

zpráva M
 $C = M^e \pmod n$

největší dělitel:
 m ($m = p \cdot q$)
 e ($(e, \varphi(m)) = 1$)
 d ($e \cdot d \equiv 1 \pmod{\varphi(m)}$)
 $M \cdot e \cdot d$

$C^d = (M^e)^d = M$

Věta: r v dělení a a m :
 $a^t \equiv a^s \pmod m \Leftrightarrow t \equiv s \pmod r$

bře 19-14:07

největší dělitel: $(7, 33)$ $p=7$
 e $m=3 \cdot 11$ $q=11$

zpráva: $29, 7, 21 \leftarrow C$
 jakéto šifra a nějaké zpráva
 Ukládá d : $7d \equiv 1 \pmod{\varphi(33)}$
 $\Rightarrow \underline{d=3}$ $\varphi(33) = 20$

$29^3 \equiv (-4)^3 \equiv -64 \equiv 2$ $252 : 33 =$
 $7^3 \equiv 7 \cdot 16 \equiv 13$
 $21^3 \equiv 21 \cdot 12 \equiv 21$

bře 19-15:02

$A: (p, g, h)$ $h = g^x$
 $M \mapsto C_2 = M \cdot h^a = M \cdot g^{x \cdot a}$ $C_1 = g^a$ $\left. \vphantom{C_2} \right\} \pmod p$
 $C_2 \cdot C_1^{-x} = M \cdot g^{x \cdot a} \cdot (g^a)^{-x}$
 $= M \cdot g^{x \cdot a - x \cdot a} = M$

bře 19-15:24