$\left(\frac{219}{383}\right) = 1$ ⟹ 383 prvočíslo

$x^2 \equiv 219 \quad (383)$

má řešení

VĚTA $p \equiv 3 \ (4)$; $(a/p) = 1$

$\sqrt{a} \equiv \pm a^{\frac{p+1}{4}}$

$219^{191} \pmod{383}$

$x^2 \equiv 219$

$x^2 \equiv 219^{191} \cdot 219 \equiv 219^{192} \quad / \sqrt{}$

$x \equiv \pm 219^{96}$

lépe: $x^2 - (219^{96})^2 \equiv 0$

$(x - 219^{96})(x + 219^{96}) \equiv 0 \quad (383)$

$1 \cdot 219^{96} \equiv 1 \cdot (219^2)^{48} \equiv 1 \cdot 86^{48} \equiv 1 \cdot (86^2)^{24}$

$\equiv 1 \cdot 119^{24} \equiv 1 \cdot (119^2)^{12} \equiv 1 \cdot 373^{12}$

$\equiv 1 \cdot (373^2)^6 \equiv 1 \cdot 100^6 \equiv 1 \cdot (100^2)^3$

$\equiv 1 \cdot 42^3 \equiv 1 \cdot 42 \cdot (42^2)^1 \equiv 42 \cdot 232 \equiv \underline{\underline{169}}$

Př. $n = 561 = 3 \cdot 11 \cdot 17$

$(a, n) = 1 \Rightarrow$

$a^2 \equiv 1 \quad (3)$
$a^{10} \equiv 1 \quad (11)$
$a^{16} \equiv 1 \quad (17)$

$\Rightarrow$

$a^{80} \equiv 1 \quad (3)$
$a^{80} \equiv 1 \quad (11)$
$a^{80} \equiv 1 \quad (17)$

$\Downarrow$

$a^{80} \equiv 1 \quad (561)$

$\Downarrow$

$a^{560} \equiv 1 \quad (561)$

Př. $p = 35 \qquad a \equiv 2$

$2^{34} \equiv \ldots \equiv 9 \not\equiv 1 \quad (35) \Rightarrow$ 35 není prvočíslo

Př. $2^{560} \equiv 1 \quad (561) \qquad 2^{280} \equiv 1$

$5^{560} \equiv 1 \qquad 5^{280} \equiv 67 \not\equiv \pm 1$

Pr. $p = 1729 \qquad a \equiv 11$

$11^{864} \equiv 1 \not\equiv \left(\frac{11}{1729}\right)$:

$\left(\frac{11}{1729}\right) = \pm 1 \left(\frac{1729}{11}\right) = \left(\frac{2}{11}\right) = -1$

$11 \equiv 3 \ (4)$ $\qquad$ $11 \equiv 3 \ (8)$

$1729 \equiv 1 \ (4)$

$2^{60} = \left(\left(\left(2^2\right)^2\right)^3\right)^5$

$a_1 z_1 \cdot a_2 z_2$

$a_1 a_2 \qquad z_1 z_2$

$(a_1 + z_1)(a_2 + z_2) - a_1 a_2 - z_1 z_2$

1	0	a
0	1	m
⋮		⋮
k	l	d
		0

$a \cdot b^c \longrightarrow (a \cdot b) \cdot (b^2)^{\lfloor c/2 \rfloor} \qquad c \equiv 1 \ (2)$

$\longrightarrow a \cdot (b^2)^{c/2} \qquad c \equiv 0 \ (2)$

$72x + 100y = 16$

má řešení vzhl. k x

$\Leftrightarrow \quad 72x = \underbrace{16 - 100y}_{\text{je dél. } 72}$ ... vzít rovnici modulo 72

$72x + 100y \equiv 16 \quad / \bmod 72$

$72y \equiv 0$

$28y \equiv 16 \quad (72)$

$16y \equiv -32$

$12y \equiv 48$

$4y \equiv -80 \equiv -8 \quad (72) \Leftrightarrow \underline{y \equiv -2 \quad (18)}$

$0y \equiv 72 \equiv 0$ V

$y = 18t - 2$ dosadíme do pův. rovnice

$72x + 100(18t - 2) = 16$

$72x + 100(18t - 2) = 16$

$72x + 1800t - 200 = 16$

$72x = -1800t + 216 \qquad / : 72$

$x = -25t + 3$

Řešení jsou právě $(x, y) = (-25t+3, 18t-2)$
$= t \cdot (-25, 18) + (3, -2)$

$72x + 100y = 1 - 45z$

kdy existují x, y? právě když RHS je děl. $(72, 100) = 4$

$72x + 100y \equiv 1 - 45z \pmod 4$

$0 \equiv 1 - z \pmod 4$ tj. $z \equiv 1 \pmod 4$

$z = 4t+1$ dosadíme

$72x + 100y + 45(4t+1) = 1$

$72x + 100y = -180t - 44$ $\exists x \Leftrightarrow$ delitel $\neq 72$

$72x + 100y \equiv -180t - 44$ (72)

$72y \equiv 0$

$28y \equiv -36t + 28$

$16y \equiv 16$

$12y \equiv -36t + 12$

$4y \equiv 36t + 4$ (72) $\Leftrightarrow$ $y \equiv 9t+1$ (18)

$0y \equiv -144t \equiv 0$ ✓

$y = 18s + 9t + 1$

$72x + 100(18s + 9t + 1) + 45(4t+1) = 1$

$72x + 1800s + 1080t + 145 = 1$

$72x = -1800s - 1080t - 144$ / :72

$x = -25s - 15t - 2$

Vereque $n = p \cdot q$
$e \pmod{\varphi(n)}$ invertibile

Sonkrone $p, q \rightsquigarrow \varphi(n) = (p-1)(q-1)$
$d \pmod{\varphi(n)}$
↳ inverse k e ; tj. $d \cdot e \equiv 1 \ (\varphi(n))$

$M \pmod n \xrightarrow{\text{sifrovalni}} M^e \pmod n$

" $C^{1/e}$ " $\pmod n \xleftarrow{\text{desifrovalni}} C \pmod n$
1/e chcene modulo $\varphi(n)$. tj.
1/e je inverze k e modulo $\varphi(n)$
tj. $1/e = d$

$C^d \pmod n$

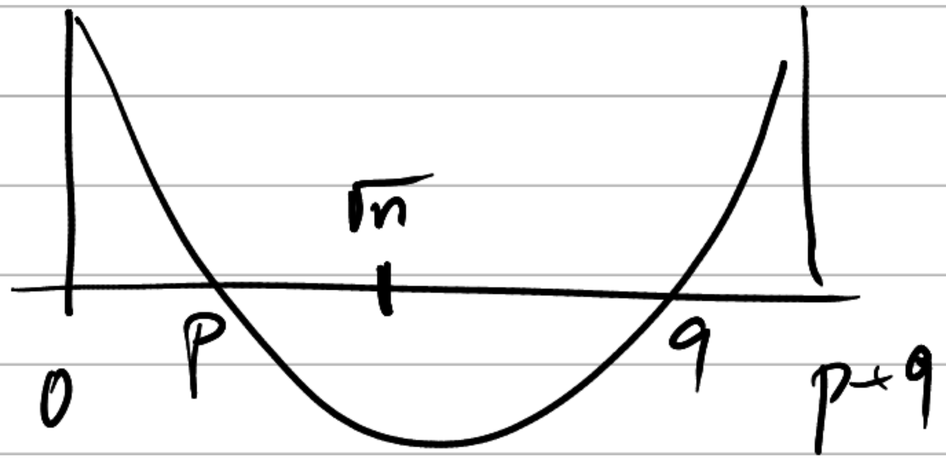
Pozn. Kolik informace má $\varphi(n) = (p-1)(q-1)$?

$$\varphi(n) = p \cdot q - p - q + 1 = n - (p+q) + 1$$

znát $\varphi(n)$ $\equiv$ znát $p+q$

$$(x-p)(x-q) = x^2 - x(p+q) + p \cdot q$$

známe



půlením intervalu lze hodnoty p, q najít

$n = p \cdot q = 33$; $e = 7$

Prelonte 29, 7, 21.

$\varphi(n) = (3-1)(11-1) = 20$

$20 \cdot d \equiv 0$

$\Rightarrow \quad 7 \cdot d \equiv 1 \quad (20)$

$6 \cdot d \equiv -2$

$d \equiv 3 \quad (20)$

Desifrordm: $29^3 \equiv (-4)^3 \equiv -64 \equiv 2$

$7^3 \equiv 7 \cdot 16 \equiv 13$

$21^3 \equiv 21$? $(21, 33) = 1$

$p=23$, $q=29$ Demonstrace RSA pro $e=487$

$n = p \cdot q = 667$

$M \equiv 25 \quad (667)$

Zašifrování: $C \equiv M^e \equiv 25^{487} \quad (667)$

zjednodušení: počítáme mod 23, 29 zvlášť

$C \equiv 25^{487} \quad (23)$

$\equiv 2^3 \equiv 8$

$C \equiv 25^{487} \quad (29)$

$\equiv (-4)^{11} \equiv -5$

$C \equiv 8 \quad (23)$

$C \equiv -5 \quad (29)$ ←

$C = 23t + 8 = 23(29s + 7) + 8$

$= 667s + 169$

$23t + 8 \equiv -5 \quad (29)$

$29t \equiv 0$

$23t \equiv -13$

$6t \equiv 13$

$5t \equiv -52 \equiv 6$

$t \equiv 7 \quad (29)$

Desifrovdm: $M \equiv 169^d$

$$
\begin{aligned}
616 \cdot d &\equiv 0 \\
487 \cdot d &\equiv 1 \pmod{616} \\
129 \cdot d &\equiv -1 \\
100 \cdot d &\equiv 4 \\
29 \cdot d &\equiv -5 \\
13 \cdot d &\equiv 19 \\
3 \cdot d &\equiv -43 \\
d &\equiv 191 \pmod{616}
\end{aligned}
$$

$M \equiv 169^{191} \quad (23)$

$\equiv 8^{-7} \equiv (8^{-1})^7 \equiv 3^7 \equiv 2 \quad (23)$

$8 \cdot 3 \equiv 1 \quad (23)$

$M \equiv 169^{191} \quad (29)$

$\equiv (-5)^{-5} \equiv ((-5)^{-1})^5 \equiv (-6)^5 \equiv -4 \quad (29)$

$\Big\} \; M \equiv 25 \; (667)$