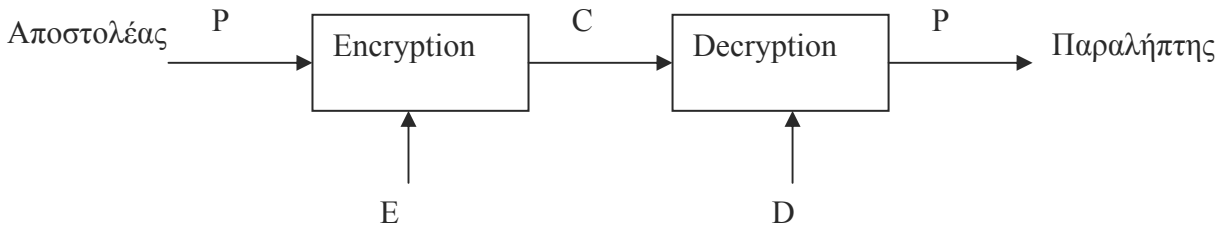
Κρυπτογραφία

Εργαστηριακό μάθημα 6
(Αλγόριθμοι Δημοσίου Κλειδιού - RSA)

Κρυπτοσυστήματα Δημοσίου κλειδιού



- Προτάθηκαν το 1976 (από τους Diffie-Hellman)
- Κάθε συμμετέχων στο σύστημα κατέχει ένα ζευγάρι κλειδιών e και d, που το ένα αντιστρέφει το άλλο: d(e(m))=m
- Ένα από τα δύο κλειδιά είναι γνωστό σε όλους (το e) και λέγεται Δημόσιο Κλειδί: απαραίτητη προϋπόθεση είναι ότι η γνώση του e δεν οδηγεί σε προσδιορισμό του μυστικού κλειδιού d.

Τρόπος λειτουργίας συστημάτων δημοσίου κλειδιού

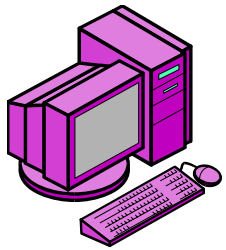
- Όταν ένα πρόσωπο A θέλει να στείλει ένα μήνυμα m σε ένα πρόσωπο B, το δημόσιο κλειδί κρυπτογράφησης του παραλήπτη B χρησιμοποιείται για τη δημιουργία του κρυπτογράμματος $E_e(m)$. Αφού το E_e είναι πλήρως διαθέσιμο σε όλους, ο οποιοσδήποτε μπορεί να κρυπτογραφήσει ένα μήνυμα με προορισμό τον B. Ωστόσο, μόνο ο B, ο οποίος γνωρίζει το ιδιωτικό του κλεδί D_B μπορεί να ανακατασκευάσει το αρχικό μήνυμα, εφαρμόζοντας τον αντίστροφο μετασχηματισμό $D_B(E_B(m))$.

Σχηματική αναπαράσταση

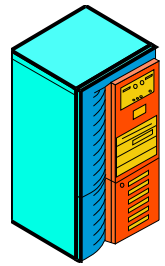
Κρυπτογράφηση με το δημόσιο κλειδί του Β

Κρυπτογραφημένο μήνυμα

Αποκρυπτογράφηση με το ιδιωτικό κλειδί του Β



Χρήστης Α

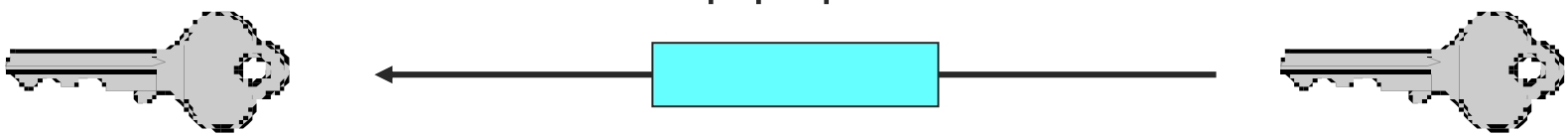


Χρήστης Β

Αποκρυπτογράφηση με το ιδιωτικό κλειδί του Α

Κρυπτογραφημένο μήνυμα

Κρυπτογράφηση με το δημόσιο κλειδί του Α



Αλγόριθμος Δημοσίου Κλειδιού RSA

- Πήρε το όνομά του από τους εμπνευστές του Rivest, Shamir, Adleman.
- Κάθε χρήστης διαλέγει τυχαία δύο πολύ μεγάλους **πρώτους** αριθμούς p, q, και υπολογίζει το γινόμενο N=pq.
  - Το N θα πρέπει να αποτελείται τουλάχιστον από 200 ψηφία και μπορεί να δημοσιοποιηθεί (να είναι γνωστό σε όλους)
  - Τα p και q κρατούνται μυστικά.
  - Κάποιος «εχθρός» γνωρίζει το N (αφού είναι δημοσίως γνωστό σε όλους). Ωστόσο, είναι πολύ δύσκολο πρόβλημα να βρει την ανάλυσή του σε γινόμενο πρώτων αριθμών – δηλαδή να βρει τα p,q. **Σε αυτό έγκειται και η ασφάλεια του RSA (Factorization problεμ).**

Ο αλγόριθμος RSA (συνέχεια)

- Με χρήση των p και q, ο χρήστης υπολογίζει τη συνάρτηση Euler φ(N), που ισούται με το πλήθος των θετικών ακεραίων που είναι πρώτοι ως προς το N.
  - Επειδή N=pq, ισχύει φ(N)=φ(p)φ(q) = (p-1) (q-1)
- Στη συνέχεια ο χρήστης διαλέγει έναν τυχαίο αριθμό e μικρότερο του φ(N) με την ιδιότητα gcd(e,φ(N))=1. Ο αριθμός e δημοσιοποιείται.
- Με τον επεκταμένο (extended) αλγόριθμο του Ευκλείδη (βλέπε επόμενη διαφάνεια), ο χρήστης υπολογίζει τον μοναδικό ακέραιο d, 1 < d < φ(N), με την ιδιότητα

  $$ed=1 \pmod{\varphi(N)}.$$

  (στην ουσία, ο d είναι ο αντίστροφος του e mod φ(N))
- Το δημόσιο κλειδί του χρήστη είναι το ζεύγος (N,e). Το ιδιωτικό του κλειδί είναι ο αριθμός d.

Επεκταμένος αλγόριθμος του Ευκλείδη

- Έστω ότι θέλουμε να βρούμε, για αριθμούς a, b, τον μέγιστο κοινό διαιρέτη τους g, καθώς και τους ακέραιους αριθμούς εκείνους x,y τέτοιους ώστε ax+by=g.

  (αποδεικνύεται ότι υπάρχουν τέτοιοι ακέραιοι και είναι μοναδικοί)
- (ειδικά στον RSA: a=φ(N), b=e και επίσης g=1. Στο d θα αποδοθεί η τιμή του y).
  - Κάνουμε τη διαίρεση του a με το b και παίρνουμε a=kb + r.
  - Αν το r είναι διάφορο του μηδενός, τότε θέτουμε a=b και b=r και κάνουμε την ίδια διαίρεση (του a με το b).
  - Σταματάμε όταν το r γίνει 0. Τότε, το τελευταίο μη μηδενικό υπόλοιπο που πήραμε είναι ο μέγιστος κοινός διαιρέτης g.
  - Από τις σχέσεις που έχουμε λάβει, αν τις «διαβάσουμε» ανάποδα θα βρούμε και τα x,y που θέλουμε (βλέπε επόμενη διαφάνεια).

Παράδειγμα επεκταμένου αλγόριθμου του Ευκλείδη

- Έστω ότι a=1925, b=693
- Έχουμε:
  - 1925 = 2 · 693 + 539 (1)
  - 693 = 1 · 539 + 154 (2)
  - 539 = 3 · 154 + 77 (3)
  - 154 = 2 · 77 (4)
- Άρα, ο μέγιστος κοινός διαιρέτης είναι το 77 (το τελευταίο μη μηδενικό υπόλοιπο που πήραμε). «Διαβάζοντας» τις σχέσεις ανάποδα, έχουμε:
- Ξεκινώντας από την (3) (και χρησιμοποιώντας τις (2), (1) διαδοχικά):

$$77 = 539 - 3 \cdot 154 = 539 - 3 \cdot (693 - 1 \cdot 539) =$$

$$= 4 \cdot 539 - 3 \cdot 693 = 4 \cdot (1925 - 2 \cdot 693) - 3 \cdot 693 =$$

$$= 4 \cdot 1925 - 11 \cdot 693$$

Δηλαδή, x=4 και y=-11.

Αλγόριθμος RSA (κρυπτογράφηση)

- Για να κρυπτογραφηθεί ένα μήνυμα m που θέλει να στείλει κάποιος χρήστης B στον χρήστη A, το m διασπάται σε μία σειρά τμημάτων $m_1, m_2, \ldots, m_p$, όπου κάθε m_i αναπαρίσταται από έναν ακέραιο μεταξύ 0 και N. Η κρυπτογράφηση γίνεται ξεχωριστά για κάθε block m_i με χρήση των δημοσίων κλειδιών e και N του A. Το κρυπτόγραμμα c_i παράγεται ως εξής:

$$c_i = m_i^e \bmod N$$

Αλγόριθμος RSA (αποκρυπτογράφηση)

- Ο Α αποκρυπτογραφεί το κρυπτόγραμμα c υπολογίζοντας το $m = c^d \bmod N$. **Η σχέση μεταξύ του d και του e εξασφαλίζει τη σωστή ανάκτηση του m**.

- Μόνο ο Α μπορεί να αποκρυπτογραφήσει το μήνυμα, αφού είναι ο μόνος που γνωρίζει το d.

Ερμηνεία της αποκρυπτογράφησης RSA

- Θεώρημα Euler: $m^{\varphi(N)} \equiv 1 \bmod(N)$ **όταν gcd(m,N)=1**

  Αν υψώσουμε και τα δύο μέλη της ισοδυναμίας εις την k και στη συνέχεια πολλαπλασιάσουμε και τα δύο μέλη με m, θα προκύψει η ακόλουθη σχέση:
  $m^{k\varphi(N)+1} \bmod N = m \bmod N$ (1)

- Αφού $ed \equiv 1 \pmod{\varphi(N)}$, υπάρχει ακέραιος k τέτοιος ώστε:
  $ed = k\varphi(N) + 1$.

- Αποκρυπτογράφηση του δέκτη:
  $c_i^d \bmod N$
  $= m_i^{ed} \bmod N =$
  $= m_i^{k\varphi(N)+1} \bmod N =$ (από την (1))
  $= m_i \bmod N = m_i$

Σύνοψη RSA και παράδειγμα

1. Ο χρήστης διαλέγει δύο τυχαίους πρώτους αριθμούς p,q – έστω p=47, q=59. Τότε N=pq=2773.
2. Υπολογίζει την ποσότητα φ(N)=46·58=2668 και διαλέγει έναν τυχαίο αριθμό e μικρότερο του 2668, πρώτο ως προς αυτόν – έστω e=17.
3. Με τον επεκταμένο αλγόριθμο του Ευκλείδη, υπολογίζει τα x,y τέτοια ώστε 2668x + 17y=1 (μια που gcd(2668,17)=1). Τότε 17y≡1 mod (2668). Εφαρμόζοντας τομ αλγόριθμο του Ευκλείδη βρίσκουμε y=157. Άρα d=157.
4. Ο χρήστης δημοσιοποιεί σε όλους τα N και e, αλλά κρατάει το d μυστικό για τον εαυτό του (προσέξτε ότι κάποιος που ξέρει τα N και e δεν μπορεί να βρει το d, γιατί δεν ξέρει τα p,q - τα οποία επίσης τα κρατάει μυστικά ο χρήστης).
5. Αν κάποιος θέλει να στείλει το μήνυμα m=31, τότε κάνει τα εξής:

   Κρυπτογράφηση :

   $c \equiv m^e \pmod N$

   $587 \equiv 31^{17} \pmod{2773}$
6. Ο χρήστης αποκρυπτογραφεί το 587 που λαμβάνει, κάνοντας χρήση του d (που μόνο αυτός γνωρίζει):

   Αποκρυπτογράφηση:

   $m \equiv c^d \pmod N$

   $31 \equiv 587^{157} \pmod{2773}$

Αναλυτικό παράδειγμα RSA

•Ο Bob θέλει να στείλει ένα μήνυμα στην Alice, κρυπτογραφημένο με RSA. Τι ενέργειες πρέπει να κάνει ο καθένας?
•Η Alice διαλέγει τυχαία δύο πρώτους αριθμούς - έστω p=37 και q=73 (στην πράξη, τα p,q πρέπει να έχουν περισσότερα από 200 ψηφία). Στη συνέχεια υπολογίζει το γινόμενο N=pq=2701.

•Η Alice διαλέγει τυχαία έναν αριθμό e μικρότερο του (p-1)(q-1) = 36·72 = 2592, που να μην έχει κοινούς διαιρέτες ούτε με το 36 ούτε με το 72. Έστω για παράδειγμα e=77.

•Η Alice βρίσκει τον αριθμό d που ικανοποιεί τη σχέση
$77d \equiv 1 (\mathrm{mod}\ 2592)$. (στην ουσία τον αντίστροφο του e, mod 2592). Με τον επεκταμένο αλγόριθμο του Ευκλείδη, βρίσκουμε ότι είναι d=101.

•**Η Alice ανακοινώνει το δημόσιό της κλειδί (e,N)= (77, 2701).**

•Το ιδιωτικό κλειδί της Alice είναι το d=101. Είναι η μόνη που το γνωρίζει

Πώς βρίσκει η Alice την τιμή του d?

- Εκτελεί τον επεκταμένο αλγόριθμο του Ευκλείδη, για τους αριθμούς φ(N)=2592 και e=77.
- $2592 = 33 \cdot 77 + 51$
- $77 = 1 \cdot 51 + 26$
- $51 = 1 \cdot 26 + 25$
- $26 = 1 \cdot 25 + 1$
- $25 = 25 \cdot 1 + 0$ -> Σταματάμε (άρα, gcd(2592,77)=1 – κάτι που αναμέναμε)

Πώς βρίσκει η Alice την τιμή του d? (συνέχεια)

- «Διαβάζουμε» τις προηγούμενες σχέσεις ανάποδα:
- $1 = 26 - 1 \cdot 25 =$

  $= 26 - 1 \cdot (51 - 1 \cdot 26) = 26 - 1 \cdot 51 + 1 \cdot 26 = 2 \cdot 26 - 1 \cdot 51 =$

  $= 2 \cdot (77 - 1 \cdot 51) - 1 \cdot 51 = 2 \cdot 77 - 2 \cdot 51 - 1 \cdot 51 = 2 \cdot 77 - 3 \cdot 51$
  $= 2 \cdot 77 - 3 \cdot (2592 - 33 \cdot 77) =$

  $= 2 \cdot 77 - 3 \cdot 2592 + 99 \cdot 77 =$

  $= -3 \cdot 2592 + 101 \cdot 77$
- Άρα d=101

Αναλυτικό παράδειγμα RSA (συνέχεια)

- Ο Bob θέλει να στείλει το μήνυμα “I miss you” στην Alice.
- Ο Bob μετατρέπει κάθε γράμμα σε αριθμό, με βάση τη θέση του στο αλφάβητο:

  I M I S S Y O U

  08 12 08 18 18 24 14 20
- Ο Bob σπάει το μήνυμά του σε blocks των δύο γραμμάτων (το δύο αυτό είναι τυχαίο – αναλόγως την υλοποίηση του RSA αλλάζει).
- 0812 0818 1824 1420 (τα ονομάζουμε P_1, P_2 ,P_3, P_4)
- Ο Bob υπολογίζει το $C_i = P_i^{77} \pmod{2701}$ για κάθε block

  $C_1 = 812^{77} = 1744 \pmod{2701}$

  $C_2 = 818^{77} = 321 \pmod{2701}$

  $C_3 = 1824^{77} = 656 \pmod{2701}$

  $C_4 = 1420^{77} = 2064 \pmod{2701}$
- Ο Bob στέλνει στην Alice τους αριθμούς 1744 0321 0656 2064

Αναλυτικό παράδειγμα RSA (συνέχεια)

Για να αποκρυπτογραφήσει το μήνυμα, η Alice χρησιμοποιεί το ιδιωτικό της κλειδί 101, κάνοντας τους ακόλουθους υπολογισμούς:

$1744^{101} = 812 \pmod{2701}$

$0321^{101} = 818 \pmod{2701}$

$0656^{101} = 1824 \pmod{2701}$

$2064^{101} = 1420 \pmod{2701}$

Συνεπώς, το αποκρυπτογραφημένο μήνυμα είναι

0812 0818 1824 1420

- Στη συνέχεια, κάνει την αντιστοίχιση των αριθμών σε γράμματα:

IM IS SY OU

Υπολογισμοί στον RSA - Square and Multiply

- **Στον RSA ανακύπτει η ανάγκη να κάνουμε πράξεις (ύψωση σε δύναμη) πολύ μεγάλων αριθμών. Αυτό αντιμετωπίζεται με την τεχνική Square-And-Multiply.**
- **Αναλύουμε τον αριθμό που θέλουμε να υψώσουμε (μήνυμα για την κρυπτογράφηση ή κρυπτόγραμμα για την αποκρυπτογράφηση) στη δυαδική του αναπαράσταση.**
- **Στη συνέχεια, με βάση το τι είναι κάθε ένα ψηφίο της δυαδικής αναπαράστασης, ανάλογα υψώνουμε στο τετράγωνο το τρέχον αποτέλεσμα και είτε το πολλαπλασιάζουμε με τον αρχικό αριθμός μας (αν το ψηφίο είναι 1) είτε δεν κάνουμε τίποτα άλλο (αν το ψηφίο είναι 0).**

Παράδειγμα

- **Square-and-multiply algorithm**
  - Input: n,x,b (b is in base 2 $(b_{k-1},\ldots,b_1,b_0)$, $b\neq 0$
  - Output: $x^b \bmod n$
  1. $z=1$
  2. for i=k-1 downto 0
     3. $z=z^2 \bmod n$
     4. if $b_i=1$ then $z=zx \bmod n$
- Complexity $O(r^3)$, where $r=[\log_2 n]$
- Example: encrypt 9726 with KU={3533,11413}: $9726^{3533} \bmod 11413$
  - 3533=(1,1,0,1,1,1,0,0,1,1,0,1)
  - Ciphertext: 5761

RSA scheme

–Key generation

- **Choose primes p,q**
- **Compute n=pq**
- **Choose e, $1<e<\phi(n)$ with $\gcd(\phi(n),e)=1$**
- **Compute $d\equiv e^{-1} \bmod \phi(n)$**
- **Private key is {d,n}**
- **Public key is {e,n}**

–Encryption

- **$C=M^e \bmod n$**

–Decryption:

- **$C^d \bmod n = M^{de} \bmod n = M$**

i	b_i	z
11	1	9726
10	1	9726^2x9726=2659
9	0	2659^2=5634
8	1	5634^2x9726=9167
7	1	9167^2x9726=4958
6	1	4958^2x9726=7783

i	b_i	z
5	0	7783^2=6298
4	0	6298^2=4629
3	1	4629^2x9726=10185
2	1	10185^2x9726=105
1	0	105^2=11025
0	1	11025^2x9726=5761

RSA – Πιστοποίηση ταυτότητας

- Έστω ότι η Alice θέλει να στείλει το μήνυμα m στον Bob και ότι θέλει να «υπογράψει» το μήνυμα, έτσι ώστε να είναι σίγουρος ο Bob ότι μιλάει με την Alice.
- Η Alice υπολογίζει την υπογραφή της $s = m^d \bmod N$, όπου d είναι το ιδιωτικό της κλειδί (και N το δημόσιό της).
- Στέλνει στον Bob τα m και s (το m μπορεί να είναι κρυπτογραφημένο με οποιονδήποτε αλγόριθμο – θεωρητικά, μπορεί ακόμα και με τον RSA!).
- Για να ελέγξει την υπογραφή ο Bob, υπολογίζει την ποσότητα $m' = s^e \bmod N$ και ελέγχει αν m'=m.

RSA – Πιστοποίηση ταυτότητας (συνέχεια)

- Ποιο πρόβλημα έχει η προηγούμενη διαδικασία?
- Ο υποκλοπέας μπορεί από την υπογραφή s να ανακτήσει το αρχικό μήνυμα m!!
- Άρα η υπογραφή πρέπει να είναι κρυπτογραφημένη:

  Η Alice λοιπόν κάνει τα εξής:
  - $s = m^d \bmod N_A$, όπου d είναι το ιδιωτικό της κλειδί (και N_A το δημόσιό της).
  - $c = s^e \bmod N_B$, όπου e είναι το δημόσιο κλειδί του Bob (και N_B το δημόσιο κλειδί του Bob).
  - Η Alice στέλνει το c. Ο Bob με δύο διαδοχικές αποκρυπτογραφήσεις (πρώτα μία με το ιδιωτικό του κλειδί για να ανακτήσει το s και μετά μία με το δημόσιο της Alice) ανακτά το m.
- Στην πράξη: η υπογραφή δεν γίνεται πάνω στο μήνυμα αλλά πάνω σε μία κατακερματισμένη τιμή του μηνύματος (βλέπε θεωρία)

Ασφάλεια του RSA

- Όσο πιο μεγάλο είναι το N (κλειδί), τόσο πιο μεγάλη η ασφάλεια (ένας εχθρός δυσκολεύεται ακόμα περισσότερο το να βρει τα p,q). Από την άλλη, ο RSA γίνεται πιο αργός.
- Τα p, q πρέπει να έχουν μεγάλη διαφορά μεταξύ τους: αν η διαφορά p-q είναι μικρή, τότε p $\approx \sqrt{N}$, και έτσι ο p (άρα και ο q) μπορούν να υπολογιστούν με δοκιμές.
- Ο 512-bit RSA-155 «έσπασε» μέσα σε 7 μήνες το 1999 (σήμερα «σπάει» σε λίγες εβδομάδες).
- Το RSA lab προτείνει σήμερα σαν μέγεθος κλειδιού τουλάχιστον 1024 bits (το οποίο ολοένα και τείνει να γίνει παρωχημένο, αφήνοντας τη θέση του σε μεγαλύτερο πλήθος bits).

Επιθέσεις χρονισμού

- **Επιθέσεις χρονισμού (timing attacks):** Μπορεί ο επιτιθέμενος να πάρει κάποια χρήσιμη πληροφορία για το μυστικό κλειδί d κατά τη διάρκεια της αποκρυπτογράφησης, παρακολουθώντας το χρόνο αποκρυπτογράφησης (αν ανακαλέσουμε την τεχνική square-and-multiply, όταν το αντίστοιχο δυαδικό ψηφίο είναι 1 τότε απαιτείται περισσότερος χρόνος για τον τρέχοντα υπολογισμό από ό,τι όταν είναι 0).
  - Μία αντιμετώπιση: καθυστερούμε τις πράξεις που εκτελούνται γρήγορα, έτσι ώστε τελικά είτε το ψηφίο είναι 0 είτε είναι 1 ο χρόνος υπολογισμού να είναι ίδιος

Υλοποίηση σε Matlab

- Διαθέσιμη στο Internet, από το Oregon University
- http://islab.oregonstate.edu/koc/ece575/02Project/Kie+Raj/