$$ggT(47,35)$$

$$47 - 35 = 12$$

$$(0\cdot 47 + 1\cdot 35) - 2\cdot(1\cdot 47 + (-1)\,35)$$

$$35 - 2\cdot 12 = 11$$

$$12 - 11$$

	a	b	$a\cdot 47 + b\cdot 35$
1x	1	0	47
-1x	0	1	35
1x	1	-1	12
-2x	-2	3	11
1x	3	-4	1
-1x			

Př.

$2^{97^{99}} \mod 26 \quad (2,26)=2$

$26 = 2 \cdot 13$

$2^{97^{99}} \equiv 0 \mod 2 \rightarrow$ zb. po dělení 26 musí být sudý

$2^{97^{99}} \equiv 2^{13k+1} \equiv 2^1 \equiv 2 \mod 13 \quad 13k+2$

$\rightarrow 2$ ~~15~~ lichý

$2^{13-1} = 2^{12} \equiv 1 \mod 13$

$2^{12k+r} = (2^{12})^k \cdot 2^r$

$\equiv 1$

$97^{99} \equiv 1^{99} \equiv 1 \mod 12$

$97 = 8 \cdot 12 + 1$

Posl. dvojic: $3^{97^{99}}$

$3^{97^{99}} \equiv$

$97^{99} \equiv 17^{99} \mod 40 \ldots$

$17 \cdot 17^{98} \equiv 17 \cdot (17^2)^{49}$

Zkusíme jednodušeji

$100 = 4 \cdot 25$

$3^{97^{99}} \equiv (-1)^{97^{99}} \equiv (-1)^{\text{liché}} \equiv -1 \mod 4$

$3^{97^{99}} \mod 25$

$97^{99} \equiv (-3)^{99} \mod 20$

$(-3)^0 \equiv 1 \pmod{20}$

$97^{99} = (-3)^3 = -27 \equiv 13 \mod 20$

$\varphi(100) = 40$

$3^{97^{99}} = [25k+23 \equiv -1 \mod 4$

$k \equiv -24 \equiv 0 \mod 4$

$3^{97^{99}} = 25(4\ell) + 23$

$= 100\ell + 23 = 100\ell + 23$

$\varphi(25) = \varphi(5^2) = (5-1) \cdot 5 = 20$

$\varphi(20) = \varphi(2^2 \cdot 5) = 1 \cdot 2 \cdot 4 = 8$

$99 \equiv 3 \mod 8$

$3^{97^{99}} = 3^{13} \equiv 3 \cdot 3^{12} \equiv 3 \cdot 9^6$

$\equiv 3 \cdot 81^3 \equiv 3 \cdot 6^3 \mod 25$

$\equiv 3 \cdot 6 \cdot 36$

$\equiv 3 \cdot 66 \equiv -2 \equiv 23 \mod 25$

$k \mid \varphi(m)$

$a^k \equiv 1 \mod n$ $k = \varphi(m)$ je nejmenší $\Rightarrow a$ je prim. kořen

12	
2	6
3	4

Př. Najděte pr. k. modulo 26.

$26 = 2 \cdot 13$

$\varphi(26) = (2-1)\cdot(13-1) = 12 = 4 \cdot 3 = 2^2 \cdot 3$

$2 \cdot 3 = 6$

$2^2 = 4$

$a^6 \not\equiv 1$

$a^4 \not\equiv 1$

$\varphi(\varphi(26)) = \varphi(12) = \varphi(2^2 \cdot 3) = 2 \cdot 2 = 4$

$(7^2)^6 = 7^{12}$

$(2-1)\cdot 2^1 \cdot (3-1)\cdot 3^0$

pr. k. 7 pro $n = p^k$, p liché

$= 2 \cdot p^k$

$= 2, 4$

$26: 3, 5, (7), 9, 11, 15, 17, 19, 21$

$3^6 \equiv 9^3 \equiv 9 \cdot 81 \mod 26$

$\equiv 9 \cdot 3 \equiv 27 \equiv 1 \mod 26$

$5^6 \equiv 25^3 \equiv (-1)^3 \equiv -1 \mod 26$

$5^4 \equiv 25^2 \equiv (-1)^2 \equiv 1 \mod 4$

$7^6 \equiv 49^3 \equiv (-3)^3 \equiv -27 \equiv -1 \mod 26$

$7^4 \equiv 49^2 \equiv (-3)^2 \equiv 9 \mod 26$

RSA veřejný klíč je $n = 95 = 5 \cdot 19$ přijali jsme č. $42 =: z$

$e = 55$

zprávu M zašifrujeme na $M^e \bmod n$

$M = 23$

$M^{e \cdot f} = M$ hledáme f t.ž. $e \cdot f \equiv 1 \mod \varphi(95)$

$\varphi(95) = \varphi(5 \cdot 19) = 4 \cdot 18 = 72$

4 4+19
4, (23), 42, 61, 80
x ✓ x x x
0-95

Hledáme inverzi k $e = 55 \mod 72$ $(55, 72) = 1$

$a \cdot 55 + b \cdot 72 = 1$

a	b	$a \cdot 55 + b \cdot 72$
0	1	72
1	0	55
-1	1	17
4	-3	4
-17	13	1

1x, -3x, -4x, 1x

$55 - 3 \cdot 17 = 4$

$17 - 4 \cdot 4 = 1$

$-17 \cdot 55 + 13 \cdot 72 = 1$

$55 \cdot 55 \equiv -17 \cdot 55 \equiv 1 \mod 72$

Inverze k $e = 55$ je 55

$z^{55} = (M^{55}) \equiv M^{55 \cdot 55} \equiv M$

$42^{55} \bmod 95 = 5 \cdot 19$

$42^{55} \equiv 2^{55} \equiv 2 \cdot 4^{27} \equiv 2 \cdot (-1)^{27}$

$\equiv -2 \equiv 3 \mod 5$

$42^{55} \equiv 4^{55} \equiv 4^{18 \cdot 3 + 1} \equiv 4^1 \equiv 4 \mod 19$

$(4^{19-1})^3 \equiv 1^3 \equiv 1$ m. F. v.