

Гала Георгиева Догова 45 616

Загаз по криптография

130g THE WIN TE RO FOWR DI SC ON TE NT plain text
 ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
 WG NZ DZ WN IS OS BH GR RE AZ WN TW crypted

EB QX ZL HD LK IV QG OM
 IC VZ XP TS KG HZ VD FL
 AL EB VB DO SG SF
 CM IC ZS CN DK AR
 ZR AN DA MO LB SE EL SO
 VU PF BS LE PC CH OF CR
 ZL KD CO ZF GS IN
 XP GS OE YU KD TH

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

EB QX ZL HD LK IV QS OM
 CV TO AP CAZI
 RC GR GY
 AL EB VB DO SG SF
 AS RC CP IALR AOL
 ZR AN DA MO LB SE EL SO ZL
 EI ANQAIN IZ SPECTS OF TO
 KD CO ZF GS IN EC OF
 DA SY WORLDZ

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

~~NTW~~ FOS NTW*E
 crypt decrypt
 T → W → N
 W → Z → T
 N → T, Z → E
 FOS
 middle
 D G H I R
 NTW*E or g/t/g
 D G H I R h/w/h
 Z*

RCCVTOGRAPGYCAZI AS
 RCCPIALROL
 EINQAINIZSPECTS OF TO
 DASY WORLDZ

NTWZE
 D G H I R
 AN FOS
 IZ ETN
 SECTS
 AS RC **IALROL
 C
 NTWZE
 AL FOS
 D G H I R
 ~ *B
 XXXXX

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

$$\text{Perm. } \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}_{26} \right\}$$

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

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

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

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

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

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

$$\Rightarrow a^2 + bc = 1$$

Общо матриците от този вид са 26^3 , Остава да намерим тези с $\det = -1$.
14 576

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

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

$$\text{Ако } a = b = c, \det = 0$$

$$\text{Ако } a = -a \quad \frac{1-a^2}{c} \in \mathbb{Z}$$

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

Б.О.О.

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

Тогав за b и c \exists 14 възможности за всяко.

Общо $26 \cdot 14 \cdot 14 = 5096$ матрици

33ag. CONVERSATION

SQZHUSSUDYK&P

2x2 matrix

CONV \rightarrow SQZH

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

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

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -\frac{1}{5} & -\frac{14}{10} \\ \frac{46}{35} & \frac{94}{70} \end{pmatrix} \pmod{26}$$

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

3x3 MATRIX

CONVERSAT \rightarrow SQTUWSSUD

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

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

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \frac{1}{68} \begin{pmatrix} 24 & 6 & 30 \\ -12 & 3 & -18 \\ 15 & 14 & -5 \\ 20 & -18 & 0 \end{pmatrix} \begin{pmatrix} 18 & 16 & 25 \\ 7 & 20 & 18 \\ 18 & 20 & 3 \end{pmatrix} = \begin{pmatrix} -4 & 1 & -5 \\ 15 & 14 & -5 \\ 20 & -18 & 0 \end{pmatrix} \begin{pmatrix} 18 & 16 & 25 \\ 7 & 20 & 18 \\ 18 & 20 & 3 \end{pmatrix} =$$

$$= \begin{pmatrix} -155 & -144 & -94 \\ 248 & 420 & 612 \\ 234 & -40 & 146 \end{pmatrix} \pmod{26} = \begin{pmatrix} -25 & -14 & -19 \\ 18 & 4 & 14 \\ 0 & -14 & 20 \end{pmatrix} = \begin{pmatrix} 1 & 12 & 7 \\ 18 & 4 & 14 \\ 0 & 12 & 20 \end{pmatrix}$$

6 zag. $n = 899$ $e = 611$ n -прост множители, преобразоване d
 Да се провери $106\ 680\ 303$ за $\forall xy: L(x) + 26L(y)$, което
 $L(A) = 0$ $L(B) = 0$ $L(C) = 2 \dots L(x) = 23$ $L(y) = 24$ $L(z) = 25$

7 zag. $2^{n-1} \equiv 1 \pmod{n}$ $341 = 11 \cdot 31$ $n_0 = 341$ $n_i = 2^{h_{i-1}} - 1$
 Индукция: Докаже се вярно за n_{i-1} т.е. $2^{h_{i-1}-1} \equiv 1 \pmod{n_{i-1}}$
 не е док. за n_i . Нека $n_{i-1} = st$ $st > 1$ $st \in \mathbb{N} \Rightarrow n_i = 2^{st} - 1$, което
 се дели на $2^h - 1$ $2^{n_i-1} = 2^{n_{i-1}-1-1} = 2^{2(2^{h_{i-1}}-1)-1} = 2^{2kh_{i-1}} = (2^{h_{i-1}})^{2k} =$
 $= (n_{i-1} + 1)^{2k} \equiv 1 \pmod{n_i} \Rightarrow 2^{h_{i-1}-1} - 1 = kn_{i-1} \quad \checkmark$

8 zag. Да се док. че.

а) Число на Кармайкъл е свободно от квадрати