1

Given:

C = „SONAFQCHMWPTVEVY"

= 18 | 14 | 13 | 0 | 5 | 16 | 2 | 7 | 12 | 22 | 15 | 19 | 21 | 4 | 21 | 24

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

$$(m_1, m_2) \to \begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix}\begin{pmatrix} m_1 \\ m_2 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$$

$\overset{7\ 4}{HE} \to \overset{10\ 7}{KH}$

$\underset{19\ 7}{TH} \to \underset{23\ 22}{XW}$

OR

$\overset{7\ 4}{HE} \to \overset{23\ 22}{XW}$

$\underset{19\ 7}{TH} \to \underset{10\ 7}{KH}$

$$\begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix}\begin{pmatrix} 7 & 19 \\ 4 & 7 \end{pmatrix} = \begin{pmatrix} 10 & 23 \\ 7 & 22 \end{pmatrix}$$

$$\begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix} = \begin{pmatrix} 10 & 23 \\ 7 & 22 \end{pmatrix}\begin{pmatrix} 7 & 19 \\ 4 & 7 \end{pmatrix}^{-1}$$

$$\begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix}\begin{pmatrix} 7 & 19 \\ 4 & 7 \end{pmatrix} = \begin{pmatrix} 23 & 10 \\ 22 & 7 \end{pmatrix}$$

$$\begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix} = \begin{pmatrix} 23 & 10 \\ 22 & 7 \end{pmatrix}\begin{pmatrix} 7 & 19 \\ 4 & 7 \end{pmatrix}^{-1}$$

$$\det = 7\cdot 7 - 4\cdot 19 = 25 \bmod 26 = 25^{-1} \in (\mathbb{Z}/26\mathbb{Z})^*$$

$$\begin{pmatrix} 7 & 19 \\ 4 & 7 \end{pmatrix}^{-1} = 25\begin{pmatrix} 7 & -19 \\ -4 & 7 \end{pmatrix} = \begin{pmatrix} 175 & -475 \\ -100 & 175 \end{pmatrix} = \begin{pmatrix} 19 & 19 \\ 4 & 19 \end{pmatrix} \bmod 26$$

$$\begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix} = \begin{pmatrix} 10 & 23 \\ 7 & 22 \end{pmatrix}\begin{pmatrix} 19 & 19 \\ 4 & 19 \end{pmatrix} = \begin{pmatrix} 282 & 627 \\ 221 & 551 \end{pmatrix} = \begin{pmatrix} 22 & 3 \\ 13 & 5 \end{pmatrix} \bmod 26$$

$$\det = 110 - 39 = 71 = 19 \bmod 26 = 11^{-1} \in (\mathbb{Z}/26\mathbb{Z})^*$$

$$\begin{pmatrix} 22 & 3 \\ 13 & 5 \end{pmatrix}^{-1} = 11\begin{pmatrix} 5 & -3 \\ -13 & 22 \end{pmatrix} = \begin{pmatrix} 55 & -33 \\ -143 & 242 \end{pmatrix} = \begin{pmatrix} 3 & 19 \\ 13 & 8 \end{pmatrix} \bmod 26$$

Test decrypt:

$$\begin{pmatrix} 3 & 19 \\ 13 & 8 \end{pmatrix}\begin{pmatrix} 18 & 13 & 5 & 2 \\ 14 & 0 & 16 & 7 \end{pmatrix} = \begin{pmatrix} 320 & 39 & 319 & 139 \\ 346 & 169 & 193 & 82 \end{pmatrix} = \begin{pmatrix} 8 & 13 & 7 & 9 \\ 8 & 13 & 11 & 4 \end{pmatrix}$$

8 8 13 13 7 11 9 4

I I N N H L J E

Gibberish

$$\begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix} = \begin{pmatrix} 23 & 10 \\ 22 & 7 \end{pmatrix}\begin{pmatrix} 19 & 19 \\ 4 & 19 \end{pmatrix} = \begin{pmatrix} 477 & 627 \\ 446 & 551 \end{pmatrix} = \begin{pmatrix} 9 & 3 \\ 4 & 5 \end{pmatrix} \bmod 26$$

$$\det = 45 - 12 = 33 = 7 \bmod 26 = 15^{-1} \in (\mathbb{Z}/26\mathbb{Z})^*$$

$$\begin{pmatrix} 9 & 3 \\ 4 & 5 \end{pmatrix}^{-1} = 15\begin{pmatrix} 5 & -3 \\ -4 & 9 \end{pmatrix} = \begin{pmatrix} 75 & -45 \\ -60 & 135 \end{pmatrix} = \begin{pmatrix} 23 & 7 \\ 18 & 5 \end{pmatrix} \bmod 26$$

Test decrypt:

$$\begin{pmatrix} 23 & 7 \\ 18 & 5 \end{pmatrix}\begin{pmatrix} 18 & 13 & 5 & 2 \\ 14 & 0 & 16 & 7 \end{pmatrix} = \begin{pmatrix} 512 & 299 & 227 & 95 \\ 394 & 234 & 170 & 71 \end{pmatrix} = \begin{pmatrix} 18 & 13 & 19 & 17 \\ 4 & 0 & 14 & 19 \end{pmatrix} \bmod 26$$

18 4 13 0 19 14 17 19

$\boxed{\text{S E N A T O R}}$ T

Promising

$$\begin{pmatrix} 23 & 7 \\ 18 & 5 \end{pmatrix}\begin{pmatrix} 18 & 13 & 5 & 2 & 12 & 15 & 21 & 21 \\ 14 & 0 & 16 & 7 & 22 & 19 & 4 & 24 \end{pmatrix} = \begin{pmatrix} 512 & 299 & 227 & 95 & 430 & 478 & 511 & 651 \\ 394 & 234 & 170 & 71 & 326 & 365 & 398 & 498 \end{pmatrix} \bmod 26 =$$

$$= \begin{pmatrix} 18 & 13 & 19 & 17 & 14 & 10 & 17 & 1 \\ 4 & 0 & 14 & 19 & 14 & 1 & 8 & 4 \end{pmatrix}^{T}$$

S E N A T O R T O O K B R I B E

18 | 4 | 13 | 0 | 19 | 14 | 17 | 19 | 14 | 14 | 10 | 1 | 17 | 8 | 1 | 4

„SENATORTOOK BRIBE"

(3) a) Given:

Matrix $A \in M_2(\mathbb{Z}/N\mathbb{Z}),\ N \in \mathbb{N}$

Prove: $\exists A^{-1}$ iff $\ker(A)$ is trivial iff $\gcd(\det(A), N) = 1$

Proof:

Suppose A is invertible:

$$AA^{-1} = A^{-1}A = I,\ I \in M_2(0,1)$$

Then we have determinants:

$$\det(AA^{-1}) = \det(A)\det(A^{-1}) = \det(I) = 1$$

So for A to be invertible, $\det(A)\det(A^{-1}) = 1$.

In $\mathbb{Z}/N\mathbb{Z}$, a number ~~invertible~~ multiplied by its inverse gives 1. So we conclude that $\det(A)$ ~~must~~ should be invertable, with its inverse being $\det(A^{-1})$.

For a number x to be invertible in $\mathbb{Z}/N\mathbb{Z}$, it must obey:

$$\gcd(x, N) = 1$$

Therefore, matrix A can be invertible iff $\gcd(\det(A), N) = 1$

A kernel of A is such vector that

$$A \ker(A) = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

In other terms:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

We have the system:

$$\begin{cases} ax + by = 0 \pmod N \\ cx + dy = 0 \pmod N \end{cases}$$

Solved for y, we have:

$$\begin{cases} x = \dfrac{-by}{a} \pmod N \\ cx + dy = 0 \pmod N \end{cases}$$

$$c\frac{-by}{a} + dy = 0 \quad | \cdot a$$

$$-cby + ady = 0$$

$$(ad - cb)y = 0$$

From the previous proof we have $\gcd(\det(A), N) = 1$,
In this case, $\gcd((ad-cb), N) = 1$, so $ad - cb \neq 0$. This means that y should be $0 \pmod N$.

Substituting for y, we have

$$x = \frac{-b \cdot 0 \pmod N}{a},$$ ~~which makes~~

which makes x also $0 \bmod N$.

since $x = y = 0 \bmod N$, the kernel is trivial

We conclude that $\gcd(\det(A), N) = 1$ makes the kernel be necessary trivial if A is to be investable

Combining the two proofs, we have:

$$\exists A^{-1} \text{ iff } \ker(A) \text{ is trivial iff } \gcd(\det(A), N) = 1$$

③ b) I
Formula: $(N^2-1)(N^2-N)$

Proof:

T1 A matrix is invertible iff the columns are lineary independent.

For the first column, we have $N \cdot N = N^2$ choices. Since the column must be different than the zero vector, we must exclude it by subtracting 1 from the possible choices, i.e. the first column can be constructed in N^2-1 ways.

For the second column, from T1 we must have it not being a multiple of the first one. There are $N-1$ scalars to multiply the first column by (N, excluding 0 to omit the zero vector). So, for the second column we have:

$$N^2-1-(N-1) = N^2 - \cancel{1} - N + \cancel{1} = N^2-N$$

The number of invertible matrices in $M_2(\mathbb{Z}/N\mathbb{Z})$ is therefore $(N^2-1)(N^2-N)$

II Invertible elements in $M_K(\mathbb{Z}/N\mathbb{Z})$ (follows from formula above):

$$\prod_{i=0}^{K-1} (N^K - N^i)$$