Instructure Manual by DR. Bashar

Caesar Cipher:

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

K=3

IN ENCRYPTION C=(P+K) MOD 26

C=(P+3) MOD 26 CAESAR= FDHVDU

C=(P+5) MOD 26

IN DECRYPTION P=(C-K) MOD 26

P= (C-K)26

EX: FDHVDU-→ P= CAESAR

NOTES of CAESAR:

1. **Customized alphabet:**

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	@	#	%	&
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

C= (P+K) MOD 30

BAS@COM WITH KEY=5

GFXBHTR

P=(C-K) MOD 30

BAS@COM

2. **THIS ALGO. DEPENDS ON KEY VALUE TO CHANGE THE LETTER:**

PlayFair Cipher 5X5 matrix depends on keyword.

Keyword=monarchy

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

PLAIN = HELLO

= HE LX LO

CIPHER= CF SU PM

IF THERE ARE DUPLICATES IN kw REMOVE IT

EX: TOWMORROW → TOWMR tomorrow

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

PLAIN = MU ST AN SI RI YA HZ

CIPHER=TY LR BL QK MK UD KX

Keyword= infinity → INFTY

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

PLAIN = PL AI NZ

=

CIPHER=RH GA YV

Keyword= Mustansiriyah → mustaniryh

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

Plain = HASHIMY

= HA SH IM Y

Cipher= FH AR NU HX

H/W: use hill cipher to find the cipher text depend on the following facts:

KEYWORD= I SEE THE SEA IN THE C

PLAIN TEXT= CO VI DV AC CI N?

Hill Cipher

$$if\ K = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}, then\ K^{-1} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}$$

WHEN MOD 26

Example: encrypt the message "BITCOIN now 35,000$"

Using the above KEY?

ANSWER:

A=0	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
J	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**
S	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**a=26**
b=27	**c**	**d**	**e**	**F**	**g**	**h**	**i**	**j**
K	**l**	**m**	**n**	**O**	**p**	**q**	**r**	**s**
T	**u**	**v**	**w**	**X**	**y**	**z=51**	**0=52**	**1**
2	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**,**
$=63	**∞=64**							

"BITCOIN now 35,000$"= BI TC OI N∞ no w∞ 35 ,0 00 $Z

= Key X (1?)) mod 65=C

$$if\ K = \begin{pmatrix} 0 & 11 & 15 \\ 7 & 0 & 1 \\ 4 & 19 & 0 \end{pmatrix}, then\ K^{-1} = \begin{pmatrix} 3 & 7 & 1 \\ 24 & 4 & 19 \\ 5 & 4 & 19 \end{pmatrix}$$

Vigenère Cipher

Example: encrypt the message that “FULL Name” “bashar m. nema” “ahmed ali omar”> key”aao”

Using the key “first three char from full name” example “bmn” by using Polyalphabetic Vigenere Cipher method?

RailFence☹Transposition methods

Plain= "DISCONNECT THE PLUGS NOW", depth=3, top-Down.

D				O				C				E				G				W
	I		C		N		E		T		H		P		U		S		O	
		S				N				T				L				N		

CIPHER TEXT CAN BE FIND BY READING EACH ROW ABOVE:

C= “**DOCEGWICNETHPUSOSNTLN**”

Plain= " depth=3, bu.

		F				H				A				T				9		
	A		F		R		A		S		N		A		E		1		9	
J				E				S				H				M				9

CIPHER TEXT CAN BE FIND BY READING EACH ROW ABOVE:

C=”**F**HAT9A**F**RASNAE19JESHM8”

P=”JAFFERHASSANHATEM1998”

To decrypt as follow:

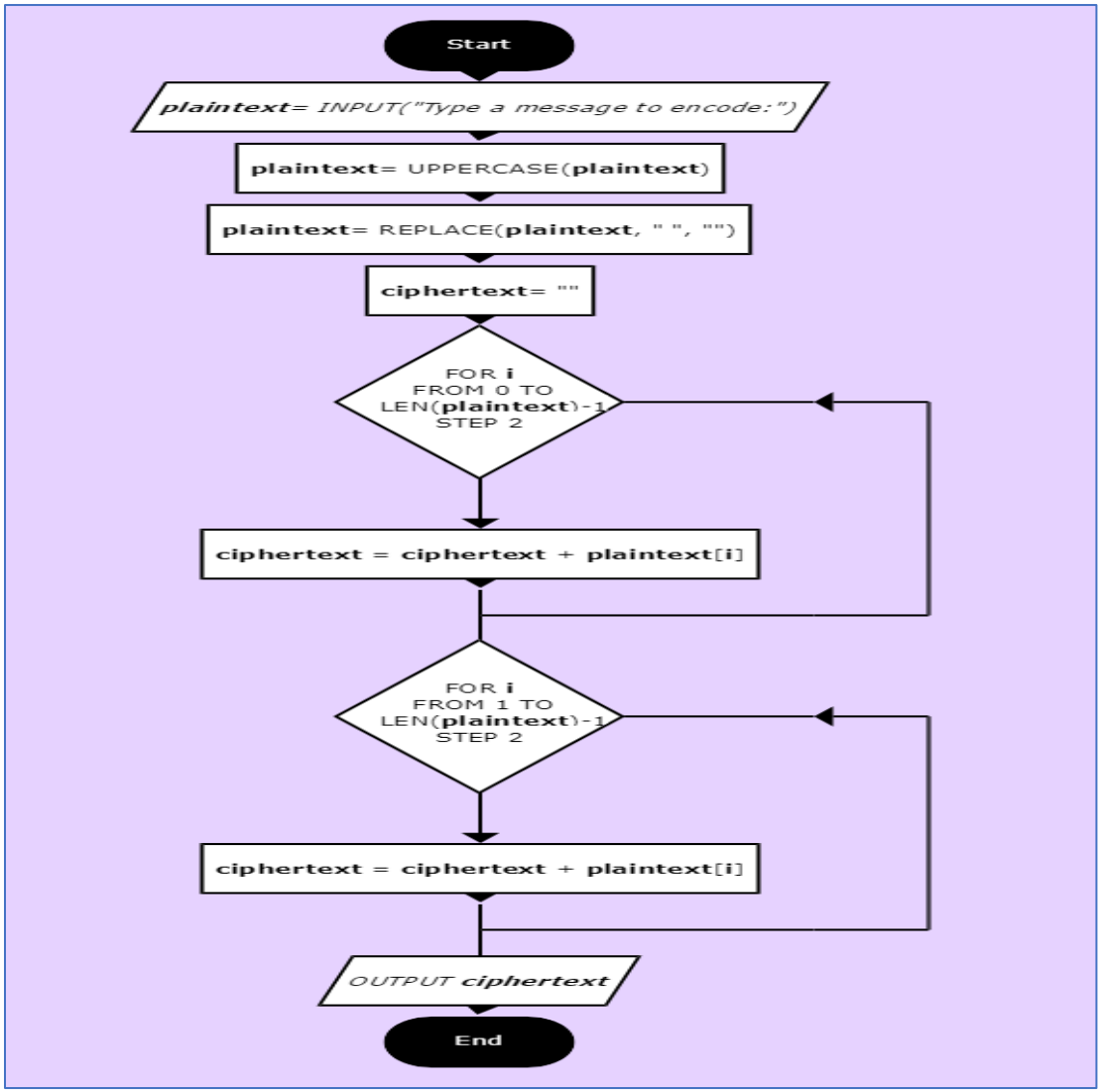
1. Number of columns of matrix= number of cipher text characters.
2. Number of rows = depth value that agree between S/R.
3. Draw the matrix depends on depth value and direction (**BU** or **TD**).
4. Distribute the cipher text DEPENDS on above idea.
5. Read zigzag to find plain text.

Example: consider the **plaintext** “This%is%a%secret%message”. Using **TD** with depth =4, let SPACE= %?

T						S						C						E						X
	h				I		%				E		r				M		S				e	
		I		%				A		S				e		%				S		G		
			S						%						T						A			

Therefore, the cipher text= “TSCE**X**HI%ERMSEI%ASE%SGS%TA”=25→ 4X25

H/W: Try to convert the following flowchart into C# program?



In RailFenec, may be use double Ciphering that of course need Double Deciphering:

Let the message =”information$security” use RF with depth =3 and BU, then encrypt result using Depth=2 and TD?

		F				A				N				C				T		
	N		O		M		T		O		$		E		U		I		Y	
I				R				I				S				R				X

C1=”FANCTNOMTO$EUIYIRISRX”

F		N		T		O		T		$		U		Y		R		S		X
	A		C		N		M		O		E		I		I		I		R	

C2=”FNTOT$UYRSXACNMOEIIIR”

P1=USING C2 DEPNDS ON DEPTH=2 AND TD???

P =USING P1 DEPNDS ON DEPTH=3 AND BU

Matrix Transposition:

Example: Grid the plaintext "Basharinmustansiriyah" using key=omar1?

O	m	a	r	1
4	3	2	5	1
B	a	s	h	a
r	$	i	n	$
m	u	s	t	a
n	s	i	r	i
y	a	h		

ciphertext= "a$aisisiha$usaBrmnyhntr

ABCDEFG…Z

0123456789

OMAR1990

NOTE(Muntader): all the **char** and **numbers** and **special char** must agree between S/R.

PLAINTEXT="INFORMATION%SECURITY"

O	**M**	**A**	**R**	**1**	**9**	**9**	**0**
7	6	5	8	2	3	4	1
I	N	F	R	M	A	T	I
O	N	%	S	E	C	U	R
I	T	Y	**X**	**X**	**X**	**X**	**X**

C= “IRXMEXACXTUXF%YNNTIOIRSX” LENGTH/KEY=CHAR IN EACH c

7	6	5	8	2	3	4	1
I	N	F	R	M	A	T	I
O	N	%	S	E	C	U	R
I	T	Y	**X**	**X**	**X**	**X**	**X**

PLAIN= INFRMATION%SECURITYXXXXX

EXAMPLE:

ENCRYPTE THE MESSGAE

“I CAN OPEN THE CAN BUT THE CAN CAN NOT OPEN IT SEALF”

USING DOUBLE MATRIX TRANSPOSTION WITH:

KEY1=”UOM1963”

KEY2=”SCIENCE”

TO FIND THE CIPHER TEXT?

U	O	M	1	9	6	3
7	**6**	**5**	**1**	**4**	**3**	**2**
I	C	A	N	O	P	E
N	T	H	E	C	A	N
B	U	T	T	H	E	C
A	N	C	A	N	N	O
T	O	P	E	N	I	T
S	E	A	L	F	**X**	**X**

C1=”NETAELENCOTXPAENIXOCHNNFAHTCPACTUNOEINBATS”

S	C	I	E	N	C	E
7	**1**	**5**	**3**	**6**	**2**	**4**
N	E	T	A	E	L	E
N	C	O	T	X	P	A
E	N	I	X	O	C	H
N	N	F	A	H	T	C
P	A	C	T	U	N	O
E	I	N	B	A	**T**	**S**

C2=”**ECNNAILPCTNTATXATBEAHCOSTOIFCNEXOHUANNENPE**”