



# 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  $q$

$$\begin{aligned} p &= 17 \\ q &= 31 \end{aligned}$$

Υπολογίζεται το γινόμενό τους  $n=pq$

$$n = 17 * 31 = 527$$

Επιλέγεται ακέραιος  $d$  πρώτος ως προς τους  $(p-1)$  και  $(q-1)$

$$\begin{aligned} (p-1) &= 16 = 2 * 2 * 2 * 2 \\ (q-1) &= 30 = 2 * 3 * 5 \\ d &= 77 = 7 * 11 \end{aligned}$$

Το ζεύγος  $(d,n)$  είναι το ιδιωτικό κλειδί

$$I.K. = (d,n) = (77,527)$$

Υπολογίζεται  $e$  τέτοιος ώστε  
 $ed \bmod (p-1)(q-1) = 1$

$$\begin{aligned} (p-1)*(q-1) &= 16 * 30 = 480 \\ 77 * e \bmod 480 &= 1 \\ e &= (480 * k + 1) / 77 \\ e &= 293 \quad (k=47) \\ e &= 773 \quad (k=124) \dots \end{aligned}$$

Το ζεύγος  $(e,n)$  είναι το δημόσιο κλειδί

$$\Delta.K. = (e,n) = (293,527)$$

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)

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

Η αποκρυπτογράφηση γίνεται με το ιδιωτικό κλειδί  $(d, n)$ :  
 $m = c^d \text{ mod } n$

Δουλεύει γιατί ισχύει η ταυτότητα:  
 $(m^e \text{ mod } n)^d \text{ mod } n = m$

$$\begin{aligned} n &= 527 \\ m &= 421 \end{aligned}$$

$$\begin{aligned} (e, n) &= (293, 527) \\ c &= 421^{293} \% 527 = 472 \end{aligned}$$

$$\begin{aligned} (d, n) &= (77, 527) \\ 472^{77} \% 527 &= 421 = m \end{aligned}$$



# 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 H/Y

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
```

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

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

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

```
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)

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



# Παραγοντοποίηση με Περιοδική Συνάρτηση

Αν η είναι ο αριθμός προς παραγοντοποίηση, δημιουργούμε τη συνάρτηση  $f(x)=a^x \text{ mod } n$  και υπολογίζουμε τις τιμές της για  $x=0,1,2,3,\dots$  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  $\gcd(a, n) = 1$ .

$n=527, \quad a=26, \quad f(x)=26**x \% 527$	
<u>x</u>	<u><math>f(x)</math></u>
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
	...

**r=24**

$$a^{*12}=95428956661682176$$
$$\gcd(95428956661682175, 527)=\mathbf{31}$$
$$\gcd(95428956661682177, 527)=\mathbf{17}$$

Αν το  $r$  βγει περιττό, ξαναδοκιμάζουμε με νέο  $a$



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

Copyright Πανεπιστήμιο Πατρών, **Σγάρμπας Κυριάκος**. «Κβαντική Επεξεργασία Πληροφορίας, Κρυπτογράφηση RSA». Έκδοση: 1.0. Πάτρα 2014. Διαθέσιμο από τη δικτυακή διεύθυνση:

[https://eclass.upatras.gr/modules/course\\_metadata/opencourses.php?fc=15](https://eclass.upatras.gr/modules/course_metadata/opencourses.php?fc=15)



# Σημείωμα Αδειοδότησης

Το παρόν υλικό διατίθεται με τους όρους της άδειας χρήσης Creative Commons Αναφορά, Μη Εμπορική Χρήση Παρόμοια Διανομή 4.0 [1] ή μεταγενέστερη, Διεθνής Έκδοση. Εξαιρούνται τα αυτοτελή έργα τρίτων π.χ. φωτογραφίες, διαγράμματα κ.λ.π., τα οποία εμπεριέχονται σε αυτό και τα οποία αναφέρονται μαζί με τους όρους χρήσης τους στο «Σημείωμα Χρήσης Έργων Τρίτων».



[1] <http://creativecommons.org/licenses/by-nc-sa/4.0/>

Ως **Μη Εμπορική** ορίζεται η χρήση:

- που δεν περιλαμβάνει άμεσο ή έμμεσο οικονομικό όφελος από την χρήση του έργου, για το διανομέα του έργου και αδειοδόχο
- που δεν περιλαμβάνει οικονομική συναλλαγή ως προϋπόθεση για τη χρήση ή πρόσβαση στο έργο
- που δεν προσπορίζει στο διανομέα του έργου και αδειοδόχο έμμεσο οικονομικό όφελος (π.χ. διαφημίσεις) από την προβολή του έργου σε διαδικτυακό τόπο

Ο δικαιούχος μπορεί να παρέχει στον αδειοδόχο ξεχωριστή άδεια να χρησιμοποιεί το έργο για εμπορική χρήση, εφόσον αυτό του ζητηθεί.

# 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**

