# Assignment 201

Q1. P.T. = GOOD MORNING.

Key = (7, 9) → additive (K2)
↓
multiplicative (K1)

| G | O | O | D | | M | O | R | N | I | N | G |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 6 | 14 | 14 | 3 | | 12 | 14 | 17 | 13 | 8 | 13 | 6 |

Encryption :- $C_i = [(P_i \times K_1) + K_2] \bmod 26$.

$C_1 = (42+9) \% 26 = 25$
$C_2 = (98+9) \% 26 = 3$
$C_3 = (98+9) \% 26 = 3$
$C_4 = (21+9) \% 26 = 4$
$C_5 = (84+9) \% 26 = 15$
$C_6 = (98+9) \% 26 = 3$
$C_7 = (119+9) \% 26 = 24$
$C_8 = (91+9) \% 26 = 22$
$C_9 = (56+9) \% 26 = 13$
$C_{10} = (91+9) \% 26 = 22$
$C_{11} = (42+9) \% 26 = 25$

| 25 | 3 | 3 | 4 | 15 | 3 | 24 | 22 | 13 | 22 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|
| Z | D | D | E | P | D | Y | W | N | W | Z |

C.T = ZDDEPDYWNWZ.

Decryption :- $P_i = [C_i - K_2) * K_i^{-1}] \bmod 26$.

$K_1 = 7$ ; $K_i^{-1} = ?$

| q | $r_1$ | $r_2$ | r | $t_1$ | $t_2$ | $t = (t_1 - (q \times t_2)]$ |
|---|---|---|---|---|---|---|
| 3 | 26 | 7 | 5 | 0 | 1 | -3 |
| 1 | 7 | 5 | 2 | 1 | -3 | 4 |
| 2 | 5 | 2 | 1 | -3 | 4 | -11 |
| 2 | 2 | 1 | 0 | 4 | -11 | 26 |

1 ← 90 ← [-11] ← 26

$k^{-1} = -11 + 26 = 15$.

$P_1 = (6 \times 15) \% 26 = 6$
$P_2 = (-6 \times 15) \% 26 = 14$
$P_3 = (-6 \times 15) \% 26 = 14$
$P_4 = (-5 \times 15) \% 26 = 3$
$P_5 = (6 \times 15) \% 26 = 12$
$P_6 = (-6 \times 15) \% 26 = 14$
$P_7 = (15 \times 15) \% 26 = 17$
$P_8 = (13 \times 15) \% 26 = 13$
$P_9 = (4 \times 15) \% 26 = 8$
$P_{10} = (13 \times 15) \% 26 = 13$
$P_{11} = (16 \times 15) \% 26 = 6$

6 14 14 3 12 14 17 13 8 13 6
G O O D M O R N I N G

P.T. = Good Morning.

Q2. PT = AFFINE CIPHER.
Key = (7, 15).
$K_1$ $K_2$

PT. A F F I N E C I P H E R
0 5 5 8 13 4 2 8 15 7 4 17

Encryption:- $C_i = [(P_i \times K_1) + K_2] \% 26$

$C_1 = (0 + 15) \% 26 = 15$
$C_2 = (35 + 15) \% 26 = 24$
$C_3 = (35 + 15) \% 26 = 24$
$C_4 = (56 + 15) \% 26 = 19$
$C_5 = (91 + 15) \% 26 = 2$
$C_6 = (28 + 15) \% 26 = 17$
$C_7 = (14 + 15) \% 26 = 3$
$C_8 = (56 + 15) \% 26 = 19$
$C_9 = (105 + 15) \% 26 = 16$
$C_{10} = (99 + 15) \% 26 = 12$
$C_{11} = (28 + 15) \% 26 = 17$
$C_{12} = (119 + 15) \% 26 = 4$

15 24 24 19 2 17 3 19 16 12 17 4
CT = P Y Y T C R D T Q M R E

C.T = P U Y T C R D T Q M R E.

Decryption:- $P_i = [(C_i - K_2) * K_1^{-1}] \bmod 26$.

$K_1 = 7$, $K_1^{-1} = ?$

| q | $r_1$ | $r_2$ | r | $t_1$ | $t_2$ | $t = (t_1 - q \times t_2)$ |
|---|---|---|---|---|---|---|
| 3 | 26 | 7 | 5 | 0 | 1 | -3 |
| 1 | 7 | 5 | 2 | 1 | -3 | 4 |
| 2 | 5 | 2 | 1 | -3 | 4 | -11 |
| 2 | 2 | 1 | 0 | 4 | -11 | 26 |
| 1 | 0 | | | [-11] | 26 | |

$K_1^{-1} = -11 + 26 = 15$.

| | |
|---|---|
| $P_1 = (0 \times 15) \% 26 = 0$ | $P_7 = (-12 \times 15) \% 26 = 2$ |
| $P_2 = (9 \times 15) \% 26 = 5$ | $P_8 = (4 \times 15) \% 26 = 8$ |
| $P_3 = (9 \times 15) \% 26 = 5$ | $P_9 = (1 \times 15) \% 26 = 15$ |
| $P_4 = (4 \times 15) \% 26 = 8$ | $P_{10} = (-3 \times 15) \% 26 = 7$ |
| $P_5 = (-13 \times 15) \% 26 = 13$ | $P_{11} = (2 \times 15) \% 26 = 4$ |
| $P_6 = (2 \times 15) \% 26 = 4$ | $P_{12} = (-11 \times 15) \% 26 = 17$ |

0 5 5 8 13 4 2 8 15 7 4 17

A F F I N E C I P H E R.

P.T = Affine Cipher.