Tema 2 criptografie

E. 13) a) $1011_{(2)} = ?_{(10)}$

$1011_{(2)} = 8 + 2 + 1 = 11_{(10)}$

b) 2B din 16 în 10

$2B_{(16)} = 16 \cdot 2 + 11 = 32 + 11 = 43_{(10)}$

c) 343 din 5 în baza 4.

$343_{(5)} = 25 \cdot 3 + 4 \cdot 5 + 3 = 75 + 23 = 98_{(10)}$

$98_{(10)} = 4^3 + 2 \cdot 4^2 + 0 \cdot 4^1 + 2 \cdot 5^0 \Rightarrow$

$\Rightarrow 98_{(10)} = 343_{(5)} = 1202_{(4)}$

d) $16_{(8)} - 5_{(8)} = 11_{(8)}$

II 13) $43^{107} \equiv x \pmod{109}$

$x = ?$

109 - prim

$\varphi(n) = 109 - 1 = 108$ (nr. prim) $\Rightarrow$

$\Rightarrow 43^{108} \equiv 1 \pmod{109} \Leftrightarrow$

$\Leftrightarrow 43^{107} \equiv 1 \cdot 43^{-1} \pmod{109}$

$\Rightarrow$ Rezolvăm: $43 \cdot y \equiv 1 \bmod 109$

$y = ?$

$109 = 2 \cdot 43 + 23$

$43 = 1 \cdot 23 + 20$

$23 = 20 + 3$

$20 = 6 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$1 = 3 - 1 \cdot 2 \Leftrightarrow 1 = 3 \cdot 7 - 1 \cdot 20 \Leftrightarrow 1 = 7 \cdot (23 - 1 \cdot 20) - 20$

$\Rightarrow 1 = 7 \cdot 23 - 8 \cdot 20$

$1 = 7 \cdot 23 - 8(43 - 23) = 15 \cdot 23 - 8 \cdot 43$

$1 = 15(109 - 2 \cdot 43) - 8 \cdot 43 \Leftrightarrow$

$\Leftrightarrow 15 \cdot 109 - 38 \cdot 43 = 1 \Rightarrow 43^{-1} \equiv -38 \equiv 71 \Rightarrow$

$\Rightarrow 43^{107} \equiv 71 \bmod 109$