ENHANCEMENT OF SYMMETRIC KEY

CRYPTOGRAPHY USING RUBIK’S CUBE

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | D Venkata Karthik  *School of Computer Science and*  *Engineering*  *VIT-AP University*  Amaravati, India venkatakarthik.20bcn7028@vitap.ac.in | KVS Sumanth Guptha  *School of Computer Science and*  *Engineering*  *VIT-AP University*  Amaravati, India  sumanth.20bce7363@vitap.ac.in | | |  |  | | --- | --- | | K Praneeth  *School of Computer Science and*  *Engineering*  *VIT-AP University*  Amaravati, India praneeth.20bce7404@vitap.ac.in |  | |

**Index Terms:** Symmetric key, Cryptography, Hill cipher and Playfair using Rubik’s Cube.

**ABSTRACT:**

Now a days ensuring security across vast open networks has become essential. With the number of crimes increasing, one must take care to effectively safeguard the data from all potential threats. Primarily to satisfy this demand, we have taken on the difficult task of providing a protected package that also gives users a secure environment for data transfer.

Aims to help users prevent fraud or detect fraud in an information-based system. The information must be secured to be free from threats. In this research paper, we will use Cryptographic techniques can prevent data theft. 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 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 lessen the possibilities to decrypt the plaintext.

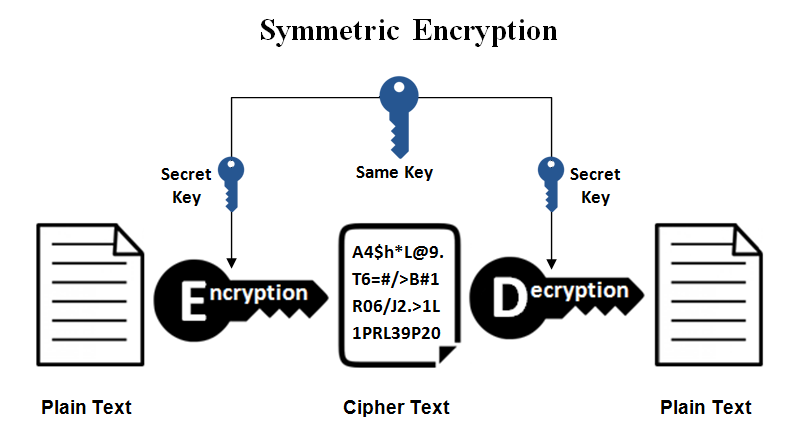
**Keywords— Cryptography, Cipher, Encryption, Decryption.**

|  |
| --- |
|  |

**INTRODUCTION**

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.

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.



The number of outcomes on a Rubik's cube will be used as the key to the Hill cypher to encrypt the plain text in order to safeguard the key from various cryptanalyst attacks. As a result, the number of keys in the Hill cypher is increased, which reduces the likelihood that the plaintext may be cracked.

**METHODS**

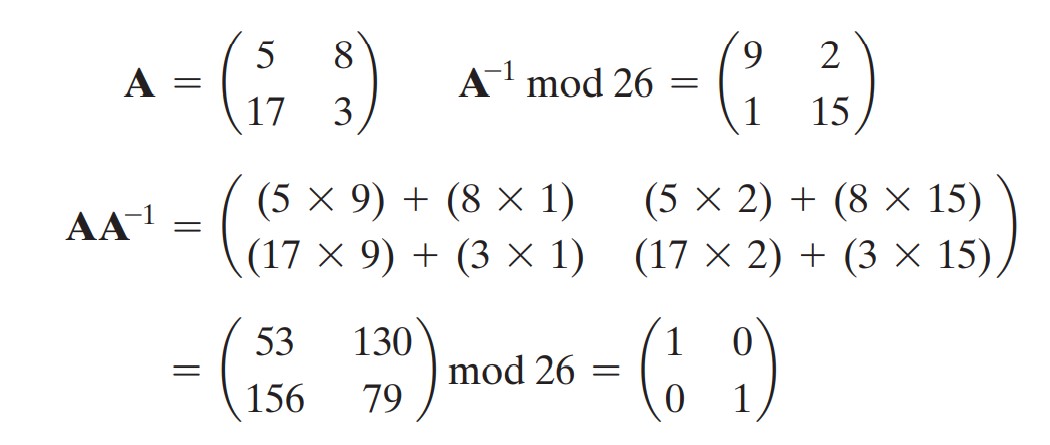
**I. Hill cipher**

We define the inverse M^(-1) of a square matrix M by the equation

M\*(M^(-1) ) = (M^(-1))\*M = I,

Where I is the identity matrix. I is a square matrix that is all zeros except for ones along the main diagonal from upper left to lower right. The inverse of a matrix does not always exist, but when it does, it satisfies the preceding equation.

For example:



For encryption of hill cipher we need to multiply the plaintext with the key to get the resultant ciphertext. That is,

Input: Plaintext that has to be converted into ciphertext. A KEY to encrypt the plain text

Output: Ciphertext

We have a simple formula for encryption

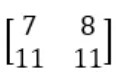
**C = K\*Pmod26**

Where C is ciphertext, K is the key, P is the plain text vector.

The KEY is generally is in format of n x n matrix and the plain text is divided into n\*1 vectors to hide the information of plaintext and transform into the text into ciphertext.

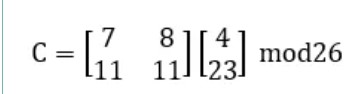
For demonstration, let us take an example:

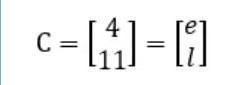
Plain text : “exam”

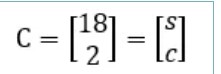
Key:

C=P\*K mod 26

For, first column





For, second column

Hence, the ciphertext is “elsc”

To deal with decryption, first we need to find the inverse of a key matrix such that,

* Find the adjacent matrix of the given key matrix K\_adj=Adjacent matrix key cipher text .
* Find the determinant of the key matrix

77-88=-11

* + Find the modulo of the determinant with 26

-11 mod26 =15=d

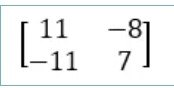
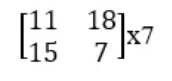
a well-known statistical algorithm that can generate multiple samples from the posterior distribution over the network's parameters, allowing us to estimate the variance of predictions.

Find the inverse number of the above result:

d x d’=1 mod26 15 x

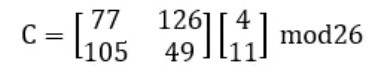
d’= 1 mod26 d’=7

Any negative numbers in K adj should be added by 26 and then the whole matrix is multiplied by d’.



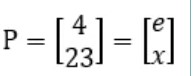
K’ =negative numbers in K\_adj.

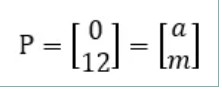
Now, this is our new key matrix. Substituting all the values in the decryption formula, we get the required plain text.



Formula for decryption of hill cipher is:



Substituting all the values in the decryption formula. For column 1

 For column 2

By Combining column 1&2 we got “exam”.

Hence, the decryption is successful and the original message has been received.

**II. Play Fair 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.

To encrypt a message using Playfair Algorithm, first, a plaintext is split into pairs of two letters. If the message contains an odd number of letters, then a letter X is added to the last letter, for example, the message “odd” will be written as -od dx.

Depending on the location of each two letters in the matrix key, encryption will do according to the rules below:

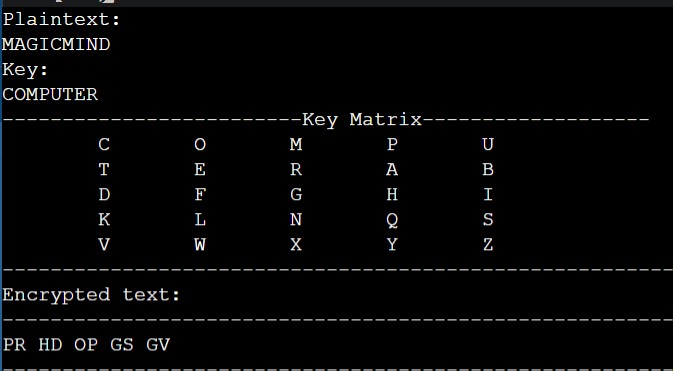
* If both the letters are in the same column, take the letter below each one (going back to the top if at the bottom)
* If both letters are in the same row, take the letter to the right of each one (going back to the left if at the farthest right)
* If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

Methodology of Playfair:

Encryption phase: We must now split the plaintext up into digraphs (that is pairs of letters). On each digraph we perform the following encryption steps:

Rules of Encryption:

* If the digraph consists of the same letter twice (or there is only one letter left by itself at the end of the plaintext) then insert the letter "X" between the same letters (or at the end), and then continue with the rest of the steps.
* If the two letters appear on the same row in the square, then replace each letter by the letter immediately to the right of it in the square (cycling round to the left hand side if necessary).
* If the two letters appear in the same column in the square, then replace each letter by the letter immediately below it in the square (cycling round to the top of the square if necessary).
* If not, draw the rectangle with the two plaintext characters' two opposing corners as its corners. Then, being sure to retain the order, swap out each plaintext letter with the letter that makes up the other corner of the rectangle that is located on the same row as that plaintext letter.



MAGICMIND is an odd numbered word, so last word is quoted as “X” to make it even numbered.

Using Key matrix, Now we encrypt our plaintext: MAGICMIND as: MA - PR GI - HD CM-OP IN-GS DX – GV (Applied the rules of encryption)

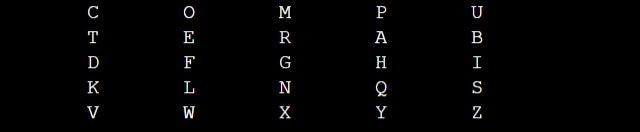
Decryption phase: With the exception of rules 2 and 3, decryption is almost identical to encryption, with the exception that we must take the letters to the left and above, respectively. We also eliminate any superfluous "X"s from the decoded text in order to expose the complete plaintext.

Rules of Decryption:

* Two ciphertext letters in the same row of the matrix are each replaced by the letter to the left, with the last element of the row circularly following the first.
* Otherwise, each ciphertext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other ciphertext letter.
* Following these rules, the plaintext becomes ‘MAGICMIND’.

{x is neglected or removed at the end since it’s a filler letter).

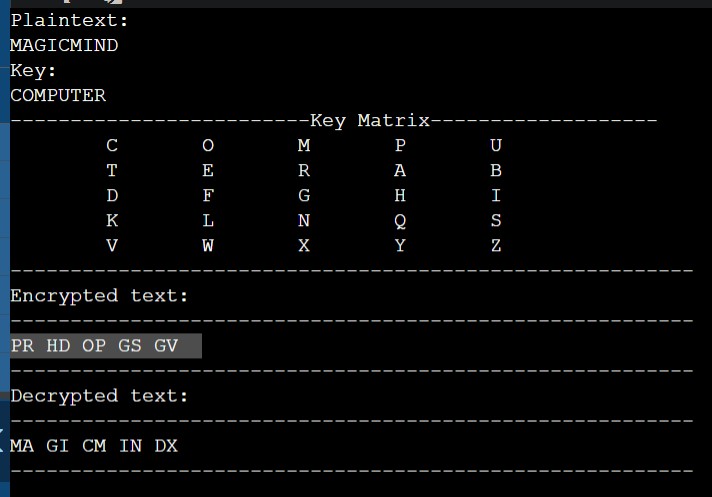
* + We shall decipher the ciphertext "PRHDOPGSGV " which has been encrypted using the keyword example. Firstly we must generate the Polybius Square which we are using, as shown in below:



* + Next step is splitting the encrypted text into:



Applying the rules of decryption for the well divided encrypted text using Key Matrix. Our Plaintext is retrieved.



**Rubik’s Cube:**

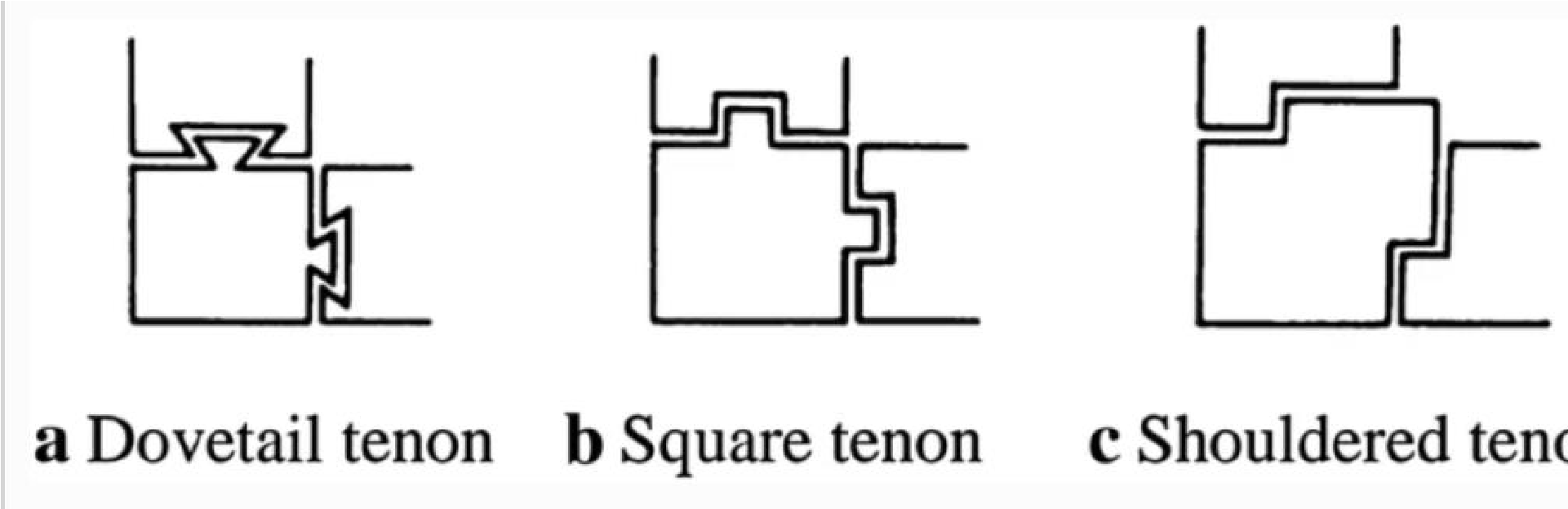
The Rubik's Cube is a widespread mechanical puzzle that has gained worldwide attention due to its unique features. As a classic brain training toy known to the public, the Rubik's Cube has been used by many scientists for scientific research and technological development.

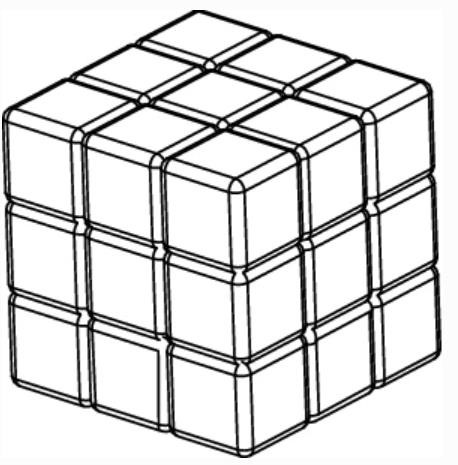
This paper provides a basic understanding of the Rubik's Cube and presents its mechanical art origin and development, characteristics, research status, and especially its application in mechanical engineering design and mechanism

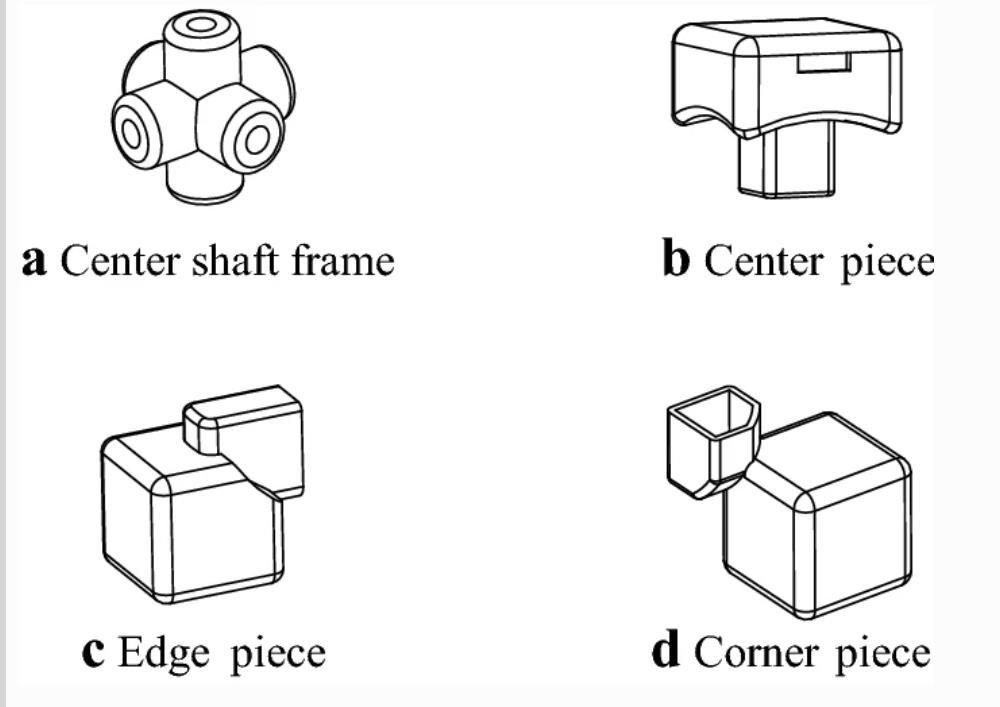
First, the invention and origin of the Rubik's cube are introduced, and then the specific characteristics of the cube itself are analyzed. Then, the previous research on the Rubik's cube in various fields at home and abroad is reviewed, including the research on scientific metaphors, reduction algorithms, characteristic applications and mechanism problems of the Rubik's cube.

Structure of Rubik’s cube:

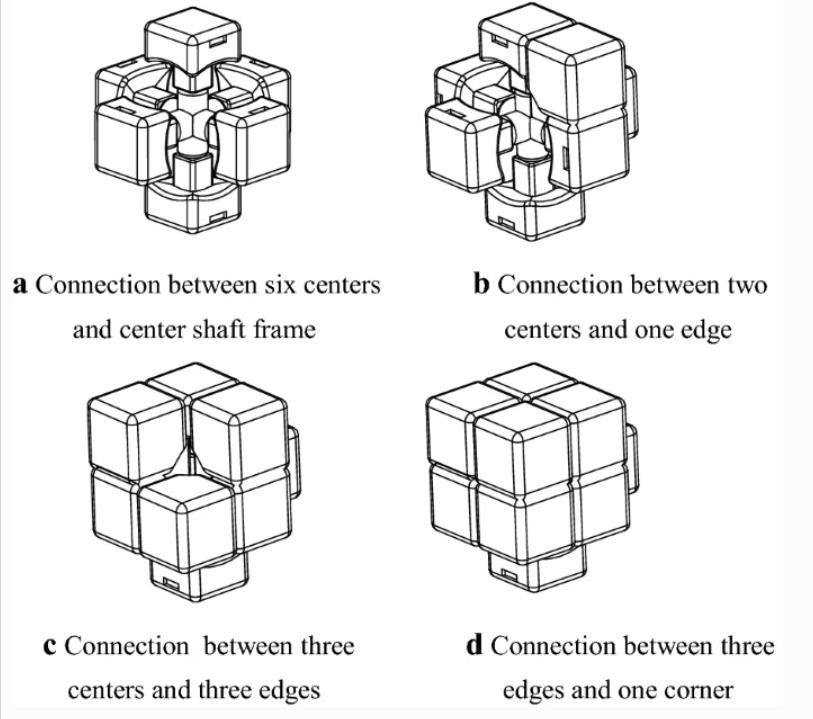
The Rubik's Cube was based on the groove between the pieces and the pins. The press and dowel method can be used so that the outer 26 pieces of the cube stay together without any center pieces. It is difficult to make this relationship precise enough for the surfaces to rotate easily [18]. The movements of the sockets and pins are shown below:



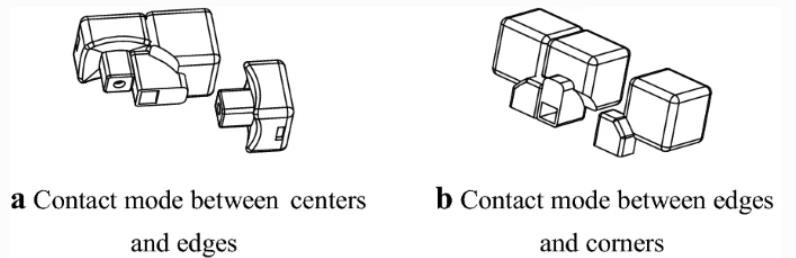
The standard 3 × 3 × 3 cube consists of 26 unique miniature cubes, also called “pieces” or “cube lets” including a center shaft frame, 6 center pieces, 8 corner pieces, and 12 edge pieces. The various types of pieces of Rubik’s Cube are shown below:



Edge boundaries consist of structural boundaries and Christmas removal of two adjacent centers. Borders on the corner detail consist of structural borders and the Christmas deletion of three adjacent edges.

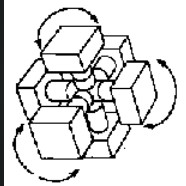


The contact modes between the centers and edges, and the edges and corners, are shown:



Mathematics of Rubik’s cube:

The unique (3 × 3 × 3) Rubik’s 3d shape has six faces. At first, each confront has the same color, and each confront has nine little external surfaces. They are 54 external surfaces in add up to. Each side of Rubik’s 3d shape is composed of diversiform color pieces after the arbitrary turn of diverse sides a few times.



* There are 12 edge piece positions. Each time when we insert an edge piece in its position, the number of possibilities after insertion at an edge piece gets reduced by 1.

Therefore,

The number of possibilities on an edge position = 12\*11\*10\*9\*8\*7\*6\*5\*4\*3\*2\*1 = 12!

Similarly, there are 8 corner piece positions. Each time when we insert in an corner piece position. The number of possibilities after insertion at an edge piece gets reduced by 1.

Therefore,

The number of possibilities on an corner positions = 8\*7\*6\*5\*4\*3\*2\*1 = 8!

Total number of possibilities that a cube can be afforded after insertion is:

12! \*8! = 19,313,344,512,000

* Considering the flips of edge pieces = 2^12
* Considering the twists of corner pieces = 3^8
* Total number of possibilities after considering flip positions is:

12!\*8!\*(2^12)\*(3^8)

However,

1. No single edge flip = 2^12/2 = 2^11
2. No single corner twist should be present = 3^8/3 = 3^7
3. No two edge pieces should be swapped = 8!/2

That is, 12! \*8!\*(2^12)\*(3^7)/(2\*2\*3) =

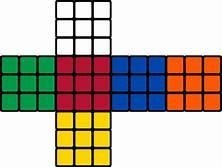
The total number of possible solutions on a Rubik’s cube are =

**43,252,003,274,489,856,000**

**Implementation of Hill cipher with Rubik’s Cube**

Suppose consider the Rubik’s cube is partially solved (Ex: White cross). Every time when we flip an edge or twist a corner, we get different corner and edge pieces. Initially, the cube is in scrambled position or whatever input we give.

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:

Procedure (Encryption):

1. Sender decides a plain text and generates a 54-bit key which is a Rubik’s cube layout before solving partially. The range of a 54-bit key is taken as numbers in a range of 1-6 where, 1-6 represents different colors as mentioned above.
2. The 54-bit key is solved partially (white cross).
3. The algorithm takes the pieces randomly to generate hill cipher key.
4. Algorithm computes if the key has inverse or not, if there exists a inverse for 54 bit key, then Hill cipher can be successfully implemented.
5. if the key is invertible, it implements c=p\*k mod 26

(In small ASCII characters). Where cipher text is generated.

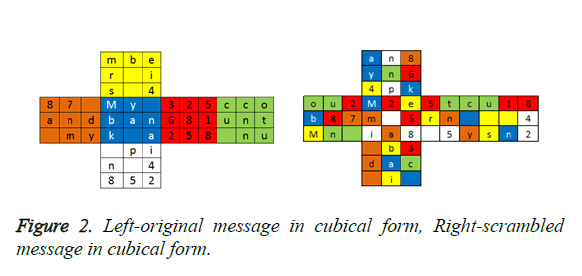
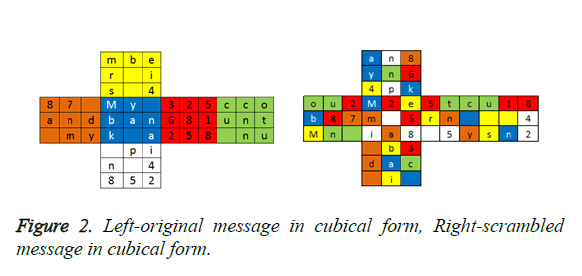
1. If the key is not invertible or doesn’t form a square matrix, by default, The system asks whether to exit or proceed with Playfair cipher encryption.

Procedure (Decryption):

1. Receiver needs to input exact 54 bit key (positions of cube).
2. The 54-bit key is solved partially (white cross) and the side which is needed to decrypt.
3. Algorithm implements p = c \* k^ (-1) mod 26  Step 4: Cipher text is reverted.

If Key is invertible Step 3 and Step 4 is implemented or else

1. We will take an input from user of ciphertext and using the obtained key. We decrypt the encrypted text to plain text.

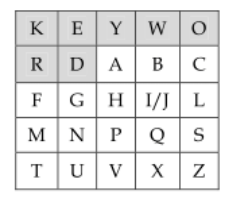


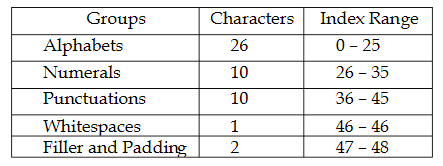
**Fig:** Encryption and Decryption

**Implementation of Play Fair cipher with Rubik’s Cube**

The Playfair cipher is a polygraphy substitution cipher that encrypts pairs of letters instead of individual letters, making it more secure than monoalphabetic substitution ciphers. The encryption process involves generating a 5x5 key square with a keyword, and then encrypting the plaintext by dividing it into pairs of letters and using their positions in the key square to generate the ciphertext pairs.

Using a Rubik's cube as the key square for the Playfair cipher adds an extra layer of complexity to the encryption process. Here is how you can implement the Playfair cipher using a Rubik's cube:





**Table:** Primary Indexing of Character Groups

Now that we have the Playfair square on the Rubik's cube, we can use it to encrypt and decrypt plaintext.

Procedure (Encryption):

1. Divide clear text into letter pairs. If the plain text contains an odd number of letters, add an "X" at the end.
2. Do the following for each pair of letters.
3. If the letters are the same, add an "X"

between them.

1. Find the positions of the stars in the Playfair square in the current direction of the

Rubik's cube.

1. If the letters are on the same line, replace each letter with the letter to the right (round to the beginning of the line if necessary).
2. If the letters are in the same column, replace each letter with the letter below it (round to the top of the column if necessary).
3. Otherwise, replace each letter with a letter in the same row and opposite column (i.e., a letter in the same row as the first letter and the second letter in the same column).
4. The resulting ciphertext is a combination of all the letter pairs obtained in step 2.

Procedure (Decryption):

1. Break the ciphertext into pairs of letters.
2. Do the following for each pair of letters.
3. Find the positions of the stars in the Playfair square in the current direction of the Rubik's cube.
4. If the letters are on the same line, replace each letter with the letter on the left (round to the end of the line if necessary).
5. If the letters are in the same column, replace each letter with the letter above it (round the column if necessary).
6. Otherwise, replace each letter with a letter in the same row and opposite column (i.e., a letter in the same row as the first letter and in the same column as the second letter).
7. If a pair of letters was originally the same (with an "X" inserted between them), remove the "X".
8. The resulting plaintext is the concatenation of all the pairs of letters obtained in step 2.

**Conclusion:**

Symmetric encryption using Rubik's Cube is a novel approach that has gained attention in recent years as a potentially secure and efficient method for encrypting data. Its mathematical complexity and randomness make it an ideal choice for encryption and decryption, and the use of physical objects adds an extra layer of security. Furthermore, its versatility in creating various key spaces and its ease of implementation make it a practical solution for securing data. With further research and development, Rubik's Cube encryption has the potential to become a viable option for securing sensitive information in various fields.

**References**

* <https://www.youtube.com/watch?v=ZtlMkzix7Bw&t=1s>(Inspired implementation of Rubik’s cube algorithm)
* <https://www.researchgate.net/publication/328693056_Application_of_Hill_Cipher_Algorithm_in_Securing_Text_Messages>
* <https://www.researchgate.net/publication/357177075_An_implementation_of_Hill_cipher_and_3x3x3_rubik's_cube_to_enhance_communication_security>
* <https://www.researchgate.net/publication/274709511_An_Efficient_Modification_to_Playfair_Cipher>
* <https://www.researchgate.net/publication/286458327_Design_and_Analysis_of_Playfair_Ciphers_with_Different_Matrix_Sizes>
* <https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/iet-net.2017.0196>
* <https://cjme.springeropen.com/articles/10.1186/s10033-018-0269-7>

(Rubik’s Cube mechanism)

.