Criptografie - Tema 1

2) CMMDC

cmmdc(12347, 54329)

$x_{54329} = (1,0)$, $x_{12347} = (0,1)$

$54329 = 12347 \cdot 4 + 4941 \Rightarrow x_{4941} = x_{54329} - 4 \cdot x_{12347}$

49388

$= (1, -4)$

$12347 = 4941 \cdot 2 + 2465 \Rightarrow x_{2465} = x_{12347} - 2 \cdot x_{4941}$

9882

$= (0,1) - 2(1,-4) = (-2, 9)$

$4941 = 2465 \cdot 2 + 11 \Rightarrow x_{11} = x_{4941} - 2 \cdot x_{2465}$

4930

$= (1,-4) - 2 \cdot (-2,9) = (5, -22)$

11

$2465 = 11 \cdot 224 + 1 \Rightarrow x_1 = x_{2465} - 224 \cdot x_{11} =$

2464

$= (-2,9) - 224 \cdot (5, -22) =$

$= (-1122, 4937)$

cmmdc $(12347, 54329) = 1$

$1 = (-1122) \cdot \cancel{12347} + 4937 \cdot \cancel{54329}$

$54329 \qquad 12347$

3) Inversul lui 3 în $\mathbb{Z}_{11}$

$(3, 11) = 1 \Rightarrow \exists u, v \in \mathbb{Z}$ a.î.

$1 = 3u + 11v \quad / \pmod{11}$

$1 \pmod{11} \equiv 3u \pmod{11}$

$3^{-1} \equiv u \pmod{11}$

$X_{11} = (1, 0)$, $X_3 = (0, 1)$

$11 = 3 \cdot 3 + 2 \Rightarrow X_2 = X_{11} - X_3 = (1, -3)$

$3 = 2 \cdot 1 + 1 \Rightarrow X_1 = X_3 - X_2 = (-1, 4)$

$1 = (-1) \cdot 11 + 4 \cdot 3 \Rightarrow u = +4 \Rightarrow$

$\Rightarrow 3^{-1} \equiv (+4) \pmod{11} \Rightarrow$ ~~$3^{-1} = 10 \pmod{11} \Rightarrow$~~

$\Rightarrow 3^{-1} = 4$ în $\mathbb{Z}_{11}$