

ЗАДАЧИ ПО КРИПТОГРАФИЯ

Йоана Левчева

Приложна математика, 4 курс, ф.н. 31492

30 май 2020 г.

Задача 1

Ще започнем, разбивайки по двойки букви открития текст и съответстващия му криптиотекст:

TH	EW	IN	TE	RO	FO	UR	DI	SC	ON	TE	NT
WG	NZ	DZ	WN	IS	OS	BH	GR	RE	AZ	WN	TW

Сега, ако разгледаме двойката $NT \rightarrow TW$, става ясно, че NTW се намират на един ред или на един стълб. От $TE \rightarrow WN$, тъй като NTW се намират на един ред или на един стълб, това означава, че $ENTW$ се намират на един ред или на един стълб. От $EW \rightarrow NZ$, тъй като ENW се намират на един ред или на един стълб, излиза, че $ENTWZ$ се намират на един ред или на един стълб. Нека приемем, че се намират на един ред и ги поставим в първия ред на таблицата ни 5×5 , представляваща ключа, за която сме приели, че J ще съвпада с I . В реда $ENTWZ$ се изпълняват условията на трите, разгледани досега двойки букви. Ключът придобива следния вид:

E	N	T	W	Z

От $FO \rightarrow OS$ следва, че FOS също са на един ред или на един стълб, а от $ON \rightarrow AZ$ следва, че те образуват правоъгълник $AOZN$, като A се намира под N и O се намира под Z . Тъй като Z се намира в края на реда, O е под него и FOS са на един ред (възможността да са на един стълб отпада заради правоъгълника $AOZN$), то излиза, че S трябва да се намира под E и F се намира под W . Нека попълним втория ред на таблицата, вземайки предвид тези заключения. Получаваме:

E	N	T	W	Z
S	A		F	O

Сега от $TH \rightarrow WG$ се образува правоъгълник TWHG и следователно H се намира под W и G се намира под T. Нека ги поставим на третия ред от таблицата. $IN \rightarrow DZ$ също образува правоъгълник IDNZ и следователно I се намира под Z и D се намира под N. От $DI \rightarrow GR$ следва, че DGIR се намират на един ред, откъдето следва, че на третия ред се намират RDGHI. За R остава да се намира под S. Ключът вече има следния вид:

E	N	T	W	Z
S	A		F	O
R	D	G	H	I

От $SC \rightarrow RE$, тъй като ESR следва, че и C се намира в същия първи стълб и понеже $C \rightarrow E$ то C се намира на последния ред. Остана да разгледаме само $UR \rightarrow BH$, при което се образува правоъгълника UBRH, тоест U се намира под H и B се намира под R. Понеже за B има единствена възможност да е на предпоследния ред, то и U излиза, че трябва да се намира на предпоследния ред. Използвайки открития текст и съответстващия му криптиртекст, успяхме да конструираме ключа до следния вид:

E	N	T	W	Z
S	A		F	O
R	D	G	H	I
B			U	
C				

Нека сега разгледаме криптиртекста, който трябва да дешифрираме и дешифрираме каквото можем, използвайки отчасти конструирания ключ:

EB	QX	ZL	HD	LK	IV	QG	OM	AL	EB	VB	DO	SG	SF
CR			GR						CR		IA		0-

ZR	AN	DA	MO	LB	SE	EL	SO	ZL	KD	CO	ZF	GS	IN
EI	N-	AN			EC		OF			-S	WO	R-	DZ

Може да предположим, че първата дума от криптиртекста е CRYPTOGRAPHY.

EB	QX	ZL	HD	LK	IV	QG	OM	AL	EB	VB	DO	SG	SF
CR	YP	TO	GR	AP	HY				CR		IA		0-

Забелязваме, че $ZL \rightarrow TO$, тоест се образува правоъгълник $ZTLO$ и мястото на L става известно. А от $IV \rightarrow HY$ от правоъгълника $IHVY$ имаме, че V е под H и Y е под I . Понеже U е точно под H следва, че V и Y се намират на последния ред. Получаваме за ключа:

E	N	T	W	Z
S	A	L	F	O
R	D	G	H	I
B			U	
C			V	Y

Използвайки последния вариант на ключа, се опитваме да дешифрираме още от криптитекста.

EB	QX	ZL	HD	LK	IV	QG	OM	AL	EB	VB	DO	SG	SF
CR	YP	TO	GR	AP	HY			SA	CR	UC	IA	LR	OL

ZR	AN	DA	MO	LB	SE	EL	SO	ZL	KD	CO	ZF	GS	IN
EI	N-	AN		S-	EC	TS	OF	TO		YS	WO	RL	DZ

От $QX \rightarrow YP$ имаме, че Q е на последния ред, а P и X на предпоследния, по-конкретно X е над Y . От $LK \rightarrow AP$ щом P е на предпоследния ред следва, че и K е на предпоследния ред, като K е под D и P е под X . Следователно Q е на последния ред под P . И остава M да е под K . Вече разполагаме с целия ключ:

E	N	T	W	Z
S	A	L	F	O
R	D	G	H	I
B	K	P	U	X
C	M	Q	V	Y

Разполагайки с ключа, можем да дешифрираме целия криптитекст:

EB	QX	ZL	HD	LK	IV	QG	OM	AL	EB	VB	DO	SG	SF
CR	YP	TO	GR	AP	HY	PL	AY	SA	CR	UC	IA	LR	OL

ZR	AN	DA	MO	LB	SE	EL	SO	ZL	KD	CO	ZF	GS	IN
EI	NM	AN	YA	SP	EC	TS	OF	TO	DA	YS	WO	RL	DZ

Z в края на изречението играе роля на допълваща буква до четен брой букви на изречението без да променя смисъла на думата. Окончателно криптитекстът се дешифрира като:

CRYPTOGRAPHY PLAYS A CRUCIAL ROLE IN MANY ASPECTS OF
TODAY'S WORLD

Задача 2

Първо ще отбележим, че $\mathbf{Z}_{26} \simeq \mathbf{Z}_2 \times \mathbf{Z}_{13}$. Нека разгледаме матрицата $K = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{Z}_{13}$. По условие $K = K^{-1}$. Следователно $KK^{-1} = KK = K^2 = I$. Това е еквивалентно на следната система:

$$\begin{aligned} a^2 + bc &= 1 \\ b(a + d) &= 0 \\ c(a + d) &= 0 \\ d^2 + bc &= 1 \end{aligned}$$

Ако $a + d \neq 0$ следва, че $b = 0$ и $c = 0$ и също $a^2 = 1$ и $d^2 = 1$. От тук получаваме две решения.

Сега, ако $a + d = 0$, имаме следните случаи:

- $a = 0$. Тогава $bc = 1$, което означава, че b и c са обратими и следователно имаме $13 - 1 = 12$ още 12 решения, защото в \mathbf{Z}_{13} има 12 обратими елемента.
- $a = 1$. Тогава $bc = 0$, т.е. имаме още $2 \cdot 13 - 1 = 25$ решения.
- $a = -1$. Аналогично, $bc = 0$ и имаме още $2 \cdot 13 - 1 = 25$ решения.
- $a \neq 0, 1, -1$. Тогава $c = (1 - a^2)b^{-1}$. Това ни дава още $(13 - 1)(13 - 3) = 120$ решения.

Сумирайки всички решения, получаваме, че в \mathbf{Z}_{13} има $2 + 12 + 25 + 25 + 120 = 184$ решения.

Остава да преброим матриците с това свойство над \mathbf{Z}_2 . Аналогично, нека разгледаме матрицата $K = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{Z}_2$. Отново получаваме същата система като при \mathbf{Z}_{13} .

Ако $a + d \neq 0$ следва, че $b = 0$ и $c = 0$ и също, че или $a = 1$ или $d = 1$. Но от $b = 0$ и $c = 0$ следва, че и $a^2 = 1$ и $d^2 = 1$, т.е. $a = 1$ и $d = 1$, което е невъзможно. Следователно от тук получаваме 0 решения.

Сега, ако $a + d = 0$, имаме следните случаи:

- $a = 0$. Тогава следва, че $d = 0$ и $bc = 1$, което означава, че b и c са обратими и следователно имаме една възможност $b = 1$ и $c = 1$. Този случай ни дава 1 решение.
- $a = 1$. Тогава и $d = 1$ и още $bc = 0$, т.е. или $b = 0$, $c = 1$ или $c = 0$, $b = 1$ или $b = c = 0$. От тук имаме още 3 решения.

Сумирайки всички решения, получаваме, че в \mathbf{Z}_2 има $1 + 3 = 4$ решения.

Тъй като $\mathbf{Z}_{26} \simeq \mathbf{Z}_2 \times \mathbf{Z}_{13}$, то над \mathbf{Z}_{26} има $4 \cdot 184 = 736$ матрици със свойство $K = K^{-1}$.

Задача 3

Ще започнем с това да преобразуваме открития текст и съответстващия му криптиотекст във вектори над \mathbf{Z}_{26} , използвайки дадената схема за кодиране:

C	R	Y	P	T	O	G	R	A	P	H	Y
2	17	24	15	19	14	6	17	0	15	7	24

V	G	Y	X	A	R	D	I	G	L	M	L
21	6	24	23	0	17	3	8	6	11	12	11

Дължината на шифрираното съобщение е 12. Тъй като m не е известно и сме предположили, че дели дължината на шифрираното съобщение, то ще започнем от случая $m = 2$.

Тъй като $m = 2$, то ще разбием открития текст и криптиотекста на 6 блока с дължина 2. Имаме следните двойки: $E_K(2, 17) = (21, 6)$, $E_K(24, 15) = (24, 23)$, $E_K(19, 14) = (0, 17)$, $E_K(6, 17) = (3, 8)$, $E_K(0, 15) = (6, 11)$, $E_K(7, 24) = (12, 11)$. От първата и третата двойка получаваме следното матрично уравнение:

$$\begin{pmatrix} 21 & 6 \\ 0 & 17 \end{pmatrix} = \begin{pmatrix} 2 & 17 \\ 19 & 14 \end{pmatrix} K$$

Пресмятаме $\begin{pmatrix} 2 & 17 \\ 19 & 14 \end{pmatrix}^{-1} = \begin{pmatrix} 10 & 25 \\ 5 & 20 \end{pmatrix}$. Тогава за ключа получаваме:

$$K = \begin{pmatrix} 10 & 25 \\ 5 & 20 \end{pmatrix} \begin{pmatrix} 21 & 6 \\ 0 & 17 \end{pmatrix} = \begin{pmatrix} 16 & 15 \\ 9 & 14 \end{pmatrix}$$

Сега да приложим ключа (също така K^{-1} съществува) към втората двойка от открития текст:

$$(24, 15) \begin{pmatrix} 16 & 15 \\ 9 & 14 \end{pmatrix} = (25, 24),$$

което очевидно не е вярно, защото трябваше да получим $(24, 23)$. Следователно, ако $m = 2$, не можем да намерим ключа.

Нека сега $m = 3$. Трябва да разбием открития текст и криптиотекста на 4 блока с дължина 3. Имаме следните тройки: $E_K(2, 17, 24) = (21, 6, 24)$, $E_K(15, 19, 14) = (23, 0, 17)$, $E_K(6, 17, 0) = (3, 8, 6)$, $E_K(15, 7, 24) = (11, 12, 11)$. Трябва да решим следната система:

$$\begin{pmatrix} 2 & 17 & 24 \\ 15 & 19 & 14 \\ 6 & 17 & 0 \\ 15 & 7 & 24 \end{pmatrix} K = \begin{pmatrix} 21 & 6 & 24 \\ 23 & 0 & 17 \\ 3 & 8 & 6 \\ 11 & 12 & 11 \end{pmatrix}$$

След известен брой аритметични операции стигаме до решението:

$$K = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix}$$

Матрицата K също така е и обратима:

$$K^{-1} = \begin{pmatrix} 12 & 3 & 20 \\ 20 & 12 & 3 \\ 3 & 20 & 12 \end{pmatrix}$$

Следователно матрицата K удовлетворява условието да е ключ.

Код на Wolfram Mathematica за случая $m = 3$:

```
plainText = {{2,17,24},{15,19,14},{6,17,0},{15,7,24}};
cryptoText = {{21,6,24},{23,0,17},{3,8,6},{11,12,11}};
xMatrix = {{x1,x2,x3},{x4,x5,x6},{x7,x8,x9}};

Solve[plainText.xMatrix==cryptoText,{x1,x2,x3,x4,x5,x6,x7,x8,x9}, Modulus->26]
{{x1->2,x2->0,x3->1,x4->1,x5->2,x6->0,x7->13 C[1],x8->1+13 C[2],x9->2+13 C[3]}}
```

```
Dimensions[{{x1->2,x2->0,x3->1,x4->1,x5->2,x6->0,x7->13 C[1],
x8->1+13C[2],x9->2+13 C[3]}}]
{1,9}
```

```
K = {{2,0,1},{1,2,0},{0,1,2}}
{{2,0,1},{1,2,0},{0,1,2}}
```

```
invK =Inverse[{{2,0,1},{1,2,0},{0,1,2}},Modulus->26]
{{12,3,20},{20,12,3},{3,20,12}}
```

```
Mod[cryptoText.{{12,3,20},{20,12,3},{3,20,12}},26]
{{2,17,24},{15,19,14},{6,17,0},{15,7,24}}
```

Задача 4

Откритият текст ще има дължина равна на дължината на криптитекста, тоест 31, и в себе си съдържа думата GESTURE. Имаме например:

***** G E S T U R E *****

Ключът се състои от ключовата дума, поставена в началото, и открития текст поставен веднага след нея. Тъй като по условие ключовата дума е с дължина 6, то ще има изместване на GESTURE с 6 позиции надясно:

k0 k1 k2 k3 k4 k5 ***** G E S T U R E *****

Забелязваме, че тъй като GESTURE има дължина 7, а отместването е с дължина 6, то G в ключа ще стои под E в открития текст. Също така при пифриране това означава, че имаме $E + G = K$, което показва, че GESTURE в ключа, може да се постави, така че да е над K в криптотекста. В криптоотрестта имаме K на точно 5 места, тоест има 5 възможности. След проверяване на случаите, само един излиза, че може да е смислен и нека дешифрираме каквото можем, използвайки тази информация:

Криптоотекст:

G	X	I	L	B	G	L	Q	Q	J	A	I	P	W	B	M	R	K	A	Z	B	W	Y	K	K	K	U	C	R	K	G
6	23	8	11	1	6	11	16	16	9	0	8	15	22	1	12	17	10	0	25	1	22	24	10	10	10	20	2	17	10	6

Ключ:

-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	E	S	T	U	R	E	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	6	4	18	19	20	17	4	-	-	-	-	-	-

Открит текст:

-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4	22	7	8	2	7	6	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	E	W	H	I	C	H	G	-	-	-	-	-	-

Разполагайки с тази информация, вече знаем, че в ключа вдясно от GESTURE се намира WHICHG, а в открития текст отляво на EWHICH имаме GESTUR. И нека отново разкирем колкото можем информация за ключа и открития текст.

Криптоотекст:

G	X	I	L	B	G	L	Q	Q	J	A	I	P	W	B	M	R	K	A	Z	B	W	Y	K	K	K	U	C	R	K	G
6	23	8	11	1	6	11	16	16	9	0	8	15	22	1	12	17	10	0	25	1	22	24	10	10	10	20	2	17	10	6

Ключ:

-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	G	E	S	T	U	R	E	W	H	I	C	H	G	-
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	6	4	18	19	20	17	4	22	7	8	2	7	6	-

Открит текст:

-	-	-	-	-	-	-	-	-	-	6	4	18	19	20	17	4	22	7	8	2	7	6	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	G	E	S	T	U	R	E	W	H	I	C	H	G	-	-	-	-	-	-	-

По аналогичен начин успяваме да открием открития текст:

Криптоотекст:

G	X	I	L	B	G	L	Q	Q	J	A	I	P	W	B	M	R	K	A	Z	B	W	Y	K	K	K	U	C	R	K	G
6	23	8	11	1	6	11	16	16	9	0	8	15	22	1	12	17	10	0	25	1	22	24	10	10	10	20	2	17	10	6

Ключ:

G	L	A	U	B	E	A	M	I	R	A	C	L	E	I	S	A	G	E	S	T	U	R	E	W	H	I	C	H	G	O
6	11	0	20	1	4	0	12	8	17	0	2	11	4	8	18	0	6	4	18	19	20	17	4	22	7	8	2	7	6	14

Открит текст:

0	12	8	17	0	2	11	4	8	18	0	6	4	18	19	20	17	4	22	7	8	2	7	6	14	3	12	0	10	4	18
A	M	I	R	A	C	L	E	I	S	A	G	E	S	T	U	R	E	W	H	I	C	H	G	O	D	M	A	K	E	S

Получихме, че ключовата дума е

GLAUBE

и откритият текст е

A MIRACLE IS A GESTURE WHICH GOD MAKES.

Задача 5

Имеме криптирания текст разделен на групи:

ACAUI MMGRC AILEE HKREG EAISW OSTHDS

На първия ред за първата клетка имаме две възможности - да съдържа A или да е забранена, което ще отбелязваме със *. За останалите клетки възможностите са да са забранени полета или да съдържат първата или втората буква от своята група.

Код на Swift за всички възможни комбинации от букви за първия ред от таблицата:

```
let firstBox: [Character] = ["*", "a"]
let secondBox: [Character] = ["*", "m"]
let thirdBox: [Character] = ["*", "a", "i"]
let fourthBox: [Character] = ["*", "h", "k"]
let fifthBox: [Character] = ["*", "e", "a"]
let sixthBox: [Character] = ["*", "o", "s"]
```

```
var myCount: Int
```

```
for first in firstBox {
    for second in secondBox {
        for third in thirdBox {
            for fourth in fourthBox {
                for fifth in fifthBox {
                    for sixth in sixthBox {
```


Нито една от 80-те различни комбинации не върши работа, ако сме приели, че има най-много по едно забранено поле в колона и ред. Но, взимайки предвид отговора на предишната задача,

A	M	I	R	A	*
C	*	L	E	I	S
A	G	E	*	S	T
U	R	E	*	W	H
I	C	H	G	O	D
M	A	K	E	*	S

```

coefficient = {0, 1};

For[first = 1, first <= 2, first++,
  For[second = 1, second <= 2, second++,
    For[third = 1, third <= 2, third++,
      For[fourth = 1, fourth <= 2, fourth++,
        For[fifth = 1, fifth <= 2, fifth++,
          polynomial =
            1 + coefficient[[first]]*x + coefficient[[second]]*x^2 +
              coefficient[[third]]*x^3 + coefficient[[fourth]]*x^4 +
              coefficient[[fifth]]*x^5 + x^6;
          If[PolynomialRemainder[x^21 + 1, polynomial, x, Modulus -> 2] ==
            0, Print[polynomial]]
        ]
      ]
    ]
  ]
]

```

Резултатът от изпълнението на програмата е:

$$\begin{array}{c}
 1 + x^2 + x^5 + x^6 \\
 1 + x^2 + x^4 + x^5 + x^6 \\
 1 + x + x^4 + x^6 \\
 1 + x + x^2 + x^4 + x^6 \\
 1 + x + x^2 + x^3 + x^4 + x^5 + x^6
 \end{array}$$

От полиномите всички, освен последния, не делят $x^7 + 1$, т.е. можем да изберем всеки от първите 4.

Задача 7

В началото имаме блок A с дължина $m = 2$ и блок B с дължина $n = 4$. Искаме да шифрираме 101101 за $h = 4$ стъпки. Тоест имаме, че $A = 10$ и $B = 1101$.

Стъпка $h = 1$:

$$\begin{aligned}
 A' &= 1101 \\
 B' &= A \oplus f_1(B) = 10 \oplus f_1(1101) = 10 \oplus 00 = 10
 \end{aligned}$$

Получаваме 110110.

Стъпка $h = 2$:

Сега имаме, че $A = 11$ и $B = 0110$. Оттук получаваме:

$$\begin{aligned}
 A' &= 0110 \\
 B' &= A \oplus f_2(B) = 11 \oplus f_2(0110) = 11 \oplus 01 = 10
 \end{aligned}$$

Получаваме 011010.

Стъпка $h = 3$: Сега имаме, че $A = 01$ и $B = 1010$. Оттук получаваме:

$$\begin{aligned} A' &= 1010 \\ B' &= A \oplus f_3(B) = 01 \oplus f_3(1010) = 01 \oplus 00 = 01 \end{aligned}$$

Получаваме 101001.

Стъпка $h = 4$: Сега имаме, че $A = 10$ и $B = 1001$. Оттук получаваме:

$$\begin{aligned} A' &= 1001 \\ B' &= A \oplus f_4(B) = 10 \oplus f_4(1001) = 10 \oplus 01 = 11 \end{aligned}$$

Получаваме 100111, което и търсихме.

Задача 8

Искаме да докажем, че броят на откритите текстове m , които се шифрират в себе си, т.е. за които $m^e \equiv m \pmod n$. Имаме още, че модулът е $n = pq$ и, че шифриращият експонент е e . Също така p и q са две големи прости числа с дължина поне 512 бита. Тъй като са прости числа, то $\gcd(p, q) = 1$. Имаме още, че m е цяло число. Тогава от китайската теорема за остатъците имаме, че системата

$$\begin{aligned} m^e &\equiv m \pmod p \\ m^e &\equiv m \pmod q \end{aligned}$$

винаги има решение и всеки две решения се различават с кратно на n .

Първо ще покажем, че $m^e \equiv m \pmod p$ има $1 + \gcd(e - 1, \varphi(p))$ решения по $\pmod p$.

Нека $p \mid m$ и

$$m^e \equiv m \pmod p$$

Тогава

$$m(m^{e-1} - 1) \equiv 0 \pmod p$$

и също така

$$m^{e-1} \not\equiv 1 \pmod p,$$

защото сме допуснали, че $p \mid m$ и значи $p \mid m^{e-1}$. От тук получаваме, че

$$m \equiv 0 \pmod p,$$

което е еквивалентно на допускането $p \mid m$.

Нека сега $p \nmid m$. Тогава

$$m = g^t,$$

където g е примитивен корен по модул p , тоест $g^{p-1} \equiv 1 \pmod{p}$ и $g^k \not\equiv 1 \pmod{p}$, $k < p-1$. Сега имаме, че

$$g^{te} \equiv g^t \pmod{p}$$

или еквивалентно

$$g^{t(e-1)} \equiv 1 \pmod{p}$$

тогава и само тогава, когато

$$t(e-1) \equiv 0 \pmod{\varphi(p)},$$

защото g е примитивен корен. Последното има $\gcd(e-1, \varphi(p)) = \gcd(e-1, p-1)$ решения. Добавяйки и тривиалното решение, получаваме, че $m^e \equiv m \pmod{p}$ има общо $1 + \gcd(e-1, p-1)$ решения.

По аналогичен начин получаваме, че $m^e \equiv m \pmod{q}$ има $1 + \gcd(e-1, q-1)$ решения. От китайската теорема за остатъци следва, че системата, а от там и броят на откритите текстове, които се шифрират в себе си, е $(1 + \gcd(e-1, p-1))(1 + \gcd(e-1, q-1))$.

Задача 9