Raju Shrestha
Roll.No. 48

Assignment-1

1. Evaluate the following

a. 7503 mod 81

→

$$\begin{array}{r|l} 81 & 7503 \\ -729 & \\ \hline 213 & \\ -162 & \\ \hline 51 & \end{array}\quad 92$$

51 → Remainder

So, when we divide 7503 by 81, the remainder is 51. //

b. -7503 mod 81

→ $-7503 = 81 \times (-92) + R$

$\therefore R = -7503 + 7452$

$= -51 + 81$

$= 30$

$$\begin{array}{r|l} 81 & -7503 \\ -7452 & \\ \hline -51 & \\ +81 & \\ \hline 30 & \end{array}\quad -92$$

$\therefore -7503 \bmod 81 = 30$ //

c. 81 mod 7503

→ 81

$$\begin{array}{r|l} 7503 & 81 \\ 00 & \\ \hline 81 & \end{array}\quad 0$$

$\therefore 81 \bmod 7503 = 81$ //

d. -81 mod 7503

→ $-81 + 7503 = 7422$

$$\begin{array}{r|l} 7503 & -81 \\ 00 & \\ \hline -81 & \\ +7503 & \\ \hline 7422 & \end{array}\quad 0$$

$\therefore -81 \bmod 7503 = 7422$ //

2. Use exhaustive key search to decrypt the following cipher text, which was encrypted using shift cipher.

BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD

→

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

Let K = 16, Then for decrypting the given text;

B	E	E	A	K	F	Y
↓	↓	↓	↓	↓	↓	↓
1	4	4	0	10	5	24
-16	-16	-16	-16	-16	-16	-16
-15	-12	-12	-16	-6	-11	8
+26	+26	+26	+26	+26	+26	+26
11	14	14	10	20	15	34
↓	↓	↓	↓	↓	↓	↓
L	O	O	K	U	P	I

D	J	X	U	Q	Y	H
↓	↓	↓	↓			
3	9	23	20	16	24	7
-16	-16	-16	-16	-16	-16	-16
-13	-7	7	4	0	8	-9
+26	+26	+26	+26	+26	+26	+26
13	19	33	30	26	34	17
↓	↓	↓	↓	↓	↓	
N	T	H	E	A	I	R

Y	J	I	Q	R	Y	H	T
24	9	8	16	17	24	7	19
-16	-16	-16	-16	-16	-16	-16	-16
8	-7	-8	0	1	8	-9	3
+26	+26	+26	+26	+26	+26	+26	+26
34	19	18	26	27	34	17	29
I	T	S	A	B	I	R	D

Y	J	I	Q	F	B	Q	D
24	9	8	16	5	1	16	3
-16	-16	-16	-16	-16	-16	-16	-16
8	-7	-8	0	-11	-15	0	-13
+26	+26	+26	+26	+26	+26	+26	+26
34	19	18	26	15	11	26	13
I	T	S	A	P	L	A	N

U	Y	J	I	I	K	F	U
20	24	9	8	8	10	5	20
-16	-16	-16	-16	-16	-16	-16	-16
4	8	-7	-8	-8	-6	-11	4
+26	+26	+26	+26	+26	+26	+26	+26
30	34	19	18	18	20	15	30
E	I	T	S	S	U	P	E

H	C	Q	D
↓	↓	↓	↓
7	2	16	3
-16	-16	-16	-16
-9	-14	0	-13
+26	+26	+26	+26
17	12	26	13
↓	↓	↓	↓
R	M	A	N

Hence, Decrypted plain text is: LOOKUPINTHEAIRITSABIRD-ITSAPLANEITSSUPERMAN.

3. Determine the number of key in affine cipher over Z_m for $m = 30, 100$ & 1225.

→ Number of key in affine cipher over $Z_m = \phi(m) * m$

$T = (P \times K_1) \bmod 26$ } encryption

$C = (T + K_2) \bmod 26$ }

$\phi(m)$ ↓ Euler phi-function

$m = 30$;

$|K| = m \times \phi(m)$

$= 30 \cdot \phi(30)$

2	30
3	15
	5

$\phi(30) = 30 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right) \times \left(1 - \frac{1}{5}\right)$ $\left[\because \phi(m) = m \times \left(1 - \frac{1}{P_1}\right) \times \left(1 - \frac{1}{P_2}\right) \times \cdots 1 - \frac{1}{P_n}\right]$

$= 30 \times \left(\frac{1}{2} \times \frac{2}{3} \times \frac{4}{5}\right) = 8$

$K = 30 \times 8 \quad (\because K = m \times \phi(m))$

$\therefore K = 240$

$m = 100$

$|K| = m \cdot \phi(m)$

$= 100 \cdot \phi(100)$

$= 100 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right)$

$= 100 \times \frac{1}{2} \times \frac{4}{5} = 40$

$\therefore K = 100 \times 40 \quad (\because K = m \times \phi(m))$

$= 4000$

2	100
2	50
5	25
	5

$m = 1225$

$|K| = m \times \phi(m)$

$\phi(m) = 1225 \times \left(1 - \frac{1}{5}\right) \times \left(1 - \frac{1}{7}\right)$

$= 1225 \times \frac{4}{5} \times \frac{6}{7}$

$= 840$

$\therefore K = m \times \phi(m)$

$= 1225 \times 840$

$= 1029000$ //

5. Suppose we are told that the plaintext "breakthrough" yields the ciphertext RUPOTEWTOIFV where the Hill cipher is used (but m is not specified). Determine the encryption matrix.

→ We know encryption method for hill cipher is;

$$C = K * P$$

Where K is encryption matrix, now encryption key K can be calculated by,

$$K = P^{-1}C$$

P & C are matrix can be formed by integer sequence of alphabet. Here, we take only 3 alphabet matrix.

$$P = \begin{bmatrix} 1 & 17 & 4 \\ 0 & 19 & 7 \\ 19 & 0 & 10 \end{bmatrix} \text{ & } C = \begin{bmatrix} 17 & 20 & 15 \\ 14 & 19 & 4 \\ 13 & 19 & 14 \end{bmatrix}$$

Now,

$K = P^{-1} * C$, we get

$$K = \begin{bmatrix} 1 & 17 & 4 \\ 0 & 19 & 7 \\ 19 & 0 & 10 \end{bmatrix}^{-1} \begin{bmatrix} 17 & 20 & 15 \\ 14 & 19 & 4 \\ 13 & 19 & 14 \end{bmatrix}$$

$$P^{-1} = \begin{bmatrix} + & - & + \\ 1 & 17 & 4 \\ 0 & 19 & 7 \\ 19 & 0 & 10 \end{bmatrix}$$

$$|P| = 1(19\times10 - 0\times7) - 17(0 - 7\times19) + 4(0 - 19\times19)$$
$$= 190 + 2261 - 1444$$
$$= 1007$$

$\therefore$ so, $P^{-1} = \frac{1}{|P|} \cdot \text{Adj. of } P$

$$= \frac{1}{1007}\begin{bmatrix} 1 & 17 & 4 & 1 & 17 \\ 0 & 19 & 7 & 0 & 19 \\ 19 & 0 & 10 & 19 & 0 \\ 1 & 17 & 4 & 1 & 17 \\ 0 & 19 & 7 & 0 & 19 \end{bmatrix}$$

$$= \frac{1}{1007}\begin{bmatrix} 190 & 170 & 43 \\ 133 & -66 & 7 \\ 361 & 323 & 19 \end{bmatrix}$$

Now, $K = P^{-1} \times C$

$$= \frac{1}{1007}\begin{bmatrix} 190 & 170 & 43 \\ 133 & -66 & 7 \\ 361 & 323 & 19 \end{bmatrix}\begin{bmatrix} 17 & 20 & 15 \\ 14 & 19 & 4 \\ 13 & 19 & 4 \end{bmatrix}$$

$$\therefore K = \begin{bmatrix} 9 & 21 & 20 \\ 4 & 25 & 23 \\ 6 & 14 & 5 \end{bmatrix}$$ which is the required encryption matrix.

6. Decrypt the following ciphertext, obtained from the Autokey cipher, by using extraustive key search :-

MALVRMAFBWBUQPTSOXALTGVWWRG

→ step-1 :-

Write the ciphertext as a sequence of numbers using the A=0, B=1 . . . . Z=25 mapping.

step-2 :-

Here we apply 0-25 (A-Z) key for decrypting the given cipher text. If we found meaningful text then we stop decrypting.

For decryption we use following formula;

$$d_z(y) = (y - z) \bmod 26$$

where z is the set of key streams & the initial value.

step-3 :-

We use key '0' i.e. 'A' for decipher the cipher text.

First we generate key stream 'z' for the decryption. so that initial character of keystream is key itself.

$$z = 0$$

Now, we subtract last value of keystream from cipher text character & apply module 26.

Then, second value would be,

$$z = 0, 12$$

Again, subtract last value of keystream i.e. 12 from another value of the value of the cipher text i.e. 0 & apply module 26.

Then we get,

$$z = 0\ 12\ 14 \text{ (where } 0 - 12 = -12 \bmod 26 \Rightarrow 14)$$

Similarly, applying same method for all character of given

Cipher text then we get keystream as,

0 12 14 23 24 23 15 11 20 7 0 1 19 23 18 1 17 23 0 0 1 18 24 23 25 23 20 12

Next, we subtract keystream value from each value of cipher text & apply modulo 26 then we get,

12 14 23 24 23 15 11 20 7 0 1 19 23 18 1 17 23 0 0 1 18 -24 23 25 23 20 12

step-4:-

After applying key 19 i.e. ↑ then we get

Lookupintheairitsabirditsaplaneitssuperman.

which we can write as,

Look up in the air its a bird its a plane its superman.

=

4. Here is how we might cryptanalyze the Hill cipher using a cipher text only attack. Suppose that we know that m=2. Break the cipher text into blocks of length two letters (diagrams). Each such diagrams are the encryption of a plain text diagrams & assume it in the encryption of a common diagrams for examde, TH or ST. Each such guess, proceed as I the known plaintext attack, until the correct encryption matrix is found.

Here is a sample of cipher text to decrypt using this method:

LMQETXYEAGTXCTUIEWNCTXLZEWUAISPZYVAPEWLMGQWYA

XFTCJMSQCADAGTXLMDXNXSNPJQSYVAPRIQSMHNOCVAXFV.

→ Lets begin by breaking the ciphertext into diagrams

LM QE TX YE AG TX CT UI EW WC TX LZ EW UA IS

PZ YV AP EW LM GQ WY AX FT CJ MS QC AD GT XL

MD XN XS NP JQ SY VA PR IQ SM NO CV AX FV.

Here, In above

LM = 2

TX = 3

QE

Taking QN as LM

$$K \times P = C$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 19 \\ 7 \end{bmatrix} = \begin{bmatrix} 11 \\ 12 \end{bmatrix}$$

$19a + 7b = 11$ —— (I)

$19c + 7d = 12$ —— (II)

Again, taking IN as TX

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 8 \\ 13 \end{bmatrix} = \begin{bmatrix} 19 \\ 23 \end{bmatrix}$$

$8a + 13b = 19$ —— (III)

$8c + 13d = 23$ —— (IV)

Now, from (I) & (III)

$$\begin{bmatrix} 19 & 7 : 11 \\ 8 & 19 : 19 \end{bmatrix}$$

In row-reduced echelon form

$$\begin{bmatrix} 19 & 7 : 11 \\ 0 & \frac{191}{19} : \frac{273}{19} \end{bmatrix}$$

So, $\frac{191}{19} + \frac{273}{19}$

$191b = 273 \bmod 26$

$9b = 13$

$b = 13 \times 3 \Rightarrow 39 \bmod 26 = 13$

Now, $19a + 7 \times 13 = 11$

$19a + 91 = 11$

$19a = -80 \bmod 26$

$a = 11 \times 24$

$= 264 \bmod 26 = 4$

Again, from (III) & (IV)

$$\begin{bmatrix} 19 & 7 : 12 \\ 8 & 19 : 23 \end{bmatrix}$$

$$\begin{bmatrix} 19 & 7 : 12 \\ 0 & \frac{101}{19} : \frac{341}{19} \end{bmatrix}$$

So, $\frac{101d}{19} = \frac{341}{19}$

$\therefore d = 9$

$19c + 7 \times 9 = 12$

$19c = -91$

$\therefore c = 11$

$\therefore$ The key is $\begin{bmatrix} 4 & 13 \\ 11 & 9 \end{bmatrix}$

as we know $P = K^{-1} C$

$$\begin{bmatrix} L \\ M \end{bmatrix} = \begin{bmatrix} 4 & 13 \\ 11 & 19 \end{bmatrix}^{-1} \begin{bmatrix} 11 \\ 12 \end{bmatrix}$$

$$= \begin{bmatrix} 23 & 13 \\ 2 & 16 \end{bmatrix} \begin{bmatrix} 11 \\ 12 \end{bmatrix}$$

$$= \begin{bmatrix} 409 \\ 423 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 19 \\ 7 \end{bmatrix}$$

$$= \begin{bmatrix} T \\ H \end{bmatrix}$$

Again, $\begin{bmatrix} Q \\ E \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 2 & 16 \end{bmatrix} \begin{bmatrix} 16 \\ 4 \end{bmatrix}$

$= \begin{bmatrix} 420 \\ 400 \end{bmatrix} \bmod 26 = \begin{bmatrix} 4 \\ 10 \end{bmatrix} = \begin{bmatrix} E \\ K \end{bmatrix}$

$\begin{bmatrix} Q \\ X \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 19 \\ 23 \end{bmatrix}$

$= \begin{bmatrix} 736 \\ 767 \end{bmatrix} \bmod 26 = \begin{bmatrix} 8 \\ 13 \end{bmatrix} = \begin{bmatrix} I \\ N \end{bmatrix}$

$\begin{bmatrix} Y \\ E \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 24 \\ 4 \end{bmatrix}$

$= \begin{bmatrix} 604 \\ 568 \end{bmatrix} \bmod 26 = \begin{bmatrix} 6 \\ 22 \end{bmatrix} = \begin{bmatrix} G \\ W \end{bmatrix}$

$\begin{bmatrix} A \\ G \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 0 \\ 6 \end{bmatrix} = \begin{bmatrix} 0 \\ 18 \end{bmatrix} = \begin{bmatrix} A \\ S \end{bmatrix}$

$\begin{bmatrix} Q \\ X \end{bmatrix} = \begin{bmatrix} I \\ N \end{bmatrix}$

$\begin{bmatrix} C \\ T \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 293 \\ 346 \end{bmatrix} = \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} H \\ I \end{bmatrix}$

$\begin{bmatrix} U \\ I \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 20 \\ 8 \end{bmatrix} = \begin{bmatrix} 564 \\ 548 \end{bmatrix} = \begin{bmatrix} 18 \\ 2 \end{bmatrix} = \begin{bmatrix} S \\ C \end{bmatrix}$

$\begin{bmatrix} E \\ W \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 4 \\ 12 \end{bmatrix} = \begin{bmatrix} 378 \\ 436 \end{bmatrix} = \begin{bmatrix} 14 \\ 20 \end{bmatrix} = \begin{bmatrix} 0 \\ 4 \end{bmatrix}$

$\begin{bmatrix} N \\ C \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 13 \\ 2 \end{bmatrix} = \begin{bmatrix} 325 \\ 305 \end{bmatrix} = \begin{bmatrix} 13 \\ 19 \end{bmatrix} = \begin{bmatrix} N \\ T \end{bmatrix}$

$\begin{bmatrix} Q \\ X \end{bmatrix} = \begin{bmatrix} I \\ N \end{bmatrix}$

$\begin{bmatrix} L \\ Z \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 11 \\ 25 \end{bmatrix} = \begin{bmatrix} 578 \\ 631 \end{bmatrix} = \begin{bmatrix} 6 \\ 7 \end{bmatrix} = \begin{bmatrix} G \\ H \end{bmatrix}$

$$\begin{bmatrix} E \\ W \end{bmatrix} = \begin{bmatrix} 0 \\ 4 \end{bmatrix}$$

$$\begin{bmatrix} U \\ A \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 20 \\ 0 \end{bmatrix} = \begin{bmatrix} 460 \\ 420 \end{bmatrix} = \begin{bmatrix} 18 \\ 4 \end{bmatrix} = \begin{bmatrix} S \\ E \end{bmatrix}$$

$$\begin{bmatrix} I \\ S \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 8 \\ 18 \end{bmatrix} = \begin{bmatrix} 418 \\ 456 \end{bmatrix} = \begin{bmatrix} 2 \\ 14 \end{bmatrix} = \begin{bmatrix} C \\ O \end{bmatrix}$$

$$\begin{bmatrix} P \\ Z \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 15 \\ 25 \end{bmatrix} = \begin{bmatrix} 670 \\ 715 \end{bmatrix} = \begin{bmatrix} 20 \\ 13 \end{bmatrix} = \begin{bmatrix} U \\ N \end{bmatrix}$$

$$\begin{bmatrix} V \\ V \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 24 \\ 21 \end{bmatrix} = \begin{bmatrix} 825 \\ 840 \end{bmatrix}$$

$$\begin{bmatrix} A \\ P \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 0 \\ 15 \end{bmatrix} = \begin{bmatrix} 195 \\ 240 \end{bmatrix} = \begin{bmatrix} 13 \\ 6 \end{bmatrix} = \begin{bmatrix} N \\ G \end{bmatrix}$$

$$\begin{bmatrix} E \\ W \end{bmatrix} = \begin{bmatrix} 0 \\ U \end{bmatrix}$$

$$\begin{bmatrix} L \\ M \end{bmatrix} = \begin{bmatrix} T \\ H \end{bmatrix}$$

$$\begin{bmatrix} G \\ Q \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 6 \\ 10 \end{bmatrix} = \begin{bmatrix} 346 \\ 382 \end{bmatrix} = \begin{bmatrix} 8 \\ 18 \end{bmatrix} = \begin{bmatrix} I \\ S \end{bmatrix}$$

$$\begin{bmatrix} W \\ Y \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 22 \\ 24 \end{bmatrix} = \begin{bmatrix} 818 \\ 846 \end{bmatrix} = \begin{bmatrix} 12 \\ 14 \end{bmatrix} = \begin{bmatrix} M \\ O \end{bmatrix}$$

$$\begin{bmatrix} A \\ X \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 0 \\ 23 \end{bmatrix} = \begin{bmatrix} 299 \\ 368 \end{bmatrix} = \begin{bmatrix} 13 \\ 4 \end{bmatrix} = \begin{bmatrix} N \\ E \end{bmatrix}$$

$$\begin{bmatrix} F \\ T \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 5 \\ 19 \end{bmatrix} = \begin{bmatrix} 362 \\ 409 \end{bmatrix} = \begin{bmatrix} 24 \\ 19 \end{bmatrix} = \begin{bmatrix} V \\ T \end{bmatrix}$$

$$\begin{bmatrix} C \\ J \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 2 \\ 9 \end{bmatrix} = \begin{bmatrix} 163 \\ 186 \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} H \\ E \end{bmatrix}$$

$$\begin{bmatrix} M \\ S \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 12 \\ 18 \end{bmatrix} = \begin{bmatrix} 510 \\ 540 \end{bmatrix} = \begin{bmatrix} 16 \\ 12 \end{bmatrix} = \begin{bmatrix} Q \\ U \end{bmatrix}$$

$$\begin{bmatrix} Q \\ C \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 16 \\ 2 \end{bmatrix} = \begin{bmatrix} 394 \\ 368 \end{bmatrix} = \begin{bmatrix} 4 \\ 4 \end{bmatrix} = \begin{bmatrix} E \\ E \end{bmatrix}$$

$$\begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 0 \\ 3 \end{bmatrix} = \begin{bmatrix} 39 \\ 48 \end{bmatrix} = \begin{bmatrix} 13 \\ 22 \end{bmatrix} = \begin{bmatrix} N \\ W \end{bmatrix}$$

$$\begin{bmatrix} A \\ G \end{bmatrix} = \begin{bmatrix} A \\ S \end{bmatrix}$$

$$\begin{bmatrix} T \\ X \end{bmatrix} = \begin{bmatrix} I \\ N \end{bmatrix}$$

$$\begin{bmatrix} L \\ M \end{bmatrix} = \begin{bmatrix} T \\ H \end{bmatrix}$$

$$\begin{bmatrix} D \\ X \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 3 \\ 23 \end{bmatrix} = \begin{bmatrix} 368 \\ 431 \end{bmatrix} = \begin{bmatrix} 4 \\ 15 \end{bmatrix} = \begin{bmatrix} E \\ P \end{bmatrix}$$

$$\begin{bmatrix} N \\ X \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 18 \\ 23 \end{bmatrix} = \begin{bmatrix} 598 \\ 641 \end{bmatrix} = \begin{bmatrix} 0 \\ 17 \end{bmatrix} = \begin{bmatrix} A \\ R \end{bmatrix}$$

$$\begin{bmatrix} S \\ N \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 18 \\ 13 \end{bmatrix} = \begin{bmatrix} 583 \\ 586 \end{bmatrix} = \begin{bmatrix} 11 \\ 14 \end{bmatrix} = \begin{bmatrix} L \\ O \end{bmatrix}$$

$$\begin{bmatrix} P \\ I \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 15 \\ 8 \end{bmatrix} = \begin{bmatrix} 449 \\ 443 \end{bmatrix} = \begin{bmatrix} 20 \\ 17 \end{bmatrix} = \begin{bmatrix} U \\ R \end{bmatrix}$$

$$\begin{bmatrix} Q \\ S \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 16 \\ 18 \end{bmatrix} = \begin{bmatrix} 602 \\ 624 \end{bmatrix} = \begin{bmatrix} 4 \\ 0 \end{bmatrix} = \begin{bmatrix} E \\ A \end{bmatrix}$$

$$\begin{bmatrix} Y \\ V \end{bmatrix} = \begin{bmatrix} T \\ I \end{bmatrix}$$

$$\begin{bmatrix} A \\ P \end{bmatrix} = \begin{bmatrix} N \\ G \end{bmatrix}$$

$$\begin{bmatrix} R \\ I \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 17 \\ 8 \end{bmatrix} = \begin{bmatrix} 495 \\ 485 \end{bmatrix} = \begin{bmatrix} 1 \\ 17 \end{bmatrix} = \begin{bmatrix} B \\ R \end{bmatrix}$$

$$\begin{bmatrix} Q \\ S \end{bmatrix} = \begin{bmatrix} E \\ A \end{bmatrix}$$

$$\begin{bmatrix} M \\ H \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 12 \\ 7 \end{bmatrix} = \begin{bmatrix} 267 \\ 364 \end{bmatrix} = \begin{bmatrix} 3 \\ 0 \end{bmatrix} = \begin{bmatrix} D \\ A \end{bmatrix}$$

$$\begin{bmatrix} N \\ O \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 13 \\ 14 \end{bmatrix} = \begin{bmatrix} 481 \\ 497 \end{bmatrix} = \begin{bmatrix} 13 \\ 3 \end{bmatrix} = \begin{bmatrix} N \\ D \end{bmatrix}$$

$$\begin{bmatrix} C \\ V \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 2 \\ 21 \end{bmatrix} = \begin{bmatrix} 319 \\ 378 \end{bmatrix} = \begin{bmatrix} 7 \\ 14 \end{bmatrix} = \begin{bmatrix} H \\ O \end{bmatrix}$$

$$\begin{bmatrix} A \\ X \end{bmatrix} = \begin{bmatrix} N \\ E \end{bmatrix}$$

$$\begin{bmatrix} F \\ V \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 5 \\ 21 \end{bmatrix} = \begin{bmatrix} 388 \\ 441 \end{bmatrix} = \begin{bmatrix} 24 \\ 25 \end{bmatrix} = \begin{bmatrix} Y \\ Z \end{bmatrix}$$

So, from the above we get the plaintext = THE KING WAS IN HIS COUNTING HOUSE COUNTING OUT HIS MONEY THE QUEENNAS IN THE PARLOUR EATING BREAD AND HONEYZ.