ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS

ΑΝΟΙΚΤΑ ακαδημαϊκά μαθήματα ΠΠ

Κβαντική Επεξεργασία Πληροφορίας

Ενότητα 31: Κρυπτογράφηση RSA

Σγάρμπας Κυριάκος

Πολυτεχνική Σχολή

Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών

Σκοποί ενότητας

Κρυπτογράφηση RSA

Περιεχόμενα ενότητας

- Κρυπτογράφηση RSA
- Δημιουργία κλειδιών
- Αποκρυπτογράφηση RSA
- Παραγοντοποίηση

Κρυπτογράφηση RSA

Κρυπτογραφικό Σύστημα RSA Διαδικασία Δημιουργίας Κλειδιών

Rivest, Shamir, Adelman

Επιλέγονται 2 πρώτοι αριθμοί p και q	p = 17 q = 31
Υπολογίζεται το γινόμενό τους n=pq	n = 17*31 = 527
Επιλέγεται ακέραιος d πρώτος ως προς τους (p-1) και (q-1)	(p-1) = 16 = 2*2*2*2 (q-1) = 30 = 2*3*5 d = 77 = 7*11
Το ζεύγος (d,n) είναι το ιδιωτικό κλειδί	Ι.Κ. = (d,n) = (77,527)
Υπολογίζεται e τέτοιος ώστε ed mod (p-1)(q-1) = 1	(p-1)*(q-1)=16*30=480 77*e mod 480 = 1 e = (480*k+1)/77 e = 293 (k=47) e = 773 (k=124) ...
Το ζεύγος (e,n) είναι το δημόσιο κλειδί	Δ.Κ. = (e,n) = (293,527)

R.Rivest, A.Shamir, L.Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM vol.21, no.2, pp.120–126, 1978.

Κρυπτογράφηση & Αποκρυπτογράφηση στο RSA

Το μήνυμα που θέλουμε να κρυπτογραφήσουμε το μετατρέπουμε σε έναν αριθμό m<n
(Πρακτικά το n είναι πολύ μεγαλύτερο από το παράδειγμα, όμως αν το μήνυμα είναι μεγαλύτερο το κόβουμε σε κομμάτια)

n=527
m=421

Η κρυπτογράφηση γίνεται με το δημόσιο κλειδί (e,n) ως:
$c=m^e \bmod n$

(e,n)=(293,527)
c=421**293%527=472

Η αποκρυπτογράφηση γίνεται με το ιδιωτικό κλειδί (d,n):
$m=c^d \bmod n$

(d,n)=(77,527)
472**77%527=421=m

Δουλεύει γιατί ισχύει η ταυτότητα:
$(m^e \bmod n)^d \bmod n = m$

Ασφάλεια RSA

Με γνωστό τον αλγόριθμο δημιουργίας κλειδιών και το δημόσιο κλειδί, πόσο εύκολο είναι να υπολογιστεί το ιδιωτικό κλειδί;

πχ. αν e=293 και n=527 πόσο είναι το d;

Αν βρούμε τα p και q, τότε το d υπολογίζεται το ίδιο εύκολα όπως το e στον αλγόριθμο δημιουργίας κλειδιών:

$d = ((p-1)*(q-1)*k+1)/e = ((p-1)*(q-1)*k+1)/293$

$n = p*q = 527$

Για την παραγοντοποίηση ενός n 129 ψηφίων χρειάστηκαν 17 χρόνια και ένα δίκτυο 1600 Η/Υ

Άρα η ασφάλεια του συστήματος RSA διασφαλίζεται από την δυσκολία παραγοντοποίησης του n και γι'αυτό επιλέγονται πολύ μεγάλοι πρώτοι αριθμοί p και q.

Παραγοντοποίηση n=p*q

```
for p=2 to sqrt(n):
    y=(n % p)
    if y==0:
        q=n/p
        print p,q
        stop
```

```
select a: gcd(a,n)=1
f=x=0
while (f<>1):
    x=x+1
    f=(a**x) % n
r=x
p=gcd(a**(r/2)-1,n)
q=gcd(a**(r/2)+1,n)

def gcd(a,b):
    m=a%b
    if m==0: return b
    return gcd(b,m)
```

Αλγόριθμος Ευκλείδη (για την εύρεση του ΜΚΔ)

Πολυπλοκότητα $O(\sqrt{n})$
ως προς το μέγεθος του αριθμού, αλλά εκθετική ως προς το πλήθος των bits

$$b = \log_2(n) \Leftrightarrow n = 2^b$$

$$O(\sqrt{n}) = O(\sqrt{2^b}) = O(2^{b/2}) = O(2^b)$$

n μήκους 2048 bit (617 δεκαδικών ψηφίων) θεωρείται ακόμη ασφαλές

Παραγοντοποίηση με Περιοδική Συνάρτηση

Αν n είναι ο αριθμός προς παραγοντοποίηση, δημιουργούμε τη συνάρτηση $f(x)=a^x \bmod n$ και υπολογίζουμε τις τιμές της για x=0,1,2,3,... μέχρι να αρχίσουν να επαναλαμβάνονται.

Για την ακρίβεια, επειδή πάντα f(0)=1, αρκεί να ελέγξουμε πότε θα ξαναεμφανιστεί f(x)=1. Το συγκεκριμένο x είναι η περίοδος r.

Και τότε:

$p=\gcd(a^{r/2}-1,n)$

$q=\gcd(a^{r/2}+1,n)$

Για να λειτουργήσει σωστά, το a θα πρέπει να είναι πρώτος ως προς το n, δηλαδή gcd(a,n)=1.

```
n=527, a=26, f(x)=26**x%527
x  f(x)
0    1
1   26
2  149
3  185
4   67
5  161
6  497
7  274
8  273
9  247
10  98
11 440
12 373
13 212
14 242
15 495
16 222
17 502
18 404
19 491
20 118
21 433
22 191
23 223
24   1
25  26
26 149
27 185
28  67
29 161
...
```

Αν το r βγει περιττό, ξαναδοκιμάζουμε με νέο a

```
r=24
a**12=95428956661682176
gcd(95428956661682175,527)=31
gcd(95428956661682177,527)=17
```

Τέλος Ενότητας

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στο πλαίσιο του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αθηνών**» έχει χρηματοδοτήσει μόνο την 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.

Σημειώματα

Σημείωμα Ιστορικού Εκδόσεων Έργου

Το παρόν έργο αποτελεί την έκδοση 1.0.

Έχουν προηγηθεί οι κάτωθι εκδόσεις:

- Έκδοση 1.0 διαθέσιμη εδώ.

Σημείωμα Αναφοράς

Σημείωμα Αδειοδότησης

Διατήρηση Σημειωμάτων

Οποιαδήποτε αναπαραγωγή ή διασκευή του υλικού θα πρέπει να συμπεριλαμβάνει:

- το Σημείωμα Αναφοράς
- το Σημείωμα Αδειοδότησης
- τη δήλωση Διατήρησης Σημειωμάτων
- το Σημείωμα Χρήσης Έργων Τρίτων (εφόσον υπάρχει)

μαζί με τους συνοδευόμενους υπερσυνδέσμους.

Σημείωμα Χρήσης Έργων Τρίτων

Το Έργο αυτό κάνει χρήση των ακόλουθων έργων:

Εικόνες/Σχήματα/Διαγράμματα/Φωτογραφίες