

Saturday
27-3-2021

Date 27-3-21

Page

Name - AMIT KUMAR SAHU
Slot - ~~6~~ slot
Reg. No - 18MIS7250

Information System Security

ASSIGNMENT - 1

* Note - Solution for questions 6, 7 and 10 are at the end of the file as they are written programs.

1. Relationship between security services and attacks

ATTACKS

Service	Release of message	Traffic Analysis	Masquerade	Replay	Modification of Message [DoS]
Peer entity Authentication			Y		
Data Origin Authentication			Y		
Access Control			Y		
Confidentiality	Y				
Traffic-flow Confidentiality		Y			
Data Integrity				Y	Y
Non-Reproduction			Y		
Availability					Y

2. Relationship between Security mechanisms and attacks.

Service	Release of Message	Traffic Analysis	Masquerade	Reply	Modification of Message	Denial of Service (DoS)
Enipherment	Y					
Digital Signature		X	Y	Y	Y	
Access Control	Y	Y	Y	Y		Y
Data Integrity				Y	Y	
Authentication	Y		Y	Y		Y
Exchange Padding		Y				
Routing Control	Y	Y				Y
Notarization			Y	Y	Y	

3. Find integers such that

a) $5x \equiv 4 \pmod{3}$

$$\text{GCD}(5, 3) = 1$$

$$\frac{b}{d} = \frac{4}{1} \Rightarrow \text{soln exists}$$

$$d \text{ mod } n = 1 \text{ mod } 3 = 3 \rightarrow 1 \text{ solution exists}$$

$$5 \cdot 5^{-1}x = 4 \cdot 5^{-1} \pmod{3}$$

$$x = 4 \cdot 5^{-1} \pmod{3}$$

$$x = 4 \cdot 2 \pmod{3}$$

$$x = 8 \pmod{3}$$

$$\boxed{x = 2}$$

$$(5 \times a) \pmod{3} = 1$$

$$(5 \times 3) \pmod{3} = 1$$

$$5^{-1} = 2$$

b) $7x \equiv 6 \pmod{5}$

$$\text{GCD}(7, 5) = 1$$

$$\frac{b}{d} = \frac{6}{1} \Rightarrow \text{soln exists}$$

$$d \text{ mod } n = 1 \text{ mod } 5 = \emptyset \rightarrow \emptyset \text{ soln exists.}$$

$$x = 6 \cdot 7^{-1} \pmod{5}$$

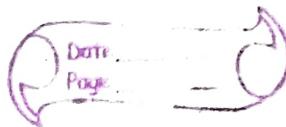
$$(7 \times a) \pmod{5} = 1$$

$$x = 6 \cdot 8 \pmod{5}$$

$$(7 \times 8) \pmod{5} = 1$$

$$x = 48 \pmod{5}$$

$$\boxed{x = 3}$$



$$c) 9x \equiv 8 \pmod{7}$$

$$\text{GCD}(9, 7) = 1$$

$$x = 8 \cdot 9^{-1} \pmod{7}$$

$$= 8 \cdot 4 \pmod{7}$$

$$= 32 \pmod{7}$$

$$\boxed{x = 4}$$

$$(9 \times a) \pmod{7} = 1$$

$$(9 \times 4) \pmod{7} = 1$$

Q4. Prove the following:

a) $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$

Ans The two assumptions imply $n | (a-b)$ and $n | (b-c)$. Thus, n divides the linear combination $(a-b) + (b-c) = a-c$ as well. This means $n | (a-c)$

b) $[(a \pmod{n}) - (b \pmod{n})] \pmod{n} = (a-b) \pmod{n}$

$$\text{LHS} = [(a \pmod{n}) - (b \pmod{n})] \pmod{n}$$

$$\text{let } A = 14, B = 17, n = 5$$

$$\begin{aligned}\text{LHS} &= [14 \pmod{5} - 17 \pmod{5}] \pmod{5} \\ &= [4 - 2] \pmod{5} \\ &= 2 \pmod{5} \\ &= 2\end{aligned}$$

$$\begin{aligned}\text{RHS} &= [14 - 17] \pmod{5} = -3 \pmod{5} = 2 \\ \text{LHS} &= \text{RHS}\end{aligned}$$

c) $(a \bmod n) * (b \bmod n) \bmod n = (a * b) \bmod n$

From quotient remainder theorem

$a = n * q_1 + r_1$ where $0 \leq r_1 < c$ and q_1 is some integer

$b = n * q_2 + r_2$ where $0 \leq r_2 < c$ and q_2 is some integer

RHS. = $(a * b) \bmod n$

$$= ((n * q_1 + r_1) * (n * q_2 + r_2)) \bmod n$$

$$= ((n * n * q_1 * q_2 + n * q_1 * r_2 + n * q_2 * r_1 + r_1 * r_2)) \bmod n$$

$$= (0 * (n * q_1 * q_2 + q_1 * r_2 + q_2 * r_1) + r_1 * r_2) \bmod n$$

We can eliminate the multiples of n when we take the mod n .

RHS = $(r_1 * r_2) \bmod n$

LHS = $(A \bmod c * B \bmod n) \bmod n$

$$= (r_1 * r_2) \bmod n$$

Therefore RHS = LHS = $(r_1 * r_2) \bmod n$

Q5. Show that an integer N is congruent modulo 9 to the sum of its decimal digits. Eg: $475 = 4+7+5=16 = 1+6=7 \pmod{9}$

Ans Clearly $9 | (10-1)$. Suppose that $9 | (10^n - 1)$, $n > 1$ then

$$10^{n+1} - 1 = 10 \cdot 10^n - 1 = 9 \cdot 10^n + (10^n - 1)$$

thus $9 | (10^{n+1} - 1)$. Therefore $9 | (10^n - 1)$ for any $n \in \mathbb{N}$

$$a = \sum_{i=0}^n a_i \cdot 10^i$$

where $a_i \in \{0, 1, \dots, 9\}$. Then

$$a - \sum_{i=0}^n a_i = \sum_{i=0}^n a_i \cdot 10^i - \sum_{i=0}^n a_i = \sum_{i=1}^n a_i (10^i - 1)$$

therefore

$$a \equiv \sum_{i=0}^n a_i \pmod{9}$$

Q6. Break the following ciphertext:

P E L C G B T E N C U L V F S B E V A S B E Z N G V B A F R P H

AT LAST

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

Q R S T U V W X Y Z

R T K M O W Y

58 $C = E([K_1, K_2], P) = P^* K_1 + K_2$

- a) 2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24.

Any value of K_1 larger than 25 is equivalent to $K_1 \bmod 26$.

- b) No, change in value of K_2 shift the relationship between plaintext letters & cipher text letters to the left as right uniformly, so that if the mapping is one-to-one it remains one-to-one.

59

"XICKGLTIZKSCRHUFM"

a b c d e f g h i j k l
z y x w v ö t s r ö p o

m n o p q r s z u v w x
n m l k f i h g f e d c

y z
B A

Decipher will be: exptographx is fun

SII

a) Key = "VITABC\$"
= "VITABCS"

\$ will take S

↓ down

V I T A B
B C S

SII

a) Key = "VITAPBC\$" \$ will take S

= "VITAPBCS"

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

hello bob come soon

be lx lo be ba om
es boy on

we also take lx because we cannot find value for
hello we have to split lx lo, similarly y for es

he \Rightarrow LS

es \Rightarrow BD

lx \Rightarrow HZ

oy \Rightarrow QX

lo \Rightarrow HR

on \Rightarrow GO

bo \Rightarrow SM

bc \Rightarrow CS

Encrypted text \Rightarrow LS HZ HR SM CS QN

om \Rightarrow QN

BD QX GO

b) "EOZAIQLNPVLW" usng key "VITAP"

CIPHERTEXT = EOZAIQLNPVLW

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

EO \Rightarrow CR

ZA \Rightarrow YP

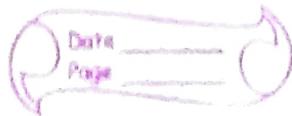
IQ \Rightarrow TO

LN \Rightarrow GR

PV \Rightarrow AP

LW \Rightarrow HY

Hence plain text is "CRYPTOGRAPHY"



~~S12~~

Computer Science [S]

SVITAP \Rightarrow [462513]

"solve the assignment individually"

key = "SVITAP" \Rightarrow [462513]

solvet heassi gnment indivi dually

Encryption ↴

4	6	2	5	1	3
1	2	3	4	5	6

ciphertext

VTOESL SIESHA ETNNGM IIDVID LYULDA

Decryption key =

1	2	3	4	5	6
1	2	3	4	5	6

1	2	3	4	5	6
1	2	3	4	5	6

Decryption key

\Rightarrow [5 3 6 1 4 2]

Decryption ↴

5	3	6	1	4	2
1	2	3	4	5	6

SOLVET HEASSI GNMENT INDIVI DUALY

5/13

key column transposition cipher with
encryption key [5 3 2 4 1]

"TPQSP|IZYRR|RRCZB|GXIO,A|EPA
ETZCO|HUMRC"

Decipher ↑	5	3	2	4	1
	1	2	3	4	5

TPQSP \Rightarrow PQPS T

IZYRR \Rightarrow RYZRI ; RRCZB \Rightarrow RCRZR

GXI0A \Rightarrow AIX0G ; EPAEE \Rightarrow EAPEE

ETZCO \Rightarrow OZTCE ; HUMRC \Rightarrow CMVRH

& the Deciphered plaintext will be.

PQPS T RYZRI RCRZR AIX0G EAPEE OZTCE
CMVRH

8.14.

Vigenère cipher

a) "send more money" with key stream [9 0 1 7 23 15 21 18 11 11
2 8 9]

s e n d m o r e m o n e y
18 4 13 3 12 14 17 4 12 14 13 4 24

key	9	0	1	7	23	25	21	14	11	11	2	8	9
+	27	4	14	10	35	29	38	18	23	25	15	12	33
mod 26	1	4	14	10	9	3	12	18	23	25	15	12	7

Cipher B E C K J D M S X Z P M H

b) Key=? that decryps "CASH NOT NEEDED"

c a s h n o t n e e d e d
2 0 18 7 13 14 19 13 4 4 3 4 3

25 4 22 3 22 15 19 5 19 21 12 8 4

1 4 14 10 9 3 12 18 23 25 15 12 7
B E C K J D M S X Z P M H

Hence the key is [25 4 22 3 22 15 19 5 19 21 12 8 4]

\$15,

"meet me at the oval place at ten rather than eight
o'clock"

$$\text{key} = \begin{bmatrix} 9 & 5 \\ 4 & 7 \end{bmatrix}$$

meet m e a t t h e u s u a l

13 5 5 20 13 5 1 20 20 8 5 21 19 21 1 12

Place a t t e n r a d h e r

16 12 1 3 5 1 20 20 5 14 18 1 20 8 5 18

extra dummy ↴

t h a n e i g h t o c l o c k

20 8 1 19 5 9 7 8 20 15 3 12 15 3 11 17

Encryption:

$$c = kp \bmod 26$$

$$\begin{bmatrix} m \\ e \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 13 \\ 5 \end{bmatrix} \bmod 26 = \begin{bmatrix} 137 \\ 100 \end{bmatrix} \bmod 26 = \begin{bmatrix} 17 \\ 22 \end{bmatrix} = \begin{bmatrix} 6 \\ v \end{bmatrix}$$

$$\begin{bmatrix} e \\ t \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 5 \\ 20 \end{bmatrix} \bmod 26 - \begin{bmatrix} 125 \\ 165 \end{bmatrix} \bmod 26 = \begin{bmatrix} 21 \\ 9 \end{bmatrix} = \begin{bmatrix} v \\ I \end{bmatrix}$$

$$\begin{bmatrix} a \\ f \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 1 \\ 20 \end{bmatrix} \bmod 26 = \begin{bmatrix} 89 \\ 145 \end{bmatrix} \bmod 26 - \begin{bmatrix} 21 \\ 15 \end{bmatrix} = \begin{bmatrix} K \\ O \end{bmatrix}$$

$$\begin{bmatrix} t \\ h \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 20 \\ 8 \end{bmatrix} = \begin{bmatrix} 212 \\ 156 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 4 \\ 26 \end{bmatrix} = \begin{bmatrix} D \\ Z \end{bmatrix}$$

$$\begin{bmatrix} e \\ v \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 5 \\ 21 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 125 \\ 172 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 25 \\ 16 \end{bmatrix} = \begin{bmatrix} Y \\ P \end{bmatrix}$$

$$\begin{bmatrix} s \\ v \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 9 \\ 21 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 255 \\ 242 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 21 \\ 8 \end{bmatrix} = \begin{bmatrix} V \\ H \end{bmatrix}$$

$$\begin{bmatrix} a \\ d \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 1 \\ 12 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 57 \\ 89 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 5 \\ 11 \end{bmatrix} = \begin{bmatrix} E \\ K \end{bmatrix}$$

$$\begin{bmatrix} p \\ l \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 16 \\ 12 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 192 \\ 184 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 10 \\ 8 \end{bmatrix} = \begin{bmatrix} J \\ H \end{bmatrix}$$

$$\begin{bmatrix} a \\ c \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 21 \\ 26 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 21 \\ 26 \end{bmatrix} = \begin{bmatrix} V \\ Z \end{bmatrix}$$

$$\begin{bmatrix} e \\ a \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 5 \\ 1 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 48 \\ 32 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 23 \\ 6 \end{bmatrix} = \begin{bmatrix} W \\ F \end{bmatrix}$$

$$\begin{bmatrix} t \\ + \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 20 \\ 20 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 260 \\ 240 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 25 \\ 6 \end{bmatrix} = \begin{bmatrix} Z \\ F \end{bmatrix}$$

$$\begin{bmatrix} e \\ n \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 5 \\ 14 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 101 \\ 123 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 23 \\ 19 \end{bmatrix} = \begin{bmatrix} W \\ S \end{bmatrix}$$

$$\begin{bmatrix} 8 \\ a \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 28 \\ 1 \end{bmatrix} = \begin{bmatrix} 166 \\ 97 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 10 \\ 26 \end{bmatrix} = \begin{bmatrix} J \\ Z \end{bmatrix}$$

$$\begin{bmatrix} e \\ r \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 5 \\ 18 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 117 \\ 151 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 13 \\ 21 \end{bmatrix} = \begin{bmatrix} m \\ u \end{bmatrix}$$

$$\begin{bmatrix} a \\ n \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 7 \\ 16 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 65 \\ 103 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 13 \\ 25 \end{bmatrix} = \begin{bmatrix} M \\ Y \end{bmatrix}$$

$$\begin{bmatrix} e \\ i \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 5 \\ 98 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 81 \\ 99 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 3 \\ 21 \end{bmatrix} = \begin{bmatrix} C \\ v \end{bmatrix}$$

$$\begin{bmatrix} g \\ h \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 7 \\ 8 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 95 \\ 91 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 17 \\ 13 \end{bmatrix} = \begin{bmatrix} Q \\ M \end{bmatrix}$$

$$\begin{bmatrix} t \\ o \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 20 \\ 15 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 240 \\ 205 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 6 \\ 23 \end{bmatrix} = \begin{bmatrix} F \\ W \end{bmatrix}$$

$$\begin{bmatrix} c \\ l \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 3 \\ 12 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 75 \\ 99 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 23 \\ 21 \end{bmatrix} = \begin{bmatrix} W \\ V \end{bmatrix}$$

$$\begin{bmatrix} o \\ c \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 15 \\ 3 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 147 \\ 96 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 17 \\ 18 \end{bmatrix} = \begin{bmatrix} G \\ R \end{bmatrix}$$

$$\begin{bmatrix} K \\ q \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 11 \\ 17 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 167 \\ 174 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 11 \\ 18 \end{bmatrix} = \begin{bmatrix} K \\ R \end{bmatrix}$$

So the final ciphertext:

GVUIGVKODZYPVHEIKJHUVZWR

ZFWSSJS DZMVDMYCTQMFWWVQRKR

Decryption

$$\text{Determinant} = (9 \times 7) - (4 \times 5) = 43.$$

$$\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}^{-1} = \frac{1}{43} \begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix} \text{ mod } 26$$

$$= 23 \begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix} \text{ mod } 26$$

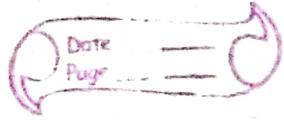
$$= \begin{bmatrix} 161 & -92 \\ 115 & 9 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix}$$

$43^{-1} \text{ in } \mathbb{Z}_{26}$ is 23

$$\text{Plain} = K^{-1}C \text{ mod } 26$$

$$\begin{bmatrix} U \\ V \end{bmatrix} = \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \begin{bmatrix} 7 \\ 22 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 13 \\ 5 \end{bmatrix} = \begin{bmatrix} M \\ E \end{bmatrix}$$

$$\begin{bmatrix} U \\ I \end{bmatrix} = \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \begin{bmatrix} 21 \\ 9 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 213 \\ 590 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 5 \\ 20 \end{bmatrix} = \begin{bmatrix} e \\ t \end{bmatrix}$$



$$\begin{bmatrix} K \end{bmatrix} = \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \begin{bmatrix} 11 \\ 15 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 1 \\ 20 \end{bmatrix} = \begin{bmatrix} Q \\ t \end{bmatrix}$$

$$\begin{bmatrix} D \end{bmatrix} = \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \begin{bmatrix} 4 \\ 26 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 20 \\ 8 \end{bmatrix} = \begin{bmatrix} t \\ h \end{bmatrix}$$

$$\begin{bmatrix} Y \end{bmatrix} = \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \begin{bmatrix} 25 \\ 16 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 5 \\ 21 \end{bmatrix} = \begin{bmatrix} e \\ v \end{bmatrix}$$

$$\begin{bmatrix} V \end{bmatrix} = \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \begin{bmatrix} 21 \\ 8 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 19 \\ 21 \end{bmatrix} = \begin{bmatrix} s \\ v \end{bmatrix}$$

$$\begin{bmatrix} E \end{bmatrix} = \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \begin{bmatrix} 51 \\ 81 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} t \\ 12 \end{bmatrix} = \begin{bmatrix} a \\ l \end{bmatrix}$$

$$\begin{bmatrix} J \end{bmatrix} = \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \begin{bmatrix} 10 \\ 8 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 16 \\ 12 \end{bmatrix} = \begin{bmatrix} p \\ l \end{bmatrix}$$

$$\begin{bmatrix} SK \end{bmatrix} = \begin{bmatrix} 5 & 12 \\ 15 & 15 \end{bmatrix} \begin{bmatrix} 11 \\ 18 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 117 \\ 17 \end{bmatrix} = \begin{bmatrix} k \\ q \end{bmatrix}$$

Hence Again play text will be

meet me at the usual place at ten rather than
eight o'clock.

S 16

YITJID GWJOW FAGTQ XCSMA ETSQV
SQAPU SQYKC PQTYJ

$$P = K^{-1}C \text{ mod } 26$$

$$K^{-1} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix}$$

$$\begin{bmatrix} Y \\ I \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 25 \\ 9 \end{bmatrix} = \begin{bmatrix} 134 \\ 113 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 4 \\ 9 \end{bmatrix} = \begin{bmatrix} D \\ I \end{bmatrix}$$

$$\begin{bmatrix} T \\ J \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 20 \\ 10 \end{bmatrix} = \begin{bmatrix} 100 + 10 \\ 40 + 70 \end{bmatrix} = \begin{bmatrix} 110 \\ 110 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 6 \\ 6 \end{bmatrix} = \begin{bmatrix} F \\ F \end{bmatrix}$$

$$\begin{bmatrix} P \\ Q \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 16 \\ 7 \end{bmatrix} = \begin{bmatrix} 80 + 7 \\ 32 + 49 \end{bmatrix} = \begin{bmatrix} 87 \\ 81 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 9 \\ 3 \end{bmatrix} = \begin{bmatrix} I \\ C \end{bmatrix}$$

$$\begin{bmatrix} BV \\ J \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 23 \\ 10 \end{bmatrix} = \begin{bmatrix} 115 + 10 \\ 46 + 70 \end{bmatrix} = \begin{bmatrix} 125 \\ 116 \end{bmatrix} = \begin{bmatrix} 21 \\ 12 \end{bmatrix} = \begin{bmatrix} U \\ L \end{bmatrix}$$

$$\begin{bmatrix} O \\ W \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 15 \\ 23 \end{bmatrix} = \begin{bmatrix} 75 + 23 \\ 30 + 161 \end{bmatrix} = \begin{bmatrix} 98 \\ 191 \end{bmatrix} = \begin{bmatrix} 20 \\ 9 \end{bmatrix} = \begin{bmatrix} T \\ I \end{bmatrix}$$

$$\begin{bmatrix} F \\ A \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 6 \\ 1 \end{bmatrix} = \begin{bmatrix} 30 + 1 \\ 12 + 7 \end{bmatrix} = \begin{bmatrix} 31 \\ 19 \end{bmatrix} = \begin{bmatrix} 5 \\ 9 \end{bmatrix} = \begin{bmatrix} E \\ S \end{bmatrix}$$

$$\begin{bmatrix} Q \\ T \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 17 \\ 20 \end{bmatrix} = \begin{bmatrix} 85 + 20 \\ 34 + 140 \end{bmatrix} = \begin{bmatrix} 105 \\ 174 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 1 \\ 18 \end{bmatrix} = \begin{bmatrix} N \\ R \end{bmatrix}$$

$$\begin{bmatrix} Q \\ X \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 17 \\ 29 \end{bmatrix} = \begin{bmatrix} 85+24 \\ 34+168 \end{bmatrix} \text{mod} 26 = \begin{bmatrix} 109 \\ 202 \end{bmatrix} = \begin{bmatrix} 5 \\ 20 \end{bmatrix} \text{mod} 26 = \begin{bmatrix} E \\ T \end{bmatrix}$$

$$\begin{bmatrix} C \\ S \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 3 \\ 19 \end{bmatrix} = \begin{bmatrix} 15+19 \\ 6+133 \end{bmatrix} = \begin{bmatrix} 34 \\ 139 \end{bmatrix} \text{mod} 26 = \begin{bmatrix} 8 \\ 9 \end{bmatrix} = \begin{bmatrix} I \\ I \end{bmatrix}$$

$$\begin{bmatrix} M \\ A \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 13 \\ 1 \end{bmatrix} = \begin{bmatrix} 65+1 \\ 26+7 \end{bmatrix} = \begin{bmatrix} 66 \\ 33 \end{bmatrix} \text{mod} 26 = \begin{bmatrix} 14 \\ 7 \end{bmatrix} = \begin{bmatrix} N \\ S \end{bmatrix}$$

$$\begin{bmatrix} E \\ T \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 5 \\ 20 \end{bmatrix} = \begin{bmatrix} 25+20 \\ 10+140 \end{bmatrix} = \begin{bmatrix} 45 \\ 150 \end{bmatrix} \text{mod} 26 = \begin{bmatrix} 19 \\ 20 \end{bmatrix} = \begin{bmatrix} S \\ T \end{bmatrix}$$

$$\begin{bmatrix} S \\ Q \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 19 \\ 17 \end{bmatrix} = \begin{bmatrix} 95+17 \\ 38+119 \end{bmatrix} = \begin{bmatrix} 112 \\ 157 \end{bmatrix} \text{mod} 26 = \begin{bmatrix} 8 \\ 1 \end{bmatrix} = \begin{bmatrix} H \\ A \end{bmatrix}$$

$$\begin{bmatrix} V \\ S \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 21 \\ 19 \end{bmatrix} = \begin{bmatrix} 105+19 \\ 42+133 \end{bmatrix} = \begin{bmatrix} 124 \\ 175 \end{bmatrix} \text{mod} 26 = \begin{bmatrix} 20 \\ 19 \end{bmatrix} = \begin{bmatrix} T \\ S \end{bmatrix}$$

$$\begin{bmatrix} Q \\ A \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 17 \\ 1 \end{bmatrix} = \begin{bmatrix} 85+1 \\ 34+5 \end{bmatrix} = \begin{bmatrix} 86 \\ 41 \end{bmatrix} \text{mod} 26 = \begin{bmatrix} 8 \\ 15 \end{bmatrix} = \begin{bmatrix} H \\ O \end{bmatrix}$$

$$\begin{bmatrix} P \\ V \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 16 \\ 21 \end{bmatrix} = \begin{bmatrix} 80+21 \\ 32+147 \end{bmatrix} = \begin{bmatrix} 101 \\ 179 \end{bmatrix} \text{mod} 26 = \begin{bmatrix} 23 \\ 23 \end{bmatrix} = \begin{bmatrix} W \\ W \end{bmatrix}$$

$$\begin{bmatrix} C \\ Q \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 19 \\ 17 \end{bmatrix} = \begin{bmatrix} 95+17 \\ 38+119 \end{bmatrix} = \begin{bmatrix} 112 \\ 157 \end{bmatrix} \text{mod} 26 = \begin{bmatrix} 8 \\ 1 \end{bmatrix} = \begin{bmatrix} H \\ A \end{bmatrix}$$

$$\begin{bmatrix} 9 \\ K \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} ? \\ 11 \end{bmatrix} = \begin{bmatrix} 35+11 \\ 14+77 \end{bmatrix} = \begin{bmatrix} 46 \\ 91 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 20 \\ 13 \end{bmatrix} = \begin{bmatrix} T \\ N \end{bmatrix}$$

$$\begin{bmatrix} C \\ P \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 3 \\ 16 \end{bmatrix} = \begin{bmatrix} 15+16 \\ 6+12 \end{bmatrix} = \begin{bmatrix} 31 \\ 18 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 5 \\ 14 \end{bmatrix} = \begin{bmatrix} E \\ N \end{bmatrix}$$

$$\begin{bmatrix} Q \\ T \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 17 \\ 20 \end{bmatrix} = \begin{bmatrix} 85+20 \\ 34+140 \end{bmatrix} = \begin{bmatrix} 105 \\ 174 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 1 \\ 18 \end{bmatrix} = \begin{bmatrix} A \\ R \end{bmatrix}$$

$$\begin{bmatrix} Y \\ J \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 25 \\ 10 \end{bmatrix} = \begin{bmatrix} 125+10 \\ 56+70 \end{bmatrix} = \begin{bmatrix} 135 \\ 126 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 5 \\ 16 \end{bmatrix} = \begin{bmatrix} E \\ P \end{bmatrix}$$

So the plain text is:

"Difficulties are things that show what men are."

S17

"MWALO LIAW WTGBH JNTAK QZJKI ADAWS
 SKQKV AYARN CSODN IIAES OGKJY Z.

using the inverse key as $\begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix}$

$$P = CK^{-1} \pmod{26}$$

$$\begin{bmatrix} M \\ W \end{bmatrix} = \begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 12 \\ 23 \end{bmatrix} \pmod{26} = \begin{bmatrix} 585 \\ 484 \end{bmatrix} \pmod{26} = \begin{bmatrix} 19 \\ 18 \end{bmatrix} = \begin{bmatrix} I \\ R \end{bmatrix}$$

$$\begin{bmatrix} R \\ L \end{bmatrix} = \begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 01 \\ 12 \end{bmatrix} \pmod{26} = \begin{bmatrix} 278 \\ 105 \end{bmatrix} \pmod{26} = \begin{bmatrix} 18 \\ 1 \end{bmatrix} = \begin{bmatrix} R \\ A \end{bmatrix}$$

$$\begin{bmatrix} O \\ L \end{bmatrix} = \begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 15 \\ 12 \end{bmatrix} \pmod{26} = \begin{bmatrix} 306 \\ 399 \end{bmatrix} \pmod{26} = \begin{bmatrix} 20 \\ 9 \end{bmatrix} = \begin{bmatrix} T \\ I \end{bmatrix}$$

$$\begin{bmatrix} I \\ A \end{bmatrix} = \begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 8 \\ 01 \end{bmatrix} \pmod{26} = \begin{bmatrix} 41 \\ 196 \end{bmatrix} \pmod{26} = \begin{bmatrix} 15 \\ 14 \end{bmatrix} = \begin{bmatrix} O \\ N \end{bmatrix}$$

$$\begin{bmatrix} I \\ W \end{bmatrix} = \begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 9 \\ 23 \end{bmatrix} \pmod{26} = \begin{bmatrix} 547 \\ 350 \end{bmatrix} \pmod{26} = \begin{bmatrix} 1 \\ 12 \end{bmatrix} = \begin{bmatrix} A \\ L \end{bmatrix}$$

$$\begin{bmatrix} W \\ T \end{bmatrix} = \begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 23 \\ 20 \end{bmatrix} \pmod{26} = \begin{bmatrix} 506 \\ 623 \end{bmatrix} \pmod{26} = \begin{bmatrix} 12 \\ 25 \end{bmatrix} = \begin{bmatrix} L \\ Y \end{bmatrix}$$

$$\begin{bmatrix} H \\ B \end{bmatrix} = \begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 8 \\ 2 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 60 \\ 161 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 8 \\ 5 \end{bmatrix} = \begin{bmatrix} H \\ E \end{bmatrix}$$

$$\begin{bmatrix} H \\ J \end{bmatrix} = \begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 8 \\ 10 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 246 \\ 238 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 12 \\ 4 \end{bmatrix} = \begin{bmatrix} L \\ D \end{bmatrix}$$

$$\begin{bmatrix} N \\ T \end{bmatrix} = \begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 14 \\ 20 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 488 \\ 434 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 20 \\ 18 \end{bmatrix} = \begin{bmatrix} T \\ R \end{bmatrix}$$

$$\begin{bmatrix} A \\ K \end{bmatrix} = \begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 01 \\ 10 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 255 \\ 98 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 21 \\ 20 \end{bmatrix} = \begin{bmatrix} Q \\ T \end{bmatrix}$$

$$\begin{bmatrix} Q \\ Z \end{bmatrix} = \begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 18 \\ 25 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 632 \\ 539 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 8 \\ 19 \end{bmatrix} = \begin{bmatrix} H \\ S \end{bmatrix}$$

$$\begin{bmatrix} J \\ K \end{bmatrix} = \begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 10 \\ 16 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 273 \\ 207 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 13 \\ A \end{bmatrix} = \begin{bmatrix} m \\ A \end{bmatrix}$$

$$\begin{bmatrix} A \\ A \end{bmatrix} = \begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 24 \\ 20 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 24 \\ 2 \end{bmatrix} = \begin{bmatrix} X \\ B \end{bmatrix}$$

$$\begin{bmatrix} D \\ A \end{bmatrix} = \begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 8 \\ 0 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 383 \\ 0 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 38 \\ 0 \end{bmatrix} = \begin{bmatrix} 5 \\ 0 \end{bmatrix} = \begin{bmatrix} e \\ n \end{bmatrix}$$

$$\begin{bmatrix} W \\ S \end{bmatrix} = \begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 23 \\ 19 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 483 \\ 616 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 15 \\ 18 \end{bmatrix} = \begin{bmatrix} O \\ R \end{bmatrix}$$

$$\begin{bmatrix} S \\ K \end{bmatrix} = \begin{bmatrix} 8 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 19 \\ 11 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 291 \\ 476 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 5 \\ 08 \end{bmatrix} = \begin{bmatrix} E \\ H \end{bmatrix}$$

$$\begin{bmatrix} R \\ K \end{bmatrix} = \begin{bmatrix} 8 \\ 21 \end{bmatrix} = \begin{bmatrix} 8 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 17 \\ 11 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 287 \\ 434 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 1 \\ 18 \end{bmatrix} = \begin{bmatrix} A \\ R \end{bmatrix}$$

$$\begin{bmatrix} V \\ A \end{bmatrix} = \begin{bmatrix} 8 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 21 \\ 1 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 65 \\ 448 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 13 \\ 6 \end{bmatrix} = \begin{bmatrix} M \\ F \end{bmatrix}$$

$$\begin{bmatrix} Y \\ A \end{bmatrix} = \begin{bmatrix} 8 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 25 \\ 1 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 73 \\ 552 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 21 \\ 12 \end{bmatrix} = \begin{bmatrix} V \\ L \end{bmatrix}$$

$$\begin{bmatrix} R \\ N \end{bmatrix} = \begin{bmatrix} 8 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 18 \\ 19 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 359 \\ 476 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 20 \\ 8 \end{bmatrix} = \begin{bmatrix} T \\ H \end{bmatrix}$$

$$\begin{bmatrix} C \\ S \end{bmatrix} = \begin{bmatrix} 8 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 3 \\ 19 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 943 \\ 196 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 1 \\ 14 \end{bmatrix} = \begin{bmatrix} A \\ N \end{bmatrix}$$

$$\begin{bmatrix} O \\ D \end{bmatrix} = \begin{bmatrix} 8 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 15 \\ 4 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 122 \\ 343 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 18 \\ 5 \end{bmatrix} = \begin{bmatrix} R \\ E \end{bmatrix}$$

$$\begin{bmatrix} N \\ I \end{bmatrix} = \begin{bmatrix} 8 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 14 \\ 9 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 235 \\ 357 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 1 \\ 19 \end{bmatrix} = \begin{bmatrix} A \\ S \end{bmatrix}$$

$$\begin{bmatrix} I \\ A \end{bmatrix} = \begin{bmatrix} 8 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 9 \\ 1 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 41 \\ 196 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 15 \\ 14 \end{bmatrix} = \begin{bmatrix} O \\ N \end{bmatrix}$$

$$\begin{bmatrix} E \\ S \end{bmatrix} = \begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 5 \\ 18 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 424 \\ 231 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 57 \\ 4 \end{bmatrix} = \begin{bmatrix} E \\ D \end{bmatrix}$$

$$\begin{bmatrix} O \\ Q \end{bmatrix} = \begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 15 \\ 17 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 421 \\ 434 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 5 \\ 18 \end{bmatrix} = \begin{bmatrix} O \\ R \end{bmatrix}$$

$$\begin{bmatrix} K \\ J \end{bmatrix} = \begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 15 \\ 10 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 252 \\ 301 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 18 \\ 15 \end{bmatrix} = \begin{bmatrix} K \\ O \end{bmatrix}$$

$$\begin{bmatrix} Y \\ B \end{bmatrix} = \begin{bmatrix} 2 & 23 \\ 21 & 7 \end{bmatrix} \begin{bmatrix} 24 \\ 2 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 98 \\ 539 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 18 \\ 19 \end{bmatrix} = \begin{bmatrix} R \\ S \end{bmatrix}$$

Hence the plain text is

"Irrationally held truths may be more harmful than seasoned errors."

S18 Since version space is \mathbb{Z}_{13} so,

$$Key = \begin{bmatrix} 1 & 8 & M \\ 1 & S & 7 \\ 2 & 5 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 8 & 13 \\ 9 & 19 & 7 \\ 2 & 5 & 0 \end{bmatrix} \text{ mod } 13$$

$$= \begin{bmatrix} 1 & 8 & 0 \\ 9 & 6 & 7 \\ 2 & 5 & 0 \end{bmatrix}$$

Encryption.

$$C = KP \text{ mod } 13$$

$$\begin{bmatrix} 1 \\ 8 \\ M \end{bmatrix} = \begin{bmatrix} 1 & 8 & 0 \\ 9 & 6 & 7 \\ 2 & 5 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 8 \\ 0 \end{bmatrix} \text{ mod } 13 = \begin{bmatrix} 65 \\ 57 \\ 42 \end{bmatrix} \text{ mod } 13$$

$$= \begin{bmatrix} 0 \\ 5 \\ 3 \end{bmatrix} = \begin{bmatrix} 0 \\ E \\ C \end{bmatrix}$$

$$\begin{bmatrix} T \\ S \\ 7 \end{bmatrix} = \begin{bmatrix} 1 & 8 & 0 \\ 9 & 6 & 7 \\ 2 & 5 & 0 \end{bmatrix} \begin{bmatrix} 9 \\ 10 \\ 7 \end{bmatrix} \text{ mod } 13 = \begin{bmatrix} 57 \\ 166 \\ 48 \end{bmatrix} \text{ mod } 13$$

$$= \begin{bmatrix} 5 \\ 10 \\ 9 \end{bmatrix} = \begin{bmatrix} E \\ T \\ I \end{bmatrix}$$

$$\begin{bmatrix} 2 \\ 5 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 8 & 0 \\ 9 & 6 & 7 \\ 2 & 5 & 0 \end{bmatrix} \begin{bmatrix} 2 \\ 5 \\ 0 \end{bmatrix} \text{ mod } 13 = \begin{bmatrix} 42 \\ 48 \\ 29 \end{bmatrix} \text{ mod } 13$$

$$= \begin{bmatrix} 3 \\ 9 \\ 3 \end{bmatrix} = \begin{bmatrix} C \\ I \\ C \end{bmatrix}$$

so the ciphered is OEC EJ I C IC

For decryption findy 'det' $\begin{bmatrix} 1 & 8 & 0 \\ 9 & 6 & 7 \\ 2 & 5 & 0 \end{bmatrix} = -35 = 8(-14)$

$$A^{-1} = \frac{1}{|A|} \text{adj}(A) = \cancel{\frac{1}{77}} \cdot \cancel{I}$$

$$\begin{array}{c|ccc} \cancel{A} & -5/11 & 0 & 8/11 \\ 77 & 2/11 & 0 & -4/11 \\ & 3/7 & 1/7 & -6/7 \end{array}$$

$$= \begin{bmatrix} -35 & 0 & 56 \\ 14 & 0 & -7 \\ 33 & \cancel{77} & -66 \end{bmatrix}$$

$$= \begin{bmatrix} -9 & 0 & 4 \\ 1 & 0 & -7 \\ 7 & 11 & -1 \end{bmatrix}$$

Decryption

$$\begin{bmatrix} 0 \\ E \\ C \end{bmatrix} = \begin{bmatrix} -35 & 0 & 56 \\ 19 & 0 & -7 \\ 33 & 11 & -60 \end{bmatrix} \begin{bmatrix} 0 \\ 5 \\ 3 \end{bmatrix} = \begin{bmatrix} 168 \\ -21 \\ -143 \end{bmatrix} \text{ mod } 13 = \begin{bmatrix} 1 \\ 8 \\ 6 \end{bmatrix} =$$

$$\begin{bmatrix} E \\ J \\ I \end{bmatrix} = \begin{bmatrix} -9 & 0 & 4 \\ 1 & 0 & -7 \\ 7 & 11 & -1 \end{bmatrix} \begin{bmatrix} 5 \\ 10 \\ 9 \end{bmatrix} = \begin{bmatrix} +9 \\ +58 \\ +138 \end{bmatrix} \text{ mod } 13 = \begin{bmatrix} 1 \\ 8 \\ 7 \end{bmatrix}$$

$$\begin{bmatrix} C \\ I \\ C \end{bmatrix} = \begin{bmatrix} -9 & 0 & 4 \\ 1 & 0 & -7 \\ 7 & 11 & -1 \end{bmatrix} \begin{bmatrix} 3 \\ 9 \\ 6 \end{bmatrix} = \begin{bmatrix} +15 \\ +18 \\ 117 \end{bmatrix} \text{ mod } 13 = \begin{bmatrix} 2 \\ 5 \\ 0 \end{bmatrix}$$

Hence

O E C E J I C Z C

& Decryption

1 8 0 2 5 7 2 5 0

1 8 M 1 S 7 2 5 0