28.04.2025

g este generator a lui $\mathbb{Z}_p^*$ dacă:

$$g^{p-1} \equiv 1 \bmod p$$

$$g^{(p-1)/q} \not\equiv 1 \bmod p$$

q factori primi ai lui $p-1$

2. $p = 17 \quad g = 5 \quad Z_{17}$

$a = 3 \quad k = 6$

$u = 5^3 \pmod{17} = 25 \cdot 5 \pmod{17} = 8 \cdot 5 \pmod{17} = 40 \pmod{17}$

$= 6$

$v = 5^6 \pmod{17} = 25^3 \pmod{17} = 8^3 \pmod{17} = 64 \cdot 8 \pmod{17}$

$= 13 \cdot 8 \pmod{17} = 104 \pmod{17} = 2 \pmod{17}$

$u = 6 \quad v = 2$

$K = 2^3 \pmod{17} = 8 \pmod{17}$

$K = 6^6 \pmod{17} = 36^3 \pmod{17} = 2^3 \pmod{17} = 8 \pmod{17}$

3 (37, 3, 19)

$m = X = 23$

$k = 3$

mesaj criptat

$p = 13 \quad g = 3 \quad a = 19 \quad k = 3$

$u = 3^3 \pmod{13} = 9 \cdot 3 \pmod{13} = 27 \pmod{13} = 1$

$v = 23 \cdot 19^3 \pmod{13} = 10 \cdot 19^3 \pmod{13} =$

$= 10 \cdot 36 \cdot 6 \pmod{13} = 10 \cdot 10 \cdot 6 \pmod{13}$

$= 100 \cdot 6 \pmod{13} = 9 \cdot 6 \pmod{13} = 54 \pmod{13} = 2$

$p = 13 \quad g = 3 \quad a = 19 \quad k = 3$

$u = 3^3 \pmod{31} = 27 \pmod{31}$

$v = 23 \cdot 19^3 \pmod{31} = 23 \cdot 361 \cdot 19 \pmod{31}$

$= 23 \cdot 20 \cdot 19 \pmod{31} = 460 \cdot 19 \pmod{31} = 26 \cdot 19 \pmod{31}$

$= 494 \pmod{31} = 29 \pmod{31}$

Răspuns (27, 29)

4. (53, 2, 3, 1)

criptat (24, 37)

Decriptați

$p = 53 \quad g = 2 \quad \alpha = 30$

$\mu = 24 \quad V = 37$

$\alpha = g^{\mu} \pmod p \Rightarrow 30 = 2^{\mu} \pmod{53}$

$2^{52} \equiv 1 \pmod{53}$

$g = [\sqrt{p}] = 7$

$\sqrt{53} \mid 7$

$49 \quad \overline{}$

$= 4$

$2^{8m+x} = 30 \pmod{53}$

$(2^8)^m \cdot 2^x = 30 \pmod{53}$

$(128)^m \cdot 2^x = 30 \pmod{53}$

$22^m \cdot 2^x = 30 \pmod{53} \Rightarrow$

$\Rightarrow 22^m = 30 \cdot 2^{-x} \pmod{53}$

$\Rightarrow 22^i = 30 \cdot 2^j \pmod{53}$

$x = 13 \qquad 30 = 2^{13} \pmod{53}$

$W = 24^{-13} \pmod{53}$

$24 = (0,1) \qquad 53 = (1,0)$

$53 = 24 \cdot 2 + 5$

$24 = 5 \cdot 4 + 4$

$5 = 4 \cdot 1 + 1$

~~$1 = 5 - 4 = 5 - 24 - 5 \cdot 4 =$~~

$1 = 5 - 4$

$4 = 24 - 5 \cdot 4$

$5 = 53 - 24 \cdot 2$

$(1,0) - (0,1) \cdot 2 = (1,-2)$

$(0,1) - (1,-2) \cdot 4 = (0,1) - (4,-8) =$

$= (-4,9)$

$(1,-2) - (-4,9) = (5,-11)$

$m \equiv v \cdot u^{-a} \bmod p$

$u^{-a} \bmod p \Rightarrow -a = -13$

Teorema lui Fermat $u^{-1} \equiv u^{p-2} \bmod p$

$u^{-13} \equiv u^{53-1-13} \equiv u^{39} \bmod 53$

$24^{39} \bmod 53$

$24^{39} \equiv 24^{32} \cdot 24^{4} \cdot 24^{2} \cdot 24^{1} \equiv 28 \cdot 49 \cdot 46 \cdot 24 \bmod 53$

$28 \cdot 49 = 1372 \equiv 47 \bmod 53$

$47 \cdot 46 = 2162 \equiv 42 \bmod 53$

$42 \cdot 24 = 1008 \equiv 18 \bmod 53$

$u^{-a} \equiv 24^{33} \equiv 1 \mod 53$

$m = v \cdot u^{-a} \mod p = 37 \cdot 1 \mod 53 = 37 \mod 53$

5 (30, 7)

$(p=43, g=3)$

$a = 30 \quad v = 7$

$\alpha = g^a \pmod{43}$

$\alpha = ?$

$\alpha = 3^a \pmod{43}$

Nu se poate rezolva

6. $p = 71 \quad g = 33 \quad a = 34$

a)

$\alpha = g^a \mod p$

$\alpha = 33^{34} \mod 71$

$33^2 = 24 \mod 71$

$33^4 \equiv 24^2 \equiv 8 \mod 71$

$33^8 \equiv 8^2 \equiv 64 \mod 71$

$33^{16} \equiv 64^2 \equiv 49 \mod 71$

$33^{32} \equiv 49^2 \equiv 58 \mod 71$

$33^{34} \equiv 58 \cdot 24 \equiv 43 \mod 71$

Cheia publică (71, 33, 43)

b) $k = 6$ criptati AZI

$A = 0 \quad Z = 25 \quad I = 8$

$u = y^k \bmod p$

$u = 33^3 \bmod 71$

$33^2 \equiv 24 \bmod 71$

$33^3 \cdot 24 \equiv 792 \equiv 11 \bmod 71$

$x^k \bmod p \quad \Rightarrow 43^3 \bmod 71 \equiv 43^2 \cdot 43 \equiv 3 \cdot 43 \equiv 129$

$\equiv 58 \bmod 71$

$v = m \cdot \alpha^k \bmod p$

$m = 0 \Rightarrow v = 0 \cdot 58 \equiv 0 \bmod 71$

$m = 25 \Rightarrow v = 25 \cdot 58 \equiv 1450 \equiv 30 \bmod 71$

$m = 8 \Rightarrow v = 8 \cdot 58 \equiv 464 \equiv 38 \bmod 71$

(11, 0) pentru A

(11, 30) pentru Z

(11, 38) pentru I