

Úloha 53.

► Příklad 53.1

Nalezněte sedmé nejmenší nezáporné řešení soustavy:

$$\begin{aligned}x &\equiv 37 \pmod{61} \\x &\equiv 5 \pmod{47} \\x &\equiv 46 \pmod{79} \\x &\equiv 6 \pmod{43} \\x &\equiv 25 \pmod{41}\end{aligned}$$

Nalezené řešení uvažujte jako 10-ti místné a výsledek rozdělte na posloupnost dvouciferných čísel. Tato čísla označte po řadě c_0, \dots, c_4 . Např. jestliže je počet rovnic 5 a jejich řešení je $x = 1234567890$, potom $c_0 = 12, c_1 = 34, c_2 = 56, c_3 = 78, c_4 = 90$. Jestliže $x = 123$ (stále předpokládáme 5 rovnic), potom za x vezmeme číslo $x = 0000000123$ a dostáváme posloupnost $c_0 = 00, c_1 = 00, c_2 = 00, c_3 = 01, c_4 = 23$.

řešení příkladu 53.1 je posloupnost $c_0 = 25, c_1 = 08, c_2 = 29, c_3 = 19, c_4 = 16$

► Příklad 53.2

Pracujte v \mathbb{Z}_{32} a dešifrujte zprávu

$$(21, 22, 14, 12, 2)$$

víte-li, že byla použita Hillova šifra s šifrovacím klíčem

$$\begin{pmatrix} 8 & 21 & 11 & c_0 & 14 \\ 14 & 19 & 28 & 5 & c_1 \\ 17 & 15 & 0 & 11 & c_2 \\ 25 & c_3 & 11 & 28 & 8 \\ 17 & 29 & 9 & 3 & c_4 \end{pmatrix}$$

kde c_0, \dots, c_4 jsou hodnoty získané z předešlé úlohy. Dešifrovanou zprávu převeďte na text za použití kódování:

$$\begin{aligned}A &\mapsto 01 & B &\mapsto 02 & C &\mapsto 03 \\ & & & & & \vdots \\ \dots & & Z &\mapsto 26\end{aligned}$$

Dále dešifrujte zprávu

$$(6, 24, 2, 11, 0)$$

Zpráva byla zašifrována stejnou metodou jako v předchozím případě. Výslednou zprávu nepřevádějte na text, ale označte její hodnoty po řadě r_0, \dots, r_4 . Tyto hodnoty použijete v následující úloze.

řešení příkladu 53.2 Dešifrovaná zpráva je **ETAPA** a hledaná posloupnost je $r_0 = 0, r_1 = 5, r_2 = 0, r_3 = 5, r_4 = 0$

► Příklad 53.3

Dešifrujte zprávu

$$\begin{pmatrix} 4143148646262828351091090716359183203159934022287971566264547705572090 \\ 0893468602732856120727471662299298045689175048439703597116919364585887 \\ 0682410178818578163504171413995105445386 \end{pmatrix} \bullet$$

víte-li, že byla použita RSA šifra s šifrovacím klíčem

$$(n, e) = \begin{pmatrix} 6565835001783979853644r_07758845823838084049732106497r_1541907845929173 \\ 373765618971568961r_2202669467584402837347384755861694139555774661221184 \\ 26r_308386352423935718950552830330314627r_4449 \\ 5323657241119332067147429523202183508173089769338397616811892380813415 \\ 25316429760821870399 \end{pmatrix} \bullet$$

kde r_0, \dots, r_4 jsou hodnoty získané z předešlé úlohy. Dešifrovanou zprávu převeďte na text. Bylo použito ASCII kódování.

řešení příkladu 53.3 Dešifrovaná zpráva je **They rested from the sea.**

1. VÝPOČET SOUSTAVY ROVNIC:

$$x = 37 \pmod{61}$$

$$x = 5 \pmod{47}$$

$$x = 46 \pmod{79}$$

$$x = 6 \pmod{43}$$

$$x = 25 \pmod{41}$$

$$x = 37 \times (47 \times 79 \times 43 \times 41 \times x_1) + 5 \times (61 \times 79 \times 43 \times 41 \times x_2) + 46 \times (61 \times 47 \times 43 \times 41 \times x_3) + 6 \times (61 \times 47 \times 79 \times 41 \times x_4) + 25 \times (61 \times 47 \times 79 \times 43 \times x_5)$$

VÝPOČET x_1 :

$$x = 37 \times (47 \times 79 \times 43 \times 41 \times x_1) = 37 \pmod{61}$$

$$(47 \times 79 \times 43 \times 41) = 48 \pmod{61}$$

$$48 \times x_1 = 1 \pmod{61} - \text{hledání inverzního prvku k } 48 \pmod{61}:$$

Použijeme rozšířený Eukleidův algoritmus.

a	b	q	r	s	t
61	48	1	13	1	0
48	13	3	9	0	1
13	9	1	4	1	-1
9	4	2	1	-3	4
4	1	4	0	4	-5
1	0			-11	14

$$x_1 = 14$$

OBDOBNĚ SPOČÍTÁME OSTATNÍ X:

$$x_2 = 17$$

$$x_3 = 18$$

$$x_4 = 34$$

$$x_5 = 16$$

DOSADÍME DO ROVNICE:

$$x = 37 \times (47 \times 79 \times 43 \times 41 \times 14) + 5 \times (61 \times 79 \times 43 \times 41 \times 17) + 46 \times (61 \times 47 \times 43 \times 41 \times 18) + 6 \times (61 \times 47 \times 79 \times 41 \times 34) + 25 \times (61 \times 47 \times 79 \times 43 \times 16) \pmod{399307159}$$

$$x = 112\,448\,962 \pmod{399307159} - \text{nejmenší nezáporné řešení}$$

CHCEME SEDMÉ NEJMENŠÍ NEZÁPORNÉ ŘEŠENÍ :

$$x = 112\,448\,962 + 6 \times 399307159 = 2\,508\,291\,916$$

ROZDĚLENÍ DO POSLOUPNOSTI:

$$\mathbf{C0} = 25, \mathbf{C1} = 08, \mathbf{C2} = 29, \mathbf{C3} = 19, \mathbf{C4} = 16$$

2. DEŠIFROVÁNÍ ZPRÁVY V HILLOVĚ ŠIFŘE

$$(x_1, x_2, x_3, x_4) \begin{pmatrix} 8 & 21 & 11 & 25 & 14 \\ 14 & 19 & 28 & 5 & 8 \\ 17 & 15 & 0 & 11 & 29 \\ 25 & 19 & 11 & 28 & 8 \\ 17 & 29 & 9 & 3 & 16 \end{pmatrix} = (21, 22, 14, 12, 2)$$

$$(21, 22, 14, 12, 2) \begin{pmatrix} 8 & 21 & 11 & 25 & 14 \\ 14 & 19 & 28 & 5 & 8 \\ 17 & 15 & 0 & 11 & 29 \\ 25 & 19 & 11 & 28 & 8 \\ 17 & 29 & 9 & 3 & 16 \end{pmatrix}^{-1} = (x_1, x_2, x_3, x_4)$$

VÝPOČET INVERZNÍ MATICE:

$$a_{i,j} = \frac{(-1)^{i+j} \cdot |A_{j,i}|}{|A|}$$

Kde $|A_{j,i}|$ je determinant submatice z matice A po vynechání i tého řádku a j tého sloupce.

VÝPOČET DETERMINANTU A:

$$\begin{vmatrix} 8 & 21 & 11 & 25 & 14 \\ 14 & 19 & 28 & 5 & 8 \\ 17 & 15 & 0 & 11 & 29 \\ 25 & 19 & 11 & 28 & 8 \\ 17 & 29 & 9 & 3 & 16 \end{vmatrix} \bmod 32 = 1$$

VÝPOČET PRVNÍHO SUBDETERMINANTU:

$$\begin{vmatrix} 8 & 21 & 19 & 11 \\ 15 & 28 & 3 & 9 \\ 25 & 11 & 29 & 17 \\ 14 & 19 & 5 & 16 \end{vmatrix} \bmod 32 = 11$$

STEJNÝ POSTUP POUŽIJEME PRO OSTATNÍ PRVKY. VÝSLEDNÁ INVERZNÍ MATICE:

$$\begin{pmatrix} 8 & 21 & 11 & 25 & 14 \\ 14 & 19 & 28 & 5 & 8 \\ 17 & 15 & 0 & 11 & 29 \\ 25 & 19 & 11 & 28 & 8 \\ 17 & 29 & 9 & 3 & 16 \end{pmatrix}^{-1} = \begin{pmatrix} 11 & 0 & 23 & 2 & 27 \\ 4 & 11 & 9 & 20 & 23 \\ 30 & 0 & 30 & 12 & 11 \\ 6 & 23 & 6 & 3 & 0 \\ 13 & 23 & 22 & 17 & 27 \end{pmatrix}$$

DEŠIFROVÁNÍ ZPRÁVY:

$$(21,22,14,12,2) \begin{pmatrix} 11 & 0 & 23 & 2 & 27 \\ 4 & 11 & 9 & 20 & 23 \\ 30 & 0 & 30 & 12 & 11 \\ 6 & 23 & 6 & 3 & 0 \\ 13 & 23 & 22 & 17 & 27 \end{pmatrix} = (5, 20, 1, 16, 1)$$

PŘEVEDENÍ DO ABECEDY:

(E, T, A, P, A)

Dešifrování 2. zprávy:

$$(6, 24, 2, 11, 0) \begin{pmatrix} 11 & 0 & 23 & 2 & 27 \\ 4 & 11 & 9 & 20 & 23 \\ 30 & 0 & 30 & 12 & 11 \\ 6 & 23 & 6 & 3 & 0 \\ 13 & 23 & 22 & 17 & 27 \end{pmatrix} = (0, 5, 0, 5, 0)$$

ROZDĚLENÍ DO POSLOUPNOSTI:

$$r_0 = 0, r_1 = 5, r_2 = 0, r_3 = 5, r_4 = 0$$

3. DEŠIFROVÁNÍ ŠIFRY V RSA

Pro rozdělení na prvočísla použijeme Fermatův faktorizační algoritmus:

$$t = \sqrt{n} \\ = 810298401934989617170799633991024857222234720756678162015160644507524111262642655346177855$$

$$t^2 - n = 15511415976630791263625471470345854146130576$$

$$\sqrt{t^2 - n} \times \sqrt{t^2 - n} = 15511415976630791263625471470345854146130576$$

$$\sqrt{t^2 - n} - \text{je odmocnitelná dvěma}$$

$$s = \sqrt{t^2 - n} = 3938453500630773127476$$

$$p = t + s \\ = 810298401934989617170799633991024857222234720756678162015160644507528049716143286119305331$$

$$q = t - s \\ = 810298401934989617170799633991024857222234720756678162015160644507520172809142024573050379$$

$$\varphi_{(n)} = (p - 1) \times (q - 1) =$$

$$= 6565835001783979853644077588458238380840497321064975541907845929173373765618971568961020 \\ 25074079040158394239505959348959345841330191779670908759833202950342141283003017992453914 \\ 740$$

$d = e^{-1}v \mathbb{Z}_{\varphi(n)}$ – použití Eukleidova rozšířeného algoritmu

d=131347547765037351427146295751319879385388030699672863111922256001440016983379865119906
61168285660266675020550870324906103166994381332242184493531113342339767842910281336930087
4159

$$zprava = sifra^d v \mathbb{Z}_n$$

Zprava=13017051057011382691584106548141849683980466215661583046245667042002432247543191758
79037435419234296093130944812397545991636428750395249547221636061658119825378428176241273
86094194

ŠIFROVÁNÍ DO ASCII:

84, 104, 101, 121, 32,

114, 101, 115, 116, 101, 100, 32,

102, 114, 111, 109, 32,

116, 104, 101, 32,

115, 101, 97, 46

PŘEVOD Z ASCII NA PÍSMENA:

THEY RESTED FROM THE SEA.

4. POUŽITÉ POMŮCKY PRO VÝPOČTY:

program Python

<http://www.wolframalpha.com/>,

handouts z přednášek Jířího Velebila <http://math.feld.cvut.cz/velebil/teaching/x01dml.html>

5. ODKAZ NA ZADÁNÍ:

ftp://math.feld.cvut.cz/pub/kalous/dml/ulohy/uloha_053.pdf