Πχ (Λύση της άσκησης 4 από φύλλο #7)

α) $x^2 \equiv 47 \bmod 11$, 11: πρώτος

$x^2 \equiv 3 \bmod 11$

$11 = 2\cdot 4 + 3 \xrightarrow{\text{Euler}} x \equiv 3^{\frac{11+1}{4}} \bmod 11 \equiv 27 \bmod 11 \equiv 5 \bmod 11$

Άρα, έχει και αλλη μία λύση την

$x \equiv -5 \bmod 11 \rightarrow \begin{cases} x \equiv 6 \bmod 11 \\ x \equiv 5 \bmod 11 \end{cases}$

β) $x^2 \equiv 47 \bmod 11^2$ Βρίσκαμε εαν υπάρχει λύση της μορφής $x^2 \equiv 47 \bmod 11$ οπου λύσεις της είναι $x \equiv \pm 5 \bmod 11$

Βρίσκω k ώστε $(5+k\cdot 11)^2 \equiv 47 \bmod 11^2 \Rightarrow$

$\Rightarrow 5^2 + 2\cdot 5\cdot 11k + k^2 11^2 \equiv 47 \bmod 11^2 \Rightarrow$

$\Rightarrow 2\cdot 5 \frac{11}{11} k \equiv \frac{22}{11} \bmod \frac{11^2}{11} \Rightarrow 2\cdot 5\cdot k \equiv 2 \bmod 11 \Rightarrow$

$\Rightarrow 5k \equiv 1 \bmod 11 \Rightarrow 5\cdot 9 = 45 \equiv 1 \bmod 11$

Άρα το $9 = 5^{-1}$ και τότε

$k \equiv 9 \bmod 11 \rightarrow x \equiv (5 + 9\cdot 11) \equiv 104 \bmod 11^2$

όμοια και για την $x \equiv 6 \bmod 11$.

γ) $x^2 \equiv 47 \bmod 11^3$ γνωστο πλεον ότι η εξίσωση: $x^2 \equiv 47 \bmod 11^2$ έχει λύση την $x \equiv 104 \bmod 11^2$

$104^2 - 47 = \mu \cdot 11^2 \equiv 1\cdot 11^2$

Βρίσκω λ ώστε $(104 + \lambda\cdot 11)^2 \equiv 47 \bmod 11^3 \Rightarrow$

$\Rightarrow 104^2 + \lambda^2 11 + 2\cdot 104\cdot\lambda\cdot 11^2 \equiv 47 \bmod 11^3 \Rightarrow$

$\Rightarrow 104^2 - 47 + 2\cdot 104\cdot\lambda\cdot 11^2 \equiv 0 \bmod 11^3 \Rightarrow$

$\Rightarrow \frac{11^2}{11^2} + 2\cdot 104\lambda \cdot \frac{11^2}{11^2} \equiv 0 \bmod \frac{11^3}{11^2} \Rightarrow$

$\Rightarrow 1 + 2\cdot 104\cdot\lambda \equiv 0 \bmod 11 \Rightarrow$

$\Rightarrow 2\cdot 104 \equiv -1 \bmod 11 \Rightarrow 2\cdot 104 \overset{\text{mod}11}{\equiv} 10 \bmod 11 \Rightarrow$

$\Rightarrow 2\cdot 5\cdot\lambda \equiv 10 \bmod 11 \Rightarrow \lambda \equiv 1 \bmod 11$

Λύση της $x^2 \equiv 47 \bmod 11^3$ είναι η εξής:

$(104 + 11^2) \bmod 11^3 \equiv (104 + 121) \bmod 11^3 \equiv 225 \bmod 11^3$

ΙΧ

Να λυθεί η $7x^2+28x \equiv 0 \bmod 45$

~~ΛΥΣΗ~~

$7x^2+4\cdot 7x = 7(x^2+4x) = 7(x^2+4x+4-4) =$

$= 7(x+2)^2 - 7\cdot 4 \equiv 0 \bmod 45 \Rightarrow$

$\Rightarrow 7(x+2)^2 \equiv 7\cdot 4 \bmod 45 \Rightarrow \quad (7,45)=1$

$\Rightarrow (x+2)^2 \equiv 4 \bmod 45$

Θέτω $y = x+2$

τότε : $y^2 \equiv 4 \bmod 45 \iff \begin{cases} y^2 \equiv 4 \bmod 3^2 & (1) \\ y^2 \equiv 4 \bmod 5 & (2) \end{cases}$

για την (1): εξετάζουμε λύση για την

$y^2 \equiv 4 \bmod 3 \equiv 1 \bmod 3 \Rightarrow y \equiv \pm 1 \bmod 3$

Άρα, για η $y^2 \equiv 4 \bmod 3^2$ έχει λύση

$(1+3k)^2 \equiv 4 \bmod 3^2 \Rightarrow 1+2\cdot 3k \equiv 4 \bmod 3^2 \Rightarrow$

$\Rightarrow \frac{2\cdot 3\cdot k}{3} \equiv \frac{3}{3} \bmod \frac{3^2}{3} \Rightarrow 2k \equiv 1 \bmod 3 \Rightarrow$

$\Rightarrow k \equiv 2 \bmod 3$ Λύση της $y^2 \equiv 4 \bmod 3^2$

$\Rightarrow \boxed{y \equiv 1+3\cdot 2 \equiv 7 \bmod 9}$

Επίσης, λύνουμε την $y^2 \equiv 4 \bmod 5 \equiv \pm 2 \bmod 5$

Δηλ.

$\left.\begin{array}{l} y \equiv 7 \bmod 9 \\ y \equiv 2 \bmod 5 \end{array}\right\} \xrightarrow[\text{Κ.Θ}]{(9,5)=1} (5C_1\cdot 7 + 9C_2\cdot 2) \bmod 45 \quad (3)$ λύση

άρα $5C_1 \equiv 1 \bmod 9$

$9\cdot C_2 \equiv 1 \bmod 5 \Rightarrow 4C_2 \equiv 1 \bmod 5 \Rightarrow C_2 \equiv 4 \bmod 5$

Άρα, όπου (3) είναι:

$x = (5\cdot 2\cdot 7 + 9\cdot 4\cdot 2) \equiv 142 \bmod 45$

Έχουμε $y \equiv 7 \bmod 45$ και $y = 2+x \Rightarrow$

$\Rightarrow x+2 \equiv 7 \bmod 45 \Rightarrow x \equiv 5 \bmod 45$

πχ:

Έστω ότι η χρήσιμη στην γινόμενο δύο διαφορετικών πρώτων $n = p \cdot q$. Αν γνωρίζουμε το n και το $\varphi(n)$ μπορούμε να βρούμε τους πρώτους;

ΛΥΣΗ

$$\left.\begin{array}{l} \varphi(n) = \varphi(p \cdot q) = \varphi(p)\,\varphi(q) = (p-1)(q-1) \\ (p,q) = 1 \\ \text{Έστω } p \text{ γνωστό} \Rightarrow q = \frac{n}{p} \end{array}\right\} (p-1)\left(\frac{n}{p}-1\right) \Rightarrow$$

$$\Rightarrow p\varphi(n) = (p-1)(n-p) \Rightarrow p^2 + p(\varphi(n) - n - 1) + n = 0$$, Άρα ο ένας Πρώτος p θα είναι μια ρίζα του:

$$x^2 + x(\varphi(n) - n - 1) + n$$

Στοιχεία Κρυπτογραφίας:

Κείμενο x $\xrightarrow{\text{Διαδικασία Κρυπτογράφησης}}$ Κρυπτογραφημένο Κείμενο $\xrightarrow{\text{Αποστολή}}$ Λήψη κρυπτ. κειμένου

$\xrightarrow{\text{Διαδικασία Απαυρυπτογράφησης}}$ Κείμενο

Με Κρυπτογρ. συμμετρικού

$E_k(x) \to D_k E_k(x) = x$ με $E_k(x)$ κλειδί της κρυπτογράφησης

Κρυπτογραφία = Επιστήμη η οποία ασχολείται με την κρυπτογράφηση κειμένων

Κρυπτανάλυση = Επιστήμη η οποία ασχολείται με την απαυρυπτογράφηση

Κλειδί: Ο "τρόπος" που θα γίνει η απαυρυπτογράφηση

Συνήθως είναι γνωστό στον αποστολέα και παραλήπτη

1) Κρυφό κλειδί (Secret key) Μεταξύ τους

2) Κοινό κλειδί (Public key) Πολλοί παραλήπτες

ΓΕΝΙΚΕΣ ΑΡΧΕΣ:

Από το Α μέχρι το Ω αντιστοιχούμε τα στοιχεία 0 έως 23 (για κάθε γράμμα του ελληνικού Αλφαβήτα)

κλειδί κρυφό $K=(1,3)$ (γενικό $k=(a,\beta$

$E_K(\gamma_i) = (\gamma_i + 3) \bmod 24$ $E_k(\gamma_i) = (a\gamma_i + \beta) \bmod 24$)

↑ γράμμα

$\gamma_i \in \mathbb{Z}_{24}$

↓ αριθμός

ΚΕΙΜΕΝΟ: ΕΠΙΘΕΣΗ

4 15 8 7 4 17 6

7 18 11 10 7 20 9

Θ Τ Μ Κ Θ Φ Κ

$D_K(k_i) = D_K(E_K(\gamma_i)) = \gamma_i$

$ax+\beta \equiv y \bmod 24$

$ax \equiv y-\beta \bmod 24$ $(a,24)=1$

$ax \equiv y+(24-\beta) \bmod 24$

$x \equiv \delta(y+24-\beta) \bmod 24.$

$K=(e,p)$ με $(e,p-1)=1$

$E_K(\gamma_i) = \gamma_i^e \bmod p = k_i$

$D_K(k_i) =$

$\gamma_i^{\varphi(p)} \equiv 1 \bmod p \Rightarrow \gamma_i \cdot \gamma_i^{\varphi(p)} \equiv \gamma_i \bmod p.$

$k_i^d \equiv \gamma_i^{ed} \bmod p$ Άλλα ποιο τοδ;

το $e \cdot d$ πρέπει $ed = \varphi(p)+1.$

Κλειδί $k=(n=p\cdot q, e)$ με p,q μεγάλοι διαφορετικοί πρώτοι και $(e,n-1)=1$

ΕΜΠΟΡΙΚΟΙ ΚΩΔΙΚΕΣ: (Public key)

Ο παραλήπτης θα πρέπει να έχει τη δυνατότητα να επιβεβαιώνει τον αυθεντικότητα του μηνύματος

Ο παραλήπτης θα πρέπει να έχει τη δυνατότητα να ελέγξει αν το μήνυμα έχει αλλάξει κατά τη μεταφορά.

Ο αποστολέας δεν έχει την δυνατότητα να αρνηθεί αποσταλμένο μήνυμα

Public key cryptography

Δεν υπάρχει κανό κλειδί
Κάθε άτομο χρησιμοποιεί δύο κλειδιά. Ένα για κρυπτογράφηση και ενά άλλο για αποκρυπτογράφηση
Το πρώτο κλειδί είναι γνωστό
Αλλά το δεύτερο όχι

Πχ

Αγγελική, Κώνας } πρέπει να ανταλλάξουν ένα μυστικό κλειδί

Έλεγχαν 2 νούμερα g και n
Αγγελική επιλέγει το a (τυχαία) "υπολογίζει"
$u = g^a \bmod n$ στέλνει u στον Κώνα.
Ο Κώνας επιλέγει τυχαία ενα b και "υπολογίζει"
$v = g^b \bmod n$. Στέλνει το v
καθορισμός του κλειδιού
Κώνας υπολογίζει το κλειδί
$k = u^b = g^{a \cdot b} \bmod n$
Αγγελική υπολογίζει $v^a \equiv g^{ba} \bmod n = k$ κοινό κλειδί