S_2/ 1. Pt. operatia:

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \underbrace{\begin{bmatrix} 6 & 1 \\ 5 & 1 \end{bmatrix}}_{M} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \bmod 26$$

găsiți regula de decriptare

În general $M \in \mathcal{M}^m(\mathbb{Z}_n)$, M^{-1} există dacă $\gcd(\det(M), n) = 1$

$\det(M) = 1$

$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ $\det(A) = ad - bc$

$$A^{-1} = \frac{1}{\det(A)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$M^{-1} = \begin{bmatrix} 1 & -1 \\ -5 & 6 \end{bmatrix}$$

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = M^{-1} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \pmod{26}$$

2. Fie A un alfabet cu 26 de caractere și ($\#A = 26$)
blocuri de lungime 2, deci criptarea va fi de forma
$x_1 x_2 \mapsto y_1 y_2$. Identificăm A cu $\mathbb{Z}_{26}$

Operația $\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 6 & 2 \\ 5 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \bmod 26$

nu este bună pt. a realiza o criptare liniară pt. că $\det(M)=2$ $(\gcd(2,26)=2\neq 1)$. Dați exemplu de $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ și $\begin{bmatrix} \bar{x}_1 \\ \bar{x}_2 \end{bmatrix}$ a.î. să se ducă în același elem. $\begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$

$$M\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = M\begin{bmatrix} \bar{x}_1 \\ \bar{x}_2 \end{bmatrix}$$

$$M = \begin{bmatrix} 6 & 2 \\ 5 & 2 \end{bmatrix}$$

$$M\begin{bmatrix} 6 \\ 5 \end{bmatrix} = \begin{bmatrix} 46 \\ 40 \end{bmatrix} = \begin{bmatrix} 20 \\ 14 \end{bmatrix}$$

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x \\ 0 \end{bmatrix} ; \begin{bmatrix} \bar{x}_1 \\ \bar{x}_2 \end{bmatrix} = \begin{bmatrix} x \\ 13 \end{bmatrix}$$

$$M\begin{bmatrix} x \\ 0 \end{bmatrix} = \begin{bmatrix} 6x \\ 5x \end{bmatrix} ; \quad M\begin{bmatrix} x \\ 13 \end{bmatrix} = \begin{bmatrix} 6x+26 \\ 5x+26 \end{bmatrix} = \begin{bmatrix} 6x \\ 5x \end{bmatrix}$$

<u>Lema Chineză a resturilor:</u>

Fie $p \geq 2$, ~~...~~ $m_i, i=\overline{1,p}$ întregi pozitivi

$\gcd(m_i, m_j)=1, \forall i,j=\overline{1,p}, i\neq j$

Atunci oricare ar fi $a_1, \ldots, a_p$ nr. întregi, există $x \in \mathbb{Z}$ sol. a sist.

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_p \pmod{m_p} \end{aligned}$$

În plus, toate sol. x sunt congr. mod $N = \prod_{i=\overline{1,p}} m_i$

3. Mihai vrea să-și țină vârsta secretă. Prietenii lui știu:

-> Acum un an, vârsta lui Mihai era div. cu 3

-> În doi ani, vârsta lui va fi multiplu de 5

-> În patru ani, va fi multiplu de 7

Câți ani are M?

x = vârsta lui M

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}$$

OBS: 3, 5, 7 sunt prime între ele => putem aplica LCR

OBS. Din dem. LCR avem:

-> $b_i = \frac{N}{m_i}$

-> $\overline{b_i} = b^{-1} \pmod{m_i}$

-> $x = \sum_{i=\overline{1,n}} a_i b_i \overline{b_i} \pmod N$

$$x = \left(1 \cdot 35\left(35^{-1} \pmod 3\right)\right) + \left(3 \cdot 21\left(21^{-1} \pmod 5\right)\right) + \left(3 \cdot 15\left(15^{-1} \pmod 7\right)\right) \pmod{105}$$

$x = 35 \cdot 2 + 3 \cdot 21 + 3 \cdot 15 = 73 \bmod 105$

Alg. de exp. rapidă

Calc. $b^r \bmod n$ pt. $b, r, n \in \mathbb{N}$. Primul lucru pe care îl facem scriem r în baza 2 $\to r = \sum_{j=\overline{0,k}} a_j 2^j$

Vrem $c = b^r \bmod n$

Pas 1 Fie $b_0 = b$ și $c = \begin{cases} 1, & \text{dacă } a_0 = 0 \\ 0, & \text{dacă } a_0 = 1 \end{cases}$

Pt. $j = \overline{1,k}$

Pas j: Calculăm $b_j = b_{j-1}^2 \bmod n$. Dacă $a_j = 1$

$\Rightarrow c \leftarrow c\, b_j \pmod n$

$a_j = 0 \to c$

Avem $c_j = b^{r_j} \pmod n$

unde $c_j = b_j \bmod n$; $r_j = \sum_{i=\overline{0,j}} a_i 2^i$

La pasul k $c = b^r \pmod n$

5. Folosind alg. de exp. rapidă calc. $5^{117} \bmod 19$

$117_{(10)} = 1110101_{(2)}$

$117 = 2^6 + 2^5 + 2^4 + 2^2 + 2^0$

$117 = 1 + 4 + 16 + 32 + 64$

$5^{117} = 5^1 \cdot 5^4 \cdot 5^{16} \cdot 5^{32} \cdot 5^{64}$

$5^1 = 5 \pmod{19}$

$5^2 = 25 = 6 \pmod{19}$

$5^4 = 5^2 \cdot 5^2 = 36 \cancel{\equiv} = 17 \cancel{\equiv} = -2 \pmod{19}$

$5^8 = 4 \pmod{19}$

$5^{16} = 16 \pmod{19} = -3$

$5^{32} = 9 \pmod{19}$

$5^{64} = 81 \equiv 5 \pmod{19}$

$5^{128} = 6 \pmod{19}$

$5^{117} = 5 \cdot (-2) \cdot (-3) \cdot 9 \cdot 5$

$= \cancel{6} = 1 \pmod{19}$

6. Folosind alg. de exp. rapidă calc $9^{-1} \bmod 26$.

<u>Th. lui Euler:</u>

Dacă $m \geq 1$ și $\gcd(m, a) = 1$ atunci $a^{\varphi(m)} = 1 \pmod m$

<u>Def.</u> $\varphi(n) = \# \{ m \mid m \equiv \cancel{m}$ și $\gcd(m, n) = 1 \}$

Th. $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$

$\varphi(n) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p^k}\right)$

$\Leftrightarrow \varphi(n) = p_1^{\alpha_1 - 1} (p_1 - 1) \dots p_k^{\alpha_k - 1} (p_k - 1)$

$a^{\varphi(m)} = 1 \pmod m$

$a \cdot a^{\varphi(m) - 1} = 1 \pmod m$

Ştim din Th. $gcd(a, n) = 1$

$\Rightarrow a^{\varphi(n)-1} = a^{-1} \pmod n$

Luăm $\left.\begin{matrix} a = 9 \\ n = 26 \end{matrix}\right\} \Rightarrow 9^{-1} = 9^{\varphi(26)-1} \pmod{26}$

$\varphi(26) = \varphi(2 \cdot 13) = \varphi(2) \cdot \varphi(13) = (2-1)(13-1) = 12$

$\Rightarrow 9^{-1} = 9^{12-1} = 9^{11} \pmod{26}$

$9^{11} = 9^8 \cdot 9^2 \cdot 9^1$

$9^1 = 9 \pmod{26}$

$9^2 = 3 \pmod{26}$

$9^4 = 9 \pmod{26}$

$9^8 = 3 \pmod{26}$

$9^{11} = 3 \cdot 3 \cdot 9 = 3 \pmod{26}$

$9^{-1} = 3 \pmod{26}$

7. $b = 15$, $a = 113$

$113 = 15 \cdot 7 + 8$ $\qquad \Rightarrow gcd(113, 15) = 1$

$15 = 8 \cdot 1 + 7$

$8 = 7 \cdot 1 + 1$

$7 = 1 \cdot 7 + 0$