Галя Георгиева Додова 45 616

Задачи по Криптография

Зад. THEWINTEROFDRSCONTENT plain text

WGNZDZWNISOSBHGRREAZWNTW crypted

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

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

TE TN

WN WT

RCCVTOGRAPGYCAZI AS

RCCPIALROL

EINQANIZSPECTS OF TO

DASY WORLDZ

2 зад. $K = K^{-1}$ Броят на матриците от ред 2 над $\mathbb{Z}_{26}$: $K = K^{-1}$.

Реш. $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d \in \mathbb{Z}_{26}\right\}$

$$K^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$$

$$K = K^{-1} \Leftrightarrow \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$$

$a = \frac{d}{ad-bc}$ $b = \frac{-b}{ad-bc}$ $c = \frac{-c}{ad-bc}$ $d = \frac{a}{ad-bc}$

$\Rightarrow ad-bc = 1$ $ad-bc = \frac{(-b)^{-1}}{b^{-1}}$ $ad-bc = \frac{-c^{-1}}{c^{-1}}$ $ad-bc = \frac{a}{d}$

$\Rightarrow ad-bc = -1 \Rightarrow \frac{a}{d} = \frac{d}{a} = -1 \Rightarrow d = -a$

$\left\{\begin{pmatrix} a & b \\ c & -a \end{pmatrix} \middle| a,b,c \in \mathbb{Z}_{26}\right\}$ и $-a^2-bc = -1$ $-(a^2+bc) = -1$

$\Rightarrow a^2+bc = 1$

Общо матриците от този вид са 26^3. $17\,576$. Остава да намерим тези с $\det = -1$.

$a^2+bc = 1 \Rightarrow a^2 = 1-bc$ $bc = 1-a^2 = (1-a)(1+a)$

$\begin{pmatrix} a & b \\ c & -a \end{pmatrix}^{-1} = -1\begin{pmatrix} -a & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ $bc = (1-a)(a+1)$ $b = \frac{1-a^2}{c}$

~~Ако $a = b = c$, $\det = 0$~~ ~~$\neq -a$~~ $\frac{1-a^2}{c} \in$ ~~$\mathbb{Z}$~~

Аналогично $\frac{1-a^2}{b} \in \mathbb{Z}$

б.о.о.

Нека фикс. a. Знаем, че за него $\exists$ 26 възможности.

Тогава за b и c $\exists$ 14 възможности за всяко.

Общо $26.14.14 = 5096$ матрици

3zag. CONVERSATION SQZHWSSWDYKRP

2x2 matrix

CONV → SQZH

$$\begin{pmatrix} 2 & 14 \\ 13 & 21 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} 18 & 16 \\ 25 & 7 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} 2 & 14 \\ 13 & 21 \end{pmatrix}^{-1}\begin{pmatrix} 18 & 16 \\ 25 & 7 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} -\frac{1}{5} & -\frac{14}{10} \\ \frac{46}{35} & \frac{24}{70} \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} -\frac{1}{5} & -\frac{14}{10} \\ \frac{20}{1} & \end{pmatrix}$$

3x3 MATRIX

CONVERSAT → SQZHWSSWD

$$\begin{pmatrix} 2 & 14 & 13 \\ 21 & 4 & 14 \\ 18 & 0 & 19 \end{pmatrix}\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}=\begin{pmatrix} 18 & 16 & 25 \\ 7 & 20 & 18 \\ 18 & 20 & 3 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}=\begin{pmatrix} 2 & 14 & 13 \\ 21 & 4 & 14 \\ 18 & 0 & 19 \end{pmatrix}^{-1}\begin{pmatrix} 18 & 16 & 25 \\ 7 & 20 & 18 \\ 18 & 20 & 3 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}=\frac{1}{68}\begin{pmatrix} 24 & 6 & 30 \\ -32 & 3 & -18 \\ 15 & 14 & -5 \\ 20 & -18 & 0 \end{pmatrix}\begin{pmatrix} 18 & 16 & 25 \\ 7 & 20 & 18 \\ 18 & 20 & 3 \end{pmatrix}=\begin{pmatrix} -4 & 1 & -5 \\ 15 & 14 & -5 \\ 20 & -18 & 0 \end{pmatrix}\begin{pmatrix} 18 & 16 & 25 \\ 7 & 20 & 18 \\ 18 & 20 & 3 \end{pmatrix}=$$

$$=\begin{pmatrix} -155 & -144 & -24 \\ 248 & 420 & 612 \\ 234 & -40 & 176 \end{pmatrix} \pmod{26}=\begin{pmatrix} -25 & -14 & -19 \\ 18 & 4 & 14 \\ 0 & -14 & 20 \end{pmatrix}=\begin{pmatrix} 1 & 12 & 7 \\ 18 & 4 & 14 \\ 0 & 12 & 20 \end{pmatrix}$$

6 зад. $n = 899$ $e = 611$ n-прости множители, преместване d

Да се дешифрира 106 680 303 за $\forall xy : d(x) + 26d(y)$, където

$d(A) = 0$ $d(B) = 0$ $d(C) = 2 \dots d(X) = 23$ $d(Y) = 24$ $d(Z) = 25$

7 зад. $2^{n-1} \equiv 1 \pmod n$ $341 = 11.31$ $n_0 = 341$ $n_i = 2^{n_{i-1}} - 1$

Индукция: Доказ. е вярно за n_{i-1} т.е. $2^{n_{i-1}-1} \equiv 1 \bmod n_{i-1}$

Ще док. за n_i. Нека $n_{i-1} = st$ $s, t > 1$ $s, t \in \mathbb{N} \Rightarrow n_i = 2^{st} - 1$, което се дели на $2^n - 1$ $2^{n_i - 1} = 2^{n_{i-1} - 1 - 1} = 2^{2(2^{n_{i-1}} - 1)} = 2^{2k n_{i-1}} = (2^{n_{i-1}})^{2k} =$

$= (n_i + 1)^{2k} \equiv 1 \pmod{n_i} \Rightarrow 2^{n_{i-1}-1} - 1 = k n_{i-1}$ ✓

8 зад. Да се док. ее.

а) Число на Кармайкъл е свободно от квадрати