Criptografie-Tema2

guzurazvan

March 2024

I. 24. Schimbări de baze
Baza 16: 0,1,2,3,4,5,6,7,8,9,A (10),B (11) ,C (12),D (13), E(14), F(15)

a) Convertiți numărul 11100 din baza 2 în baza 10.
b) Convertiți numărul 3D din baza 16 în baza 10.
c) Convertiți numărul 231 din baza 6 în baza 4.
d) Scădeți numerele 32 și 17 în baza 8.

a)$11100_2 = (1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0)_{10} = (16 + 8 + 4 + 0 + 0)_{10} = 28_{10}$

b)$3D_{16} = (3 \cdot 16^1 + 13 \cdot 16^0)_{10} = (48 + 13)_{10} = 61_{10}$

c)$231_6 = (2 \cdot 6^2 + 3 \cdot 6^1 + 1 \cdot 6^0)_{10} = (72 + 18 + 1)_{10} = 91_{10}$
$91_{10} = 22 \cdot 4 + 3$
$22 = 5 \cdot 4 + 2$
$5 = 1 \cdot 4 + 1$
$1 = 0 \cdot 4 + 1$
$\Rightarrow 91_{10} = 1123_4$

d)$32_8 = (3 \cdot 8^1 + 2 \cdot 8^0)_{10} = (24 + 2)_{10} = 26_{10}$
$17_8 = (1 \cdot 8^1 + 7 \cdot 8^0))_{10} = 15_{10}$
$26_{10} - 15_{10} = 11_{10}$
$11_{10} = (1 \cdot 8^1 + 3 \cdot 8^0)_{10} = 13_8$
Deci $32_8 - 17_8 = 13_8$

II. 24. Calculează $(97^{167}) mod 173$

$(97^{167}) mod 173$
$\equiv (97^{(1+83 \cdot 2)}) mod 173$
$\equiv (97 \cdot (97^2)^{83}) mod 173$
$\equiv (97 \cdot 9409^{83}) mod 173$

$\equiv (97 \cdot 9409^{(1+41\cdot 2)}) mod 173$
$\equiv (97 \cdot 9409 \cdot (9409^2)^{41}) mod 173$
$\equiv (97 \cdot 145 \cdot (145^2)^{41}) mod 173$
$\equiv (14065 \cdot 21025^{41}) mod 173$
$\equiv (52 \cdot 92^{(1+20\cdot 2)}) mod 173$
$\equiv (52 \cdot 92 \cdot (92^2)^{20}) mod 173$
$\equiv (4784 \cdot 8464^{20}) mod 173$
$\equiv (113 \cdot 160^{10\cdot 2} mod 173$
$\equiv (113 \cdot 25600^{10}) mod 173$
$\equiv (113 \cdot 169^{5\cdot 2}) mod 173$
$\equiv (113 \cdot 28561^5) mod 173$
$\equiv (113 \cdot 16^{(1+2\cdot 2)}) mod 173$
$\equiv (113 \cdot 16 \cdot (16^2)^2) mod 173$
$\equiv (1808 \cdot 256^2) mod 173$
$\equiv (78 \cdot 83^2) mod 173$
$\equiv (78 \cdot 6889) mod 173$
$\equiv (78 \cdot 142) mod 173$
$\equiv (11076) mod 173$
$\equiv (4) mod 173$
$= 4$