Hill Cipher $K = \begin{bmatrix} 6 & 5 \\ 3 & 5 \end{bmatrix}$ $C = P.K \bmod 26$

part 1

plaintext = first name = $\underbrace{Mo}\underbrace{ay}\underbrace{ed}$

$$P = \begin{bmatrix} m & o \\ a & y \\ e & d \end{bmatrix} = \begin{bmatrix} 12 & 14 \\ 0 & 24 \\ 4 & 3 \end{bmatrix}$$

$$C = \text{"kaughj"}$$

$$C = \begin{bmatrix} 12 & 14 \\ 0 & 24 \\ 4 & 3 \end{bmatrix}_{3\times 2} \begin{bmatrix} 6 & 5 \\ 3 & 5 \end{bmatrix}_{2\times 2} \bmod 26$$

$$= \begin{bmatrix} 114 & 130 \\ 72 & 120 \\ 33 & 35 \end{bmatrix} \bmod 26 = \underbrace{\begin{bmatrix} 10 & 0 \\ 20 & 16 \\ 7 & 9 \end{bmatrix}}_{} = \begin{bmatrix} k & a \\ u & q \\ h & j \end{bmatrix}$$

part 2

$$K = \begin{bmatrix} 6 & 5 \\ 3 & 5 \end{bmatrix}$$

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

$$\det K = 6(5) - 3(5) = 15$$

$$\underline{(\det K)^{-1}} \bmod \underline{26} = ? = 7$$

$$(1 \times 15) \bmod 26 = 15 \neq 1$$

$$\vdots$$

$$(7 \times 15) \bmod 26 = 1$$

$$K^{-1} \bmod 26 = 7 \begin{bmatrix} 5 & -5 \\ -3 & 6 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 35 & -35 \\ -21 & 42 \end{bmatrix} \bmod 26 = \begin{bmatrix} 9 & 17 \\ 5 & 16 \end{bmatrix} \bmod 26$$

$$P = \begin{bmatrix} 10 & 0 \\ 20 & 16 \\ 7 & 9 \end{bmatrix} \begin{bmatrix} 9 & 17 \\ 5 & 16 \end{bmatrix} \bmod 26 =$$

$$= \begin{bmatrix} 90 & 170 \\ 260 & 596 \\ 108 & 263 \end{bmatrix} \bmod 26 = \begin{bmatrix} 12 & 14 \\ 0 & 24 \\ 4 & 3 \end{bmatrix} = \begin{bmatrix} m & o \\ a & y \\ e & d \end{bmatrix}$$

part 3

NO.
$$\begin{bmatrix} 6 & 3 \\ 2 & 5 \end{bmatrix}$$

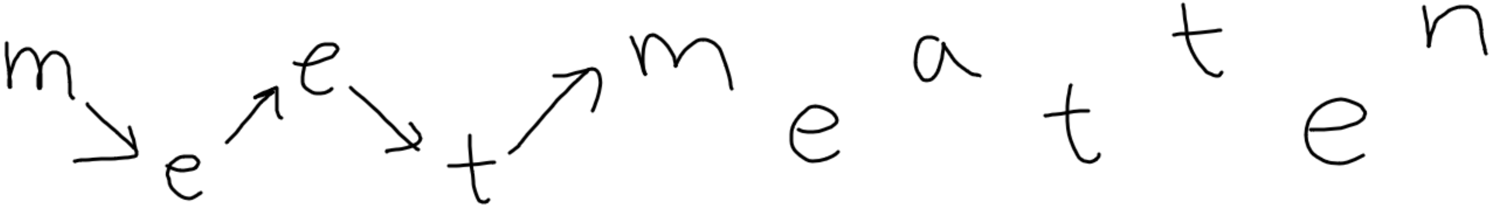
$$\det K = \det\begin{pmatrix} 6 & 3 \\ 2 & 5 \end{pmatrix} = 30 - 6 = 24$$

since det(K) is not prime wrt 26, we won't get unique multiplicative inverse modulo.

Transposition Cipher :

- rail fence

P = meet me at ten



C = mematnetete

<u></u>**encryption**: Write plaintext diagonally, read horizonally.

```
m   e   m   a   t   n
  e   t   e   t   e
```

decryption:

write horizontally,

read diagonally.

More complex:

plaintext = Attack postponed until two am

Key:	4	3	1	2	5	6	7
	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

Ciphertext:

ttna aptm tsuo aodw coix knly

→ petz

Decryption:

Key: 4 3 1 2 5 6 7

read horizontally →

t
t
n
a

$$4 = \frac{\text{length of ciphertext}}{\text{length of key}}$$

two stage

$$P \xrightarrow{K} \underline{\underline{C}} \xrightarrow{K} \underbrace{C'}_{\text{output}}$$

Key:	4	3	1	2	5	6	7
	t	t	n	a	a	p	t
	m	t	s	u	o	a	o
	d	w	c	o	i	x	k
	n	l	y	p	e	t	z

Final output

ciphertext:

nscyauop t t wltmdn aoie

→ paxt tokz