$n = 2021 = 43 \cdot 47$

$e = 11$ — veřejné

d — tajné

Zpráva $c = 21$ — původní zpráva ... M

Zašifr.

$$c \equiv M^e \bmod n, \quad e \cdot d \equiv 1 \bmod \varphi(n)$$

$$\varphi(2021) = \varphi(43 \cdot 47) = (43-1)\cdot(47-1) = 1932$$

a	b	a·11 + b·1932
0	1	1932
1	0	11
−175	1	7
176	−1	4
−351	2	3
[527]	−3	1

$$19\,\overline{11}\,\overline{2} : 11 = 175$$
$$83$$
$$62$$
$$\boxed{7}$$

$$527 \cdot 11 \equiv 1 \bmod \varphi(2021)$$

d

$$c^d \equiv (M^e)^d \equiv M^{e \cdot d} \equiv M^{11 \cdot 527} \equiv M^{k \cdot \varphi(2021) + 1} \equiv M \cdot M^{k \cdot \varphi(2021)} \equiv M \cdot 1 \equiv M$$

$$c^d = 21^{527} \bmod 2021$$

$$21^{527} \bmod 43 \qquad 21^{527} \bmod 47$$

$527 \equiv 23 \bmod 42$

$527 = 12 \cdot 42 + 23$

$$21^{527} \equiv 21^{23} \equiv 21 \cdot 21^{22} \equiv 21 \cdot (21^2)^{11} \bmod 43$$
$$\equiv 21 \cdot 441^{11} \equiv 21 \cdot 11^{11}$$
$$\equiv 21 \cdot 11 \cdot 11^{10} \equiv 21 \cdot 11 \cdot 121^5$$
$$\equiv 231 \cdot 121^5 \equiv 16 \cdot 35^5$$
$$\equiv 16 \cdot (-8)^5 \equiv 16 \cdot (-8) \cdot (-8)^4$$
$$\equiv 16 \cdot (-8) \cdot 64^2 \equiv 16 \cdot (-8) \cdot 21^2$$
$$\equiv 16 \cdot \underbrace{(-8) \cdot 11}_{-88 \equiv -2} \equiv 11 \bmod 43$$

$21^{527} \equiv 21^{11\cdot 46+21} \equiv 21^{21} \mod 47$

$\equiv 21 \cdot 21^{20} \equiv 21 \cdot 441^{10} \equiv 21 \cdot 18^{10}$

$\equiv 21 \cdot 324^5 \equiv 21 \cdot 42^5 \equiv 21 \cdot (-5)^5$ $\quad 324 = 6\cdot 47 + 42$

$\equiv 21 \cdot (-5) \cdot 25^2 \equiv -105 \cdot 625 \equiv -11 \cdot 14 \equiv -154 \equiv -13 \mod 47$

$\left(\equiv 21^{21} \equiv (3\cdot 7)^{21} \equiv 3^{21} \cdot 7^{21} \right)$

$21^{527} \equiv k \cdot 43 + 11 \equiv -13 \mod 47$

$-4k \equiv -24 \mod 47 \quad / \cdot 4^{-1} \mod 47$

$-k \equiv -6$

$k \equiv 6$

$21^{527} = 43 \cdot 8 + 11 = 43 \cdot (47k+6) + 11$

$= 2021k + 269 \equiv$

M

Př. šifra ElGamal

$p = 997$, $g = 11$ společné

prim. kořen

x ... mocnina – soukromé Alice

$x = 23$

$g^x = 11^{23} \equiv 659 \mod 997$

y ... mocnina – soukromé Boba

$(gy, g^{x\cdot y} \cdot M)$ posílá Bob Alici

$g^{x\cdot y} = (g^y)^x$ → najde inverzi d mod p

$d \cdot (g^{x\cdot y} \cdot M) \equiv M \mod p$

Dohodli: $p = 997$, $g = 11 \mod p$

Alice si zvolila $x = 23$, poslala $g^x \equiv 11^{23} \equiv 659 \mod 997$

Bob si zvolil $y = 25$ (neznámé Alice), poslal Alici $g^y \equiv 11^{25} \equiv 976 \mod 997$ + správě $c = M \cdot (g^x)^y \equiv 20 \mod 997$

Alice dešifruje z $C \to M$.

$$(g^y)^x = 976^{23} \equiv 950 \mod 997$$

a	b	$a \cdot 950 + b \cdot 997$
0	1	997
1	0	950
−1	1	47
21	−20	10
−85	87	7
106	−101	3
−297	283	1

$950 : 47 = 20$
10

$$(-297) \cdot C \equiv (-297) \cdot (M \cdot g^{xy}) \equiv (-297) \cdot 20 \equiv \underbrace{42}_{M} \mod 997$$

Př.

$p = 41$, $g = 11$

Alice zvolila $x = 10$, poslala g^x mod 41 ← nepotřebuji k dešifr. (potřeboval to Bob k zašifr.)

Bob poslal Alici $g^y = 22$, $c = 6 = M \cdot g^{xy}$ (už počítáno mod 41).

Dešifrujte.

$g^{xy} = 22^{10} \equiv 2^{10} \cdot 11^{10} \mod 41$

$= (2^5)^2 \cdot (11^2)^5 \equiv (-9)^2 \cdot (-2)^5 \equiv 81 \cdot (-32)$

$\equiv 32$; $11^2 \equiv 121 \equiv 9$

$\equiv (-1) \cdot 9 \equiv -9 \equiv 32$

a	b	$a \cdot 41 + b \cdot 32$
1	0	41
0	1	32
1	-1	9
-3	4	5
4	-5	4
-7	9	1

$9 \cdot 32 \equiv 1 \mod 41$, tedy $(g^{xy})^{-1} \equiv 9 \mod 41$

$M \equiv c \cdot 9 \equiv 6 \cdot 9 \equiv 54 \equiv 13 \mod 41$

$$\begin{pmatrix} 3 & 5 & 6 & 7 \\ -2 & 1 & 0 & 5 \end{pmatrix} \cdot \begin{pmatrix} 2 & 8 \\ -1 & -5 \\ 9 & 11 \end{pmatrix} \times$$

$2 \times 4 \qquad 3 \times 2$

$$\begin{pmatrix} 2 & 8 \\ -1 & -5 \\ 9 & 11 \end{pmatrix} \cdot \begin{pmatrix} 3 & 5 & 6 & 7 \\ -2 & 1 & 0 & 5 \end{pmatrix} = \begin{pmatrix} 2\cdot 5 + 8\cdot(-2) & & & \\ & & & \\ & & & \end{pmatrix}$$

$3 \times 2 \qquad 2 \times 4$

$$= \begin{pmatrix} -10 & 18 & 12 & 54 \\ 7 & -10 & -6 & -32 \\ 5 & 54 & 54 & 118 \end{pmatrix}_{3 \times 4}$$

$$\begin{pmatrix} 1 & 0 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 2 \end{pmatrix} = 4$$

$$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 2 & 1 \\ 2 & 0 & 4 & 2 \end{pmatrix}$$

$4 \times 1 \qquad 1 \times 4$

4×4

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

Násobení matic není komutativní, záleží na pořadí

$$x_1 + 2x_2 + 4x_3 = -2$$
$$x_1 + x_2 - x_3 = 4$$
$$x_1 + x_2 + x_3 = 0$$

$$\left(\begin{array}{ccc|c} x_1 & x_2 & x_3 & \\ 1 & 2 & 4 & -2 \\ 1 & 1 & -1 & 4 \\ 1 & 1 & 1 & 0 \end{array}\right) \sim \text{nadále} \left(\begin{array}{ccc|c} 1 & 2 & 4 & -2 \\ 0 & -1 & -5 & 6 \\ 0 & -1 & -3 & 2 \end{array}\right) \cdot(-1) \cdot(-1) \sim \left(\begin{array}{ccc|c} 1 & 2 & 4 & -2 \\ 0 & 1 & 5 & -6 \\ 0 & 0 & 2 & -4 \end{array}\right)$$

$2x_3 = -4$

$x_3 = -2$

$x_2 + 5x_3 = -6$

$x_2 = -6 - 5 \cdot (-2) = 4$

$x_1 = -2 - 2 \cdot x_2 - 4 \cdot x_3$

$= -2 - 2 \cdot 4 - 4 \cdot (-2)$

$= -2$

$(x_1, x_2, x_3) = (-2, 4, -2)$

Zkouška:

$$\begin{pmatrix} 1 & 2 & 4 \\ 1 & 1 & -1 \\ 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} -2 \\ 4 \\ -2 \end{pmatrix} = \begin{pmatrix} -2 \\ 4 \\ 0 \end{pmatrix}$$