$p = 7 \quad q = 11 \quad n = p \cdot q = 77$

$\varphi(n) = 6 \cdot 10 = 60$

menší dělitel $e = 13 \qquad (e, \varphi(n)) = 1$

inverze e mod $\varphi(n)$?

$60 = 4 \cdot 13 + 8 \qquad 13 = 8 + 5 \qquad 8 = 5 + 3 \qquad 5 = 3 + 2$

$3 = 2 + 1 \qquad 1 = 3 - 2 = 3 - 1(5 - 3) = 2 \cdot 3 - 5$

$= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 = 2 \cdot 8 - 3(13 - 8)$

$= 5 \cdot 8 - 3 \cdot 13 = 5 \cdot (60 - 4 \cdot 13) - 3 \cdot 13$

$= -23 \cdot 13 + 5 \cdot 60 \Rightarrow e^{-1} = 37 = d$

šifra $M \to C = M^e \bmod n \qquad C^d = M^{e \cdot d} = M \bmod n$

bře 26-13:59

$M = 5$

$C = 5^{13} \bmod 77 = 26$

26^{37}

bře 26-14:30

Rabin: $p = 7, \; q = 11 \quad n = 77$

$M = 5 \qquad M^2 = 25 \bmod 77$

hledáme $x^2 \equiv 25 \bmod 77$:

$x = -37 \cdot 5 \pm 2 \cdot 11 \cdot (-2) = -185 \pm 44 = -229 \; (16) \; (5)$

$(7) \; x = 25^2 \bmod 7 = +4$ $\qquad (8) \; x = 25^3 \bmod 11 = 5 \bmod 11$

$11 = 7 + 4 \qquad 7 = 4 + 3 \qquad 4 = 3 + 1 \qquad 1 = 4 - 3 =$

$= 4 - (7 - 4) = 2 \cdot 4 - 7 = 2 \cdot (11 - 7) - 7 = 2 \cdot 11 - 3 \cdot 7$

bře 26-14:39

n řád prvku a mod n:

nejmenší r $a^r = 1 \bmod n$

řád prvku je nesoudělné $(a, n) = 1$

$a, a^2, \ldots, a^r$

primitivní kořeny: $a, \ldots, a^n$ jsou všechna nesoudělná s n

$\Rightarrow$ řád a je $\varphi(n)$

pro p prvočíslo je $g, g^2, \ldots, g^{p-1}$ jsou právě všechna nenulová mod p.

bře 26-14:59

Alice $h = g^x \qquad (p, g, h)$ veřejný klíč

Bob: $M \mapsto C_1 = g^y$

$C_2 = M \cdot h^y = M \cdot g^{y \cdot x}$

Alice $(C_1, C_2) = C_2 \cdot C_1^{-x} = M \cdot (g^y)^x \cdot (g^x)^{-y}$

$= M$

bře 26-15:14