

# Задачи по Криптография – 2021

**Име: Надежда Росенова Францева**

ФН: 62 391

13ag. Да се дешифрира криптомехана  
EB QX ZL HD LK IV QG OM AL EB VB DO SG SF  
EB AN DA MO LB SE EL SO ZL KD CO ZF GS IN.  
анко е известено, че е използвана шифрът на Playfair,  
трябва да се дешифрира в THE WINTER OF OUR DISCONTENT  
и шифрът в WGNZD ZWNISOSBYGRBEAZWNTW.

P-e:

От гаденото изодразување, че идни  $NT \rightarrow TW$   
 $TE \rightarrow WN$   
 $EW \rightarrow NZ$ ,  
то 5-те букви ( $E, N, T, W$  и  $Z$ ) се нацирнат  
кај едни редени ка една колона. Акологично  
за  $FO \rightarrow DS = FS, FO$  се идни ка едни ред или колона.  
Останалите букви подреди се по правилото кај  
правозаписната според 2-ма гаденски текста и  
изодразувајќи табличката:

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

## Демография:

EB	QX	ZL	KD	LK	IU	QG	OM	AL	EB	UB	DO	SG	SF
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
CR	YP	TO	GR	FP	HY	PL	AY	SA	CR	CU	IA	LR	DL
										(UC)			
ZR	AN	DA	MO	LB	SE	EL	SO	ZL	KD	CO	ZF	GS	IU
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
EI	NM	AN	YA	SP	EC	TS	OF	TO	DA	YS	WO	RL	DZ

2 задача. Често се приема за полезно шифрирането и дешифрирането трансформации да съвпадат в случаи на шифрата на Хил това означава  $K = K^{-1}$ . Да се определи броя на матриците от ред 2 над  $\mathbb{Z}_{26}$ , за които това е изпълнено.

Тук използваме кратка програмка, която пресича броя на матриците, които на квадрат дават единичната, като работим в  $\mathbb{Z}_{26}$ .

=> отв.: 736 броя

C++ код:

```
#include <iostream> using namespace std; void matrixPower2(int matr[][2], int res[][2]) {  
    for (int i = 0; i < 2; i++) { for (int j = 0; j < 2; j++) { res[i][j] = 0; for (int k = 0; k < 2; k++) {  
        res[i][j] += matr[i][k] * matr[k][j]; } } } for (int i = 0; i < 2; i++) { for (int j = 0; j < 2; j++) { int  
        tmp = res[i][j]; res[i][j] = res[i][j] - (tmp / 26) * 26; } } } int main() { int matrix[2][2]; int  
    matrixCounter = 0; for (int i = 0; i < 26; i++) { matrix[0][0] = i; for (int j = 0; j < 26; j++) {  
        matrix[0][1] = j; for (int k = 0; k < 26; k++) { matrix[1][0] = k; for (int l = 0; l < 26; l++) {  
            matrix[1][1] = l; int result[2][2]; matrixPower2(matrix, result); if (result[0][0] == 1 &&  
                result[1][1] == 1 && result[0][1] == 0 && result[1][0] == 0) { matrixCounter++; } } } } }  
    cout << "Count of matrices which fulfill the condition K = K^-1: " << matrixCounter <<  
    endl; return 0; }
```

Заг. Да се намери кюлот на шифърът на Хенър, който шифрира обобщението CRYPTOGRAPHY в VGYXARDIGLML. Длъжината на кюлота е неизвестна (ко може да допускне, че дели дължината на шифрираното обобщение). Изволнуването е схемата за кодиране:

P-e:

2 17 24 15 19 14 6 17 0 15 7 24  
CRYPTOGRAPHY

2 6 24 23 0 17 3 8 6 11 12 11  
VGYXARDIGLML

A → 0  
B → 1  
C → 2  
D → 3  
E → 4  
F → 5  
G → 6  
H → 7  
I → 8  
J → 9  
K → 10  
L → 11  
M → 12  
N → 13  
O → 14  
P → 15  
Q → 16  
R → 17  
S → 18  
T → 19  
U → 20  
V → 21  
W → 22  
X → 23  
Y → 24  
Z → 25

Разбиване открития текст на парчета и разширяване всеко парче като вектор над  $\mathbb{Z}_{26}$ . Откритият текст е с д-ка 12 = 3 парчета, които да бъдат с д-ка: 2, 3, 4 или 6. Заделивайки, че дължините 2, 4 и 6 водят до определеност и кога да получим р-е с тях = 3 остава 3. Търсит кюлот - матрица  $3 \times 3$ . Нека това бъде матрицата

$$K = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

Ние знаем, че:

$$(2, 17, 24)_{1 \times 3} \cdot K_{3 \times 3} = (21, 6, 24)_{1 \times 3}$$

$$(15, 19, 14)_{1 \times 3} \cdot K_{3 \times 3} = (23, 0, 17)_{1 \times 3}$$

$$(6, 17, 0)_{1 \times 3} \cdot K_{3 \times 3} = (3, 8, 6)_{1 \times 3}$$

$$(15, 7, 24)_{1 \times 3} \cdot K_{3 \times 3} = (11, 12, 11)_{1 \times 3}$$

Така образуване системата:

$$\left. \begin{array}{l} 2a + 14b + 24c = 21 \\ 2d + 14e + 24f = 6 \\ 2g + 14h + 24i = 24 \\ 15a + 19b + 14c = 23 \\ 15d + 19e + 14f = 0 \\ 15g + 19h + 14i = 14 \\ 6a + 14b + 0c = 3 \\ 6d + 14e + 0f = 8 \\ 6g + 14h + 0i = 6 \\ 15a + 4b + 24c = 11 \\ 15d + 4e + 24f = 12 \\ 15g + 4h + 24i = 11 \end{array} \right\} \cdot 19 + b \ Z_{26} = 4 \pmod{26}$$

Започване да е дупрекое, като за всички  
със знаци  $-III$  се означават повторящите  
се от предишната стъпка

$$\left. \begin{array}{l} 1.a + 14.b + 4.c = 16 \\ 1.d + 14.e + 4.f = 6 \\ 1.g + 14.h + 4.i = 9 \\ 15.a + 19.b + 14.c = 23 \\ 15.d + 19.e + 14.f = 0 \\ 15.g + 19.h + 14.i = 14 \\ 6.a + 14.l + 0.c = 3 \\ 6.d + 14.h + 0.f = 8 \\ 6.g + 14.b + 0.i = 6 \\ 15.a + 4.b + 24.c = 11 \\ 15.d + 4.e + 24.f = 12 \\ 15.g + 4.h + 24.i = 11 \end{array} \right\} + \left| \cdot 20 \right| \left| \cdot 11 \right|$$

Всичко  
 $\equiv 0 \pmod{26}$

$$\begin{array}{l}
 -\text{III} \\
 \left. \begin{array}{l}
 0a + 14b + 6c = 14 \\
 0d + 14e + 6f = 14 \\
 0g + 14h + 6i = 12 \\
 0a + 11b + 2c = 11 \\
 0d + 11e + 2f = 24 \\
 0g + 11h + 2i = 4 \\
 0a + 5b + 16c = 5 \\
 0d + 5e + 16f = 0 \\
 0g + 5h + 16i = 6
 \end{array} \right\} \cdot 8 \Rightarrow
 \end{array}$$

$$\begin{array}{l}
 -\text{III} \\
 \left. \begin{array}{l}
 0a + 1b + 22c = 1 \\
 0d + 1e + 22f = 24 \\
 0g + 1h + 22i = 18 \\
 0a + 11b + 2c = 11 \\
 0d + 11e + 2f = 24 \\
 0g + 11h + 2i = 4 \\
 0a + 5b + 16c = 5 \\
 0d + 5e + 16f = 0 \\
 0g + 5h + 16i = 6
 \end{array} \right\} \cdot 21
 \end{array}$$

$$\begin{array}{l}
 -\text{III} \\
 \left. \begin{array}{l}
 0a + 0b + 20c = 0 \\
 0d + 0e + 20f = 0 \\
 0g + 0h + 20i = 14 \\
 0a + 0b + 10c = 0 \\
 0d + 0e + 10f = 10 \\
 0g + 0h + 10i = 20
 \end{array} \right\} \cdot 10 \Rightarrow
 \end{array}$$

$\cdot 25$   
 $0g + 0h + 1i = 2$   
 $+ \text{ no (mod 26)}$   
 $+ \text{ no (mod 26)}$

$$\begin{array}{l}
 -\text{III} \\
 \left. \begin{array}{l}
 1a + 14b + 4c = 16 \\
 1d + 14e + 4f = 6 \\
 1g + 14h + 4i = 9 \\
 0a + 1b + 22c = 1 \\
 0d + 1e + 22f = 24 \\
 0g + 1h + 22i = 18 \\
 0a + 0b + 1c = 0 \\
 0d + 0e + 1f = 1 \\
 0g + 0h + 1i = 2
 \end{array} \right\} \cdot 22 \Rightarrow
 \end{array}$$

$\cdot 4$   
 $\cdot 22$

$$\begin{array}{l}
 -\text{III} \\
 \left. \begin{array}{l}
 1a + 14b + 0c = 16 \\
 1d + 14e + 0f = 2 \\
 1g + 14h + 0i = 1 \\
 0a + 1b + 0c = 1 \\
 0d + 1e + 0f = 2 \\
 0g + 1h + 0i = 0
 \end{array} \right\}
 \end{array}$$

Нарпайл нағызасынан күннөрдө  $K = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix}_{3 \times 3}$

zag. Да се шифрира блока  $101101$ , ако е използват недалажирана функция с  $m=2$ ,  $n=4$ ,  $h=4$  и трансформации  $f_1, \dots, f_4$ , зададени чрез:

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
$f_1$	00	10	11	11	01	01	01	10	10	01	10	11	00	00	00	00
$f_2$	10	11	00	11	10	11	01	01	01	11	10	00	10	11	01	00
$f_3$	10	00	00	01	01	10	10	11	01	11	00	10	11	10	11	01
$f_4$	11	10	01	10	00	10	00	00	10	01	00	10	01	11	10	11

P-e: Правим шифрирането на 4 стъпки:

Разделяне блока  $101101$  на  $A=10$  и  $B=1101$ .

$$B' = A \oplus f_1(B) = \underbrace{B}_{A'} = 10 \oplus f_1(1101) = 10 \oplus 00 = 10 \\ = \underbrace{101101}_{A \quad B} \rightarrow \underbrace{110110}_{A' \quad B'}$$

II

Полученото в II-та стъпка блок  $110110$  разделяме отнова на два блока:  $A=11$  и  $B=0110$ .

$$B' = 11 \oplus f_2(0110) = 11 \oplus 01 = 10 \\ = \underbrace{110110}_{A \quad B} \rightarrow \underbrace{011010}_{A' \quad B'}$$

III

Блокът, получен във III-та стъпка,  $011010$  разделяме на  $A=01$  и  $B=1010$ .

$$B' = 01 \oplus f_3(1010) = 01 \oplus 00 = 01 \\ = \underbrace{011010}_{A \quad B} \rightarrow \underbrace{101001}_{A' \quad B'}$$

IV

Почеден първи разделяне  $101001$  на  $A=10$  и  $B=1001$ .

$$B' = 10 \oplus f_4(1001) = 10 \oplus 01 = 11 \\ = \underbrace{101001}_{A \quad B} \rightarrow \underbrace{100111}_{A' \quad B'}$$

$\Rightarrow$  Получихме криптотеката 100111

8 заг. Дадена е крипто системата RSA с модул  $n = pq$  и шифрирана експонента  $e$ . Докажете, че образът на открийте текстове  $m$ , които са шифрирани в съде си, м.е. за които  $m^e \equiv m \pmod{n}$ , е  $(1 + \gcd(e-1, p-1))(1 + \gcd(e-1, q-1))$ .

Доказателство:

Нулатът е решение на загадката винаги.

Търсим решението на  $m^{e-1} \equiv 1 \pmod{n}$ .

Нека първо  $N$  да бъде просто число.

$\Rightarrow$  групата на останъците по модул  $N$  е циклическа

$\Rightarrow$  има генератор-число  $k$ ,  $k \in (0, N)$ : за всяко  $i \in [1; n-1]$

$$\exists x: k^x \equiv i \pmod{N}$$

$$\text{Вземаме } h = k^{\frac{n-1}{\gcd(e-1, n-1)}}$$

$$h = 1 \Leftrightarrow \gcd = 1 \Rightarrow 0 \text{ и } 1 \text{ са единствените решения}$$

$$\text{Нека } \gcd > 1 \Rightarrow y = h^{e-1} = h^{\frac{e-1}{\gcd(e-1, n-1)} \cdot (n-1)} = h^{(n-1)} \equiv 1 \pmod{n}$$

$$\Rightarrow \exists \text{ някои едно квадратично решение } y$$

Како поблизо на  $y$  на степен, чиято ползване даде други решения, докато не запознат да се побираят.

Число е доказано, че периодът на  $y$  е точно

$$g = \gcd(e-1, n-1). \text{ Освен това } y^g \equiv 1 \pmod{n}.$$

Да докажем, че  $g$  е наималкото число с такова свойство: Тъй като  $n$  е просто,  $h^{\frac{n-1}{g}} \equiv 1 \pmod{n}$

Он  $h$ -генератор  $\Rightarrow$  това не е изпълнено за никакъв  $l < n-1$

Ако има число  $g_1 < g$ :  $y^{g_1} \equiv 1 \pmod{n} \Rightarrow$  противоречие,

зашупто оттам също, че  $h^{\frac{(n-1)q}{g_1}} \equiv 1 \pmod{n}$ ,  
което е невъзможно.

$\Rightarrow$  Оттук възможният  $\gcd(e-1, n-1)$  решението +  
+ кулакови (онуе едно решение).

Задаване, че всеко друго решение трябва да е  
от вида  $\frac{n-1}{k}$ , където  $k/e$ , което не можем.

Обобщаване за две прости числа:

Знам, че има  $(1 + \gcd(e-1, p-1))$  р-е за  $p$  и

$(1 + \gcd(e-1, q-1))$  решения по модул  $q$ .

Нека те означим с  $tai$  и  $tbj$ .

За всички  $a_i, b_j$  мрсам  $m_{ij}$ :  $m_{ij} \equiv a_i \pmod{p}$   
и  $m_{ij} \equiv b_j \pmod{q}$

От Китайската Теорема за останалиците такова  
число има и то е единствено по модул  $n$ . То

се криптира в видът си и  $m_{ij}$  е уникатно.

Тогава има нюк  $((1 + \gcd(e-1, p-1)) \cdot (1 + \gcd(e-1, q-1)))$  р-е.

Нека докажем, че има нюк  $p$ -е:

Нека  $m_1$  да изпълнява условието, което не е  
сред нюките  $p$ -е. Тогава  $m_1 = c \cdot d$

$$m_1 \equiv c \pmod{p}$$

$$m_1 \equiv d \pmod{q}$$

Или  $\frac{c}{e} \equiv \frac{d}{e}$  трябва да не е средните нюки.

Нека  $\frac{c}{e} \equiv \frac{d}{e} \Rightarrow m = c + kp$

$$(c + kp)^e \equiv c + kp \pmod{pq}$$

$$(c + kp)^e \equiv c + kp \pmod{p}$$

$$c^e \equiv c \pmod{p}$$
 Промиворезе,

зашупто всички  $p$ -е на последното сравнение не са  
средните и изпълняват.

$\Rightarrow$  Има нюк  $p$ -е на мрсакото в условието.  $\square$

Задача. Найдем  $\beta$  через алгоритма Фохлиг-Хелмана  
 $\log_2 66 \in \mathbb{Z}_{101}^*$ .

Решение: Для упрощения пусть  $a=2$ ,  $\beta=66$ ,  $p=101$  — простое число.

Тогда  $x$ , такова что  $2^x \equiv 66 \pmod{101}$ .

$$1 \not\in \mathbb{Z}_p^* \Leftrightarrow p-1 = 100 = 2^2 \cdot 5^2 \Rightarrow m^{(1)} = a_0 + a_1 \cdot 2, g_0 = 2 \\ m^{(2)} = b_0 + b_1 \cdot 5, g_1 = 5$$

Задача  $g_0 = 2$ , находим  $a_0$  и  $a_1$ :

$$a_0: \quad d \frac{a_0 \cdot (p-1)}{g_0} \equiv \beta \frac{p-1}{g_0} \pmod{p}$$

$$d \frac{a_0 \cdot 100}{2} \equiv 66 \frac{100}{2} \pmod{101}$$

$$2^{50a_0} \equiv 66^{50} \pmod{101}$$

$$2^{50a_0} \pmod{101} = -1 \Rightarrow a_0 = 1$$

$$a_1: \quad d \frac{a_1 \cdot (p-1)}{g_1} \equiv \beta_1 \frac{p-1}{g_1}, \text{ тогда } \beta_1 = \beta \cdot d$$

$$\Rightarrow \beta_1 = 66 \cdot 2^{-1} \pmod{101} = 66 \cdot 51 \pmod{101} = 33$$

$$\Rightarrow 2^{a_1 \cdot \frac{100}{2}} \equiv 33^{\frac{100}{4}} \pmod{101}$$

$$2^{50a_1} \equiv 33^{25} \pmod{101}$$

$$2^{50a_1} \pmod{101} = -1 \Rightarrow a_1 = 1$$

$$\text{Тогда } a_0 = 1 \text{ и } a_1 = 1 \Rightarrow m^{(1)} = 1 + 1 \cdot 2 = 3 \pmod{2^2}$$

Задача  $g_1 = 5$ , найдем  $b_0$  и  $b_1$ :

$$b_0: \quad d \frac{b_0 \cdot \frac{100}{5}}{5} \equiv 66 \frac{100}{5} \pmod{101}$$

$$2^{20b_0} \pmod{101} = 87 \Rightarrow b_0 = 3$$

$$b_1: \text{Түзбө 101-кеңілдік} \quad \beta_2 = \beta \cdot d = 66 \cdot 2 \pmod{101} = 84, \\ \text{кейде } 2^{-3} \pmod{101} = (2^{-1})^3 \pmod{101} = 51^3 \pmod{101} = 38$$

$$(error) \quad 2^{b_1 \cdot \frac{100}{5}} \equiv 84^{\frac{100}{5^2}} \pmod{101}$$

$$2^{20b_1} \equiv 84^4 \pmod{101}$$

$$2^{20b_1} \pmod{101} = 95 \quad = \leftarrow \quad b_1 = 1$$

$$\text{Ом } b_0 = 3 \quad \text{и } b_1 = 1 = 8 \text{ м}^{(2)} = 3 + 1 \cdot 5 = 8 \pmod{5^2}$$

$$\text{Ом } m^{(1)} \text{ и } m^{(2)} \text{ нағызындағы c-нама: } \begin{cases} x = 3 \pmod{4} \\ x = 8 \pmod{25} \end{cases}$$

Ом Күтәйсіктерде мөндеу 3а оқынушынан:

$$x = 83 \pmod{100}$$

$$= \leftarrow \quad 66 = 2^{83} \pmod{101}$$

10 заг. Нека  $n = pq$ , където  $p$  и  $q$  са прости числа.  
 Узвестен е алгоритъм А, който ханура  
 решение на сравнението  $x^2 \equiv c \pmod{n}$  в  $F(n)$   
 отговор за всичко  $c$ , когато е квадрат на  
 елемент от  $Z_n$ . Да се покаже, че Е веро-  
 ятността алгоритъм А, който прави  $n$  в  
 (захвати брой)  $2(F(n) + 2 \log_2 n)$  отговори.

Доказателство:

Избиране се случайко число  $m$ ,  $m \in \{0, n\}$  и  
 решаване сравнението  $x^2 \equiv m^2 \pmod{n}$  в  $F(n)$   
 отговори, използвайки алгоритъм А. Алгоритъмът  
 има възможност да избере корен  $k$  с вероятност  $1/4$ .  
 Избиране следващите 4 възможности се случва всяка  
 от  $m$ мес. сума вероятност  $1/4$ :

- 1)  $k \equiv m \pmod{p}$ ,  $k \equiv m \pmod{q}$
- 2)  $k \equiv m \pmod{p}$ ,  $k \equiv -m \pmod{q}$
- 3)  $k \equiv -m \pmod{p}$ ,  $k \equiv m \pmod{q}$
- 4)  $k \equiv -m \pmod{p}$ ,  $k \equiv -m \pmod{q}$

В случаи 2)  $\gcd(k-m, n) = p$ , затова  $(k-m)$  е  
 делът на  $p$ , а  $(k+m)$  е делът на  $q \Rightarrow (k-m)$  не е  
 делът на  $q$ .

В случаи 3)  $\gcd(k-m, n) = q$ , затова  $(k-m)$  е  
 делът на  $q$ , а  $(k+m)$  е делът на  $p \Rightarrow (k-m)$  не е  
 делът на  $p$ .

В останалите случаи получаваме че  $pq$ , или 1.  
 От 2) и 3) случаи се изключва  $\gcd(k-m, n)$  с  
 общи делители с вероятност  $\frac{1}{2}$ .

За  $\gcd$  им тривъдим около  $2 \log_2 n$  отговори.

Този като вероятността за успех е  $\frac{1}{2}$ ,  
 захвати брой повторения е в  $2(F(n) + 2 \log_2 n)$  отговори.

11 здаг. Помредиумите A и B използват системата на Diffie и Hellman, използвайки дискретен логоритъм, за да уговорят тайни клюци. Те използват крайното поле  $GF(2^{10}) = F_2[X] / (x^{10} + x^3 + 1)$ . Помредиумът B избира клюц  $C_B = 0100010100$ , който представлява елемента  $x + x^5 + x^7$  от  $GF(2^{10}) = F_2[X] / (x^{10} + x^3 + 1)$ . Ако тайният клюц на A е  $x_A = 2$ , какъв е клюцът, който A и B ще използват при комуникация помежду си?

P-e:

В условието са загадана еднакъв еднакъв публичен клюц (куза  $\{C_B\}$ ) и другият тайни клюци ( $x_A$ ). От системата на Diffie и Hellman  $\Rightarrow$  трябва да пресметнем  $C_B^{x_A} \text{ mod } p$  в зададеното поле.

Преминаване  $(x + x^5 + x^7)^2$  в  $GF(2^{10})$

$$\begin{aligned}
 & (x + x^5 + x^7)(x + x^5 + x^7) = \\
 & = x^2 + x^6 + x^8 + x^6 + x^{10} + \underbrace{x^{10}}_{x^{10} \cdot x^2} + x^8 + \underbrace{x^{12}}_{x^{10} \cdot x^2} + x^{12} + \underbrace{x^{14}}_{x^{10} \cdot x^4} = \\
 & \text{Заместване } x^{10} \text{ с } x^3 + 1: \\
 & = x^2 + x^6 + x^8 + x^6 + x^3 + 1 + x^2(x^3 + 1) + x^8 + x^2(x^3 + 1) + x^4(x^3 + 1) = \\
 & = x^2 + x^6 + x^8 + x^6 + x^3 + 1 + x^5 + x^2 + x^8 + x^5 + x^2 + x^7 + x^4 =
 \end{aligned}$$

погрешдане 2е:

$$\begin{aligned}
 & = 1 + 3x^2 + x^3 + x^4 + \underbrace{2x^5}_{0} + \underbrace{2x^6}_{0} + x^7 + \underbrace{2x^8}_{0} = \\
 & \text{съобразяване, че } 2x^n = 0 \text{ при } n > 4 \\
 & = x^2 + x^3 + x^4 + x^7
 \end{aligned}$$

Получение:

$$\frac{1}{x^0} \frac{0}{x^1} \frac{1}{x^2} \frac{1}{x^3} \frac{1}{x^4} \frac{0}{x^5} \frac{0}{x^6} \frac{1}{x^7} \frac{0}{x^8} \frac{0}{x^9}$$

12 заг. Дадени са простото число  $p=101$ , прimitивен елемент  $d=2$  и  $x_u=43$ . Използвайки системата на ElGamal, напишете единичен подпис за обобщенето  $m=26$ . Търсете единичното на генериране подпис.

P-e: Ои утвърдявамо:

- $p=101$  - просто число
- $d=2$  - прimitивен елемент
- $x_u=43$  - частен ключ
- $m=26$  - обобщение

Използвайки системата на ElGamal:

- Генериране на ключове:

Изчисляване  $a^{x_u} \pmod{p} = 2^{43} \pmod{101} = 86 \Rightarrow$   
 =  
 Използване публичният ключ:  $(101, 2, 86)$   
 частен ключ:  $43$

- Избиране  $1 < k < p-1$ . Нека  $k=47$ .

Изчисляваме  $a = d^k \pmod{p} = 2^{47} \pmod{101} = 63$

$b = s^k \cdot m \pmod{p} = 86^{47} \cdot 26 \pmod{101} = 92$

Получаване двойката  $(a, b) = (63, 92)$  - цифров текст

Нека сега направим проверка като дешифрираме  $(63, 92)$  с частния ключ  $x_u=43$ . Тръбва да получим обобщенето  $m=26$ .

Изчисляване  $m$  по формулата:

$$m = b (a^{x_u})^{-1} \pmod{p} = 92 (63^{43})^{-1} \pmod{101} = \\ = 92 \cdot 42 \pmod{101} = 26$$

Получихме оригиналното обобщение  $m$ .

Така напишахме единичен подпис  $(63, 92)$  за  $m=26$ .

13 задача. Наищеме корень квадратного уравнения на Pohlig - Hellman  $\log_3 135$  в группе  $\mathbb{Z}_{353}^*$ .

Решение: Определим  $a = 3, \beta = 135, p = 353$  - параметры.

Тогда  $x$ , такова что  $3^x \equiv 135 \pmod{353}$ .  
 $|Z_p^*| = p-1 = 352 = 2^5 \cdot 11 = \gamma m^{(1)} = a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + a_3 \cdot 2^3 + a_4 \cdot 2^4$   
 $g_0 = 2, g_1 = 11$        $m^{(2)} = b_0 \cdot 11^0 = b_0$

Задача:  $g_0 = 2$ , находим  $a_0, a_1, a_2, a_3$  и  $a_4$ :

$$a_0: 3^{146a_0} \equiv 135^{146} \pmod{353}$$

$$3^{146a_0} \pmod{353} = 1 \Rightarrow a_0 = 0$$

$$a_1: \beta_1 = 135 \cdot 3^{-0} \pmod{353} = 135$$

$$\Rightarrow 3^{146a_1} \equiv 135^{\frac{352}{2^5}} \pmod{353}$$

$$3^{146a_1} \equiv 135^{88} \pmod{353}$$

$$3^{146a_1} \pmod{353} = 1 \Rightarrow a_1 = 0$$

$$a_2: \beta_2 = \beta_1 \cdot d^{-1} = 135 \cdot 3^{-0} \pmod{353} = 135$$

$$\Rightarrow 3^{146a_2} \equiv 135^{\frac{352}{2^3}} \pmod{353}$$

$$3^{146a_2} \equiv 135^{44} \pmod{353}$$

$$3^{146a_2} \pmod{353} = 1 \Rightarrow a_2 = 0$$

$$a_3: \beta_3 = \beta_2 \cdot d^{-1} = 135 \cdot 3^{-0} \pmod{353} = 135$$

$$3^{146a_3} \equiv 135^{22} \pmod{353}$$

$$3^{146a_3} \pmod{353} = -1 \Rightarrow a_3 = 1$$

$$\text{ax: } \beta_4 = \beta_3 \cdot \alpha \stackrel{-(\alpha_3)}{=} 135 \cdot 3^{-1} \cdot 2^3 \pmod{353} = 135 \cdot 118^8 \pmod{353} = \\ = 16$$

$$3^{146 \text{ au}} \equiv 16^{11} \pmod{353}$$

$$3^{146 \text{ au}} \pmod{353} = -1 \Rightarrow \text{ax} = 1$$

$$\Rightarrow m^{(1)} = 0 + 0 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 = 8 + 16 = 24 \pmod{2^5}$$

3a  $g_1 = 11$ , находим  $b_0$ :

$$3^{\frac{352}{11} b_0} \equiv 135^{\frac{352}{11}} \pmod{353}$$

$$3^{32 b_0} \equiv 135^{32} \pmod{353}$$

$$3^{32 b_0} \pmod{353} = 337 \Rightarrow b_0 = 4$$

$$\Rightarrow m^{(0)} = 4 \pmod{11}$$

Ом  $m^{(1)}$  и  $m^{(2)}$  нонъяване сүзмемама:

$x = 24 \pmod{32}$
$x = 4 \pmod{11}$

Ом Күтайскама меопека 3a оствамзегүме:

$$x = 312 \pmod{352}$$

$$\Rightarrow 135 = 3^{312} \pmod{353}$$

14 заг. Дадени са сързък карасъвашщ вектор  
 $a = (2, 3, 7, 13, 27, 53, 106, 213, 425, 851)$ ,  
 модулът  $m = 1529$  и  $t = 64$ . Шифрирайте  
 обединението LONDON. Използвайте кодиращо:

P-e:

Използване криптоалгоритма на Merkle-Hellman, основаваща се на задачата за разшифруване. Кеха първо намерих публичният ключ  $b$  чрез умножаване на всеки елемент в  $a$  с  $t$  по модул  $m$ :

$$(2 \cdot t) \pmod{m} = (2 \cdot 64) \pmod{1529} = 128$$

$$(3 \cdot t) \pmod{m} = (3 \cdot 64) \pmod{1529} = 192$$

$$(7 \cdot t) \pmod{m} = (7 \cdot 64) \pmod{1529} = 448$$

$$(13 \cdot 64) \pmod{1529} = 832$$

$$(27 \cdot 64) \pmod{1529} = 199$$

$$(53 \cdot 64) \pmod{1529} = 334$$

$$(106 \cdot 64) \pmod{1529} = 668$$

$$(213 \cdot 64) \pmod{1529} = 1400$$

$$(425 \cdot 64) \pmod{1529} = 1207$$

$$(851 \cdot 64) \pmod{1529} = 949$$

$\Rightarrow$  Генериране б-ра  $b = (128, 192, 448, 832, 199,$   
 $334, 668, 1400, 1207, 949)$

Сега кеха шифриране откритият текст LONDON като първо ѝ разделим на двойки:

$$LO = 10001 \quad 10100_2$$

$$ND = 10011 \quad 00111_2$$

$$ON = 10100 \quad 10011_2$$

A	00011
B	00101
C	00110
D	00111
E	01001
F	01010
G	01011
H	01100
I	01101
J	01110
K	01111
L	10001
M	10010
N	10011
O	10100
P	10101
Q	10110
R	10111
S	11000
T	11001
U	11010
V	11011
W	11100
X	11101
Y	11110
Z	11111

Взимане на първата двойка -  $LD = 10001 \ 10100_2$ .

Умножаване всеки бит по съответното зерно в B  
и събиране на резултата:

$$1.128 + 0.192 + 0.448 + 0.832 + 1.199 + 1.334 + 0.668 + 1.1400 + \\ 0.1204 + 0.949 = 128 + 199 + 334 + 1400 = \underline{2061}$$

Академичен постъпване с бинарна и третична  
двойки:

$$ND = 10011 \ 00111 \\ = 1.128 + 1.832 + 1.199 + 1.1400 + 1.1204 + 1.949 = \underline{4415}$$

$$DN = 10100 \ 10011 \\ = 1.128 + 1.448 + 1.334 + 1.1204 + 1.949 = \underline{3066}$$

Така наричане Криптотекста: 2061 4415 3066

16 заг. Нека  $n = pq$ , където  $p$  и  $q$  са прости числа. Нашерете корените на уравнението  $x^2 - ax + n = 0$ , където  $a = n + 1 - \varphi(n)$ . Нашерете между корени в една връзка и обяснете, как може да се намери  $p$  и  $q$  с помощта на прост алгоритъм за намиране на квадратни корени. Нашерете разлагането на  $n$  при  $n = 15\ 049$ ,  $\varphi(n) = 14\ 800$ .

Решение:

$$\begin{aligned} x^2 - ax + n &= 0 \\ x^2 - (n+1-\varphi(n))x + n &= 0 \end{aligned}$$

Както възприем бирегбиг, че  $n = pq$ , а  $\varphi(n) = (p-1)(q-1)$ , то получаваме:

$$\begin{aligned} a_1 &= 1 & b &= -(n+1-(p-1)(q-1)) \\ D &= (pq + 1 - (pq - p - q + 1))^2 - 4pq = \\ &= (pq + 1 - pq + p + q - 1)^2 - 4pq = \\ &= (p + q)^2 - 4pq = \\ &= p^2 + 2pq + q^2 - 4pq = \\ &= p^2 - 2pq + q^2 = \\ &= (p - q)^2 \end{aligned}$$

$$x_{1,2} = \frac{-b \pm \sqrt{D}}{2a_1} = \frac{p+q \pm (p-q)}{2} = \begin{cases} x_1 = \frac{p+q+p-q}{2} = \frac{2p}{2} = p \\ x_2 = \frac{p+q-p+q}{2} = \frac{2q}{2} = q \end{cases}$$

$$= \begin{cases} x_1 = p, \\ x_2 = q \end{cases}$$

Три така зададените кофициенти на квадратното уравнение ( $a_1 = 1$ ,  $b = -(n+1-\varphi(n))$ ,  $c = n$ ) лесно може да намерим  $p$  и  $q$  чрез решаване на у-ето.

Нека разгледим  $n = 15\ 049$ , како  $\ell(n) = 14\ 800$ .  
Задесаваше ће кв. у-е:

$$\begin{aligned}x^2 - \underbrace{(15\ 049 + 1 - 14\ 800)}_{250}x + 15\ 049 &= 0 \\x^2 - 250x + 15\ 049 &= 0 \\D = 250^2 - 4 \cdot 15\ 049 &= 62\ 500 - 60\ 196 = 2304 = 48^2\end{aligned}$$

$$x_{1,2} = \frac{250 \pm 48}{2} \Rightarrow x_1 = 298/2 = 149 = p \\x_2 = 202/2 = 101 = q$$

=> Каперуме  $p = 149$ ,  $q = 101$

18 заг. Криптоанализ на Окамото - Училен:

Да се докаже, че дешифрирането е дефинирано коректно (т.е. че  $L(c^{p-1} \pmod{p^2})$  и  $L(g^{p-1} \pmod{p^2})$  са константа елиминират  $\mathbb{Z}_p^*$ ) и че то наистина взема обекта от началния текст.

Доказателство за коректност:

Нека разгледаме дешифрирането:

Криптираното обединение с може да се дешифрира с гостинския кюс  $(p, q)$  както следва:

1) Изчисляване  $a = \frac{(c^{p-1} \pmod{p^2}) - 1}{p}$

2) Изчисляване  $b = \frac{(g^{p-1} \pmod{p^2}) - 1}{p}$

$a$  и  $b$  ще бъдат цели числа.

3) Използвайки Раширен евклидов алгоритъм, изчисляване  $b' = b^{-1} \pmod{p}$

4) Изчисляване  $m = ab' \pmod{p}$

$m$  = дешифрирането на  $c$

Искаме да докажем, че  $ab' \pmod{p}$  от 4-та стъпка на дешифрирането е равно на оригиналното обединение  $m$ . Ние имаме:

$$(g^m h^r)^{p-1} \equiv (g^m g^{nr})^{p-1} \equiv (g^{p-1})^m g^{p(p-1)r} p \equiv (g^{p-1})^m \pmod{p^2}$$

Така че да се взематови  $m$  трябва да вземем дискретен логаритъм с основа  $g^{p-1}$ .

Групата  $(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p^2\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$

Ние определяме  $3$ , което е подгрупа на  $\mathbb{Z}/p^2\mathbb{Z}^*$  и керовата множеството е  $p-1$

$$H = \{x : x^{p-1} \pmod{p^2} = 1 + rp, 0 < r < p\}$$

За всеки елемент  $x \in (\mathbb{Z}/p^2\mathbb{Z})^*$ , ние имаме

$$x^{cmp-1} \pmod{cmp^2} \in H \text{ и } cm \pmod{p} \text{ раздели } x^{cmp-1} - 1$$

$L(x) = \frac{x-1}{p}$  требва да се разглежда като полином

от циклическа група  $\mathbb{Z}/p\mathbb{Z}$  като групата  $\mathbb{Z}/p\mathbb{Z}$  е лесно да се провери, че  $L(ab) = L(a) + L(b)$  и че  $L$  е изоморфизъм между тези две групи. Както е в случаите с обикновените полиноми,  $L(x)/L(g)$  в известния случаи е полином на  $x$  с основа  $g$ .

$$\frac{L((g^{p-1})^m)}{L(g^{p-1})} = m \pmod p, \text{ където } m - \text{ оригиналният текст}$$

□

19 заг. Нека гъве погрешка, да речем Алис и Боб, използват RSA с един и същ модул  $n$ , но с различни (публични) шифриращи експоненти  $e_1$  и  $e_2$ .

a) Докажете, че Алис може да дешифрира обобщените, изпратени до Боб.

Дбо: Нека Алис:  $(e_1, d_1)$  - знае  $e_1, d_1$

Боб:  $(e_2, d_2)$  - знае  $e_2, d_2$

модул  $n$  и знае и от Алис, и от Боб

$n = p \cdot q$ ,  $p, q$  - прости числа, не се знаят

Знанието на  $d_1$  от Алис и позволява разлагането на  $n$ .

$$\exists k: e_1 d_1 = 1 + k \cdot \varphi(n)$$

Потенце Алис знае  $e_1$  и  $d_1$ , то тя може да намери  $k$ .

Понастоящем  $e_1 d_1 - 1 = 2^s \cdot t$  като  $t$  е кратно

$$a^{e_1 d_1 - 1} = a^{2^s \cdot t} = 1 \pmod{n}$$

$$\text{за } \forall a: (a, n) = 1$$

Ако  $\exists i \in [1, s]$ , за което  $a^{2^{i-1} \cdot t} \not\equiv \pm 1 \pmod{n}$   
 $[1, s]$  - инт. от ест. числа и  $a^{2^i \cdot t} \equiv 1 \pmod{n}$ ,  
 то можем да разложим  $n$

$$a^{2^i \cdot t} - 1 = (a^{2^{i-1} \cdot t} - 1) \cdot (a^{2^{i-1} \cdot t} + 1)$$

Лявата страна е делима на  $n \Rightarrow$  и дясната е делими на  $n$ . Обаче  $n$  не делите като първите, като вторите множител.  $\Rightarrow p$  не делите едните множители, а  $q$  - другите. Този  $Alice$  може да определи какъм прости числа ( $p$  или  $q$ ), трябва да:  $HOD(a^{2^{i-1} \cdot t} - 1, n)$

Како  $\text{KOD}(a^{2^{i-1} \cdot t} - 1, n)$  е кемривилен генератор на  $n$ .

Приези  $a$ , за които не даватиме го разлагане, м.е. за такова  $i \in [1, S]$ , за което

$$\begin{aligned} a^{2^{i-1} \cdot t} &\not\equiv \pm 1 \pmod{n} \\ a^{2^i \cdot t} &\equiv 1 \pmod{n} \end{aligned}$$

и числата, за които:

$$1) a^t \equiv 1 \pmod{n} \quad \text{или} \quad 2) a^{2^j \cdot t} \equiv -1 \pmod{n}$$

за всекое  $j \in [1, S]$

Може да се докаже, че браят на мероз  $a$  не  
касава при поповицата от всички останци  $\pmod{n}$ .  
Означаванието брой операции е две. Което доказва,  
че може да дешифрира обобщения, изпратени  
го Бод.  $\square$

5) Докажете, че криптографията може да дешифрира обобщение, изпратено едновременно от Алис и Бод, при условие, че  $\gcd(e_1, e_2) = 1$ .

Доказателство: Нека откъде Алис:  $(e_1, d_1)$

Бод:  $(e_2, d_2)$

$$n = p \cdot q$$

Нека обобщението е  $m$

$$\Rightarrow c_1 = m^{e_1} \pmod{n}$$

$$c_2 = m^{e_2} \pmod{n}$$

} криптомесажи

Нека криптосистемът е  $E$ . Той приема

$$c_1 \text{ и } c_2 \text{ и знае } n.$$

$E$  изчислява:

- $t_1 = e_1^{-1} \pmod{e_2}$ ,  $e_1$  и  $e_2$  - нубири

$$t_2 = \frac{t_1 \cdot e_1 - 1}{e_2} \Rightarrow e_2 t_2 + 1 = t_1 e_1$$

$$\underbrace{c_1 \cdot c_2}_{\substack{t_1 \\ t_2}} \equiv m^{e_1 t_1} \cdot m^{-e_2 t_2} \pmod{n},$$

$t_1, t_2$  - пресмятане  
 $c_1, c_2$  - приемане

$$m^{e_2 t_2 + 1} \cdot m^{-e_2 t_2} \pmod{n},$$

$$\Leftrightarrow \underbrace{m}_{\text{обобщението}}$$

$\Rightarrow E$  може да получи обобщението.  $\square$

20 заг. Криптосистемата на Рабин:

a) Как можем да прешифтуваме ефективно квадратни корени в  $\mathbb{Z}_n$ ?

Ако изберем  $B=0$ , шифрираме ќе биде:

$$E_K(x) = x^2 \pmod{n} = y$$

А дешифрираме ќе биде:

$$D_K(y) = \sqrt{\frac{B^2}{4} + y} - \frac{B}{2} = \sqrt{y} = \sqrt{x^2 \pmod{n}}$$

=> При избор  $B=0$  се прешифтува ефективно квадратни корени в  $\mathbb{Z}_n$ .

б) Дешифрираме в така описаната с-ма не е определено еднозначно. Покажете, че то може да биде кратично еднозначно како добавим известен излишок в откритиятеком.

Име имаме 4 решения:

остатък  
↑

$$au + bv \in QR \pmod{p_u}, au + bv \in QR \pmod{q_u}$$

$$au - bv \in QR \pmod{p_u}, au - bv \in NQR \pmod{q_u}$$

$$-au + bv \in NQR \pmod{p_u}, -au + bv \in QR \pmod{q_u}$$

$$-au - bv \in NQR \pmod{p_u}, -au - bv \in NQR \pmod{q_u}$$

↓  
излишък

=> Символ на лкоди за първия и за последния корен ще е 1:  $\left( \frac{ua+vb}{p_u q_u} \right) = \left( \frac{-ua-vb}{p_u q_u} \right) = 1$

=> Ул. означава уникатно решение  $m'$ :

$$\left( \frac{m'}{p_u} \right) = 1, \quad 0 < m' < \frac{p_u}{2}$$

Символ на лкоди допълната половина на измервания излишък

b) Докажете, че ако разполагате с алгоритъм за разлагане на  $n$  на прости илюминанци, то можете ефективно да разделяте системата на Рабин.

Доказахме в 10-та задача следната Теорема:  
Криптосистема на Рабин  $\Leftrightarrow$  Задача за разлагане на прости илюминанци

$\Rightarrow$  Ако можете да разложите  $n$  на прости илюминанци, то можете и да решите съвържанието  $x^2 \equiv c \pmod{n}$   $\Rightarrow$  можете и да разделяте с-система на Рабин.

v) Докажете, че системата на Рабин може да бъде разбита чрез атака с избрани криптомесажи (chosen ciphertext attack).

I) Избиране на число  $x$ , генериране криптомесажа  $c = x \cdot x \pmod{n}$

II) Генериране криптографски хеш  $h \neq \pm x$ , такова че  $h \cdot h = c \pmod{n}$ . Това  $h$  е третището квадратен корен на  $c$ .

III)  $-h$  е четвъртият квадратен корен на  $c$ .

Рабин показва, че ако хашерите дава корен  $x$  и  $h$ , като  $h \neq \pm x \pmod{n}$ , тогава илюминанци можете да изчислите  $p = q$ , затворто  $\gcd(x-h, n) = p$  или  $\gcd(x+h, n) = q$ .  $\square$

22 заг. Нека  $C$  е двоичен нуелект  $[9,4,4]$ -код с пораждаща матрица

$$g = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}_{4 \times 9}$$

$\uparrow \uparrow \uparrow \uparrow \uparrow \uparrow \uparrow \uparrow \uparrow$   
 $u_1 \ u_2 \ u_3 \ u_4 \ u_5 \ u_6 \ u_7 \ u_8 \ D$

Да се опише структурата на достъп, реализирана от този код. (Достъпът е да се опишат минималните авторизирани способства).

P-e: Om  $g_{4 \times 9} \Rightarrow H_{(9-4) \times 9} = H_{5 \times 9}$

$$H = \left( \begin{array}{ccccccccc} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{array} \right)_{5 \times 9} \rightarrow \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{matrix}$$

$E$

Om Теоремата  $\Rightarrow$  структурата на достъп се задава от минималните авторизирани способства  $\delta$  думи ког  $\Rightarrow$  търсит минималните думи. Първо нека напиша всички думи:

кулевата:	0 0 0 0 0 0 0 0 0
1-нзрви peg:	0 1 1 0 1 0 0 0 0
2-втори peg:	1 0 0 1 0 1 0 0 0
3-трети peg:	1 1 0 0 0 0 1 0 0
4-четвърти peg:	1 0 1 1 0 0 0 1 0
5-пети peg:	0 1 1 1 0 0 0 0 1

- Излизане



↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

10 фраз:

	U1	U2	U3	U4	U5	U6	U7	U8	D
1-fu u 2-pu peg:	1	1	1	1	1	1	0	0	0
1-fu u 3-mu peg:	1	0	1	0	1	0	1	0	0
1-fu u 4-mu peg:	1	1	0	1	1	0	0	1	0
1-fu u 5-mu peg:	0	0	0	1	1	0	0	0	① - u4u5
2-pu u 3-mu peg:	0	1	0	1	0	1	1	0	0
2-pu u 4-mu peg:	0	0	1	0	0	1	0	1	0
2-pu u 5-mu peg:	1	1	1	0	0	1	0	0	① - u1u2u3u6
3-mu u 4-mu peg:	0	1	1	1	0	0	1	1	0
3-mu u 5-mu peg:	1	0	1	1	0	0	1	0	① - u1u3u4u7
4-mu u 5-mu peg:	1	1	0	0	0	0	0	1	① - u1u2u8

10 фраз:

1-fu, 2-pu u 3-mu peg:	0	0	1	1	1	1	1	0	
1-fu, 3-mu u 4-mu peg:	0	0	0	1	1	0	0	1	0
1-fu, 3-mu u 5-mu peg:	1	1	0	1	1	0	1	0	① - u1u2u4u5u7
1-fu, 2-pu u 4-mu peg:	0	1	0	0	1	1	0	1	0
1-fu, 2-pu u 5-mu peg:	1	0	0	0	1	1	0	0	① - u4u5u6
1-fu, 4-mu u 5-mu peg:	1	0	1	0	1	0	0	1	① - u1u3u5u8
2-pu, 3-mu u 4-mu peg:	1	1	1	0	0	1	1	1	0
2-pu, 3-mu u 5-mu peg:	0	0	1	0	0	1	1	0	① - u3u6u7
2-pu, 4-mu u 5-mu peg:	0	1	0	1	0	1	0	1	① - u2u4u6u8
3-mu, 4-mu u 5-mu peg:	0	0	0	0	0	1	1	1	① - u4u8

5 фраз:

1fu, 2pu, 3mu, 4mu peg:	1	0	0	0	1	1	1	1	0
1fu, 2pu, 3mu, 5mu peg:	0	1	0	0	1	0	0	0	① - u2u5
2pu, 3mu, 4mu, 5mu peg:	1	0	0	1	0	1	1	1	① - u1u4u6u7u8
1fu, 2pu, 4mu, 5mu peg:	0	0	1	1	1	1	0	1	① - u3u4u5u6u8
1fu, 3mu, 4mu, 5mu peg:	0	1	1	0	1	0	1	1	① - u1u3u5u7u8

Всички: 1 1 1 1 1 1 1 1 1 - u1u3u4u5u6u7u8

Он всички 32 фраз, трябва съм думите, завръща-  
щи на 1, заместо последната координата е  
асоциирана с дума D.

Напирайте минималните думи, като съмврпие  
тези, които се покриват:

14U5                    17U8  
И12U3U5U4       И14U6U7U8  
И12U3U5U6U7U8   И2U3U5U7U8  
И3U4U5U6U8

Направе погодование:

$$\Gamma_{\min} = \{ \text{И2U3U4}, \text{И4U5}, \text{И12U3U6}, \text{И1U3U4U7}, \text{И1U2U8}, \\ \text{И1U5U6}, \text{И1U3U5U8}, \text{И3U6U7}, \text{И2U4U6U8}, \text{И7U8}, \\ \text{И2U5} \}$$

$$\Gamma_{\min} = \{ \text{И2U5}, \text{И4U5}, \text{И7U8}, \text{И12U8}, \text{И1U5U6}, \text{И2U3U4}, \\ \text{И3U6U7}, \text{И1U3U3U6}, \text{И1U3U4U7}, \text{И1U3U5U8}, \\ \text{И2U4U6U8} \}$$