

ЗАДАЧИ ПО КРИПТОГРАФИЯ

Йоана Левчева

Приложна математика, 4 курс, ф.н. 31492

15 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 $b = 0$ или $c = 0$ 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 запишем кое число съответства на всяка буква от открития текст и съответстващия му криптиотекст, 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