MB141 – 12. cvičení
Šifrování

Martin Čadek

Jarní semestr 2020

(A)

Příklad 1. Šifrou RSA s veřejným klíčem $n = 95$ a $e = 55$ bylo posláno číslo $Z = 42$. Šifru prolomte a určete zaslanou zprávu $M \in \{1, 2, \ldots, 94\}$.

Prolomit tuto šifru je jednoduché. Protože je n malé a dělitelné evidentně 5, je

$$n = 95 = 5 \cdot 19$$

$e = 55$ je šifrovací exponent. Máme-li šifrovat M mod 95, zašifrujeme ji tak, že spočítáme $M^e = M^{55}$ mod 95. K dešifrování musíme najít dešifrovací exponent d. K němu potřebujeme znát hodnotu Eulerovy funkce φ na čísle n. Tu bychom ovšem rozkladu na prvočísla, obecně nepočítali. Máme-li rozklad $n = p \cdot q$, platí

$$\varphi(n) = (p-1)(q-1), \quad \varphi(95) = 4 \cdot 18 = 72.$$

Dešifrovací exponent d je inverze k $e = 55$ modulo $\varphi(n) = 72$.

B

Příklad 1. Šifrou RSA s veřejným klíčem $n = 95$ a $e = 55$ bylo posláno číslo $Z = 42$. Šifru prolomte a určete zaslanou zprávu $M \in \{1, 2, \ldots, 94\}$.

Pozor! Zde se často dělá chyba, když se inverze počítá modulo $n = 95$. Inverzi najdeme Mě na pomocí Bezoutovy rovnosti:

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

Tedy $d \equiv -17 \equiv 55 \mod 72$.

Nyní zpátky dešifrujeme tak, že počítáme

$$Z^d \equiv (M^e)^d = M^{ed} = M^{\varphi(n) \cdot k + 1}$$
$$= \left(M^{\varphi(n)}\right)^k \cdot M \equiv 1^k \cdot M \equiv M \mod 95$$

My počítáme $Z^d = 42^{55}$ nejdříve mod 5 a pak mod 19.

Počítáme modulo 5

$$(42)^{55} \equiv 2^{55} \equiv \left(2^4\right)^{13} \cdot 2^3 \equiv 1^{13} \cdot 8 \equiv 3 \mod 5$$

Použili jsme malou Fermatovu větu $2^{5-1} \equiv 1 \mod 5$. Zde to lze i bez ní. Víme $2^4 = 16 \equiv 1 \mod 5$.

Příklad 1. Šifrou RSA s veřejným klíčem $n = 95$ a $e = 55$ bylo posláno číslo $Z = 42$. Šifru prolomte a určete zaslanou zprávu $M \in \{1, 2, \ldots, 94\}$.

(c)

Počítání modulo 19

$(42)^{55} \equiv 4^{55} \equiv 2^{110} = (2^{18})^6 \cdot 2^2 \equiv 1 \cdot 4 \equiv 4 \mod 19$

Teď už bylo použití malé Fermatovy věty

$2^{19-1} \equiv 1 \mod 19$ podstatné!

Víme tedy, že $M = 19k + 4$ a dále, že

$M = 19k + 4 \equiv 3 \mod 5$

$4k + 4 \equiv 3 \mod 5$

$4k \equiv -1 \mod 5$

$4k \equiv 4 \mod 5$

$k \equiv 1 \mod 5$

Proto $M \equiv 19k + 4 = 19(5l + 1) + 4 = 95l + 23$

Tedy zaslaná zpráva je $M = 23$.

(A)

Příklad 2. Šifrou RSA s veřejným klíčem $n = 115$ a $e = 15$ bylo posláno číslo $Z = 47$. Šifru prolomte a určete zaslanou zprávu $M \in \{1, 2, \ldots, 114\}$.

Postupujeme stejně jako v předchozím příkladu

$$n = 115 = 5 \cdot 23$$

$$\varphi(n) = 4 \cdot 22 = 88$$

Najdeme inverzi k $e = 15$ modulo 88

15	88	$d \cdot 15 + c\,88$
0	1	88
1	0	15
-5	1	13
6	-1	2
47	-8	1

$47 \cdot 15 - 8 \cdot 88 = 1$

$47 \cdot 15 \equiv 1 \mod 88$

$d = 47$

Musíme spočítat

$47^{47} \mod 115.$

Počítáme modulo 5

$$(47)^{47} \equiv 2^{47} \equiv (2^4)^{11} \cdot 2^3 \equiv 1 \cdot 8 \equiv 3 \mod 5$$

(B)

Příklad 2. Šifrou RSA s veřejným klíčem $n = 115$ a $e = 15$ bylo posláno číslo $Z = 47$. Šifru prolomte a určete zaslanou zprávu $M \in \{1, 2, \ldots, 114\}$.

Počítání mod 23 je jednoduché $47^{47} \equiv 1^{47} \equiv 1 \bmod 23$.

Tedy $M = 23k + 1 \equiv 3 \bmod 5$

$3k + 1 \equiv 3 \bmod 5$

$3k \equiv 2 \bmod 5$

$-2k \equiv 2 \bmod 5$

$-k \equiv 1 \bmod 5$

$k \equiv 4 \bmod 5$

Pak $M \equiv (23k+1) = 23(5k+4) + 1 = 115k + 93$.

Zaslaná zpráva je $\underline{\underline{M = 93}}$.

Příklad 3. Alice a Bob komunikují šifrou Elgamal. Oba se dohodli na prvočísle $p = 41$ a na primitivním kořenu $g = 11$. Alice si za svůj tajný klíč zvolila číslo 10. Jaký údaj poskytla Bobovi? Bob jí posléze poslal zprávu (22, 6). Pomozte Alici s dešifrováním zprávy.

(A)

Ač se to po nás nechce, předpokládáme se, že $g = 11$ je skutečně primitivní kořen modulo 41. To znamená, že nejmenší přirozené číslo n takové, že $g^n \equiv 1 \bmod 41$ je $n = \varphi(41) = 40$.

Protože $40 = 2^3 \cdot 5$ musí být n s vlastností $g^n \equiv 1 \bmod 41$ dělitelem čísla 40. Aby tedy g byl primitivní kořen, musí být $g^8 \not\equiv 1 \bmod 41$ a $g^{20} \not\equiv 1 \bmod 41$.

Počítáme mod 41

$11^8 \equiv (11^2)^4 \equiv (121)^4 \equiv (-2)^4 \equiv 16 \bmod 41$

$11^{20} \equiv ((11^2)^5)^2 \equiv (-2)^{10} \equiv 1024 \equiv -1 \bmod 41$

Tedy $g = 11$ je skutečně primitivní kořen mod 41.

Příklad 3. Alice a Bob komunikují šifrou Elgamal. Oba se dohodli na prvočísle $p = 41$ a na primitivním kořenu $g = 11$. Alice si za svůj tajný klíč zvolila číslo 10. Jaký údaj poskytla Bobovi? Bob jí posléze poslal zprávu (22, 6). Pomozte Alici s dešifrováním zprávy.

(B)

Alice poskytne Bobovi hodnotu $g^{10} = 11^{10} \bmod 41$, což je

$11^{10} \equiv (11^2)^5 \equiv (121)^5 \equiv (-2)^5 \equiv -32 \equiv 9 \bmod 41.$

Bob má zprávu M a Alici pošle dvojici čísel $(g^b,\ M \cdot g^b) \equiv (11^b,\ M(11^{10})^b) \equiv (22, 6)$, kde b je Bobův tajný klíč. K dešifrování zprávy Alici její tajný klíč 10. Provede to takto:

(1) Prvně umocní první číslo ve dvojici, tj. 22 na svůj tajný klíč 10 a najde inverzi k $22^{10} \bmod 41$.

$22^{10} = (22^2)^5 \equiv (-8)^5 \equiv (-8) \cdot 64 \cdot 64 \equiv (-8)\,23 \cdot 23 \equiv -20 \cdot 23 \equiv -9 \equiv 32 \bmod 41$

484

Příklad 3. Alice a Bob komunikují šifrou Elgamal. Oba se dohodli na prvočísle $p = 41$ a na primitivním kořenu $g = 11$. Alice si za svůj tajný klíč zvolila číslo 10. Jaký údaj poskytla Bobovi? Bob jí posléze poslal zprávu $(22, 6)$. Pomozte Alici s dešifrováním zprávy.

(C)

Najdeme inverzi k 32 mod 41

32	41	$d\,32 + c\,41$
0	1	41
1	0	32
-1	1	9
4	-3	5
9	-7	1

$9 \cdot 32 - 7 \cdot 41 = 1$

$9 \cdot 32 \equiv 1 \bmod 41$

$d = 9$

(Šlo rychleji uhodnout výpočtem inverze k $-9 \equiv 32$, neboť $-9 \cdot 9 \equiv -81 \equiv 1 \bmod 41$)

(2) Samotnou zprávu M dokončíme pak takto

$$M \equiv \underbrace{M \cdot (11^{10})^b}_{6} \cdot \{(11^b)^{10}\}^{-1}$$

$$\equiv 6 \cdot 9 \equiv 13 \bmod 41$$

(A)

Příklad 4. V Rabinově kryptosystému je soukromým klíčem dvojice prvočísel $p = 23$ a $q = 31$. Veřejným klíčem je součin $n = pq = 713$. Zašifrujte zprávu $M = 327$ a ukažte, jak se bude dešifrovat.

Šifrování v Rabinově kryptosystému spočívá v tom, že spočítáme $M^2 \bmod n$. To lze udělat bez znalosti prvočísel p a q. V praxi na to existuje speciální software, pro malá n to zkusíme na kalkulačce:

$327^2 = 106\,929 \equiv 106\,929 - 149 \cdot 713 \equiv 692 \mod 713.$

Se znalostí $p = 23$, $q = 31$ to lze spočítat bez kalkulačky: nejprve spočteme $M^2 \bmod 23$ a pak $\bmod 31$.

$C = 327^2 \equiv 5^2 \equiv 2 \mod 23$

$C = 327^2 \equiv 17^2 \equiv 10 \mod 31$

Z těchto dvou kongruencí spočítáme $C \bmod 713$ - viz minulé cvičení.

$C = 31x + 10 \equiv 2 \mod 23$

$8x + 10 \equiv 2 \mod 23$

(B)

Příklad 4. V Rabinově kryptosystému je soukromým klíčem dvojice prvočísel $p = 23$ a $q = 31$. Veřejným klíčem je součin $n = pq = 713$. Zašifrujte zprávu $M = 327$ a ukažte, jak se bude dešifrovat.

$$8x \equiv -8 \mod 23$$

$$x \equiv -1 \equiv 22 \mod 23$$

Podle $x = 23y + 22$ a $C \equiv 31(23y+22) + 10 = 713y + 692$

Dešifrování zprávy C - použijeme znalost obě prvočísla. Můžeme to udělat dvojím způsobem

I. Pomocí vzorečku: M je jedna z těchto 4 zpráv

$$\pm a p C^{\frac{q+1}{4}} \pm b q C^{\frac{p+1}{4}}$$

kde $C^{\frac{q+1}{4}}$ berem mod q a $C^{\frac{p+1}{4}}$ berem mod p.

a a, b jsou čísla z Bezoutovy věty

$$ap + bq = 1.$$

Najdeme nejprve tato čísla.

Příklad 4. V Rabinově kryptosystému je soukromým klíčem dvojice prvočísel $p = 23$ a $q = 31$. Veřejným klíčem je součin $n = pq = 713$. Zašifrujte zprávu $M = 327$ a ukažte, jak se bude dešifrovat.

(C)

23	31	$a23 + b31$
0	1	31
1	0	23
-1	1	8
-4	3	1

$a = -4,\ b = 3$

$(-4) \cdot 23 + 3 \cdot 31 = \underline{1}$

Počítáme mod 23

$C^{\frac{23+1}{4}} \equiv (692)^6 \equiv 2^6 \equiv 2^5 2 \equiv 9 \cdot 2 \equiv 18 \mod 23$

Počítáme mod 31

$C^{\frac{31+1}{4}} \equiv (692)^8 \equiv 10^8 \equiv 100^4 \equiv 7^4 \equiv 49 \cdot 49 \equiv 18 \cdot 18 \equiv$

$\equiv 36 \cdot 9 \equiv 5 \cdot 9 \equiv 14 \mod 31.$

Řešení je $\pm 4 \cdot 23 \cdot 14 \pm 3 \cdot 31 \cdot 18$, což dává

110, 327, 386, 603 mod 713. Zpráva 327 je mezi nimi.

(D)

Příklad 4. V Rabinově kryptosystému je soukromým klíčem dvojice prvočísel $p = 23$ a $q = 31$. Veřejným klíčem je součin $n = pq = 713$. Zašifrujte zprávu $M = 327$ a ukažte, jak se bude dešifrovat.

II. Odmocniny modulo p a q

Spočítáme $C^{\frac{p+1}{4}} \equiv 692^6 \equiv 18 \mod 23$

$C^{\frac{q+1}{4}} \equiv 692^8 \equiv 14 \mod 31$

Platí, že $(\pm 18)^2 \equiv 2 \equiv 692 \mod 23$

$(\pm 14)^2 \equiv 14 \equiv 692 \mod 31$

Tedy $M \equiv \pm 18 \mod 23$

$M \equiv \pm 14 \mod 31$

Z těchto 4 variant vyřešíme dvě:

$M \equiv 14 \mod 31$

znamená $M = 31k + 14$. Potom

(E)

Příklad 4. V Rabinově kryptosystému je soukromým klíčem dvojice prvočísel $p = 23$ a $q = 31$. Veřejným klíčem je součin $n = pq = 713$. Zašifrujte zprávu $M = 327$ a ukažte, jak se bude dešifrovat.

$M_1 = 31k + 14 \equiv 18 \mod 23$

$8k \equiv 4 \mod 23$

$2k \equiv 1 \mod 23$

$k \equiv 12 \mod 23$

$M_2 = 31k + 14 \equiv -18 \mod 23$

$8k \equiv -32 \mod 23$

$8k \equiv 14 \mod 23$

$4k \equiv 7 \mod 23$

$4k \equiv -16 \mod 23$

$k \equiv -4 \equiv 19 \mod 23$

Tedy $M_1 \equiv 31(23 \cdot l + 12) + 14 \equiv \underline{386}$ a $M_2 = 31(23l + 19) + 14 \equiv \underline{603}$.

Další řešení jsou

$M_3 \equiv -M_1 \equiv 713 - 386 = \underline{327}$ a $M_4 \equiv -603 \equiv 713 - 603 \equiv \underline{110}$

Je vidět, že výpočet čísel a, b takových, že

$a \cdot 23 + b \cdot 31 = 1$

jsme nahradili řešením soustav kongruencí.