

# RSA

## ΠΑΡΑΔΕΙΓΜΑ1

Δίνονται  $N=26$ ,  $k=3$ ,  $l=4$ . Το μήνυμα αποτελείται από τρι-γραφήματα (αφού  $k=3$ ) ενώ το κρυπτογράφημα από τετρα-γραφήματα (αφού  $l=4$ ). Υποθέτουμε ότι στέλνουμε τη λέξη **YES**.

Δίνονται επίσης  $n=46927$  και  $b=39423$

### Κωδικοποίηση

$$\left. \begin{array}{l} Y \rightarrow 24 \\ E \rightarrow 4 \\ S \rightarrow 18 \end{array} \right\} \Rightarrow 18 * 26^0 + 4 * 26^1 + 24 * 26^2 = 16346$$

Υπολογίζουμε την δύναμη  $16346^{39423} \bmod 46927 = 21166$

Το 21166 θέλω να το γράψω στη μορφή:  $\alpha_3 26^3 + \alpha_2 26^2 + \alpha_1 26 + \alpha_0 = 21166$ . Με συνεχείς διαιρέσεις τελικά καταλήγουμε :

$$\alpha_3 = 1 \rightarrow B, \quad \alpha_2 = 5 \rightarrow F, \quad \alpha_1 = 8 \rightarrow I, \quad \alpha_0 = 2 \rightarrow C$$

Οπότε το κρυπτογράφημα είναι το : **BFIC**

### Αποκωδικοποίηση

Ο παραλήπτης γνωρίζει  $(n,a) = (46927, 26767)$

Υπολογίζει  $21166^{26767} \bmod 46927 = 16346$ . Τον αριθμό αυτόν τον γράφουμε με βάση το 26 στην εξής μορφή:  $\alpha_3 26^3 + \alpha_2 26^2 + \alpha_1 26 + \alpha_0 = 16346 \Rightarrow 24 * 26^2 + 4 * 26 + 18 = 16346$ . Είναι λοιπόν:

$$24 \rightarrow Y, \quad 4 \rightarrow E, \quad 18 \rightarrow S.$$

## ΠΑΡΑΔΕΙΓΜΑ 2

$p=100003$ ,  $q=200017$ ,  $b=23456789$ .

Είναι  $n=pq=20002300051$ . Ισχύει  $\text{ΜΚΔ}(b, n) = 1$ .

Μήνυμα: ΕΠΙΘΕΣΗ ΣΤΙΣ ΟΚΤΩ.

Η αρίθμηση των γραμμάτων γίνεται ως εξής: 01, 02, 03, ...24 και 25 το κενό. Έτσι μετά την αντικατάσταση έχουμε :

05 16 09 08 05 18 07 25 18 19 09 18 25 15 10 19 24 .

Τα χωρίζουμε σε πεντάδες ( $k=5$ ) οπότε έχουμε:

05160 90805 18072 51819 09182 51510 19240 (το μηδέν στο τέλος προστέθηκε για να συμπληρωθεί πεντάδα)

### Κωδικοποίηση

$$05160^b \pmod{n} = 05160^{23456789} \pmod{20002300051} = 15632873174$$

κ.ο.κ

### Αποκωδικοποίηση

Υπολογίζεται  $a = 7983352061$ . Τις τιμές που έχουμε βρει από την κωδικοποίηση τις υψώνουμε στο  $a$  και το αποτέλεσμα το παίρνουμε ως προς  $\text{mod } n$ . Δηλαδή:

$$\text{π.χ } 15632873174^{7983352061} \bmod 20002300051 = 05160$$

Αφού το κάνουμε αυτό βάζουμε τα αποτελέσματα στη σειρά και τα χωρίζουμε σε δυάδες. Δηλαδή :

05160, 90805, 18072, 51819, 09182, 51510, 19240

05 | 16 | 09 | 08 | 05 | 18 | 07 | 25 | 18 | 19 | 09 | 18 | 25 | 15 | 10 | 19 | 24 | 0

Ε Π Ι Θ Ε Σ Η \_ Σ Τ Ι Σ \_ Ο Κ Τ Ω

### ⇒ Παρατηρήσεις

1. Για τον υπολογισμό των  $x^b \pmod{n}$  γράφουμε τον εκθέτη στο δυαδικό σύστημα αρίθμησης.
2. Γνώση του  $\varphi(n)$  ισοδυναμεί με γνώση παραγοντοποίησης του  $n$ .  
 $\varphi(n) = (p-1)(q-1) = pq - (p+q) + 1 = n - (p+q) + 1 \Rightarrow p+q$  γνωστό  
 $(p-q)^2 = (p+q)^2 - 4pq = (p+q)^2 - 4n \Rightarrow p-q$  γνωστό.  
Έχουμε επομένως γνώση των  $p, q$
3. Σπάμε τον κώδικα εάν καταφέρουμε να παραγοντοποιήσουμε το  $n$ . Άρα χρειαζόμαστε αλγορίθμους παραγοντοποίησης.
4. Οι πρώτοι  $p, q$  θα πρέπει να έχουν περισσότερα από 130 ψηφία και τα  $p-1, q-1, p+1, q+1$  να έχουν μεγάλους παράγοντες.
5. Οι  $p, q$  πρέπει να είναι της ίδιας τάξης μεγέθους αλλά με διαφορετικό αριθμό ψηφίων.