part-1

$$C = E([a,b], p)$$

$$= (ap + b) \bmod 26$$

$a = 3$, $b = 7$

plain text:

My name is [___]. I am a graduate student.

a, b, c, ..., z

0, 1, 2, , 25

$m = 12$

$(3(12) + 7) \bmod 26 \rightarrow 16 \rightarrow p$

my $\longrightarrow$ rb

$y = 24$

$(3(24)+7) \bmod 26 = 1 \rightarrow b$

rb uhrt fj [varies] F hr

h zghqphmt jmpqtum

Ciphertext

part 2

$$C = (3p + 7) \bmod 26$$

$$C + 19 = (3p) \bmod 26$$

1P

$$(9 \cdot 3) \bmod 26 = 1$$

$$a(c + 19) = p \bmod 26$$

$$p = (9c + 15) \bmod 26$$

Decryption

$r = 16 \quad (9(16) + 15) \bmod 26 = 12 \rightarrow m$

$b = 1 \quad (9(1) + 15) \bmod 26 = 24 \rightarrow y$

my . . . . . .

part 3

C = Not one-to-one

$E([a,b],p) = E([2,3],p)$

$=$

$a = 0$ $\quad C = (2(0)+3) \bmod 26 = 3 \rightarrow d$

$n = 13$ $\quad (2(13)+3) \bmod 26 = 3$

a and 26 should not have any common factors.

2, 13

$a \neq \underline{2}, 4, 6, \ldots$

$a \neq \underline{13}, \ldots$

$b = 0, 1, 2, \ldots, 25$ ← 26 b's

$a = 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$

→ 12 a's

$[a, b]$

→ $26 \times 12 = 312$ keys

Using Affine caesar cipher,
the most frequent letter of
cipher is 'b', the second
most frequent letter is 'U'.
Break the code.

$e=4$ $(\underline{a}(4)+\underline{b}) \bmod 26 = 1$ ① $\underline{b=1}$

$t=19$ $(\underline{a}(19)+\underline{b}) \bmod 26 = 20$ ② $a=20$

② − ① : $(15a) \bmod 26 = 19$

$a \neq 1$

$a \neq 2$

$\boxed{a = 3}$

$$(3(4) + b) \bmod 26 = 1$$

$$12$$

$$\boxed{b = 15}$$

$$[a, b] = [3, 15]$$

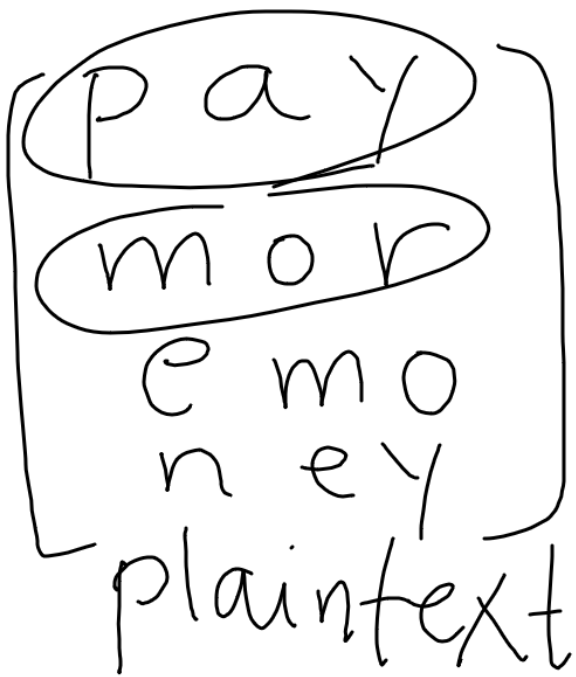
Hill Cipher :

$$C = (P \cdot K) \bmod 26$$

matrix $n \times n$

C, P : row vectors $1 \times n$

$$K = \begin{pmatrix} K_{11} & K_{12} & \cdots & K_{1n} \\ \vdots & \ddots & & \vdots \\ K_{n1} & K_{n2} & \cdots & K_{nn} \end{pmatrix}$$



plaintext :

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

pay more money

P_1 P_2 . . . .

$$[p \quad a \quad y] = [15 \quad 0 \quad 24]$$

$$\left([15 \quad 0 \quad 24] \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \right) \bmod 26$$

1×3 $\quad$ 3×3

$$[303 \quad 303 \quad 531] \bmod 26 = [17 \quad 17 \quad 11]$$

R R L

rrl mwb kas pdh

$$\begin{bmatrix} r & r & l \\ m & w & \\ \vdots & & \\ \vdots & & \end{bmatrix}$$

$$C = (P \cdot K) \bmod 26$$

$$C \cdot K^{-1} = (P \cdot K \cdot K^{-1}) \bmod 26$$

Inverse Matrix of K

$$P = (C \cdot K^{-1}) \bmod 26$$