Tema 1 Criptografie

① a = 44557 b = 66559

Euclid + Bezout

$x_{44557} = (0,1)$; $x_{66559} = (1,0)$

$66559 = 44557 + 22002 \Rightarrow x_{22002} = (1,-1)$

$44557 = 22002 \cdot 2 + 553 \Rightarrow x_{553} = (-2,3)$

$22002 = 553 \cdot 39 + 435 \Rightarrow x_{435} = (79,-118)$

$553 = 435 + 118 \Rightarrow x_{118} = (-81,121)$

$435 = 118 \cdot 3 + 81 \Rightarrow x_{81} = (322,-481)$

$118 = 81 + 37 \Rightarrow x_{37} = (-403,602)$

$81 = 37 \cdot 2 + 7 \Rightarrow x_7 = (1128,-1685)$

$37 = 7 \cdot 5 + 2 \Rightarrow x_2 = (-6043,9027)$

$7 = 2 \cdot 3 + 1 \Rightarrow x_1 = (19257,-28766)$

$2 = 2 \cdot 1 + 0$

$\Rightarrow (66559, 44557) = 1 \Rightarrow$

$\Rightarrow \exists x, y \in \mathbb{Z}^*$ a.î. $66559 \cdot x + 44557 \cdot y = 1$

$\Rightarrow \begin{cases} x = 19257 \\ y = -28766 \end{cases}$

(2) $14 \cdot X \equiv 1 \pmod{53}$ $X = ?$

$(53, 14) = 1 \Rightarrow \exists\ 14^{-1} \mod 53$ ✱ de asemenea prim

$\boxed{x_{53} = (1, 0);\ x_{14} = (0, 1)}$

$53 = 14 \cdot 3 + 11 \Rightarrow x_{11} =$

$x_{11} = (1, -3)$.

$14 = 11 + 3 \Rightarrow x_3 = (-1, 4)$

$11 = 3 \cdot 3 + 2 \Rightarrow x_2 = (4, -15)$.

$3 = 2 + 1 \Rightarrow x_1 = (-5, 19) \Rightarrow$

$\Rightarrow 1 = -5 \cdot 53 + 19 \cdot 14 \Rightarrow$

$\Rightarrow$ ~~$\mod$~~ $19 \cdot 14 \equiv 1 \pmod{53}$

$\Rightarrow 14^{-1} \equiv x \equiv 19 \pmod{53}$

(3) Pt. complexitate avem a, b și știm că pb. poate fi recursivă.

'Operația de bază: '%' - modulo, operație simplă.; (a și b - date de intrare)

p.p. $c \equiv a \pmod{b}$; $(a, b) \Rightarrow (b, c)$;

Și prin op. modulo succesive și interschimb. $\Rightarrow$ se micșorează foarte repede nr. de cif $\Rightarrow$

$\Rightarrow O(\log(n))$