ENHANCEMENT OF SYMMETRIC KEY CRYPTOGRAPGHY USING RUBIK'S CUBE

FACULTY: DR. SRINIVASA REDDY KONDA

OUR TEAM

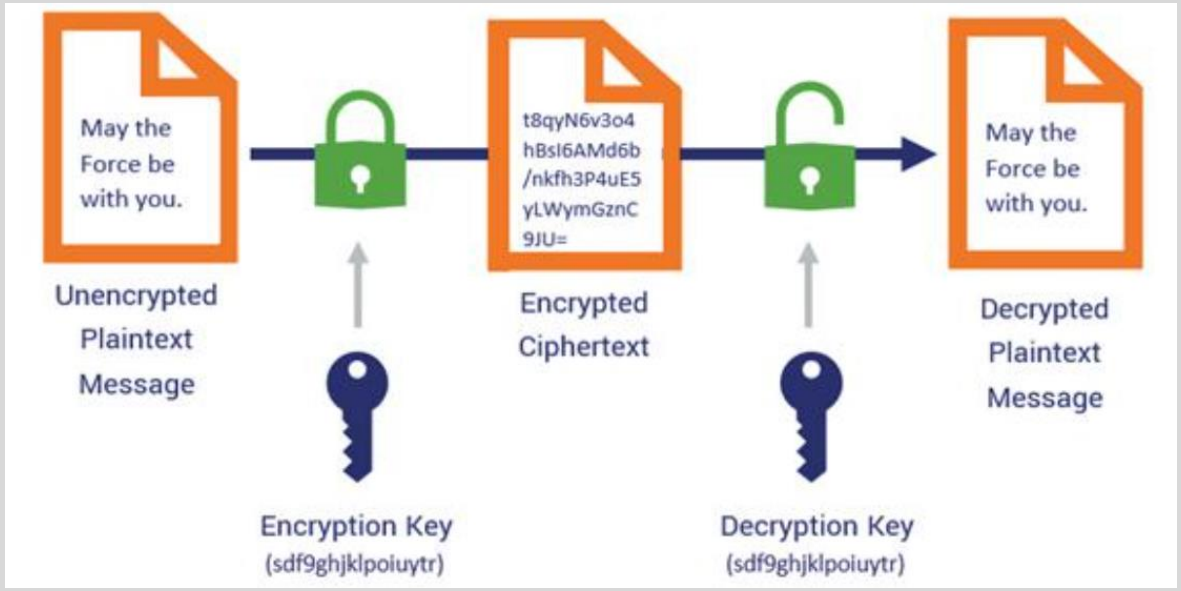
1. D. VENKATA KARTHIK 20BCN7028
2. K.V.S. SUMANTH GUPTHA 20BCE7363
3. K PRANEETH 20BCE7404

Abstract

- The current scenario is such that the assurance of security in large open networks has become the need of the hour. With increase in the rate of crimes, one needs to take precautions to protect the data in an efficient manner from all possible attacks. Basically for this need we have undertaken the task of providing such a secured package, which also provides secured data transmission environment to the user.
- This all is possible using cryptography, hill cipher and playfair cipher using Rubik's Cube.
- The main objective of this project is to enhance the working of hill cipher, playfair cipher using a simple puzzle. To protect the key of hill cipher from various cryptanalyst attacks, we are going to use the number of possible outcomes on a Rubik's cube as a key to Hill cipher to encrypt the plain text. This results in widen the range of keys in hill cipher and also lessen the possibilities to decrypt the plaintext.

Introduction to Symmetric Key Encryption

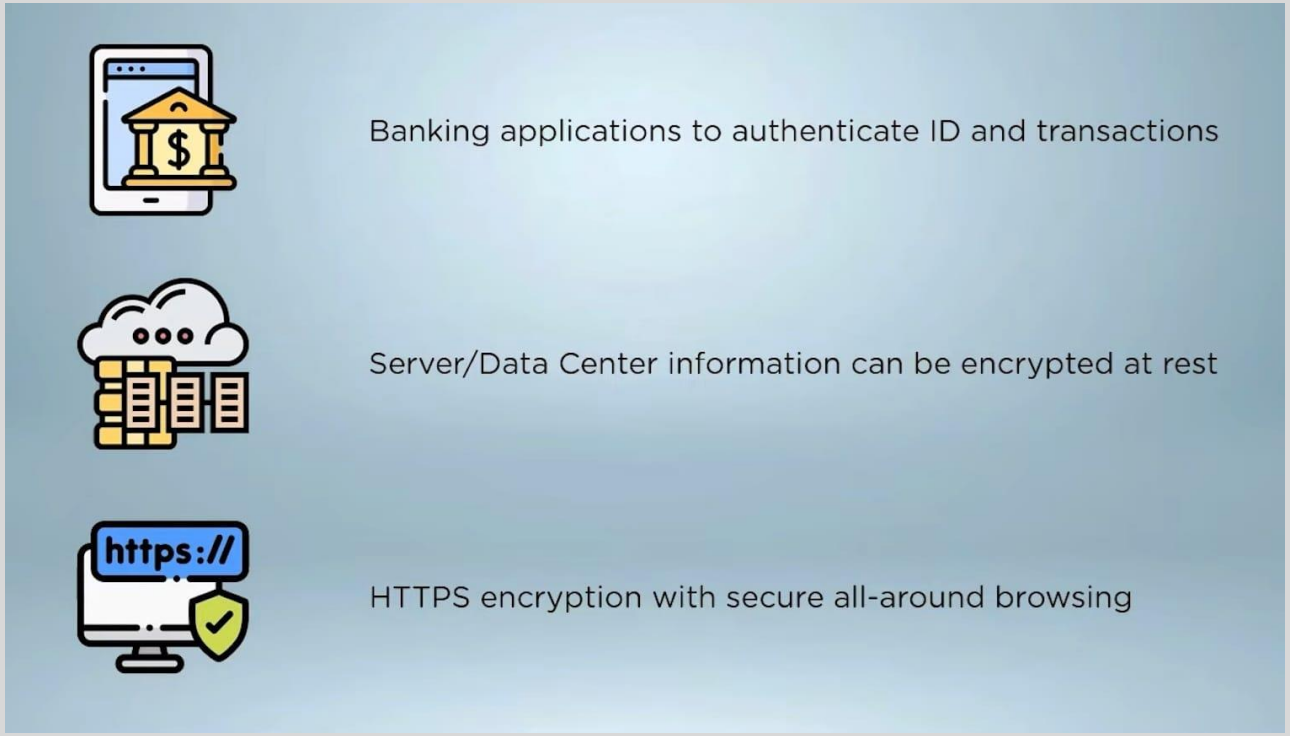
- Symmetric key encryption, also called private key in cryptography.
- It is an encryption method where only one key is used to encrypt and decrypt messages.
- This method is commonly used in banking and data storage applications.
- Identity theft as well as protect stored data.
- Symmetric key encryption relies on mathematical functions to encrypt and decrypt messages.
- Symmetric encryptions going to be used are: Hill cipher and playfair.



Advantages of Symmetric Key Cryptography

1) Security: Symmetric key encryption is essentially unbreakable and requires users to keep track of only one key.

2) Time of execution is faster than Asymmetric key cryptosystems and easy to compute.



Hill Cipher

Hill cipher is a polygraphic substitution cipher based on linear algebra. Each letter is represented by a number modulo 26.

Formula for Encryption of hill cipher is:

$$C = K*P \bmod 26$$

Formula for Decryption of hill cipher is:

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

PlayFair Cipher

- Multiple letter encryption cipher.
- In this algorithm, an alphabets table of 5×5 grid is created as a key for encrypting the plaintext.
- Each of the 25 alphabets must be unique, since we have 26 letters in English alphabet, one letter (usually J) is omitted from the table.
- If the plaintext contains J, then it is replaced by I. The sender and the receiver decide on a particular key.

Rules of Playfair Cipher

- Key: Monarchy

1. Digrams.
2. Repeating Letters - Filler letter.
3. Same Column | ↓ | Wrap around.
4. Same row | → | Wrap around.
5. Rectangle | ⇆ | Swap

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

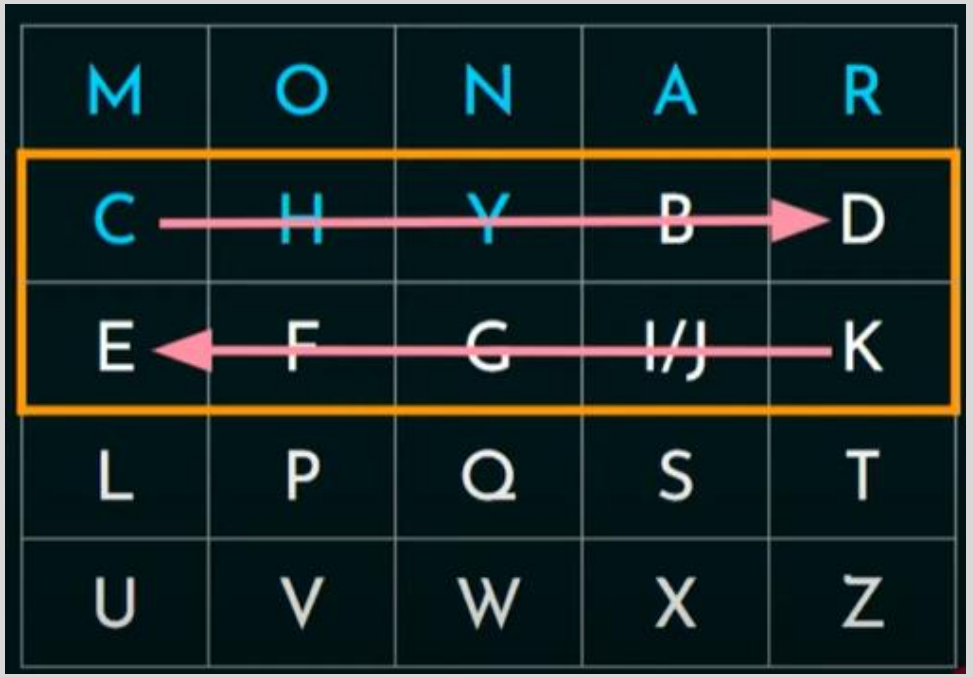
Example 1: attack

Digrams: at ta ck

at	ta	ck
RS	SR	DE

Plaintext: attack

Digrams: RSSRDE



Rubik's Cube Concept On Symmetric Key Cryptosystem

- Consider this scenario:

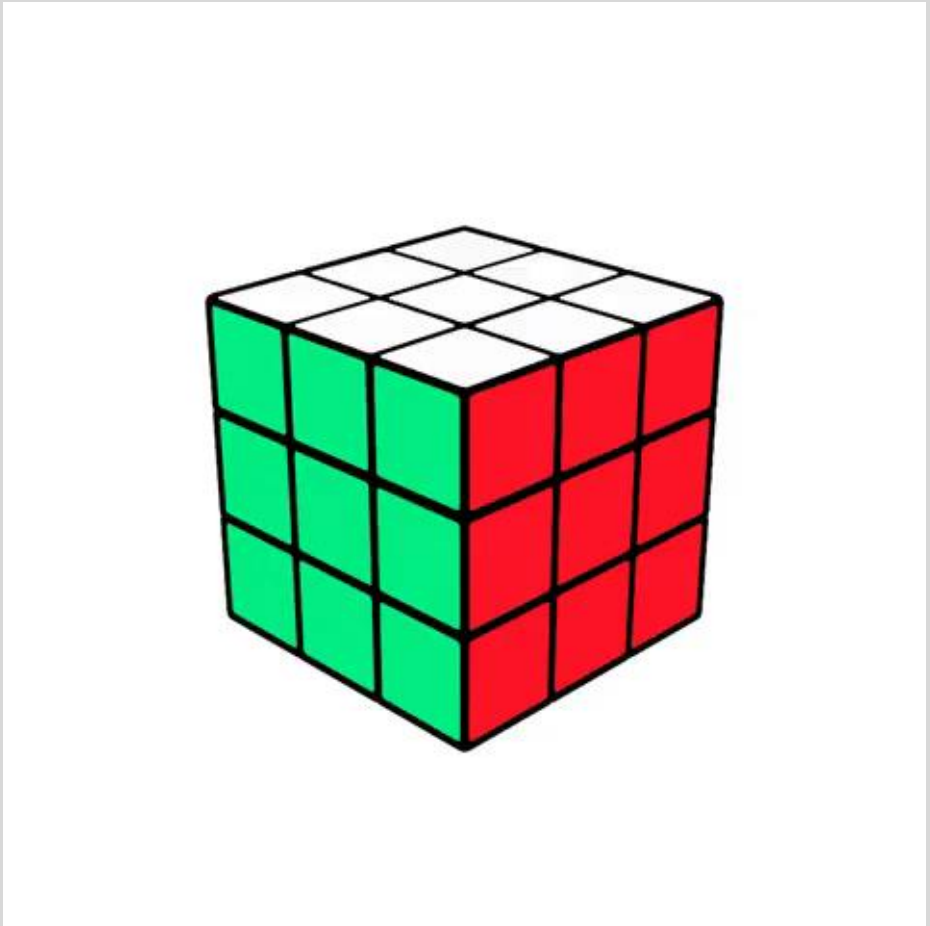
Alice gets a Rubik's Cube and uses the techniques to solve the Rubik's Cube

She notices there is a strange thing about Rubik's Cube.

Each time when she tries to solve the Rubik's Cube,

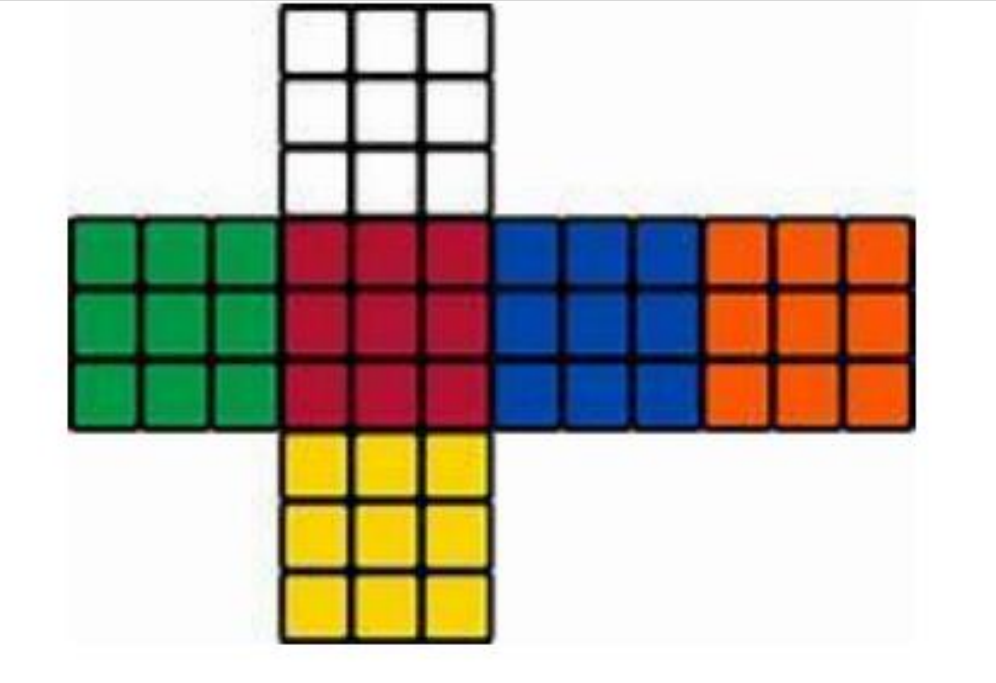
Her pieces get's mixed up with different positions.

Therefore, she decided to use the concept as a key for symmetric key encryption



Implementation of Hill Cipher with Rubik's Cube

- Unfolding the cube and making into 2D will appear like as shown:



- After solving up to white cross, let us assume the six faces of cubes are shown like below:


THANK YOU