$a^{\varphi(m)} \equiv 1 \pmod m$

$a^r \equiv 1$ r nejm. = řád a

primitivní kořen g +.ř.

každé a, $(a,m)=1$ je tvaru

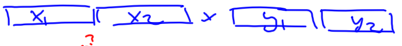
$a \equiv g^{x_a} \pmod m$

x_a ... diskrétní logaritmus

počítání odmocnin

mod $p = 4k+3$:

$X \equiv y^2$ známe y, chceme y



$10^1\, x_1 y_1 + 10^2\, x_2 y_1 = (x_1+x_2)(y_1+y_2) - x_1y_1 - x_2y_2$

4 4-14:01

$460 \cdot 103^{17} = \underbrace{460 \cdot 103}_{\text{result}} \cdot \underbrace{(103^2)^8}_{\text{base}^{\text{exp}}}$

$256 \cdot 103^1 = \underbrace{256 \cdot 103}_{\text{result}} \cdot \underbrace{(103^2)^0}_{1}$

$C^d = (M^e)^d = M^{de} \equiv M^1 \pmod n$

$de \equiv 1 \pmod{\varphi(n)}$

4 4-14:25

$C \equiv M^2 \pmod n$ $n = p \cdot q$

$C \equiv M^2 \pmod p$ resp. q

$\left(C^{(p+1)/4}\right)^2 = C^{(p+1)/2} = M^{p+1}$

$= M^2 \cdot \underbrace{M^{p-1}}_{\equiv 1} \equiv M^2 = C \pmod p$

$\Rightarrow C^{(p+1)/4}$ je druhá odmocnina z C

$\rightsquigarrow$ jsou dvě .... $\pm C^{(p+1)/4}$

$M \equiv \pm C^{(p+1)/4} \pmod p$

$M \equiv \pm C^{(q+1)/4} \pmod q$

$X + Y = 2$ zaps $(X+Y, n) = p$ "2 zaps $p \cdot q$"

4 4-14:41

$M \equiv 327 \pmod{23 \cdot 31}$ $= 713$

$C = M^2 = 327^2 \equiv 692 \pmod{713}$

$M \equiv \pm C^6 = \pm 692^6 \equiv \pm 5 \pmod{23}$

$M \equiv \pm C^8 = \pm 692^8 \equiv \pm 14 \pmod{31}$

$+5, -14 \Rightarrow M \equiv 327 \pmod{713}$

$g^{ab} = \underbrace{(g^b)^a}_{\text{veřejné}} = (g^a)^b$ tlice

4 4-14:54

veřejné: $(p, g, h \equiv g^x)$ prim. kořen

soukromé: x

M zpráva

$C \begin{cases} C_1 = g^y \\ C_2 = M \cdot h^y = M \cdot (g^x)^y = M \cdot g^{xy} \end{cases}$

dešifrování: $M = M \cdot g^{xy} / (g^y)^x = C_2 / C_1^x$

4 4-15:09

Rozpoznání primitivní kořenů mod m: jak poznat, jestliže řád g je $\varphi(m)$?

Věta: g je prim. kořen $\Leftrightarrow$ nesplňuje $g^{\varphi(m)/q_i} \equiv 1 \pmod m$ q_i jsou prvočíselní dělitelé $\varphi(m)$

Dk. Pokud $g^{\varphi(m)/q_i} \equiv 1$, pak řád g je max. $\varphi(m)/q_i \Rightarrow$ g není prim. kořen.

Naopak pokud g není prim. kořen, pak řád g je $r \mid \varphi(m)$ ale $r \neq \varphi(m) \Rightarrow r \mid \frac{\varphi(m)}{q_i}$

$\Rightarrow x^{\varphi(m)/q_i} = (x^r)^{\cdots} \equiv 1^{\cdots} = 1$. □

4 4-15:18