Hill Cipher ⇒ developed by Mathematician Lester Hill in 1929

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o

15	16	17	18	19	20	21	22	23	24	25
p	q	r	s	t	u	v	w	x	y	z

Note: In previous ciphers we take one character or two characters and convert them to ciphertext. But here we ~~have~~ can take 'm' plaintext letters and substitute to get 'm' ciphertext.

Procedure

* Select a Message to Encrypt.

welcome — if m=2 [we are going to take 2 characters

we lc om e → add any character to 'e' So it becomes 2 characters

↓

we lc om ea

* Select a key.

if the m value is 2 then key shd be 2x2 matrix

if the m value is 3 then key shd be 3x3 matrix

So the size of ~~key~~ the key depends on number of characters we take to encrypt.

So let key = 'test' (key size is 4)

* Assign a numerical value equivalent to each
a → 0, b → 1 ....

* Convert the key "test" to a 2×2 matrix

$$K = \begin{bmatrix} t & e \\ s & t \end{bmatrix} = \begin{bmatrix} 19 & 4 \\ 18 & 19 \end{bmatrix}$$ using table

* Convert the message 'Welcome' to a 'n' Component vector. where n = 2

Plain text — We lc om ea

$$\begin{pmatrix} w \\ e \end{pmatrix} \begin{pmatrix} l \\ c \end{pmatrix} \begin{pmatrix} o \\ m \end{pmatrix} \begin{pmatrix} e \\ a \end{pmatrix}$$

$$\begin{pmatrix} 22 \\ 4 \end{pmatrix} \begin{pmatrix} 11 \\ 2 \end{pmatrix} \begin{pmatrix} 14 \\ 12 \end{pmatrix} \begin{pmatrix} 4 \\ 0 \end{pmatrix}$$

* Ciphertex = K * P mod 26 = $K * \begin{pmatrix} w \\ e \end{pmatrix}$ mod 26

$$= \begin{pmatrix} 19 & 4 \\ 18 & 19 \end{pmatrix} * \begin{pmatrix} 22 \\ 4 \end{pmatrix} \text{ mod } 26$$

$$= \begin{pmatrix} 19*22 + 4*4 \\ 18*22 + 19*4 \end{pmatrix} \text{ mod } 26$$

$$= \begin{pmatrix} 418 \\ 434 + 16 \\ 396 \\ 415 + 76 \end{pmatrix} \text{ mod } 26$$

$$= \begin{pmatrix} 434 \\ 453 \\ 490 \end{pmatrix} \text{ mod } 26 = \begin{pmatrix} 18 \\ 14 \\ 4 \end{pmatrix}$$ using table.

$$\Rightarrow \begin{pmatrix} t \\ o \end{pmatrix} \begin{pmatrix} s \\ e \end{pmatrix}$$

$$k * \begin{pmatrix} l \\ c \end{pmatrix} \bmod 26 = \begin{pmatrix} 19 & 4 \\ 18 & 19 \end{pmatrix} * \begin{pmatrix} 11 \\ 2 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 19*11 + 4*2 \\ 18*11 + 19*2 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 209 + 8 \\ 198 + 38 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 9 \\ 2 \end{pmatrix} = \begin{pmatrix} j \\ c \end{pmatrix}$$

$$k * \begin{pmatrix} o \\ m \end{pmatrix} \bmod 26 = \begin{pmatrix} 19 & 4 \\ 18 & 19 \end{pmatrix} * \begin{pmatrix} 14 \\ 12 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 19*14 + 4*12 \\ 18*14 + 19*12 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 266 + 48 \\ 252 + 228 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 314 \\ 480 \end{pmatrix} \bmod 26 = \begin{pmatrix} 2 \\ 12 \end{pmatrix} = \begin{pmatrix} c \\ m \end{pmatrix}$$

$$k * \begin{pmatrix} e \\ a \end{pmatrix} \bmod 26 = \begin{pmatrix} 19 & 4 \\ 18 & 19 \end{pmatrix} * \begin{pmatrix} 4 \\ 0 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 19 \times 4 + 4 \times 0 \\ 18 \times 4 + 19 \times 0 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 76 \\ 72 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 24 \\ 20 \end{pmatrix} = \begin{pmatrix} y \\ u \end{pmatrix}$$

Plain text = Welcome a

∴ Ciphes Text = jccmyu se

Decryption

Plaintext = $k^{-1} c \bmod 26$

$k^{-1} = 1/|k|\ adj(k)$

$|k|$ – determinant of k
$adj(k)$ – adjoint of k

(1) Compute $\frac{1}{|k|}$

$$k = \begin{bmatrix} 19 & 4 \\ 18 & 19 \end{bmatrix}$$

$$|k| = \begin{vmatrix} 19 & 4 \\ 18 & 19 \end{vmatrix} = (19 \times 19) - (18 \times 4)$$
$$= 361 - 72$$
$$= 289$$

Note
The result $|k|$ shd not be equal to '0'. If zero then these is something wrong.
ie) $\frac{1}{|k|} = \frac{1}{0}$ = undefined. So we cannot selelt key like this.

(2) Determine Multiplicative Inverse.

$289\ x \bmod 26 = 1$
$\Rightarrow 3\ x \bmod 26 = 1$
$3 * 9 \bmod 26 = 1$
So $\boxed{x = 9}$

$26 \overline{)289}\ (11$
26
29
26
3

15-5
18
21
24
27

Note: gcd(289, 26) shd be 1, then we can find the multiplicative Inverse.

So $\boxed{\frac{1}{|k|} = 9}$

* Compute adj(k)

$$k = \begin{pmatrix} 19 & 4 \\ 18 & 19 \end{pmatrix}$$

Now interchange 19 and 19 and change the sign for 4 and 18.

$$\text{So adj}(k) = \begin{pmatrix} 19 & -4 \\ -18 & +19 \end{pmatrix}$$

* $k^{-1} = \frac{1}{|k|} \text{adj}(k)$

$$= 9 * \begin{pmatrix} +19 & -4 \\ -18 & +19 \end{pmatrix}$$

$$= \begin{pmatrix} +9*9 & -4*9 \\ -18*9 & +19*9 \end{pmatrix} = \begin{pmatrix} +81 & -36 \\ -162 & +171 \end{pmatrix}$$

Since we have negative numbers, add 26 with the negative numbers.

$$k^{-1} = \begin{pmatrix} 81 & -36+26 \\ -162+26 & 171 \end{pmatrix} = \begin{pmatrix} 81 & \\ & 171 \end{pmatrix}$$

$$= 9 * \begin{pmatrix} 19 & -4+26 \\ -18+26 & 19 \end{pmatrix}$$

$$= 9 * \begin{pmatrix} 19 & 22 \\ 8 & 19 \end{pmatrix}$$

$$k^{-1} = \begin{pmatrix} 171 & 198 \\ 72 & 171 \end{pmatrix}$$

* $K^{-1} * C \bmod 26 = \begin{pmatrix} 181 & 198 \\ 72 & 171 \end{pmatrix} \begin{pmatrix} 18 \\ 4 \end{pmatrix} \bmod 26$

$= \begin{pmatrix} 171 \times 18 + 198 \times 4 \\ 72 \times 18 + 171 \times 4 \end{pmatrix} \bmod 26$

$= \begin{pmatrix} 3078 + 792 \\ 1296 + 684 \end{pmatrix} \bmod 26$

$= \begin{pmatrix} 3870 \\ 1980 \end{pmatrix} \bmod 26$

$= \begin{pmatrix} 22 \\ 4 \end{pmatrix} = \begin{pmatrix} w \\ e \end{pmatrix}$ //

$= \begin{pmatrix} 171 \\ 81 \end{pmatrix} * 11 + 198 * 14 \\ 72 * 11 + 171 * 14 \end{pmatrix} \bmod 26$

$= \begin{pmatrix} 1881 \\ 891 \end{pmatrix} + 2772 \\ 792 + 2394 \end{pmatrix} \bmod 26$

$= \begin{pmatrix} 4653 \\ 3663 \\ 3186 \end{pmatrix} = \begin{pmatrix} 25 \\ 14 \end{pmatrix} =$

$K^{-1} * C \bmod 26 = \begin{pmatrix} 171 \\ 81 & 198 \\ 72 & 171 \end{pmatrix} \begin{pmatrix} 9 \\ 2 \end{pmatrix} \bmod 26$

$(e^{-1} * \begin{pmatrix} j \\ c \end{pmatrix} \bmod 26$

$= \begin{pmatrix} 171 \\ 81 \times 9 + 198 \times 2 \\ 72 \times 9 + 171 \times 2 \end{pmatrix} \bmod 26$

$= \begin{pmatrix} 1539 \\ 729 + 396 \\ 648 + 342 \end{pmatrix} \bmod 26.$

$= \begin{pmatrix} 1935 \\ 1125 \\ 990 \end{pmatrix} \bmod 26$

$= \begin{pmatrix} 11 \\ 2 \end{pmatrix} = \begin{pmatrix} l \\ c \end{pmatrix}$ *

//

$K^{-1} * C \bmod 26 = K^{-1} * \begin{pmatrix} c \\ m \end{pmatrix} \bmod 26$

SPB
DATE:

$$\begin{pmatrix} 171 & 198 \\ 72 & 171 \end{pmatrix} \begin{pmatrix} 2 \\ 12 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 171 \times 2 + 198 \times 12 \\ 72 \times 2 + 171 \times 12 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 342 + 2376 \\ 144 + 2052 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 2718 \\ 2196 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 14 \\ 12 \end{pmatrix} = \begin{pmatrix} o \\ m \end{pmatrix} //$$

$K^{-1} * C \bmod 26 = K^{-1} * \begin{pmatrix} y \\ u \end{pmatrix} \bmod 26$

$$= \begin{pmatrix} 171 & 198 \\ 72 & 171 \end{pmatrix} \begin{pmatrix} 24 \\ 20 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 171 \times 24 + 198 \times 20 \\ 72 \times 24 + 171 \times 20 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 4104 + 3960 \\ 1728 + 3420 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 8064 \\ 5148 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 4 \\ 0 \end{pmatrix} = \begin{pmatrix} e \\ a \end{pmatrix} //$$

PT = welcome a.