COLLEGE OF BUSINESS EDUCATION

DAR-ES-SALAAM CAMPUS

INDIVIDUAL ASSIGNMENT

COURSE: DIT (A-TFC)

SUBJECT NAME: IT SECURITY

NAME: HENERY MWOMBEKI DIONIZ

REG NUMBER: 02.9585.21.01.2021

LECTURER NAME: ENG. MAKANTA. A. A

QUES TIONS

---

01. Encryption of the plain text message “PLEASE STUDY HARD TIME IS VERY SHORT” Using the Caesar cipher, play fair cipher and vigenere cipher
    - Caesar cipher key=**5**
    - Playfair and vigenere cipher the keyword = “**BUSINESS**”

i. Caesar cipher
Key=5
plaintext: "**PLEASE STUDY HARD TIME IS VERY SHORT**"

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

P = U L = G E = J A = V S = N E = J S = N T = Y U = P D = Y Y = D

H = C A = V R = M D = Y T = Y I = D M = H E = J I = D S = N V = Q E = J R = M Y = D S = N H = C O = J R = M T = Y

Therefore: PLEASE STUDY HARD TIME IS VERY SHORT = UGJVN YDYMJ DYNQJ JDCVN

ii. Playfair
keyword=BUSINESS
PLAINTEXT= PLEASE STUDY HARD TIME IS VERY SHORT

Table for the keyword "BUSINESS":

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

Break the plaintext into digraphs (pairs of two letters):

PL EA SE ST UD YH AR DT IM EI SV ER YS HO RT

Apply the Playfair rules for encryption

PL = SQ
EA = UB
SE = IH
ST = OP
UD = KY
YH = RA
AR = CE
DT = ID
IM = HI
EI = LD
SV = TR
ER = XA
YS = KY
HO =LE
RT =OH

Therefore: PLEASE STUDY HARD TIME IS VERY SHORT= SQ UB IH OP KY RA CE ID HI LD TR XA KY LE OH

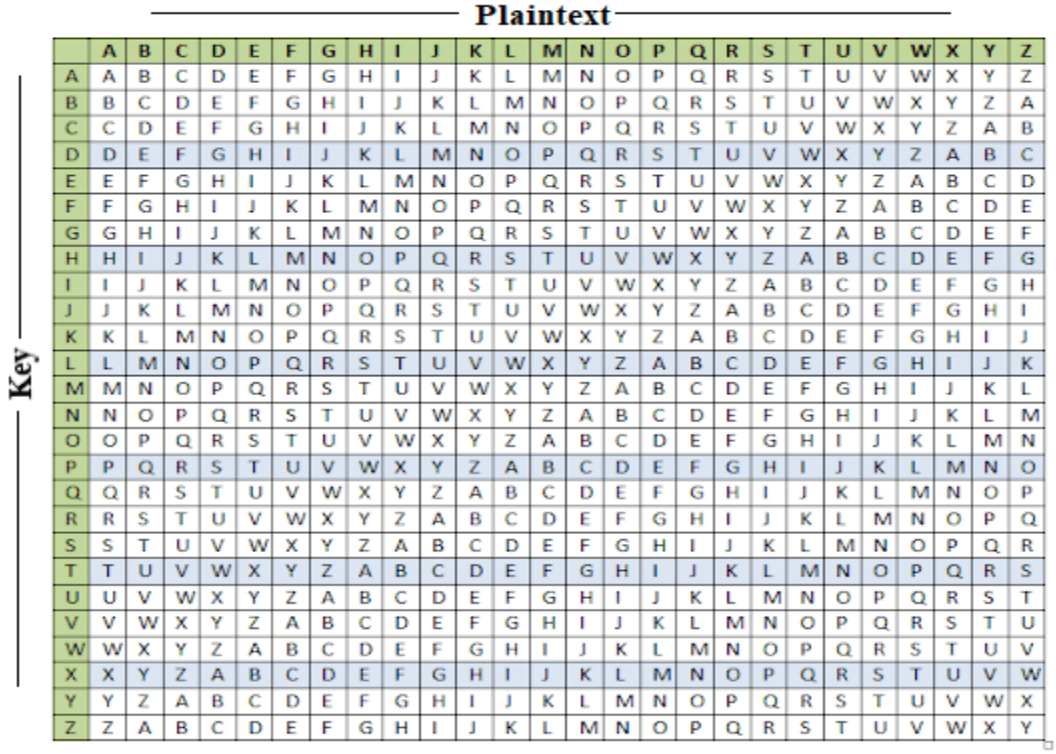
iii. vigenere cipher
keyword = "**BUSINESS**"
PLAINTEXT= PLEASE STUDY HARD TIME IS VERY SHORT

Step 1: Align the keyword with the plaintext

Plaintext: P L E A S E S T U D Y H A R D T I M E I S V E R Y S H O R T

Keyword: B U S I N E S S B U S I N E S S B U S I N E S S B U S I N E

By USING TABLE



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

Encrypt text will be: Q F W I F I C L C F L Z E E V Q A X F V K D K M U A

Using formula: ci=(pi+ki)(mod 26)
Plaintext: 15 11 4 0 18 4 18 19 20 3 24 7 0 17 3 19 8 12 3 8 18 8 18 20 7 3
Keyword: 1 20 18 8 13 4 8 18 18 8 13 18 4 13 18 18 8 11 8 13 18 18 8 18 13 19
Ciphertext: 16 5 22 8 5 8 2 11 2 5 11 25 4 4 21 16 0 23 5 21 10 3 10 12 20 0

Ciphertext: Q F W I F I C L C F L Z E E V Q A X F V K D K M U A