

Name: Karl Kinji S. Landicho

Section: BSIT 3A

Assignment#4

Requirement:

Decrypt: ZAF STA PWH TXP LUX LBV ANK SUT QMO LLM FSL YAE FTW JPI

3 X 3 key MATRIX MOD 26:

| | | | | | | | | | |
|----|---|---|----|----|---|----|----|---|----|
| Z | A | F | S | T | A | P | W | H | T |
| 25 | 0 | 5 | 18 | 19 | 0 | 15 | 22 | 7 | 19 |

| | | | | | | | | |
|----|----|----|----|----|----|---|----|---|
| X | P | L | U | X | L | B | V | A |
| 23 | 15 | 11 | 20 | 23 | 11 | 1 | 21 | 0 |

| | | | | | | | |
|----|----|----|----|----|----|----|----|
| N | K | S | U | T | Q | M | O |
| 13 | 10 | 18 | 20 | 19 | 16 | 12 | 14 |

| | | | | | |
|----|----|----|---|----|----|
| L | L | M | F | S | L |
| 11 | 11 | 12 | 5 | 18 | 11 |

| | | | | | | | | |
|----|---|---|---|----|----|---|----|----|
| Y | A | E | F | T | W | J | P | I |
| 21 | 0 | 4 | 5 | 19 | 22 | 9 | 15 | 18 |

Key Inverse:

$$\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

Solutions:

ZAF

$$\begin{aligned}(1, 2, 3) &= (25 \ 0 \ 5) \\&= (25 \times 4 + 0 \times 15 + 5 \times 24 \quad 25 \times 9 + 0 \times 17 + 5 \times 0 \quad 25 \times 15 + 0 \times 6 + 5 \times 17) \bmod 26 \\&= (220 \ 225 \ 460) \\&= (12 \ 17 \ 18) \\&= (M \ R \ S) \text{ M R S}\end{aligned}$$

STA

$$\begin{aligned}(1, 2, 3) &= (18 \ 19 \ 0) \\&= (18 \times 4 + 19 \times 15 + 0 \times 24 \quad 18 \times 9 + 19 \times 17 + 0 \times 0 \quad 18 \times 15 + 19 \times 6 + 0 \times 17) \bmod 26 \\&= (357 \ 485 \ 384) \\&= (19 \ 17 \ 20) \\&= (T \ R \ U) \text{ T R U}\end{aligned}$$

PWH

$$\begin{aligned}(1, 2, 3) &= (15 \ 22 \ 7) \\&= (15 \times 4 + 22 \times 15 + 7 \times 24 \quad 15 \times 9 + 22 \times 17 + 7 \times 0 \quad 15 \times 15 + 22 \times 6 + 7 \times 17) \bmod 26 \\&= (558 \ 509 \ 476) \\&= (12 \ 15 \ 8) \\&= (M \ P \ I) \text{ M P I}\end{aligned}$$

TXP

$$\begin{aligned}(1, 2, 3) &= (19 \ 23 \ 15) \\&= (19 \times 4 + 23 \times 15 + 15 \times 24 \quad 19 \times 9 + 23 \times 17 + 15 \times 0 \quad 19 \times 15 + 23 \times 6 + 15 \times 17) \bmod 26 \\&= (781 \ 562 \ 678) \\&= (1 \ 16 \ 2) \\&= (B \ Q \ C) \text{ F Y O}\end{aligned}$$

LUX

$$\begin{aligned}(1, 2, 3) &= (11 \ 20 \ 23) \\&= (11 \times 4 + 20 \times 15 + 23 \times 24 \quad 11 \times 9 + 20 \times 17 + 23 \times 0 \quad 11 \times 15 + 20 \times 6 + 23 \times 17) \bmod 26 \\&= (896 \ 439 \ 676) \\&= (12 \ 23 \ 0) \\&= (M \ X \ A) \text{ U P E}\end{aligned}$$

LBV

$$\begin{aligned}(1, 2, 3) &= (11 \ 1 \ 21) \\&= (11 \times 4 + 1 \times 15 + 21 \times 24 \quad 11 \times 9 + 1 \times 17 + 21 \times 0 \quad 11 \times 15 + 1 \times 6 + 21 \times 17) \bmod 26 \\&= (563 \ 116 \ 528) \\&= (17 \ 12 \ 8) \\&= (R \ M \ I) \text{ R M I}\end{aligned}$$

ANK

$$\begin{aligned}(1, 2, 3) &= (0 \ 13 \ 10) \\&= (0 \times 4 + 13 \times 15 + 10 \times 24 \quad 0 \times 9 + 13 \times 17 + 10 \times 0 \quad 0 \times 15 + 13 \times 6 + 10 \times 17) \bmod 26 \\&= (435 \ 221 \ 248) \\&= (19 \ 13 \ 14) \\&= (T \ N \ O) \text{ T N O}\end{aligned}$$

SUT

$$\begin{aligned}(1, 2, 3) &= (18 \ 20 \ 19) \\&= (18 \times 4 + 20 \times 15 + 17 \times 24 \quad 18 \times 9 + 20 \times 17 + 19 \times 0 \quad 18 \times 15 + 20 \times 6 + 19 \times 17) \bmod 26 \\&= (780 \ 502 \ 713) \\&= (0 \ 8 \ 11) \\&= (A \ I \ L) \text{ W I L}\end{aligned}$$

QMO

$$\begin{aligned}(1, 2, 3) &= (16 \ 12 \ 14) \\&= (16x4+12x15+14x24 \quad 16x9+12x17+14x0 \quad 16x15+12x6+14x17) \bmod 26 \\&= (580 \ 348 \ 550) \\&= (8 \ 10 \ 4) \\&= (I \ K \ E) \text{IKE}\end{aligned}$$

LLM

$$\begin{aligned}(1, 2, 3) &= (11 \ 11 \ 12) \\&= (11x4+11x15+12x24 \quad 11x9+11x17+12x0 \quad 11x15+11x6+12x17) \bmod 26 \\&= (497 \ 286 \ 435) \\&= (3 \ 0 \ 19) \\&= (D \ A \ T) \text{DAT}\end{aligned}$$

FSL

$$\begin{aligned}(1, 2, 3) &= (5 \ 18 \ 11) \\&= (5x4+18x15+11x24 \quad 5x9+18x17+11x0 \quad 5x15+18x6+11x17) \bmod 26 \\&= (554 \ 351 \ 365) \\&= (8 \ 13 \ 1) \\&= (I \ N \ B) \text{ING}\end{aligned}$$

YAE

$$\begin{aligned}(1, 2, 3) &= (21 \ 0 \ 4) \\&= (21x4+0x15+4x24 \quad 21x9+0x17+4x0 \quad 21x15+0x6+4x17) \bmod 26 \\&= (180 \ 189 \ 383) \\&= (24 \ 7 \ 19) \\&= (Y \ H \ T) \text{KIM}\end{aligned}$$

FTW

$$(1, 2, 3) = (5 \ 19 \ 22)$$

$$= (5 \times 4 + 19 \times 15 + 22 \times 24 \qquad 5 \times 9 + 19 \times 17 + 22 \times 0 \qquad 5 \times 15 + 19 \times 6 + 22 \times 17) \bmod 26$$

$$= (833 \ 368 \ 505)$$

$$= (1 \ 4 \ 11)$$

$$= (\text{B} \ \text{E} \ \text{T}) \text{B E R}$$

JPI

$$(1, 2, 3) = (9 \ 15 \ 18)$$

$$= (9 \times 4 + 15 \times 15 + 18 \times 24 \qquad 9 \times 9 + 15 \times 17 + 18 \times 0 \qquad 9 \times 15 + 15 \times 6 + 18 \times 17) \bmod 26$$

$$= (693 \ 336 \ 531)$$

$$= (17 \ 24 \ 11)$$

$$= (\text{R} \ \text{Y} \ \text{L}) \text{L Y X}$$

FINAL ANSWER: MRS TRU MPI BQC MXA RMI TNO AIL IKE DAT INB YHT BET RYL