Temă

2) $K_e(n=28829, e)$, $m=11111$

$s=?$

$n=p\cdot q$

$\sqrt{28829}$ | 1

1 | $26\cdot 6=156$

188 | $329\cdot 9=2961$

156

$=3229$

$[\sqrt{n}]=169$

$170^2-28829=28900-28829=00071$

$171^2-28829=412$

$172^2-28829=755$

$173^2-28829=1100$

$174^2-28829=1447$

$175^2-28829=\dots$

$176^2-28829=2147$

$177^2-28829=2500=50^2$

$n=177^2-50^2=\underbrace{127}_{p}\cdot\underbrace{227}_{q}$

$\varphi(n)=(p-1)(q-1)=126\cdot 226=28476$

$(3,28476)\neq 1$

$(5,28476)=1 \Rightarrow e=5$

$m=\underbrace{11111}$

$d \cdot e \equiv 1 \pmod{\varphi(m)}$

$5d \equiv 1 \pmod{28476}$

$X_{28476} = (1,0), \quad X_5 = (0,1)$

$28476 = 5 \cdot 5695 + 1 \Rightarrow X_1 = (1,0) - 5695(0,1) = (1, -5695)$

$1 = 28476 + (-5695) \cdot 5 \Rightarrow 5^{-1} = 5695$ in $\mathbb{Z}_{28476} \Rightarrow$

$\Rightarrow d = -5695 = 22781$

$s \equiv 11111^{22781} \pmod{28829} = 7003$

3)

$p = 1223$

$q = 1987$

$\varphi(n) = (p-1)(q-1) = 1222 \cdot 1986 = 2.426.892$

$e = 948047$

$d \cdot e = 1 \pmod{\varphi(n)}$

$X_{2426892} = (1,0)$

$X_{948047} = (0,1)$

$2426892 = 948047 \cdot 2 + 530798,$

$X_{530798} = (1,-2)$

$948047 = 530798 \cdot 1 + 417249$

$X_{417249} = (0,1) - (1,-2) = (-1,3)$

$X_{530798} = 417249 \cdot 1 + 113549$

$X_{113549} = (1,-2) - (-1,3) = (2,-5)$

$417249 = 113549 \cdot 3 + 76602$

$X_{76602} = (-1,3) - 3(2,-5) = (-7,18)$

$113549 = 76602 \cdot 1 + 36947$

$X_{36947} = (2,-5) - (-7,18) = (9,-23)$

$76602 = 36947 \cdot 2 + 2708$

$X_{2708} = (-9,18) - 2(9,-23) = (-25,64)$

$36947 = 2708 \cdot 13 + 1743$

$X_{1743} = (9,-23) - 13(-25,64) = (334,-855)$

$2708 = 1743 \cdot 1 + 965$

$X_{965} = (-25,64) - (334,-855) = (-359, 919)$

$1743 = 965 \cdot 1 + 778$

$X_{778} = (334,-855) - (-359, 919) = (693, -1774)$

$965 = 778 \cdot 1 + 187$

$x_{187} = (-359, 919) - (693, -1774) = (-1052, 2693)$

$778 = 187 \cdot 4 + 30$

$x_{30} = (693, -1774) - 4(-1052, 2693) = (4901, -12546)$

$187 = 30 \cdot 6 + 7$

$x_7 = (-1052, 2693) - 6(4901, -12546) = (-30.458, 77969)$

$30 = 7 \cdot 4 + 2$

$x_2 = (4901, -12546) - 4(-30458, 77969)$

$= (126733, -324422)$

$7 = 2 \cdot 3 + 1$

$x_1 = (-30458, 77969) - 3(126733, -324422)$

$= (-410657, 1051235)$

$d = 1051235$

$s = 1070777^{1051235} \pmod{2430101} = 153337$