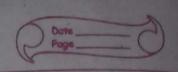
	Raju Shrestha Roll.No. A8 Assignment-1
1.	Evaluate the following
a.	7503 mod 81
7	81) 7503 (9Z
	-729
	213
	-162
	51 - Remainder
	so, when we divide 7503 by 81, the remainder is 51.
	Charles on the second second some of the second sec
	X 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3
b.	-7503 mod 81
. 7	-7503 = 81x(-92)+R -81)-7503(-92-
	R = -7503 +7452 -7452
	= -51+8151
	= 30 +81
	30
	7503 mod 81 = 30
	81 mod 7503
-	31 7503) 81 (0
	00
	81-
	81 mod 7503 = 81, -
d.	-81 mod 7503
7	-81+7503 = 7422 7503) -81 (0
	00
	-81
	+ 7503
	7422 1 mad 7503 = 7422
	1303 = +424



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

BEEAKFYDJXUQYMYJIQRYHTYJIQFBQDUYJIIKFUHCQD

>	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	1=8	N=13	S=18	X = 23
		The second second second second			

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

E=4 J=9 0=14 T=19 Y=24

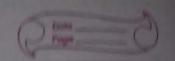
	B	E	E		A	K	F	У
	1	4	4	9	Ö	10	5	24
	-16 -	-16	-16	-	-16	-16	-16	-16
-	-15	-12	12	A.	-16	-6	0-11	8
-	+26	+26	+26	636	+26	+26	+26	+26
-	11	14	14		10	20	15	34
	L	· ·	0	A.F.Ca.	K	U	p	1
	- E. W3	Rawin C	18-16-1		Ref. Str. Tax			

-	}	J	X	Y	Q	Y	H
-	3	ğ	23	20	16	24	7
-	-16	-16	-16	-16	-16	-16	-16
1	-13	-7	7	4	0	8	-9
	+26	+26	+26	+26	+26	+26	+26
	13	19	33	30	2,6	34	17
	N	Ť	H	E	A	1	0
				1		-	

							Date Page		
	¥ 24	J + 9	1 8	Q 16	R	y 24	H + 7	T 19	
	-16	-16	-16 -8	-16	-16	-16	-16	-16	
	+26	+26	+26	+26	+26	+26	+26	+26	
	34	19 T	3	26 A	27	34	17 R	29	
-,0>	X	TIT	T T	Q	OF A	В	Q Q	p :	
	24 -16	g -16	8 -16		5	* *	16	13	
	8 +26	-7		+26	-11	-15	0,	-13	
	34	19	18		15.	1111	26	13	
(on his sin	. C.S.	3		P	A Lin	30 - 30	MAIN S	
	Ų	*	J	Ţ	Ī	K	t	Ų	
	10 -16 -4	-16	<u>9</u> -16	-16	-16	-16	-16	20	
	+26	8 +26	-7 +26	-8	-8 +26	-6 +26	-11	4	
	30 E	34 I	19	18	18	20	15		
								E	
							1		1

						C	Durke Page	
H	Ç	Q		0			Year	
7	2	16		3		-	- 10	
-16	-16	-16	M -	16			3 3 4 3	
-9	-14	0	-	13				
+26	+26	+26			0.04	426	4,12	
17	12	26		13	1000	3	*	
R	M	1 A	-	N		T. Int.	1	
		Section 1						
					OOKUPI	NTHEAI	RITSABIR	V-
ITS	APLANEIT	SSUPER	MAN	. 12		P	NAME OF THE OWNER.	
1-		31-	4)-	935	1			
	11		1		000	* 1		
	ermine th		eral	key in	affine	cipher	over 2m	
	m=30,100		0.000	C'al	alack Y	- 4/2	1 v no	
7 1/10	mber of k						ler phi-funct	\
- TO SEE	C = (T+K			ncrypu	ori	٤١١	ier phi-funct	ion
m	=30;	2		3333	7			
	IKI= mx	dem)			1	30		
		\$(30)			3			
						5		
	ф(30) = 30	$\times \left(1 - \frac{1}{2}\right)$) x (1.	$-\frac{1}{3}$) x	(1-1)	1:0	(m) = mx(1	-1)x
	= 30	$\times \left(\frac{1}{2}\right) \times$	2 x	1 :	= 8		$\left(1-\frac{1}{p_2}\right)\chi$.	1-1 Pn
	K - 30	×8 (· k -	myh	(m)			
	.'. K = 2A			4	("))			
						- 19		
						Charles of		

	O Date of the second of the se
	Page
1	m=100 . 2 100 .
	1K1 = m. o(m) 2 50
	= (00.0(100)
	$= 100 \times (1 - \frac{1}{2}) \times (1 - \frac{1}{6})$
	The solution of the Southern Consumer Consumer
	$= 100 \times 1 \times A = 40$
	of mitaryous Commence to the service of A area Commence
	$ K = 100 \times 40$ (: $K = m \times \phi(m)$
	= A000
	ship to terrain and bearing so a consister on a second
	m = 1225.
	$ K = m \times \phi(m)$
	$\phi(m) = 1225 \times (1-1) \times (1-1)$
	= 1225 x 4 x 6 5 7
	5 7
	= 840
	\cdot
,	= 1225 x 840
	= 1029000
Will de la	
Page	and the property of the state o
	A CONTRACTOR OF THE PARTY OF TH
	And the second s
4886	
No late	



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

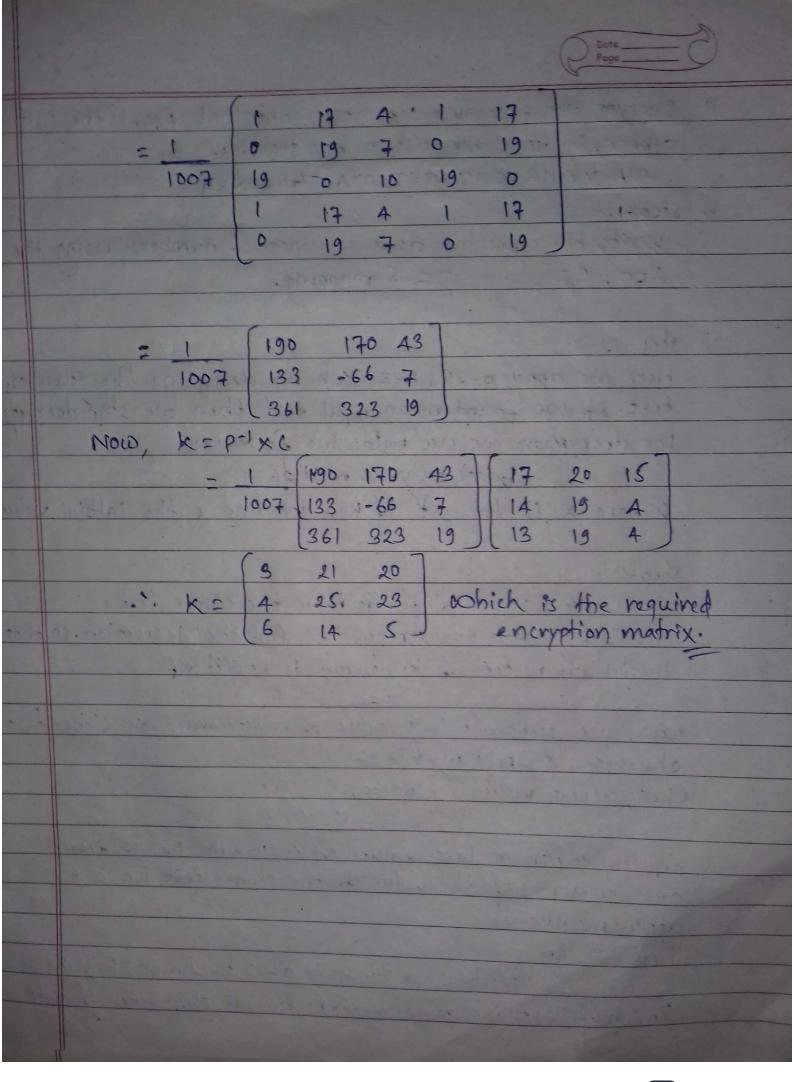
We know encryption method for hill cipher is;

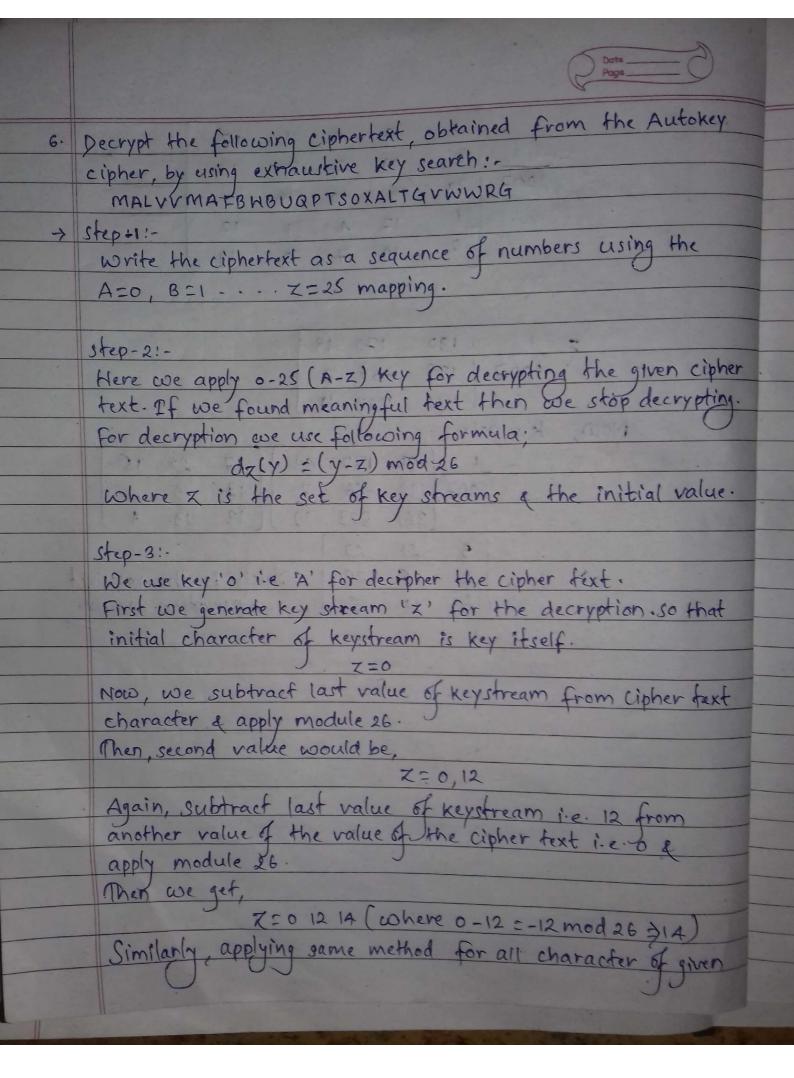
where k is encryption matrix, now encryption key k can be calculated by,

p & c are matrix can be formed by integer sequence of alphabet. Here, we take only 9 alphabet

NOW,

1p1=1(19×10-0×7)-17(0-7×19)+4(0-19×19) = 190+2261-1444





Date Page

Cipher text then we get keystream as,

0 12 14 23 24 23 15 11 20 701 1923 18 117 23 00 11824 23 25 23

20 12

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

12142324231511207011923181172300118-242325232012

Step-A:-

superman.

which we can covite as,

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

4: Here is how we might cryptanalyze the Hill Lipher using a cipher bext 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 example, 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 AP GT XL
MD XN XS NP JQ SY VA PR IQ SM NO CV AX FV.

```
Here, in above
 LM = 2
 TX=3
 QE .
Paking M as LM
   KXP=C
  19C+7d=12-10
Again, taking IN as TX
    a 6 [8] [19]
    c d)[13]=[23
    8C+ 13d=23-(V)
Now, from () ((11)
    19 7:11
    8 19:19
In row-reduced echelon form
    19 7:11
     0 191 : 273
    19 19
    1946 = 273 mod 26
    96=13.
    b = 13 x3 => 39 mod 26 = 13
Now, 199+7×13 511
    199+91=11
```

199 = - 80 mod 26 .. = 264 mod 26 Again, 19:23 19 341 ... d=q ·. C=11 as we know p=k-1p A23

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

$$= \begin{bmatrix} 420 \\ A00 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 4 \\ 10 \end{bmatrix} = \begin{bmatrix} E \\ K \end{bmatrix}$$

$$= \begin{bmatrix} 43 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 19 \\ 23 \end{bmatrix}$$

$$= \begin{bmatrix} 436 \\ 767 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 8 \\ 13 \end{bmatrix}, \begin{bmatrix} 7 \\ N \end{bmatrix}$$

$$= \begin{bmatrix} 23 & 13 \\ 421 & 16 \end{bmatrix} \begin{bmatrix} 24 \\ 4 \end{bmatrix}$$

$$= \begin{bmatrix} 604 \\ 568 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 6 \\ 22 \end{bmatrix} = \begin{bmatrix} Gr \\ N \end{bmatrix}$$

$$= \begin{bmatrix} 604 \\ 568 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 6 \\ 22 \end{bmatrix} = \begin{bmatrix} Gr \\ N \end{bmatrix}$$

$$= \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 0 \\ 6 \end{bmatrix} = \begin{bmatrix} 203 \\ 8 \end{bmatrix} = \begin{bmatrix} A \\ 5 \end{bmatrix}$$

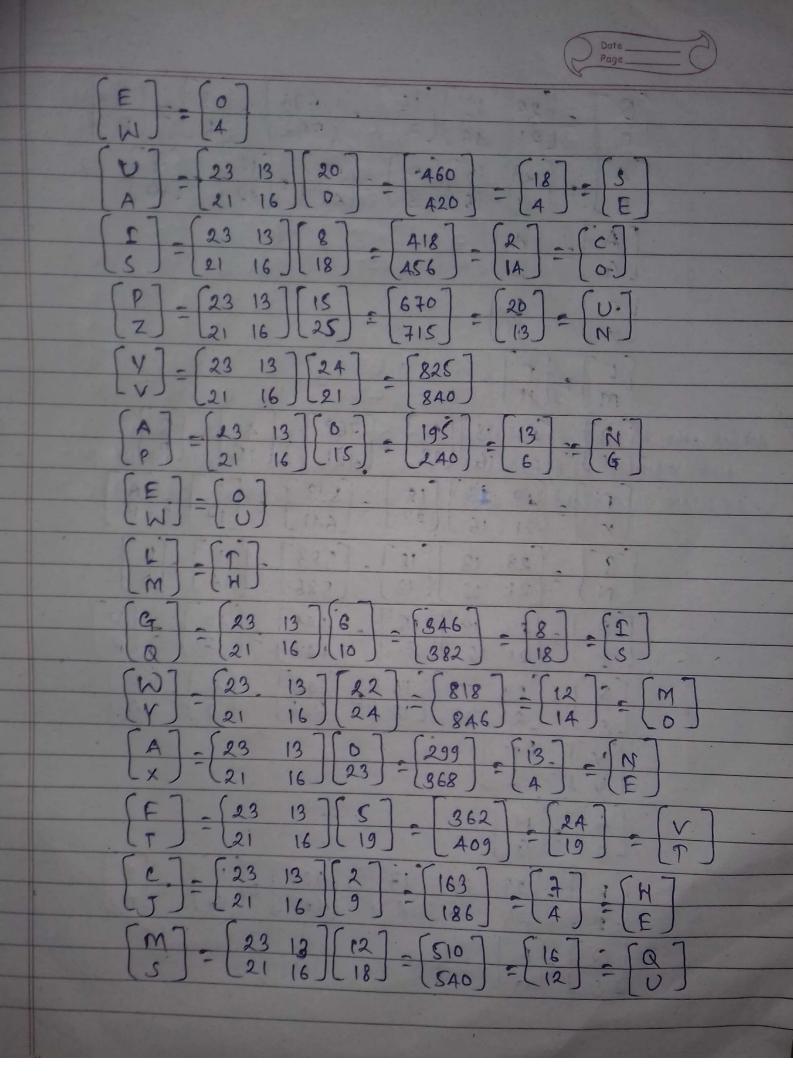
$$= \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 29 \\ 8 \end{bmatrix} = \begin{bmatrix} 564 \\ 688 \end{bmatrix} = \begin{bmatrix} 18 \\ 2 \end{bmatrix} = \begin{bmatrix} 6 \\ 4 \end{bmatrix}$$

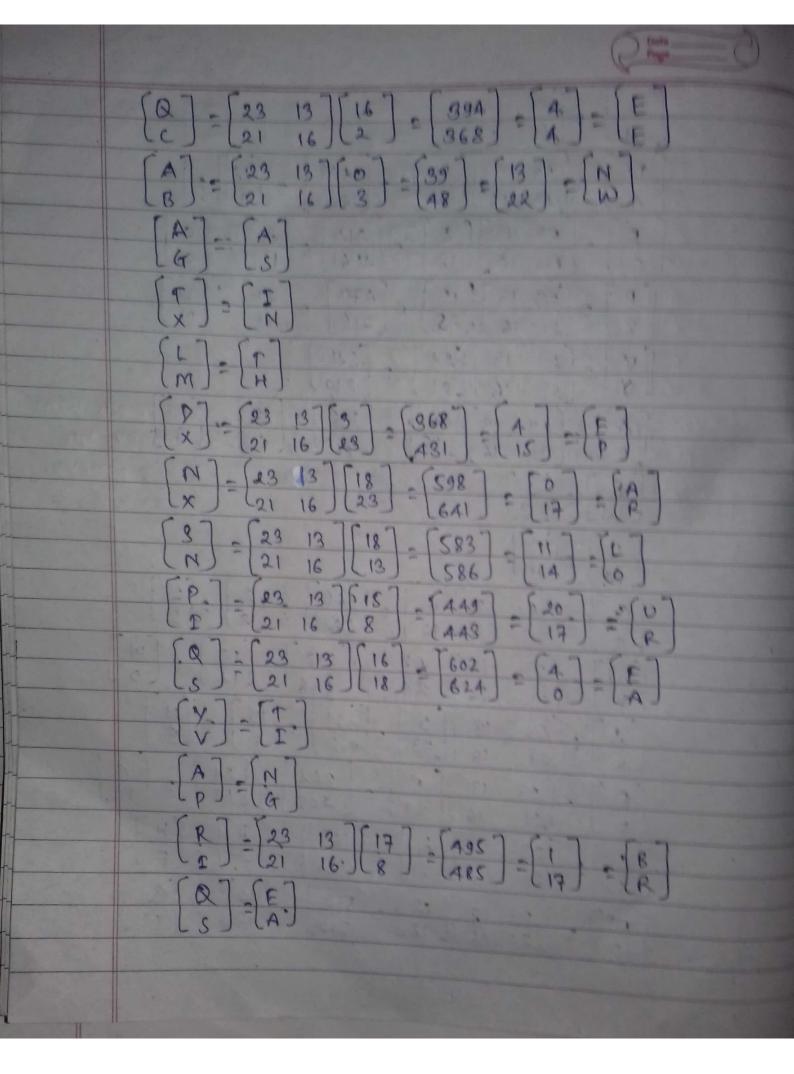
$$= \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 13 \\ 21 & 23 \end{bmatrix} = \begin{bmatrix} 328 \\ 436 \end{bmatrix} = \begin{bmatrix} 14 \\ 20 \end{bmatrix} = \begin{bmatrix} 0 \\ 4 \end{bmatrix}$$

$$= \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 13 \\ 21 & 23 \end{bmatrix} = \begin{bmatrix} 328 \\ 305 \end{bmatrix} = \begin{bmatrix} 13 \\ 19 \end{bmatrix} = \begin{bmatrix} N \\ T \end{bmatrix}$$

$$= \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 13 \\ 23 \end{bmatrix} = \begin{bmatrix} 325 \\ 305 \end{bmatrix} = \begin{bmatrix} 13 \\ 4 \end{bmatrix} = \begin{bmatrix} 6 \\ 7 \end{bmatrix} = \begin{bmatrix} 17 \\ 17 \end{bmatrix}$$

$$= \begin{bmatrix} 17 \\ 18 \end{bmatrix} = \begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 23 \\ 25 \end{bmatrix} = \begin{bmatrix} 578 \\ 631 \end{bmatrix} = \begin{bmatrix} 6 \\ 7 \end{bmatrix} = \begin{bmatrix} 6 \\ 7 \end{bmatrix} = \begin{bmatrix} 6 \\ 7 \end{bmatrix}$$





= $\begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 13 \\ 14 \end{bmatrix} = \begin{bmatrix} 481 \\ 497 \end{bmatrix} = \begin{bmatrix} 13 \\ 3 \end{bmatrix} = \begin{bmatrix} N \\ D \end{bmatrix}$ $\begin{bmatrix} 23 & 13 \\ 21 & 16 \end{bmatrix} \begin{bmatrix} 2 \\ 21 \end{bmatrix} = \begin{bmatrix} 319 \\ 378 \end{bmatrix} = \begin{bmatrix} 7 \\ 14 \end{bmatrix} = \begin{bmatrix} H \\ 0 \end{bmatrix}$ $\begin{bmatrix} 23 & 13 \\ 21 & 16 \\ 21 \end{bmatrix} = \begin{bmatrix} 388 \\ AA1 \end{bmatrix} = \begin{bmatrix} 24 \\ 25 \\ \end{bmatrix} = \begin{bmatrix} y \\ z \end{bmatrix}$ SO, from the above we got the plaintext = THE KING WAS IN HIS COUNTING HOUSE COUNTING OUT HIS MONEY THE QUEENNAS IN THE PARLOUR EATING BREAD AND HONEYZ.