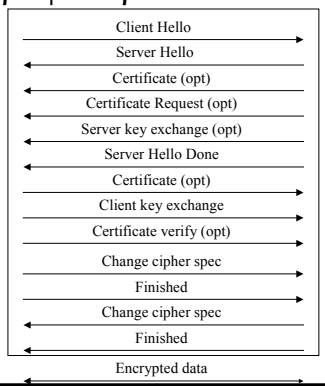
- Το πρωτόκολλο SSL παρεμβάλλεται μεταξύ του TCP/IP και του επιπέδου εφαρμογής προκειμένου να:
  - πιστοποιεί τον εξυπηρέτη στον εξυπηρετούμενο
  - πιστοποιεί τον εξυπηρετούμενο στον εξυπηρέτη
  - κρυπτογραφεί την επικοινωνία



Ανατομία του πρωτοκόλλου SSL

- Δύο επί μέρους πρωτόκολλα
  - χειραψία SSL
  - ανταλλαγή δεδομένων SSL
- Στόχοι χειραψίας
  - Να πιστοποιηθεί ο εξυπηρέτης στον εξυπηρετούμενο
  - Συμφωνία πάνω στους αλγόριθμους κρυπτογραφίας που θα χρησιμοποιηθούν για την επικοινωνία
  - Προαιρετικά, πιστοποίηση εξυπηρετούμενου στον εξυπηρέτη
  - Δημιουργία «διαμοιραζόμενων μυστικών» μέσω τεχνικών κρυπτογραφίας δημόσιου κλειδιού για την κρυπτογράφηση της επικοινωνίας
  - Εγκαθίδρυση του κρυπτογραφημένου διαύλου επικοινωνίας

Χειραψία πρωτοκόλλου SSL



Βήματα χειραψίας SSL (1)

- *Client Hello* – αποστέλλονται στον εξυπηρέτη:
  - αριθμός έκδοσης SSL του εξυπηρετούμενου
  - λίστα υποστηριζόμενων αλγόριθμων κρυπτογράφησης και αντιστοίχων μεγεθών κλειδιών
  - ταυτότητα της συνόδου κ.τ.λ.
- *Server Hello – αποστέλλονται στον εξυπηρετούμενο*
  - αριθμός έκδοσης SSL του εξυπηρέτη
  - ο πιο κατάλληλος αλγόριθμος κρυπτογράφησης
  - το επιλεγμένο μήκος κλειδιών

Βήματα χειραψίας SSL (2)

- *Certificate* - (προαιρετικό, αν απαιτείται πιστοποίηση του εξυπηρέτη)
  - ο εξυπηρέτης αποστέλλει το πιστοποιητικό του στον εξυπηρετούμενο. Το πιστοποιητικό περιέχει το δημόσιο κλειδί του εξυπηρέτη. Ο εξυπηρετούμενος διακριβώνει την ταυτότητα του εξυπηρέτη.
- *Certificate request* - (προαιρετικό, αν απαιτείται πιστοποίηση του εξυπηρετούμενου)
  - *ο εξυπηρέτης αποστέλλει ένα μήνυμα με το οποίο ζητά το πιστοποιητικό του εξυπηρετούμενου.*

Βήματα χειραψίας SSL (3)

- *Server key exchange* - (προαιρετικό, αν το πιστοποιητικό του εξυπηρέτη δεν είναι επαρκές για την ανταλλαγή κλειδιών που θα ακολουθήσει)
- *Server Hello Done*
  - Ο εξυπηρέτης υποδεικνύει ότι έχει τελειώσει την προκαταρκτική φάση εγκαθίδρυσης της συνόδου
- *Certificate* (προαιρετικό, αν ο εξυπηρέτης έχει αποστείλει μήνυμα certificate request)
  - ο εξυπηρετούμενος αποστέλλει το πιστοποιητικό του, ο εξυπηρέτης το επαληθεύει

Βήματα χειραψίας SSL (4)

- *Client key exchange*
  - ο εξυπηρετούμενος δημιουργεί το προκαταρκτικό μυστικό (premaster secret) για τη συγκεκριμένη σύνοδο, το κρυπτογραφεί με το δημόσιο κλειδί του εξυπηρέτη και το αποστέλλει σ' αυτόν.
- *Certificate verify* (προαιρετικό, αν ο εξυπηρέτης έχει ζητήσει το πιστοποιητικό του εξυπηρετούμενου)
  - το μήνυμα αυτό επιτρέπει στον εξυπηρέτη να ολοκληρώσει τη διαδικασία επαλήθευσης του πιστοποιητικού

Βήματα χειραψίας SSL (5)

- *Change cipher spec*
  - Ο εξυπηρετούμενος είναι έτοιμος να μεταβεί σε ασφαλή επικοινωνία
- *Finished*
  - Ο εξυπηρετούμενος τελείωσε το δικό του τμήμα της χειραψίας
- *Change cipher spec*
  - Ο εξυπηρέτης είναι έτοιμος να μεταβεί σε ασφαλή επικοινωνία
- *Finished*
  - Ο εξυπηρέτης έχει τελειώσει το δικό του τμήμα της χειραψίας

Ανταλλαγή δεδομένων στο SSL

- Με συμμετρικό αλγόριθμο κρυπτογραφίας
- Το κλειδί παράγεται με βάση το *προκαταρκτικό μυστικό*
- Ο αλγόριθμος παραγωγής εξαρτάται από τον συμμετρικό αλγόριθμο κρυπτογραφίας που θα χρησιμοποιηθεί και το μήκος των κλειδιών

SessionKey = genKey(premasterSecret, cipher, keyLen)

Σε ποιο σημείο κρυπτογραφούμε;

- Κρυπτογράφηση από άκρο σε άκρο
  - Απαραίτητο κλειδί για κάθε επικοινωνιακό εταίρο
  - Πιθανή επίθεση με ανάλυση κυκλοφορίας
- Κρυπτογράφηση σε επικοινωνιακό κανάλι
  - Κάθε κόμβος ξέρει μόνο τους γείτονές του
  - Η πληροφορία είναι εκτεθειμένη σε κάθε ενδιάμεσο επικοινωνιακό κόμβο
  - Απαιτείται πρόσβαση σε όλα τα ενδιάμεσα κανάλια
- Συνδυασμός των δύο κρυπτογραφήσεων