Hill Cipher

- Jeyeshwar U
- Sanketh BK
- R Harish

What is it?

→ A polygraphic substitution cipher using linear Algebra → matrix multiplication.

Trivia →

:- Invented by Lester S. Hill in 1929
:- Thought to be the first cipher to operate on more than 3 symbols at once.

WORKING :-

→ ABCDE.... ⇒ 01234..
Each letter mapped to 0-25.
i.e represented by a no % 26

TECHNIQUE :-

i) Encryption :- $KM = C$ (an $Ax = B$ system)
where K = Keymatrix ; M → Message ; C → Ciphertext

ii) Decryption $K^{-1}C = M$

⇒ So this relies on the simple technique of Matrix multiplication.
→ Using a key matrix (& its inverse) the matrix message can be transformed to ciphertext & vice versa.

EXAMPLES:-

Assume M:- HELP ME SIR
K = ABC ACC ABD [3×3 matrix]

i) Finding C → Ciphertext

a) HELP ME SIR $\xrightarrow[3]{\text{Group into}}$ HEL | PME | SIR

—x—

FAQ's

i) what is ciphertext ?=
A: The encrypted message is known as ciphertext

—x—

b) Convert to digits from 0-25

$$\begin{pmatrix} H \\ E \\ L \end{pmatrix}\begin{pmatrix} P \\ M \\ E \end{pmatrix}\begin{pmatrix} S \\ I \\ R \end{pmatrix} \Rightarrow \begin{pmatrix} 7 \\ 4 \\ 11 \end{pmatrix}\begin{pmatrix} 15 \\ 12 \\ 4 \end{pmatrix}\begin{pmatrix} 18 \\ 8 \\ 17 \end{pmatrix}$$

FAQ's:-

—x—

i) Why only 0-25 why not anything else?
A. This depends on the alphabet scheme/language to represent a letter uniquely we choose 26 in English as there are 26 letters

—x—

c) Key matrix →

$$\begin{bmatrix} A & B & C \\ A & C & C \\ A & B & D \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 3 \\ 1 & 2 & 4 \end{bmatrix}$$

d) For each vector in message apply the key transformation)

$$\text{Key}\begin{pmatrix}H\\E\\L\end{pmatrix} \Leftrightarrow \begin{bmatrix}1 & 2 & 3\\1 & 3 & 3\\1 & 2 & 4\end{bmatrix}\begin{bmatrix}7\\4\\11\end{bmatrix} = \begin{bmatrix}48\\52\\59\end{bmatrix} \% 26 \Rightarrow \begin{bmatrix}22\\0\\7\end{bmatrix} \Rightarrow \begin{bmatrix}W\\A\\H\end{bmatrix}$$

Ily for $\Rightarrow K\begin{pmatrix}P\\M\\E\end{pmatrix} = \begin{bmatrix}Z\\L\\D\end{bmatrix} \Rightarrow K\begin{pmatrix}S\\I\\R\end{pmatrix} = \begin{bmatrix}H\\P\\Y\end{bmatrix}$

So cipher text HELPMESIR ⇒ WAHZLDHPY

DECRYPTION:

$$\Rightarrow K^{-1}\begin{pmatrix}W\\A\\H\end{pmatrix} \cdot \begin{pmatrix}H\\E\\L\end{pmatrix}$$

⇒ So we need to find K^{-1} so that $K^{-1}C = M$

∴ From above Key matrix ⇒ ABC ABC ABD

$$K^{-1} = \begin{bmatrix}6 & -2 & -3\\-1 & 1 & 0\\-1 & 0 & 1\end{bmatrix}$$

$$\therefore \begin{bmatrix}W\\A\\H\end{bmatrix} \Rightarrow \begin{bmatrix}22\\0\\7\end{bmatrix}$$

Now $K^{-1}\begin{bmatrix}W\\A\\H\end{bmatrix} \Rightarrow$

DATE: PAGE:

$$\begin{bmatrix} 6 & -2 & -3 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 22 \\ 0 \\ 7 \end{bmatrix} = \begin{bmatrix} 111 \\ -22 \\ -45 \end{bmatrix} \bmod 26$$

$$\begin{bmatrix} H \\ E \\ L \end{bmatrix} \leftarrow \begin{bmatrix} 7 \\ 4 \\ 11 \end{bmatrix}$$

Hill cipher

the message can be decrypted.

FAQ

1) Why is it not used everywhere? Why AES ciphers are used?
A. Because it's not 'secure'

DISADVANTAGES OF HILL CIPHER:-

i) Susceptible to known linear attack.
→ If one word is known and its ciphertext then the key can be found.

→ This is again Linear Algebra as to solve a 2×2 [bigraphic] system we need 2 equations

Assume 'BAAL' is to be encrypted.
You know KT is the ciphertext & also it's a 2×2 cipher

$$\therefore K \begin{bmatrix} 6 \\ A \end{bmatrix} = \begin{bmatrix} K \\ T \end{bmatrix} \Rightarrow K \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 10 \\ 19 \end{bmatrix}$$

DATE: PAGE:

$K\begin{bmatrix}A\\L\end{bmatrix} = \begin{bmatrix}H\\S\end{bmatrix} \rightarrow K\begin{bmatrix}0\\11\end{bmatrix} = \begin{bmatrix}7\\18\end{bmatrix}$

∴ This means First col of K is $\begin{bmatrix}10\\19\end{bmatrix}$ &

11 times second col. = $\begin{bmatrix}7\\18\end{bmatrix}$ $[7+26]$

$\therefore K = \begin{bmatrix}10 & 3\\19 & 4\end{bmatrix}$.

So the Key is found! [or Ketd]

⇒ This susceptibility of KLA makes Hill ciphers not reliable.

FAQ:

Q. Why is it even referred to/ studied, ? Is it just for history sake?

A. No. Hill cipher technique of matrix transformation is used widely in a combination of other techniques. It is even used in AES [the best standard today]

Q. Why?

Because it is one of the simplest techniques to achieve → 'Shannons diffusion'

Diffusion → Changing one letter of the message should (statistically) change every letter with probability ½ [of the ciphertext]

⇒ This ensures its patterns are dispersed over the ciphertext making it hard to find.

DATE: PAGE:

Diffusion in action:

Assume M = ACT ; Key = GYBNQRKURP

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} (\%26)$$

or ACT ⇒ POH

Now say M = CAT

$$M \begin{pmatrix} C \\ A \\ T \end{pmatrix} = \begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix} (\%26)$$ or CAT ⇒ FIN

* Every letter has changed.

FAQs:

Q. How?

A: Again → matrix multiplication

Since $y_i = Ax_i$

or $y_1 = x_1 * A_{i1} + x_2 * A_{i2} + x_3 * A_{i3}$

$y_2 \not\propto x$

or y depends on x.

The matrix multiplication ensures that if 1 x_i is altered a whole column

⇒ the ith column after Ax_i [If x_i where $i \to 1$ or the first element then the whole first column is altered after $A_{j1} x_1$]

* This guarantees high diffusion

BIBLIOGRAPHY:

i) Hill Cipher - Wikipedia

ii) Hill Cipher based remote data possesion checking in cloud storage - Wiley - Lanxiang Chen - Gongde Guo, et. al

iii) LS Hill - Cryptography in an algebraic alphabet - American Mathematical Monthly - 1929