ЗАДАЧИ ПО КРИПТОГРАФИЯ

Йоана Левчева
Приложна математика, 4 курс, ф.н. 31492

10 юни 2020 г.

Задача 1

Ще започнем, разбивайки по двойки букви откриитя текст и съответстващия му криптотекст:

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 стълб. Нека приемем, че се намират на един ред и ги поставим в първия ред на таблицата ни 5x5, 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, взимайки предвид тези заключения. Получаваме:

E	N	T	W	Z
S	A		F	O

Сега от TH → 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 → DZ също образува правоъгълник IDNZ и следователно I се намира под Z и D се намира под N. От DI → 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 → RE, тъй като ESR следва, че и C се намира в същия първи стълб и понеже C → E то C се намира на последния ред. Остана да разгледаме само UR → 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 криптотекст, 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 криптотекста, който трябва да дешифрираме и дешифрираме каквото можем, използвайки отчасти конструирания ключ:

EB	QX	ZL	HD	LK	IV	QG	OM	AL	EB	BV	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 криптотекста е CRYPTOGRAPHY.

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

Забелязваме, че ZL → TO, тоест се образува правоъгълник ZTLO и мястото на L става известно. А от IV → 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 криптотекста.

EB	QX	ZL	HD	LK	IV	QG	OM	AL	EB	BV	DO	SG	SF
CR	YP	TO	GR	AP	HY			SA	CR	UC	IA	LR	0L

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 → YP имаме, че Q е на последния ред, а P и X на предпоследния, по-конкретно X е над Y. От LK → 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 криптотекст:

EB	QX	ZL	HD	LK	IV	QG	OM	AL	EB	BV	DO	SG	SF
CR	YP	TO	GR	AP	HY	PL	AY	SA	CR	UC	IA	LR	0L

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 криптотекстът 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:

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

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*13 - 1 = 25 решения.
- $a = -1$. Аналогично, $bc = 0$ и имаме още 2*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*184 = 736 матрици със свойство $K = K^{-1}$.

Задача 3

Ще започнем с това да преобразуваме откритития текст и съответстващия му криптотекст 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 криптотекста 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 криптотекста 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 криптотекста, 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:

k_0 k_1 k_2 k_3 k_4 k_5 * * * * * * * * * * * * * * 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 шифриране 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 криптотрекста 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:

Криптотекст:

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 разкрием колкото можем информация за ключа и открития текст.

Криптотекст:

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:

Криптотекст:

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

Имаме криптотекста, 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 своят 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 {
```

```
                    myCount = 0
                    for box in "\(first)\(second)\(third)\(fourth)\(fifth)\(sixth)" {
                        if box == "*" {
                            myCount += 1
                        }
                    }
                    if myCount == 0 || myCount == 1 {
                            print("\(first)\(second)\(third)\(fourth)\(fifth)\(sixth)")
                    }
                }
            }
        }
    }
  }
}
```

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 MIRACLE IS A GESTURE WHICH GOD MAKES

можем да конструираме следната таблица, която обаче има една колона с две забранени места:

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

Задача 6

$x^{21}+1$ е характеристичен полином на периодична редица с период 21 (тя просто копира елемента 21 позиции назад). Ако полиномът на друга редица дели този полином, то значи и периодът ѝ ще го дели. Това означава, че ако намерим полином, който дели този, но не дели x^3+1 и x^7+1, тогава периодът на редицата, която генерира ще дели 21, но няма да дели 3 и няма да дели 7 следователно ще е точно 21. Полиномът, който ще намерим, трябва да е най-малко от 6та степен, тъй като полином от n-та може да породи редица с цикъл с дължина най-много 2^{n-1}, а ние искаме $2^4 < 21 < 2^5$ следователно трябва да е поне от 6-та степен. Тъй като търсим полином от 6-та степен, имаме, че той никога не дели x^3+1.

С този код на $Wolfram\ Mathematica$ намираме всички полиноми от 6-та степен над $Z2$, които делят $x^{21}+1$.

```
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:

$$1 + x^2 + x^5 + x^6$$
$$1 + x^2 + x^4 + x^5 + x^6$$
$$1 + x + x^4 + x^6$$
$$1 + x + x^2 + x^4 + x^6$$
$$1 + x + x^2 + x^3 + x^4 + x^5 + x^6$$

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 $h = 1$:

$$A' = 1101$$
$$B' = A \oplus f_1(B) = 10 \oplus f_1(1101) = 10 \oplus 00 = 10$$

Получаваме 110110.

Стъпка $h = 2$:
Сега имаме, че $A = 11$ и $B = 0110$. Оттук получаваме:

$$A' = 0110$$
$$B' = A \oplus f_2(B) = 11 \oplus f_2(0110) = 11 \oplus 01 = 10$$

Получаваме 011010.

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

$$A' = 1010$$
$$B' = A \oplus f_3(B) = 01 \oplus f_3(1010) = 01 \oplus 00 = 01$$

Получаваме 101001.

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

$$A' = 1001$$
$$B' = A \oplus f_4(B) = 10 \oplus f_4(1001) = 10 \oplus 01 = 11$$

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 $m^e \equiv m \mod n$. Имаме още, че модулът е $n = pq$ и, че шифриращата експонента 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

$$m^e \equiv m \mod p$$
$$m^e \equiv m \mod q$$

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

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

Нека $p \mid m$ и

$$m^e \equiv m \mod p$$

Тогава

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

и също така

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

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

$$m \equiv 0 \mod p,$$

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

Нека сега $p \nmid m$. Тогава

$$m \equiv g^t \mod p,$$

където g е примитивен корен по модул p, тоест $g^{p-1} \equiv 1 \mod p$ и $g^k \not\equiv 1 \mod p$, $k < p-1$. Следователно можем да решаваме сравнението спрямо t. Сега имаме, че

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

или еквивалентно

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

тогава и само тогава, когато

$$t(e-1) \equiv 0 \mod \varphi(p),$$

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

По аналогичен начин получаваме, че $m^e \equiv m \mod q$ 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

Следният код на $WolframMathematica$

```
For[i = 1, i <= 101, i++,
    value = Mod[2^i, 101];
    If[value == 1, Print[i]];
]
```

с изход

```
100
```

показва, че 2 поражда Z^*_{101}. По същия начин

```
For[i = 1, i <= 101, i++,
    value = Mod[2^i, 101];
    If[value == 66, Print[i]];
]
```

с изход

```
83
```

получаваме, че отговорът е 83, но все пак ще приложим алгоритъма на $Pohlig - Hellman$.

В случая $q = 101$, $q - 1 = 100 = 2^2.5^2$, $\alpha = 2$, $\alpha^{-1} = 51$. Търсим това m, за което

$$2^m = 66 \mod 101.$$

Извършваме пресмятанията

$$\beta_1 = 2^{\frac{100}{2}} = 2^{50} = 100$$
$$\beta_2 = 2^{\frac{100}{5}} = 2^{20} = 95$$

$$p_1 = 2 \quad \begin{array}{c|cc} i & 0 & 1 \\ \hline \beta_1^i & 1 & 100 \end{array}$$

$$p_2 = 5 \quad \begin{array}{c|ccccc} i & 0 & 1 & 2 & 3 & 4 \\ \hline \beta_1^i & 1 & 95 & 36 & 87 & 84 \end{array}$$

Нека $2^m \equiv c \mod 101$, където $c = 66$. Тогава

$$\begin{array}{ccccc} & c = 66, & c^{\frac{100}{2}} = 100, & \Longrightarrow & b_0 = 1 \\ p_1 = 2, n_1 = 2 & c_1 = c\alpha^{-1} = 33, & c_1^{\frac{100}{2^2}} = 100 & \Longrightarrow & b_1 = 1 \\ & \Longrightarrow m^{(1)} = 1 + 1.2^1 = 3 & & & \end{array}$$

$$\begin{array}{ccccc} & c = 66, & c^{\frac{100}{5}} = 87, & \Longrightarrow & b_0 = 3 \\ p_2 = 5, n_2 = 2 & c_1 = c\alpha^{-3} = 84, & c_1^{\frac{100}{5^2}} = 95 & \Longrightarrow & b_1 = 1 \\ & \Longrightarrow m^{(2)} = 3 + 1.5^1 = 8 & & & \end{array}$$

Сега остава да пресметнем m.

$$M_1 = \frac{100}{4} = 25 \text{ и } y_1 \equiv M_1^{-1} \mod 4, \text{ тоест } y_1 = 1$$
$$M_2 = \frac{100}{25} = 4 \text{ и } y_2 \equiv M_2^{-1} \mod 25, \text{ тоест } y_2 = 19$$

За m получаваме

$$m = 3.25.1 + 8.4.19 = 683,$$

за което имаме $2^{683} \equiv 2^{83} \equiv 66 \mod 101$. Следователно $\log_2 66 = 83$ в Z^*_{101}.

Задача 10

Нека m е случайно число, такова че $0 < m < n$, и решаваме сравнението $x^2 \equiv m^2 \mod n$ във $F(n)$ стъпки с помощта на алгоритъма A. Нека k е едно от четирите решения на $x^2 \equiv m^2 \mod n$. Всяка от следните възможности се реализира с вероятност $\frac{1}{4}$:

1) $k \equiv m \mod p$, $k \equiv m \mod q$
2) $k \equiv m \mod p$, $k \equiv -m \mod q$
3) $k \equiv -m \mod p$, $k \equiv m \mod q$
4) $k \equiv -m \mod p$, $k \equiv -m \mod q$

В случай 2) имаме $gcd(k-m,n)=p$, а в случай 3) - $gcd(k-m,n)=q$. Следователно пресмятането на $gcd(k-m,n)$ намира разлагането с вероятност $\frac{1}{2}$. Това пресмятане изисква $2\log n$ стъпки. Така при всеки избор за m ще извършваме $F(n)+2\log n$ стъпки като вероятността за успех е $\frac{1}{2}$. Очакваният брой опити до намиране на разлагането на n е два, което е и твърдението на теоремата.

Задача 11

Елементите на GF(2^{10}) може да се представят като полиноми от степен по-малка от 10 над GF(2). Тогава операциите се извършват по $\mod R$, където R е неразложим полином от степен 10 над GF(2). В нашата задача този полином е $x^{10}+x^3+1$. Умножението извършваме по стандартния начин и по $\mod 2$ и след това взимаме остатъка по $\mod R$, пак по $\mod 2$.

В задачата търсим общия ключ $k_{A,B}=C_B^{x_A}=(x+x^5+x^7)^2$. Тоест имаме да извършим умножението $(x+x^5+x^7)(x+x^5+x^7)$:

$$(x+x^5+x^7)(x+x^5+x^7)=x^2+2x^6+2x^8+x^{10}+2x^{12}+x^{14},$$

което по $\mod 2$ е

$$x^2+x^{10}+x^{14}.$$

Сега остава да пресметнем остатъка при деление (накрая по $\mod 2$) на

$$x^2+x^{10}+x^{14}$$

с полинома

$$x^{10}+x^3+1.$$

За целта ще запишем полинома

$$x^{14}+x^{10}+x^2 \text{ във вида } 100010000000100$$

и

$$x^{10}+x^3+1 \text{ във вида } 10000001001.$$

Ще използваме *long notation* по $\mod 10000001001$:

1	0	0	0	1	0	0	0	0	0	0	0	1	0	0
1	0	0	0	0	0	0	1	0	0	1				
0	0	0	0	1	0	0	1	0	0	1	0	1	0	0
			*	1	0	0	0	0	0	0	1	0	0	1
				0	0	0	1	0	0	1	1	1	0	1

Така получихме, че общият ключ $k_{A,B}$ е 00010011101, тоест

$$k_{A,B}=x^7+x^4+x^3+x^2+1.$$

Задача 12

Генериране на ключове в схемата на ElGamal:

1) По условие $p = 101$ и $\alpha = 2$ е пораждащ елемент на Z_{101}^*.
2) По условие $a = 43$ и наистина $1 \leq a \leq p - 2 = 99$.
3) Пресмятаме $y = \alpha^a = 2^{43} \mod 101$. Получаваме, че $y = 86$.
4) Публичният ключ е тройката $(p, \alpha, y) = (101, 2, 86)$. Частен ключ е $a = 43$.

Генериране на подписи в схемата на ElGamal:

1) Избираме случайното число $k = 23, 1 \leq k \leq p - 2 = 99$, за което $gcd(k, p - 1) = gcd(23, 100) = 1$.
2) Пресмятаме $r = \alpha^k = 2^{23} \mod 101$. Получаваме, че $r = 53$.
3) Пресмятаме $s = k^{-1}(h(m) - ar) = 87(26 - 43.53) \mod 100$, като предварително за удобство сме избрали $h(m) = m$. Получаваме, че $s = 89$.
4) Подписът за m е двойката $(r, s) = (53, 89)$.

Верифициране на подписи в схемата на ElGamal:

1) Получаваме публичния ключ $(p, \alpha, y) = (101, 2, 86)$.
2) Проверяваме дали $1 \leq r = 53 \leq p - 1 = 100$, което очевидно е изпълнено и следователно не отхвърляме подписа.
3) Пресмятаме $u = y^r r^s = 86^{53} 53^{89} \mod 101$. Получаваме, че $u = 20$.
4) Пресмятаме $h(m) = m = 26$ и $v = \alpha^{h(m)} = 2^{26} \mod 101$. Получаваме $v = 20$.
5) Приемаме подписа, защото $u = v$.

Задача 13

Следният код на $Wolfram\ Mathematica$

```
For[i = 1, i <= 353, i++,
    value = Mod[3^i, 353];
    If[value == 1, Print[i]];
]
```

с изход

```
352
```

показва, че 3 поражда Z_{353}^*. По същия начин

```
For[i = 1, i <= 353, i++,
    value = Mod[3^i, 353];
    If[value == 135, Print[i]];
]
```

с изход

```
312
```

получаваме, че отговорът е 312, но все пак ще приложим алгоритъма *Baby step/giant step*.

Този код

```
n = 352;
m = Ceiling[Sqrt[352]];
alfa = 3;
beta = 135;

gama = beta;
i = 1;
While[gama != 3,
    gama = Mod[gama*PowerMod[alfa, -m, 353], 353];
    For[j = 0, j <= m, j++,
        If[gama == Mod[alfa^j, 353], If[gama == 3, Print[i*m + j]]
        ]
    ];
i++
]
```

с изход

```
2072
```

имплементира алгоритъма и чрез него получаваме, че $x = 2072$, за което имаме $3^{2072} \equiv 3^{312} \equiv 135 \mod 353$. Следователно $\log_3 135 = 312$ в Z^*_{353}.

Задача 14

По условие имаме свръхнарастващ вектор $a = (2, 3, 7, 13, 27, 53, 106, 213, 425, 851)$, модулът $m = 1529$ и $t = 64$. Трябва да шифрираме съобщението LONDON. Векторът b получаваме чрез слабо умножение на a с t по модул m, защото $m \geq \max a = 851$. За b получаваме

$$b = (128, 192, 448, 832, 199, 334, 668, 1400, 1207, 949).$$

Сега ще шифрираме текста LONDON, позовавайки се на таблицата от условието

$$\text{LO} \rightarrow 10001\ 10100 \rightarrow 128 + 199 + 334 + 1400 = 2061$$
$$\text{ND} \rightarrow 10011\ 00111 \rightarrow 128 + 832 + 199 + 1400 + 1207 + 949 = 4715$$
$$\text{ON} \rightarrow 10100\ 10011 \rightarrow 128 + 448 + 334 + 1207 + 949 = 3066$$

Така криптотекстът е

$$2061\ 4715\ 3066.$$

Задача 15

(i) Искаме 3 да дели $\varphi(n) = \varphi(pq) = \varphi(p).\varphi(q) = (p-1)(q-1)$. Това означава, че 3 дели или $p-1$, или $q-1$. Тоест или $p \equiv 1 \mod 3$, или $q \equiv 1 \mod 3$, или и $p \equiv 1 \mod 2$ и $q \equiv 1 \mod 3$.

(ii) Ако g генерира Z_p^*, където (по условие) p е нечетно просто число. Кубичен корен можем да запишем като

$$g^{3i} \equiv g^j \mod p,$$

където i и j са цели числа. Това е еквивалентно на

$$3i \equiv j \mod (p-1).$$

Тъй като 3 е просто число, то $gcd(p-1,3) = 1$ или $gcd(p-1,3) = 3$. Ако $gcd(p-1,3) = 3$, то от *Теорема 7.8* от *Лекция 7* имаме, че $3i \equiv j \mod (p-1)$ има 3 решения. Ако $gcd(p-1,3) = 1$, то от *Следствие 7.9* от *Лекция 7* имаме, че $3i \equiv j \mod (p-1)$ има точно едно решение.

В случая, когато $p \equiv 1 \mod 3$, то $gcd(p-1,3) = 3$, тоест $y^3 \equiv x \mod p$ има 3 решения. И също така $q \equiv 2 \mod 3$, то $gcd(q-1,3) = 1$, тоест $y^3 \equiv x \mod q$ има едно решение. Сега от *Китайската теорема за остатъците* получаваме, че $y^3 \equiv x \mod n$ има $3.1 = 3$ решения.

В случая, когато $p \equiv q \equiv 1 \mod 3$, имаме, че $gcd(p-1,3) = 3$ и $gcd(q-1,3) = 3$, тоест $y^3 \equiv x \mod p$ има 3 решения и $y^3 \equiv x \mod q$ има също 3 решения. От *Китайската теорема за остатъците* получаваме, че $y^3 \equiv x \mod n$ има $3.3 = 9$ решения.

Сега по условие имаме два различни кубични корена y и z на даден елемент x от C_n. Тогава е изпълнено

$$y^3 \equiv z^3 \equiv x \mod n.$$

Последното можем да запишем още така

$$y^3 - z^3 \equiv (y-z)(y^2 + yz + z^2) \mod n.$$

Вероятността $gcd(y-z,n) \neq \pm 1, \pm n$, е

$$\mathrm{P}(y \equiv z \mod p, y \not\equiv z \mod q) + \mathrm{P}(y \not\equiv z \mod p, y \equiv z \mod q).$$

Когато $y \not\equiv z \mod p$ и $y \not\equiv z \mod q$, тогава и $y \not\equiv x \mod n$. В този случай няма как да открием нетривиален делител. Вероятността за това е $\frac{2}{3}$, ако $p \equiv 2 \mod 3$ и $q \equiv 1 \mod 3$, и ако $p \equiv 1 \mod 3$ и $q \equiv 2 \mod 3$. Когато $p \equiv q \equiv 1 \mod 3$, вероятността е $\frac{4}{9}$. Окончателно, вероятността за успех е

$$\tfrac{2}{3}.\tfrac{2}{3} + \tfrac{4}{9}.\tfrac{1}{3} = \tfrac{16}{27}.$$

Ако имаме, оракул, който може да смята кубични корени в Z_n^*, можем да разложим n по следния начин:

1.) Генерираме произволно $y \in Z_n^*$ и пресмятаме $y^3 \equiv x \mod n$.

2.) Подаваме x на оракула и с вероятност $\frac{16}{27}$, от предишната част на задачата, той връща $y \neq z$, като по този начин получаваме разлагане на n.

Обратно, имайки разлагането на n, с *Китайската теорема за остатъците*, можем да пресметнем кубичните корени.

Следователно проблемът за криптанализ на RSA с $e = 3$ е еквивалентен на разлагането на n.

Задача 16

Имаме, че $n = pq$, тоест

$\varphi(n) = \varphi(pq) = \varphi(p).\varphi(q) = (p-1)(q-1) = pq - (p+q) + 1 = n - (p+q) + 1$,

и от това, че по условие

$$a = n + 1 - \varphi(n)$$

можем да забележим, че също

$$a = p + q.$$

От $pq = n$ и $p + q = a$ излиза, че p и q са корени на уравнението

$$x^2 - ax + n = 0$$

и могат да се определят от $p = \frac{a+\sqrt{a^2-4n}}{2}$ и $q = \frac{a-\sqrt{a^2-4n}}{2}$.

В нашата задача $n = 15049$ и $\varphi(n) = 14800$. Тогава за a получаваме

$$a = n + 1 - \varphi(n) = 15049 + 1 - 14800 = 250.$$

От тук за p получаваме

$$p = \frac{250+\sqrt{250^2-4.15049}}{2} = 149$$

и за q получаваме

$$q = \frac{250-\sqrt{250^2-4.15049}}{2} = 101.$$

Задача 17

По условие $G = \{x \in Z_{p^2}$, за които $x \equiv 1 \mod p\}$

(i) За да докажем, че G е група относно операцията умножение в Z_{p^2}, трябва да установим, че са изпълнение четирите аксиоми:

1) $x_1 x_2 \in G$ за всяко $x_1 \in G$, $x_2 \in G$:

Имаме, че

$$x_1 \in G, \text{ тоест } x_1 \equiv 1 \mod p$$
$$x_2 \in G, \text{ тоест } x_2 \equiv 1 \mod p$$

От тези две твърдения и от свойствата на $\mod$ получаваме, че $x_1 x_2 \equiv 1 \mod p$. Следователно $x_1 x_2 \in G$.

2) $x_1(x_2 x_3) = (x_1 x_2)x_3$ за всяко $x_1 \in G$, $x_2 \in G$, $x_3 \in G$:

Имаме, че

$$x_1 \in G, \text{ тоест } x_1 \equiv 1 \mod p$$
$$x_2 \in G, \text{ тоест } x_2 \equiv 1 \mod p$$
$$x_3 \in G, \text{ тоест } x_3 \equiv 1 \mod p$$

Като в 1) имаме $x_2 x_3 \equiv 1 \mod p$ и аналогично $x_1(x_2 x_3) \equiv 1 \mod p$. За $(x_1 x_2)x_3$ първо имаме, че $x_1 x_2 \equiv 1 \mod p$ и после $(x_1 x_2)x_3 \equiv 1 \mod p$. От тук получаваме, че $x_1(x_2 x_3) \equiv (x_1 x_2)x_3 \equiv 1 \mod p$

3) Съществува $e \in G$, такъв че $xe = ex = x$ за всяко $x \in G$:

Неутралният елемент $e = 1 \in G$ на Z_{p^2} ни върши работа. Имаме, че

$$x \in G, \text{ тоест } x \equiv 1 \mod p$$
$$1 \in G, \text{ за което очевидно имаме } 1 \equiv 1 \mod p$$

От горните две, отново като в 1), получаваме $1.x \equiv x.1 \equiv x \equiv 1 \mod p$.

4) За всеки елемент $x \in G$ съществува $x^{-1} \in G$, такъв че $xx^{-1} = x^{-1}x = 1$:

Ако $x \in G$, тоест $x \equiv 1 \mod p$, то можем да запишем това и като $x = 1 + kp$, където k е цяло число, такова че $0 \leq k < p$. Аналогично, ако съществува $x^{-1} \in G$, тоест $x^{-1} \equiv 1 \mod p$, то можем да го запишем и като $x^{-1} = 1 + lp$, където l е цяло число, такова че $0 \leq l < p$. Тогава

$$xx^{-1} \equiv (1 + kp)(1 + lp) \equiv 1 + lp + kp + klp^2 \equiv 1 + (k + l)p \mod p^2$$

От тук получаваме, че $xx^{-1} \equiv 1 \mod p$, когато $k + l \equiv 0 \mod p$. Следователно всеки елемент $x = 1 + kp \in G$ има за обратен елемент $x^{-1} = 1 + (p - k)p$.

(ii) Трябва да докажем, че $|G| = p$. Всяко число $x \in Z_{p^2}$ можем да представим като $x = k_1 + k_2 p$, където k_1, k_2 са цели числа, такива че $0 \leq k_1 \leq p - 1$ и $0 \leq k_2 \leq p - 1$. Имаме, че $x \in G$ само ако $k_1 \equiv 1 \mod p$. За k_2 имаме p възможности, откъдето и следва, че $|G| = p$.

(iii) Първо ще докажем, че имаме хомоморфизъм, тоест трябва да докажем, че $L(x_1.x_2) = L(x_1) + L(x_2)$. Нека $x_1 \in G$ и $x_2 \in G$. Да ги запишем като $x_1 = 1 + kp$, където $0 \leq k \leq p - 1$ и $x_2 = 1 + lp$, където $0 \leq l \leq p - 1$. Разглеждаме

$$L(x_1.x_2) = L((1+kp)(1+lp) \mod p^2) = L(1+(k+l)p) = \tfrac{1+(k+l)p-1}{p} \mod p = k+l \mod p$$

и

$$L(x_1) + L(x_2) = \tfrac{1+kp-1}{p} + \tfrac{1+lp-1}{p} \mod p = k+l \mod p.$$

Сега трябва да докажем, че е биекция. Ще започнем с инекцията. Нека $x_1 \in G$, $x_2 \in G$ и $x_1 \neq x_2$. Нека още $x_1 = 1+kp$, където $0 \leq k \leq p-1$ и $x_2 = 1+lp$, където $0 \leq l \leq p-1$. Да разглеждаме

$$L(x_1) = \tfrac{1+kp-1}{p} \mod p = k \mod p$$

и

$$L(x_2) = \tfrac{1+lp-1}{p} \mod p = l \mod p.$$

Тъй като $x_1 \neq x_2$, то $k \neq l$, откъдето следва, че и $L(x_1) \neq L(x_2)$. Така доказахме инекцията.

Остана да докажем сюрекцията. Тя следва от инекцията, защото Z_p и G са крайни с еднакъв брой елементи.

(iv) Имаме, че

$$(p+1)^n \mod p^2 = \textstyle\sum_{i=0}^{n} \binom{n}{i} p^i \mod p^2 = 1+np,$$

което означава, че $p+1$ поражда G.

Сега нека $x_1 \in G$. Тогава

$$x_1 = \log_{p+1}(x_2) \Leftrightarrow x_2 = (p+1)^{x_1} \mod p^2.$$

Тъй като $(p+1)^{x_1} \mod p^2 = 1+px_1$, получаваме

$$x_1 = \tfrac{x_2-1}{p} \mod p = L(x_2).$$

Тоест получихме, че $(p+1)^{L(x_2)} \mod p^2 = x_2$ за всяко x_2, което трябваше да докажем.