SEMESTRÁLNÍ PRÁCE – Y36DMA (DISKRÉTNÍ MATEMATIKA)

ANTONÍN DANĚK

ÚLOHA 287

Příklad 287.1

Zadání:
Nalezněte sedmé nejmenší nezáporné řešení soustavy. Nalezené řešení uvažujte jako 10-ti místné a výsledek rozdělte na posloupnost dvouciferných čísel. Tato čísla označte po řadě c0, …, c4.

x = 6 mod 41
x = 18 mod 67
x = 30 mod 73
x = 2 mod 38
x = 23 mod 61

Výsledek:

$\boldsymbol{c_0 = 29}$; $\boldsymbol{c_1 = 23}$; $\boldsymbol{c_2 = 22}$; $\boldsymbol{c_3 = 34}$; $\boldsymbol{c_4 = 18}$

Příklad 287.2

Zadání:

Dešifrujte zprávy (25, 3, 21, 7, 32) a (12, 10, 31, 9, 4), zašifrované pomocí Hillovi šifry s šifrujícím klíčem:

7	24	8	16	$c0$
$c1$	33	11	1	5
0	$c2$	17	15	12
25	14	13	23	$c3$
$c4$	36	6	30	3

Výsledek:

Zpráva (25, 3, 21, 7, 32) odpovídá po dešifrování a převodu na text slovu **LINKA**.
Zpráva (12, 10, 31, 9, 4) odpovídá po dešifrování: $\boldsymbol{r_0 = 5}$; $\boldsymbol{r_1 = 1}$; $\boldsymbol{r_2 = 2}$; $\boldsymbol{r_3 = 5}$; $\boldsymbol{r_4 = 4}$

Příklad 287.3

Zadání:
Dešifrujte zprávu:
96923061265555641973274136629536150573356838227599326617943448058122216155761502103542216481235577553902277330864519562447664185147830674329136381341544455156198413653983781566645163297064507845653 81
Víte-li, že byla použita šifra RSA s šifrovacím klíčem:
n=
61510889178195000693240040550634831052014762070139779739014440097212501889069280486959199141653040883630284042235778260482423534446867452730784073465241348347326289203445417635826186563126236210841057
e=37259523259080051367973118079377448049623303409029681626912864131931939655902900476 69497196984345165

Výsledek:
Zpráva:14805649593499143660036814617397374594957438007270333665765488013776126935685461771855933283407069396121239606336383976129790350177451438823781772793667170824486609 48343
Po převedení na ASCII znaky: **were there. But I was sadly conscious that up to now I had never found**

Řešení příkladu 287.1:
Nejdříve je třeba ověřit, zda jsou moduly po dvou nesoudělné. Pomocí funkce GCD se dá zjistit, že toto platí.

```
def GCD(a,b):
    r=min(a,b)
    while ((a % b)!= 0):
        q=a/b
        r=a%b
        a=b
        b=r
    return r
```

Dále stačí řešit standardním způsobem, užitím čínské věty o zbytcích.

$m_1 = 41\ ;\ m_2 = 67;\ m_3 = 73;\ m_4 = 38;\ m_5 = 61; a_1 = 6;\ a_2 = 18;\ a_3 = 30;\ a_4 = 2;\ a_5 = 23;$

$M = m_1 * m_2 * m_3 * m_4 * m_5\ ;\ M = 41 * 67 * 73 * 38 * 61\ ;\ \boldsymbol{M = 464830858}$

$M_1 = m_2 * m_3 * m_4 * m_5\ ;\ M_1 = 67 * 73 * 38 * 61\ ;\ \boldsymbol{M_1 = 11337338}$

$M_2 = m_1 * m_3 * m_4 * m_5\ ;\ M_2 = 41 * 73 * 38 * 61\ ;\ \boldsymbol{M_2 = 6937774}$

$M_3 = m_1 * m_2 * m_4 * m_5\ ;\ M_3 = 41 *\ 67 * 38 * 61\ ;\ \boldsymbol{M_3 = 6367546}$

$M_4 = m_1 * m_2 * m_3 * m_5\ ;\ M_4 = 41 *\ 67 * 73 * 61\ ;\ \boldsymbol{M_4 = 12232391}$

$M_5 = m_1 * m_2 * m_3 * m_4\ ;\ M_5 = 41 * 67 * 73 * 38\ ;\ \boldsymbol{M_5 = 7620178}$

$t_i = M_i^{-1} mod\ m_i$

$t_1 = 11337338^{-1} mod\ 41\ ;\ \boldsymbol{t_1 = 16}$

$t_2 = 6937774^{-1} mod\ 67\ ;\ \boldsymbol{t_2 = 52}$

$t_3 = 6367546^{-1} mod\ 73\ ;\ \boldsymbol{t_3 = 35}$

$t_4 = 12232391^{-1} mod\ 38\ ;\ \boldsymbol{t_4 = 1}$

$t_5 = 7620178^{-1} mod\ 61\ ;\ \boldsymbol{t_5 = 20}$

$q_i = M_i * t_i$

$q_1 = 11337338 * 16\ ;\ \boldsymbol{q_1 = 181397408}$

$q_2 = 6937774\ * 52\ ;\ \boldsymbol{q_2 = 360764248}$

$q_3 = 6367546 * 35$; $\boldsymbol{q_3 = 222864110}$

$q_4 = 12232391 * 1$; $\boldsymbol{q_4 = 12232391}$

$q_5 = 7620178 * 20$; $\boldsymbol{q_5 = 152403560}$

$y = (a_1 * q_1 + a_2 * q_2 + a_3 * q_3 + a_4 * q_4 + a_5 * q_5)\ mod\ M$

$y = (6 * 181397408 + 18 * 360764248 + 30 * 222864110 + 2 * 12232391 + 23 * 152403560) mod\ M$

$y = 17797810874\ mod\ 464830858$; $\boldsymbol{y = 134238270}$

Hledám sedmé nejmenší nezáporné řešení soustavy, proto:
$x = y + 6 * M$; $x = 134238270 + 6 * 464830858$

$\boldsymbol{x = 2923223418}$

$\boldsymbol{c_0 = 29}$; $\boldsymbol{c_1 = 23}$; $\boldsymbol{c_2 = 22}$; $\boldsymbol{c_3 = 34}$; $\boldsymbol{c_4 = 18}$

Řešení příkladu 287.2:
Pro dešifrování zprávy (25, 3, 21, 7, 32), při práci Z_{37}, budeme potřebovat dešifrující klíč. **Šifrující klíč je**:

7	24	8	16	29
23	33	11	1	5
0	22	17	15	12
25	14	13	23	34
18	36	6	30	3

Dešifrující klíč získáme tak, že najdeme **inverzní matici** k matici šifrující. Inverzní matice se dá nalézt např. prostřednictvím přidružené jednotkové matice, pomocí Gaussovy eliminační metody. Úpravy musíme provádět modulo 37.

Dešifrující klíč je:

6	5	32	2	5
9	24	0	1	22
33	25	1	10	3
16	16	3	19	23
0	27	35	25	13

Nyní stačí zleva vynásobit zašifrovaný vektor dešifrujícím klíčem:

$$\left\{\begin{pmatrix} 6 & 5 & 32 & 2 & 5 \\ 9 & 24 & 0 & 1 & 22 \\ 33 & 25 & 1 & 10 & 3 \\ 16 & 16 & 3 & 19 & 23 \\ 0 & 27 & 35 & 25 & 13 \end{pmatrix} * \begin{pmatrix} 25 \\ 3 \\ 21 \\ 7 \\ 32 \end{pmatrix}\right\} mod\ 37 = \begin{pmatrix} 12 \\ 9 \\ 14 \\ 11 \\ 1 \end{pmatrix} = \begin{pmatrix} \boldsymbol{L} \\ \boldsymbol{I} \\ \boldsymbol{N} \\ \boldsymbol{K} \\ \boldsymbol{A} \end{pmatrix}$$

Pro dešifrování 2. Zprávy použijeme stejný dešifrující klíč:

$$\left\{\begin{pmatrix} 6 & 5 & 32 & 2 & 5 \\ 9 & 24 & 0 & 1 & 22 \\ 33 & 25 & 1 & 10 & 3 \\ 16 & 16 & 3 & 19 & 23 \\ 0 & 27 & 35 & 25 & 13 \end{pmatrix} * \begin{pmatrix} 12 \\ 10 \\ 31 \\ 9 \\ 4 \end{pmatrix}\right\} mod\ 37 = \begin{pmatrix} \boldsymbol{5} \\ \boldsymbol{1} \\ \boldsymbol{2} \\ \boldsymbol{5} \\ \boldsymbol{4} \end{pmatrix}$$

$\boldsymbol{r_0 = 5}$; $\boldsymbol{r_1 = 1}$; $\boldsymbol{r_2 = 2}$; $\boldsymbol{r_3 = 5}$; $\boldsymbol{r_4 = 4}$

Řešení příkladu 287.3:
Mám zprávu:
969230612655556419732741366295361505733568382275993266179434480581222161557615021035422216481235577553902277330864519562447664185147830674329136381341544455156198413653983781566645163297064507845653812 zašifrovanou pomocí RSA. Znám hodnoty **n**=
615108891781950006932400405506348310520147620701397797390144400972125018890692804869591991416530408836302840422357782604824235344468674527307840734652413483473262892034454176358261865631262362108410572 a
e=372595232590800513679731180793774480496233034090296816269128641319319396559029004766949719698434516 5

Pro dešifrování potřebuji dešifrovací klíč **(d,e)**. Číslo e již znám ze zadání. Číslo d se dá získat takto:

$\boldsymbol{d \equiv\ e^{-1}(\ mod\ \varphi(n)\ )}$**;** kde $\varphi(n)$ se spočítá $\varphi(n) = (p-1) * (q-1)$ **Je třeba vypočítat prvočísla p a q.**

Vím, že $n = p * q$ a číslo n znám.

Nyní potřebuji nalézt číslo, které bude po umocnění na 2 větší než n. (První větší, tzn. číslo o 1 menší bude po umocnění menší než n).

Pro odmocnění se dá použít Python skript:

```
def RSASQRT( n ) :
    l = 1
    h = n
    while h - l > 1 :
        c = (l + h) / 2
        if c * c < n :
            l = c
        else :
            h = c
    return h
```

***a**=RSASQRT(n) =*
7842887808594166081234794020563969745675480865610391475574764637484893238549322339318802378931642001

*Zjistíme, o kolik je druhá mocnina čísla **a** větší, než skutečné **n**.*

$b = \boldsymbol{a} * \boldsymbol{a} - \boldsymbol{n}$; *b =175587693261838885558253765687470317873378164429 44*

*Číslo **b** potřebujeme rozložit, abychom ho mohli odečíst / přičíst od čísla **a**.*

*Zkusíme číslo **b** odmocnit výše zmíněným skriptem.*

***c**= RSASQRT(b) = 4190318523237092599985288*

*Můžeme ověřit, že **b=c*c**; Nyní už tedy stačí dopočítat koeficienty **p** a **q**:*

$$p = a + c =$$

=784288780859416608123479402056396974567548086561039147557476463748489323855351265784203947153162728 9

$$q = a - c =$$

=784288780859416608123479402056396974567548086561039147557476463748489323854513202079556528633165671 3

Když mám prvočísla **p** a **q**, mohu vypočítat Eulerovu funkci:

$\varphi(n) = (p-1) * (q-1) =$
615108891781950006932400405506348310520147620701397797390144400972125018890692804869591991416530408679445084250474460980128354933189279613798223422444583971977970142336589405371815079255214783475570 56

Nyní mám všechny hodnoty, potřebné pro výpočet dešifrovacího klíče. Pro výpočet inverze pomůže následující funkce, využívající rozšířený Euklidův algoritmus.

```
def INV(a,b):
    s2=1
    s1=0
    r2=0
    r1=1
    while ((a % b)!= 0):
        q=a/b
        r=a%b
        a=b
        b=r
        s=s2-q*s1
        r=r2-q*r1
        s2=s1
        r2=r1
        s1=s
        r1=r
    return s1
```

$d \equiv e^{-1}(\ mod\ \varphi(n)\ ) =$
102873712717747839028355026213812771540293410908896700610712091752084350066089232064008458454547570569467165467223327455759732338893662767568830863921048386638494846361676882841347685074241326581384 37

Tím jsem získal klíč a nyní stačí zprávu dešifrovat pomocí modulárního umocňování.

$zprava = (sifra)^d \ (mod\ n)$

zprava =
*{*9692306126555564197327413662953615057335683822759932661794344805812221615576150210354
2216481235577553902277330864519562447664185147830674329136381341544455156198413653983
7815666451632970645078456538 1^**10287371271774783902835502621381277154029341090889670061071209175208435006608923206400845845454757056946716546722332745575973233889366276756883086392104838663849484636167688284134768507424132658138437**} mod
6151088917819500069324004055063483105201476207013977973901444009721250188906928048695
9199141653040883630284042235778260482423534446867452730784073465241348347326289203445
4176358261865631262362108410 57

Jelikož se jedná o příliš velká čísla, je třeba použít modulární umocňování. Python má takovou funkci již implementovanou, takže stačí zavolat **pow(zprava, d, n)**, čímž jsem získal otevřenou zprávu:
1480564959349914366003681461739737459495743800727033366576548801377612693568546177185593328340706939612123960633638397612979035017745143882378177279366717082448660948343

Zbývá převést kód zprávy na ASCII text. Pomůže procedura:

```
def NUMBERTOMESSAGE(message):
    while(message!=0):
        residue=message%256
        print( chr(residue) )
        message=message/256
```

Vyjde text: **were there. But I was sadly conscious that up to now I had never found**