Ασφάλεια

ΛΙΑΓΚΟΥ ΒΑΣΙΛΙΚΗ

Εργαστήριο

A. RSA Κρυπτογράφηση
B. RSA Από-Κρυπτογράφηση
C. Υπογραφή RSA
D. Επαλήθευση Υπογραφής RSA

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Αλγόριθμοι Δημόσιου Κλειδιού

Απόλυτη Ασφάλεια (Perfect Secrecy)

- Σε αντίθεση με τα συμμετρικά συστήματα, στα συστήματα ΔΚ η απόλυτη ασφάλεια δεν είναι εφικτή
  - Δεδομένου ενός ΔΚ pk και ενός κρυπτογραφήματος $c \leftarrow \mathrm{Enc}_{pk}(m)$
  - … ένας εχθρός με άπειρους υπολ. πόρους (unbounded) θα βρει το m με πιθανότητα 1.

… π.χ. δοκιμάζοντας κάθε πιθανό ιδιωτικό κλειδί μέχρι να βρει το σωστό

Problem
FACTORING
RSAP
SQROOT
DLP
DHP

Schneier, Bruce. Applied Cryptography. John Wiley & Sons, Inc., 2nd edition, 1996.

Μήκος «κλειδιού» στα Συστήματα ΔΚ

- Στα συστήματα ΔΚ η υπολογιστική ασφάλεια λογίζεται διαφορετικά …
- Πόσο «δύσκολο» είναι να αντιστρέψεις μια μονόδρομη συνάρτηση (one-way);
  - Π.χ. Πόσο «δύσκολο» είναι να παραγοντοποιήσεις το modulus n στους πρώτους παράγοντες p και q;
  - Π.χ. Πόσο δύσκολο είναι να βρεις το διακριτό λογάριθμο (mod p) του g^x ;
- Το μέγεθος δυσκολίας εξαρτάται από το μήκος του modulus
  - π.χ.: $\log_2(n) = 1024$ bit
- Αντιστοίχηση Συμμετρικών Συστημάτων και Συστημάτων ΔΚ ως προς το επίπεδο ασφάλειας που προσφέρουν
  - Βάσει του μήκους κλειδιού

Symmetric Key	RSA Key
56	430
80	760
96	1020
128	1620

Πηγή: RSAsecurity.com

J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

H. Mel, D. Baker. Cryptography Decrypted. Addison-Wesley, 2001

Κρυπτογραφία Δημόσιου Κλειδιού
Ο αλγόριθμος RSA

Ο αλγόριθμος RSA

1. Η Alice επιλέγει τυχαία δύο πρώτους αριθμούς p, q ϵ Z^*_N
2. Η Alice υπολογίζει N = p * q
3. Η Alice διαλέγει αριθμό e ϵ $Z^*_{\Phi(N)}$
4. Η Alice υπολογίζει αριθμό d ϵ Z_N^*, ώστε $e * d \equiv 1 \pmod{\phi(N)}$
5. Η Alice διαγράφει τα p και q

- Δημόσιο Κλειδί : (e, N)
- Ιδιωτικό Κλειδί : d

- Έστω αριθμός $m \in Z_N^*$
  - Κρυπτογράφηση: $m^e \bmod n \Rightarrow c$
  - Αποκρυπτογράφηση: $c^d \bmod n \Rightarrow m$

(Υπολογιστική) Ασφάλεια

- RSA problem. Ανάγεται στο:
- Factoring problem: Πρόβλημα εύρεσης πρώτων παραγόντων μεγάλων αριθμών
  - Για μεγάλο N, (>= 1024 bit), «δύσκολο» να βρεθούν οι πρώτοι παράγοντες p και q
    - Υπολογιστικά Αδύνατο

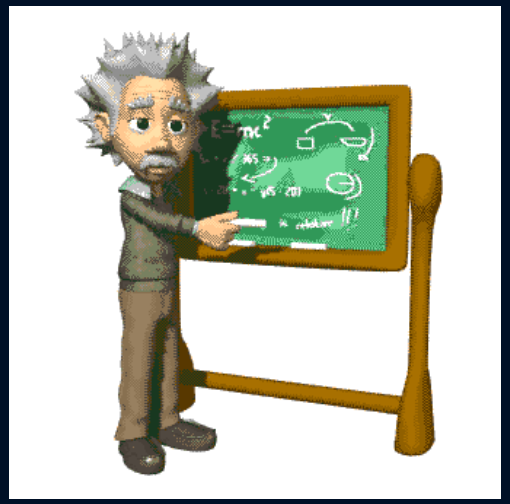
J. Katz, Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.

Κρυπτογραφία Δημόσιου Κλειδιού
Ο αλγόριθμος RSA

RSA Problem

Δίνονται: Ακέραιος N, θετικός ακέραιος e σχετικά πρώτος με $\Phi(N)$, και ένα στοιχείο y ε Z^*_N.

Υπολόγισε: έναν αριθμό x ώστε $x^e = y \bmod N$



- Ας δούμε την Ασυμμετρία
  - Έστω η ομάδα Z^*_N.
  - Αν η παραγοντοποίηση του N είναι γνωστή τότε το RSA problem γίνεται εύκολο:
    1. Υπολόγισε $\Phi(N)=(p-1)(q-1)$
    2. Υπολόγισε $d = e^{-1} \bmod \Phi(N)$
    3. Υπολόγισε $x = y^d \bmod N$

Κρυφή είσοδος (trapdoor):
οι αριθμοί p, q

RSA

- Ο RSA είναι αλγόριθμος ασύμμετρης κρυπτογράφησης. Κατά την κρυπτογράφηση απαιτεί τη χρήση δημοσίου κλειδιού, ενώ κατά την αποκρυπτογράφηση τη χρήση ιδιωτικού κλειδιού.
- a. Με την εντολή:
- openssl genrsa –out private.key 1024
- θα δημιουργηθεί το ιδιωτικό κλειδί private.key του RSA μήκους 1024 bits.

RSA

- Για τη δημιουργία του δημόσιου κλειδιού public.pem από το ιδιωτικό κλειδί private.key που φτιάξαμε στο προηγούμενο βήμα θα πρέπει να δώσετε την
- εντολή:
- openssl rsa –in private.key –pubout –out public.pem

RSA

- Κατασκευάστε και ένα 2ο δημόσιο κλειδί public2.pem από το ίδιο ιδιωτικό private.key.
- Δείτε τα αρχεία private.key, public.pem και public2.pem.
- Τι παρατηρείτε για τα public.pem και public2.pem, είναι αναμενόμενο;
- Εδώ μπορείτε να δείτε λεπτομεριες για την αποθήκευση του κλειδιού με την μορφή pem
- https://www.thedigitalcatonline.com/blog/2018/04/25/rsa-keys/

Κρυπτογράφηση RSA

- Για να κρυπτογραφήσουμε το lab.txt θα χρησιμοποιήσουμε το δημόσιο κλειδί του παραλύπτη public.pem.
- Η εντολή είναι:
- openssl rsautl –encrypt –inkey public.pem –pubin –in lab4.txt –out
- testRSA.txt

Αποκρυπτογράφηση RSA

- Για να αποκρυπτογραφήσουμε το testRSA.txt θα χρησιμοποιήσουμε το
- private.key. Η εντολή είναι:
- openssl rsautl –decrypt –inkey private.key –in testRSA.txt –out
- testRSADec.txt

Δημιουργία Υπογραφής

- Χρησιμοποιώντας το private.key μπορείτε να υπογράψετε ψηφιακά ένα αρχείο PlainText.txt
- Με την εντολή:
- openssl rsautl –sign –inkey private.key –in PlainText.txt –out testSigned_ID.txt

Επαλήθευση της ψηφιακής υπογραφής

- Χρησιμοποιώντας το private.key μπορείτε
- SIgnedfromAMforID
- Χρησιμοποιήσετε το δημόσιο κλειδί μπορείτε να πιστοποιησετε την υπογραφή TestSigned
- Με την εντολή:
- openssl rsautl –verify –inkey publicAM.pem –pubin –in testSigned –out testVerified.txt