HILL CIPHER

by- Mridul Narang(039)
Dinesh Thawani(199)

CRYTOGRAPHY

- a cipher (or cypher) is an algorithm for performing encryption or decryption

- Cryptography is the study of Secret (crypto-)-Writing (-graphy).It is the science or art of

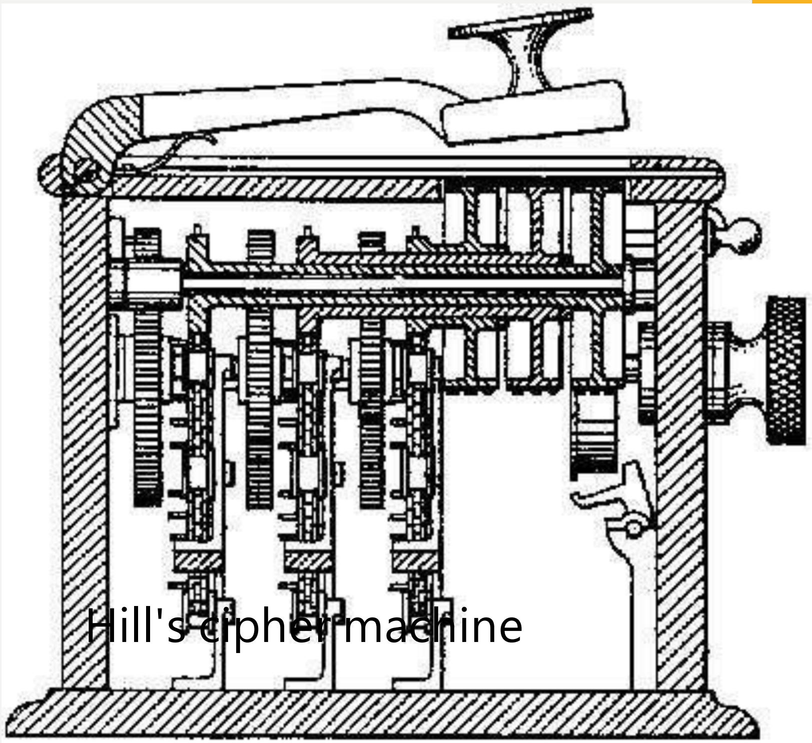
  encompassing the principles and methods of transforming an intelligible message into one that is intelligible and then transforming the message back to its original for

ENCRYPTION TECHNIQUE

- There are basically two types of encryption techniques
- Substitution :In this technique letters of plaintext are replaced by or by numbers and symbols.
- Transposition: Transposition (or permutation) does not alter any of the bits in the plaintext, but instant moves the position around within it.

HILL CIPHERS

- The core of Hill-cipher is matrix manipulations. It is a multi-letter cipher, developed by the mathematician Lester Hill in 1929.
- Uses matrices to encrypt and decrypt
- Uses modular arithmetic (Mod 26)



Hill's cipher machine

HISTORY

- Invented by Lester S. Hill in 1929.
- The Hill cipher is a polygraphic substitution cipher based on linear algebra, as it can work on digraphs, trigraphs (3 letter blocks) or theoretically any sized blocks.

- To counter charges that his system was too complicated for day to day use, Hill constructed a cipher machine for his system using a series of geared wheels and chains. However, the machine never really sold.

ENCRYPTION

Assign each letter in alphabet a number between 0 and 25 $a=0, b=1, c=2\ldots\ldots, z=25$

Change message into $2 \text{ x } 1$ letter vectors

Convert product vectors to letters

Change each vector into $2 \text{ x } 1$ numeric vectors

Multiply each numeric vector by encryption matrix

DECRYPTION

- Change message into $2 \text{ x } 1$ letter vectors
- Change each vector into $2 \text{ x } 1$ numeric vectors
- Multiply each numeric vector by decryption matrix
- Convert new vectors to letters

THANK YOU

REFERENCES

- Wikipedia
    - https://en.wikipedia.org/wiki/Hill_cipher