Assignment 02.

1. PT = SECURITY IS IMPORTANT.

Key = L

→ 1) Create a table of all letters & map to integer values:

PT:	S	E	C	U	R	I	T	Y	I	S	I	M	P	O	R	T	A	N	T
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
	18	4	2	20	17	8	19	24	8	18	8	12	15	14	17	19	0	13	19

2) Convert the key to it's int value.

Key $\overset{L}{\downarrow}$ 11

3) Encryption: $C_i = (P_i * K) \bmod 26$

$C_1 = (18 \times 11) \bmod 26 = 16$

$C_2 = (4 \times 11) \bmod 26 = 18$

$C_3 = (2 \times 11) \bmod 26 = 22$

$C_4 = (20 \times 11) \bmod 26 = 12$

$C_5 = (17 \times 11) \bmod 26 = 5$

$C_6 = (8 \times 11) \bmod 26 = 10$

$C_7 = (19 \times 11) \bmod 26 = 1$

$C_8 = (24 \times 11) \bmod 26 = 4$

$C_9 = (8 \times 11) \bmod 26 = 10$

$C_{10} = (18 \times 11) \bmod 26 = 16$

$C_{11} = (8 \times 11) \bmod 26 = 10$

$C_{12} = (12 \times 11) \bmod 26 = 2$

$C_{13} = (15 \times 11) \bmod 26 = 9$

$C_{14} = (14 \times 11) \bmod 26 = 24$

$C_{15} = (17 \times 11) \bmod 26 = 5$

$C_{16} = (19 \times 11) \bmod 26 = 1$

$C_{17} = (0 \times 11) \bmod 26 = 0$

$C_{18} = (13 \times 11) \bmod 26 = 13$

$C_{19} = (19 \times 11) \bmod 26 = 1$

16	18	22	12	5	10	1	4	10	16	10	2	9
Q	S	W	M	F	K	B	E	K	Q	K	C	J
24	5	1	0	13	1							
Y	F	B	A	N	B							

CT = QSWMFKBEKQKCJYFBANB.

Decryption :- $P_i = (i * K^{-1}) \bmod 26.$

$K = 11, \quad K^{-1} = ?$

q	r_1	r_2	r	t_1	t_2	$t = (t_1 - (q * t_2))$
2	26	11	4	0	1	-2
2	11	4	~~4~~ 3	~~0~~ 1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
	1	0		$\boxed{-7}$	26	

$K^{-1} = -7 + 26 = \underline{\underline{19}}.$

$P_1 = (16 \times 19) \bmod 26 = 18$
$P_2 = (18 \times 19) \bmod 26 = 4$
$P_3 = (22 \times 19) \bmod 26 = 2$
$P_4 = (12 \times 19) \bmod 26 = 20$
$P_5 = (5 \times 19) \bmod 26 = 17$
$P_6 = (10 \times 19) \bmod 26 = 8$
$P_7 = (1 \times 19) \bmod 26 = 19$
$P_8 = (4 \times 19) \bmod 26 = 24$
$P_9 = (10 \times 19) \bmod 26 = 8$

$P_{10} = (16 \times 19) \bmod 26 = 18$
$P_{11} = (10 \times 19) \bmod 26 = 8$
$P_{12} = (2 \times 19) \bmod 26 = 12$
$P_{13} = (9 \times 19) \bmod 26 = 15$
$P_{14} = (24 \times 19) \bmod 26 = 14$
$P_{15} = (5 \times 19) \bmod 26 = 17$
$P_{16} = (1 \times 19) \bmod 26 = 19$
$P_{17} = (0 \times 19) \bmod 26 = 0$
$P_{18} = (13 \times 19) \bmod 26 = 13$
$P_{19} = (1 \times 19) \bmod 26 = 19$

18	4	2	20	17	8	19	24	8	18	8
S	E	C	U	R	I	T	Y	I	S	I

12	15	14	17	19	0	13	19
M	P	O	R	T	A	N	T

Q2. P.T = Attack is today.
Key = D.

P.T = "A T T A C K   IS   T O D A Y
0 19 19 0 2 10   8 18   19 14 3 0 24.

Key   D
3

Encryption :- $C_i = (P_i * K) \bmod 26.$

$c_1 = (0 \times 3) \bmod 26 = 0$

$c_2 = (19 \times 3) \bmod 26 = 5$

$c_3 = (19 \times 3) \bmod 26 = 5$

$c_4 = (0 \times 3) \bmod 26 = 0$

$c_5 = (2 \times 3) \bmod 26 = 6$

$c_6 = (10 \times 3) \bmod 26 = 4$

$c_7 = (8 \times 3) \bmod 26 = 24$

$c_8 = (18 \times 3) \bmod 26 = 2$

$c_9 = (19 \times 3) \bmod 26 = 5$

$c_{10} = (14 \times 3) \bmod 26 = 16$

$c_{11} = (3 \times 3) \bmod 26 = 9$

$c_{12} = (0 \times 3) \bmod 26 = 0$

$c_{13} = (24 \times 3) \bmod 26 = 20.$

0	5	5	0	6	4	24	2	5	16	9	0	20
A	F	F	A	G	E	Y	C	F	Q	J	A	U

C.T. = AFFAGEYCFQJAU.

$K = 3$, $K^{-1} = ?$

q	r_1	r_2	r	t_1	t_2	$t = (t_1 - (q * t_2))$
7	26	3	5	0	1	-7
0	3	5	3	1	-7	1
1	5	3	2	-7	1	-8
1	3	2	1	1	-8	9
2	2	1	0	-8	9	-26
	1	0		$\boxed{9}$	-26	

$K = 3$, $K^{-1} = 9$.

$P_i = (C_i \times K^{-1}) \bmod 26$.

$P_1 = (0 \times 9) \text{ Mod } 26 = 0$	$P_8 = (2 \times 9) \% 26 = 18$
$P_2 = (5 \times 9) \text{ mod } 26 = 19$	$P_9 = (5 \times 9) \% 26 = 19$
$P_3 = (5 \times 9) \text{ mod } 26 = 19$	$P_{10} = (16 \times 9) \% 26 = 14$
$P_4 = (0 \times 9) \text{ mod } 26 = 0$	$P_{11} = (9 \times 9) \% 26 = 3$
$P_5 = (6 \times 9) \text{ mod } 26 = 2$	$P_{12} = (0 \times 9) \% 26 = 0$
$P_6 = (4 \times 9) \text{ mod } 26 = 10$	$P_{13} = (20 \times 9) \% 26 = 24$
$P_7 = (24 \times 9) \text{ mod } 26 = 8$	

0	19	19	0	2	10	8	18	19	14	3	0	24
A	T	T	A	C	K	I	S	T	O	D	A	Y

P.T = Attack is today.