Classical Encryption Techniques

Ramandeep Sharma
Assistant Professor
PCTE Baddowal
Ludhiana,Punjab,India

Richa Sharma
Assistant Professor
PCTE Baddowal
Ludhiana,Punjab,India

Harmanjit Singh
Assistant Professor
PCTE Baddowal
Ludhiana,Punjab,India

ABSTRACT

This paper reviews some of the classical encryption and modern techniques which are widely used to solve the problem in open networked systems, where information is being received and misused by adversaries by means of facilitating attacks at various levels in the communication. In this paper the proposition of building the basics of classical encryption and modern techniques and the comparison has been done between each of them.

Keywords

Cipher Text, Decryption, Encryption, Substitution, Modern Encryptions, Secret Key

1. INTRODUCTION

In an open networked systems, information is being received and misused by adversaries by means of facilitating attacks at various levels in the communication [1].Data encryption is sought to be the most effective means to counteract the attacks [2].There are two classes of encryption in use, which are referred to as i) Symmetric-key encryption using secret keys and ii) Asymmetric-key encryption using public and private keys. Public-key algorithms are slow, whereas Symmetric-key algorithms generally run

1000 times faster [3]. Symmetric-Key cryptography has been - and - still is - extensively used to solve the traditional problem of communication over an insecure

channel [4].In open network like the internet, data encryption has been widely used to ensure information security. Each type of data has its own inherent characteristics. Therefore, different encryption techniques should be used to protect the confidential data from unauthorized use. For text data, there are many encryption algorithms while the algorithm applicable to text data may not be applicable to image data. There are basically two goals i) To introduce the rudiments of encryption vocabulary and ii)To trace the history of some early approaches to cryptography and to show through this history a common failing of humans to get carried away by the technological and scientific hubris of the moment[5].

Classical Encryption Techniques

A. Building Blocks

i. Two building blocks of all classical encryption techniques are substitution and transposition.
ii. Substitution means replacing an element of the plaintext with an element of cipher text.
iii. Transposition means rearranging the order of appearance of the elements of the plaintext.
iv. Transposition is also referred to as permutation.

B. Symmetric Cipher Model

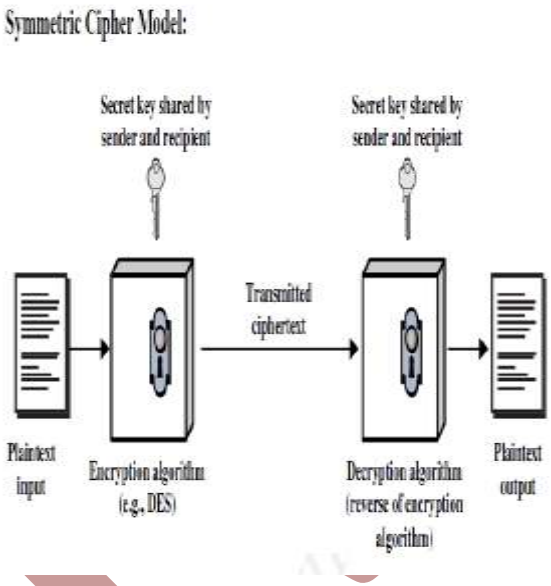


Fig 1: Symmetric Cipher Model

A symmetric encryption scheme has five ingredients:

1. **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.
2. **Encryption Algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
3. **Secret Key:** The secret key is also input to encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time.
4. **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and secret key.
5. **Decryption Algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

C. Cryptography

Cryptographic systems are characterized along three independent dimensions:

1. **The type of operations used for transforming plaintext to ciphertext:** All encryption algorithms are based on two general principles: ***substitution,*** in which each element in the plaintext(bit, letter, group of bits or letters) is mapped into another element, and ***transposition,*** in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost.
2. **The number of keys used:** If both sender and receiver use the same key, the system is reffered to as **symmetric, single key, secret key,** or

conventional encryption. If the sender and receiver use different keys, the system is reffered to as asymmetric , two key, or public-key encryption.

3. **The way in which the plaintext is processed:** A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

D. Cryptanalysis

Cyptanalytic attacks rely on the nature of the algorithm plus some knowledge of the general characteristics of the plaintext.

E. Brute-force attack

The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

Substitution Techniques

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.

A. Ceaser Cipher

This is the earliest known example of a substitution cipher.Each character of a message is replaced by a character three position down in the alphabet.

i. Plaintext: are you ready

ii. Cipher text: DUH BRX UHDGB

If we represent each letter of the alphabet by an integer that corresponds to its position in the alphabet, the formula for replacing each character 'p' of the plaintext with a character 'C' of the cipher text can be expressed as

C = E (3, p) = (p + 3) mod 26

A more general version of this cipher that allows for any degree of shift would be expressed by:

C = E (k, p) = (p + k) mod 26

The formula for decryption would be:

p = D (k, C) = (C - k) mod 26

In these formulas, 'k' would be the secret key. The symbols 'E' and 'D' represent encryption and decryption.

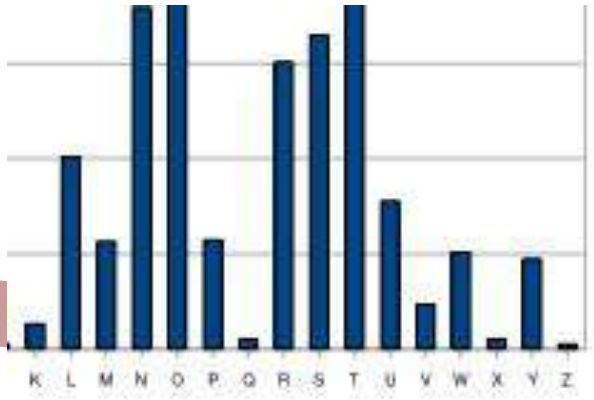
B. Mono-alphabetic Ciphers

In a mono-alphabetic cipher, our substitution characters are a random permutation of the 26 letters of the alphabet:

Plaintext letters: a b c d e f.....

Substitution letters: t h i j a b.....

The key now is the sequence of substitution letters. In other words, the key in this case is the actual random permutation of the alphabet used. Note that there are 26! permutations of the alphabet. That is a number larger than 4 × 10^26. The All-Fearsome Statistical Attack: If you know the nature of plaintext, any substitution cipher, regardless of the size of the key space, can be broken easily with a statistical attack. When the plaintext is plain English, a simple form of statistical attack consists measuring the frequency distribution for single characters, for pairs of characters, for triples of characters, etc., and comparing those with similar statistics for English. Figure 1 shows the relative frequency of the letters in a sample of English text. Obviously, by comparing this distribution with a histogram for the characters in a piece of cipher text, you may be able to establish the true identities of the cipher text characters.



C. Multiple Chaaracter Encryption to Mask Plain Text Structure

One character at a time substitution obviously leaves too much of the plaintext structure in cipher text. So how about destroying some of that structure by mapping multiple characters at a time to cipher text characters? The best known approach that carries out multiple-character substitution is known as Playfair Cipher.

i. Constructing the Matrix for Pair Wise Substitutions in PlayFair Cipher:In Playfair cipher, you ?rst choose an encryption key. You then enter the letters of the key in the cells of a 5 × 5 matrix in a left to right fashion starting with the ?rst cell at the top-left corner. You ?ll the rest of the cells of the matrix with the remaining letters in alphabetic order. The letters I and J are assigned the same cell. In the following example, the key is "smythework".

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

ii. Substitution Rules for Pairs of Characters in Playfair Cipher: Two plaintext letters that fall in the same row of the 5 × 5 matrix are replaced by letters to the right of each in the row. The "rightness" property is to be interpreted circularly in each row, meaning that the first entry in each row is to the right of the last entry. Therefore, the pair of letters "bf" in plaintext will get replaced by "CA" in cipher text.

a. Two plaintext letters that fall in the same column are replaced by the letters just below them in the column. The "belowness" property is to be considered circular, in the sense that the topmost entry in a column is below the bottommost

entry. Therefore, the pair "ol" of plaintext will get replaced by "CV" in cipher text.

b. Otherwise, for each plaintext letter in a pair, replace it with the letter that is in the same row but in the column of the other letter. Consider the pair "gf" of the plaintext. We have 'g' in the fourth row and the first column; and 'f' in the third row and the ?fth column. So we replace 'g' by the letter in the same row as 'g' but in the column that contains 'f'. This given us 'P' as a replacement for 'g'. And we replace 'f' by the letter in the same row as 'f' but in the column that contains 'g'. That gives us 'A' as replacement for 'f'. Therefore, 'gf' gets replaced by 'PA'.

D. Dealing with Duplicate Letters in a key and Repeating Letters in Plaintext

You must drop any duplicates in a key. Before the substitution rules are applied, you must insert a chosen "?ller" letter (let's say it is 'x') between any repeating letters in the plaintext. So a plaintext word such as "hurray" becomes "hurxray".

E. Play Fair

i. Playfair was thought to be unbreakable for many decades.

ii. It was used as the encryption system by the British Army in World War 1. It was also used by the U.S. Army and other Allied forces in World War 2.

iii. But, as it turned out, Playfair was extremely easy to break.

iv. As expected, the cipher does alter the relative frequencies associated with the individual letters and with diagrams and with trigrams, but not sufficiently.

v. The figure shows the single-letter relative frequencies in descending order (and normalized to the relative frequency of the letter 'e') for different ciphers. There is still considerable information left in the distribution for good guesses.

vi. The cryptanalysis of the Playfair cipher is also aided by the fact that a diagram and its reverse will encrypt in a similar fashion. That is, if AB encrypts to XY, then BA will encrypt to YX. So by looking for words that begin and end in reversed diagrams, one can try to compare then with plaintext words that are similar. Example of words that begin and end in reversed diagrams: receiver, departed, repairer, redder, denuded, etc.

This figure is from Chapter 2 (page no.42) of William Stallings: "Cryptography and Network Security", Fourth Edition, Prentice-Hall.[6].

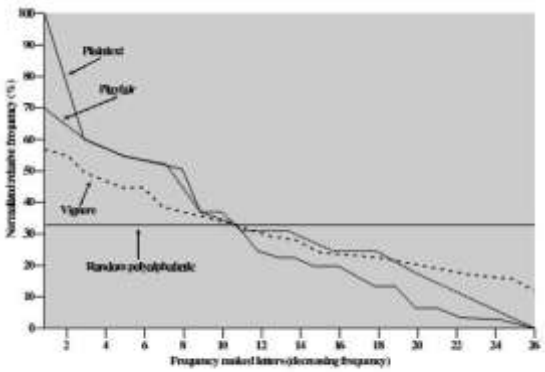


Figure 2.6 Relative Frequency of Occurrence of Letters

F. Multi-Letter Cipher: The Hill Cipher

The Hill cipher takes a very di?erent (more mathematical) approach to multi-letter substitution:

i. You assign an integer to each letter of the alphabet. For the sake of discussion, let's say that you have assigned the integers 0 through 25 to the letters 'a' through 'z' of the plaintext.

ii. The encryption key, call it K, consists of a 3×3 matrix of integers:

$$\mathrm{K} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix}$$

Now we can transform three letters at a time from plaintext, the letters being represented by the numbers p1, p2, and p3, into three cipher text letters c1, c2, and c3 in their numerical representations by

$$\begin{aligned} c_1 &= (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \ mod\ 26 \\ c_2 &= (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \ mod\ 26 \\ c_3 &= (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \ mod\ 26 \end{aligned}$$

The above set of linear equations can be written more compactly in the following vector-matrix form:

$$\vec{\mathrm{C}} = [\mathrm{K}]\,\vec{\mathrm{P}} \ mod\ 26$$

Obviously, the decryption would require the inverse of K matrix.

$$\vec{\mathrm{P}} = \left[\mathrm{K}^{-1}\right]\vec{\mathrm{C}} \ mod\ 26$$

This works because

$$\vec{\mathrm{P}} = \left[\mathrm{K}^{-1}\right][\mathrm{K}]\,\vec{\mathrm{P}} \ mod\ 26 = \vec{\mathrm{P}}$$

How Secure is the Hill Cipher?

It is extremely secure against cipher text attacks only. That is because the key space can be made extremely large by choosing the matrix elements from a large set of integers (The key space can be made even large by generalizing the technique to larger-sized matrices). But it has zero security when the plaintextcipher text pairs are known. The key matrix can be calculated easily from a set of known pairs.

G. One Time Pad

The key is to be used to encrypt and decrypt a single message and then is discarded. Each new message requires a new key of the same length as the new message. Such a scheme known as One Time Pad, is unbreakable.

The one Time Pad offers complete security but, in practice, has two fundamental difficulties:

1. There is the practical problem of making large quantities of random keys.
2. Even more daunting is the problem of key distribution and protection. For every message to be sent , a key of equal length is needed by both sender and receiver.

Transposition Techniques

A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is reffered to as a transposition cipher.

A. Rail Fence

The simplest such cipher is the rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. For example, to encipher the message "meet me after the toga party" with a rail fence of depth 2, we write the following:

m e m a t r h t g p r y

e t e f e t e o a a t

The encrypted message is

MEMATRHTGPRYETEFETEOAAT

This sort of thing would be trivial to cryptanalyze. A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of the columns then becomes the key to the algorithm. For example,

Key: 4 3 1 2 5 6 7

Plaintext: a t t a c k p

o s t p o n e

d u n t i l t

w o a m x y z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. For the type of columnar transposition just shown, cryptanalysis is fairly straightforward and involves laying out the ciphertext in a matrix and playing around with column positions. Digram and trigram frequency tables can be useful. The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is a more complex permutation that is not easily reconstructed. Thus, if the foregoing message is reencrypted using the same algorithm,

Key: 4 3 1 2 5 6 7

Input: t t n a a p t

m t s u o a o

d w c o i x k

n l y p e t z

Output: NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

To visualize the result of this double transposition, designate the letters in the original plaintext message by the numbers designating their position. Thus, with 28 letters in the message, the original sequence of letters is

01 02 03 04 05 06 07 08 09 10 11 12 13 14

15 16 17 18 19 20 21 22 23 24 25 26 27 28

After the first transposition we have

03 10 17 24 04 11 18 25 02 09 16 23 01 08

15 22 05 12 19 26 06 13 20 27 07 14 21 28

which has a somewhat regular structure. But after the second transposition, we have

17 09 05 27 24 16 12 07 10 02 22 20 03 25

15 13 04 23 19 14 11 01 26 21 18 08 06 28

This is a much less structured permutation and is much more difficult to cryptanalyze.

B. Steganography

1. Character Marking: Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.
2. Invisible Ink: A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.
3. Pin Punctures: Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of light.
4. Typewriter Correction Ribbon: Used between lines typed with a balck ribbon, the results of typing with the correction tape are visible only under a strong light.

Modern Techniques

A. S-DES

Simplified DES has a process of key generation instead of using key as it is for encryption and the key generation process of S-DES generates 2 sub keys after processing the initial 10 bit input, it has 8 bit plaintext input the two sub keys are generated at both transmission and receiving ends the two keys are applied to 2 complex functions respectively, with the inclusion of initial permutation, expansion permutations expansions and s-boxes the security is substantial when compared with the classical techniques, Sdes gave some structure and formation to encryption techniques with step to step procedures for both encryption and decryption. [7]

B. DES

DES enhances the structure of S-DES by increasing the key size from 10-bits to 64-bits out of which its affective length is 56-bits [8].16 rounds are introduced with each round containing XOR, substitutions and permutations for 16 rounds 16 keys are generated each of 48-bits which strengthens the security of this algorithm further, in terms of processing DES is 3 times faster than 3 DES [9].DES takes plain text in 64-bits of block these 64-bits are divided in to 32- bits each the right half of 32-bits goes through the expansion block which increase the bit count from 32 to 48-bits by reusing some bits

after expansion block comes XOR operation with sub-key which is also of 48-bits result of this operation is again of 48-bits, these 48-bits now goes in to 8 S-boxes the 48- bits are divided into 8 parts of 6-bits each going in to S-box1 to S-box8, the overall result of S-box substitution is reduced from 48 to 32-bits which is then XOR with the left half of the initial plaintext block to give a 32-bit result which is placed on right and the initial right half of the block is placed at left to get the 64-bit output of its round similarly this output of 1st round becomes input of the 2nd round and same procedure is pursued till the 16th round, after 16th round there is a 32 bit swap and finally the bits are placed in inverse permutation table to get the encrypted message, reverse method is applied to yield the result [7].

Proposed Technique

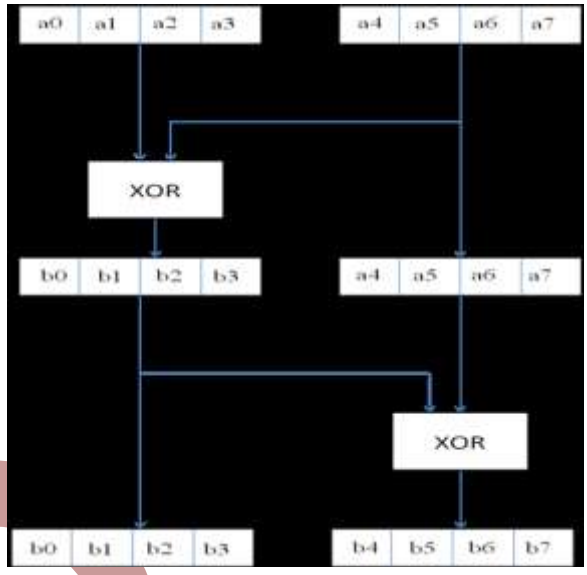
The proposed algorithm (fig 5) uses the positive features of the classical cryptographic algorithm like scrambling of bits and combines it with the main advantage of a modern cryptographic algorithm, i.e., the usage of a key. In this algorithm, the key is of 64-bits or more. The actual message to be encrypted is split into block of 64-bits (8 alphabets). Every block is enciphered using a Playfair cipher. The resulting encrypted text undergoes intensive scrambling as shown in fig 2. The scrambled text, which is also 8 bits, is further enciphered using a Vigenere cipher.

	a0	a1	a2	a3	a4	a5	a6	a7
+	a1	a1	a3	a3	a5	a5	a7	a7
=	b0	b1	b2	b3	b4	b5	b6	b7
+	b2	b3	b2	b3	b6	b7	b6	b7
=	c0	c1	c2	c3	c4	c5	c6	c7
+	c0	c1	c2	c3	c0	c1	c2	c3
=	d0	d1	d2	d3	d4	d5	d6	d7

The Vigenere ciphered text (d0d1…d7) is split into 2 parts of 4 bits each. These 2 parts are used for selecting the particular value in the 16 X 16 Substitution Box (fig 3). The first part (first 4 bits) is taken as the row and the second part (last 4 bits) is taken as the column. The resultant 64 bit is virtually unrecognizable and unbreakable using brute force approach.

Now the 64 bits are XOR-Scrambled M times (M=1, 2 or 3) (fig 4). Then, the 64-bits are further spilt into 4 blocks of 16 bits each which are then XOR-ed block-wise as shown in fig 5. The blocks are further merged and XOR-ed again as shown. The whole process is performed N times.

In this experiment we take the value of N between 1 and 16. Finally the output is further scrambled using the same S-Box as shown in fig 3.



Avalanche Effect

A desirable property of any encryption algorithm is that a small change in either the plain text or the key should produce a significant change in the cipher text [6].Avalanche effect is the phenomenon that describes the effect in the output cipher text if a single or few bits are changed in the plain text, whereas this change that occurs at the output should be sufficient if we want to create a secure algorithm [7].In next section

comparison will be made with other techniques on the basis of avalanche effect.

Calculation of Avalanche Effect

The Avalanche Effect is calculated as:

Avalanche Effect = No. Of bits flipped in the Ciphered Text / No. Of bits in the Ciphered Text * 100%

Comparison of Avalanche Effect

Avalanche Effect refers to a desirable property of cryptographic algorithms where, if an input is changed slightly (for example, flipping a single bit) the output changes significantly (e.g., more than half the output bits flip). In our case, we take the input plain text as “DISASTER”. Flipping one bit from the plain text, we get “DISCSTER” (on flipping A (01000001) to C (01000011)). The key used is “SRIRAMSR”.

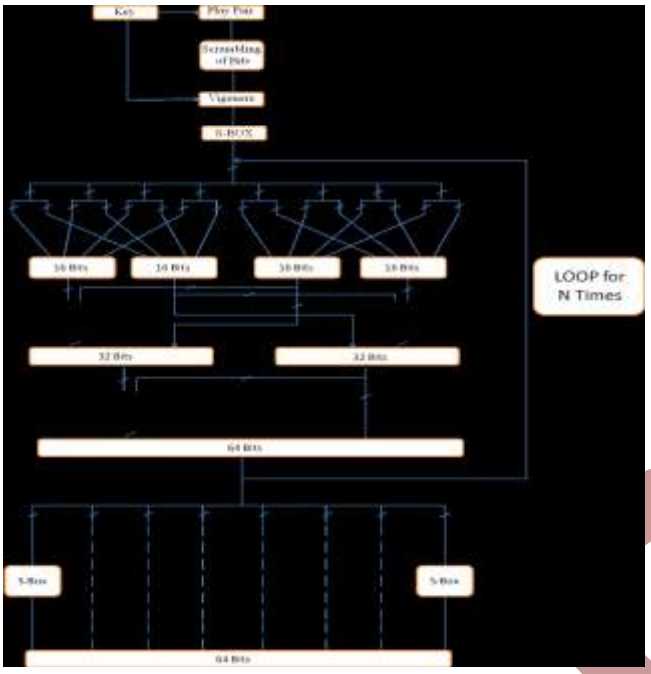
KEY: SRIRAMSR

0101001101010010010010010101001001000001010011010101001101010010

PLAIN TEXT 1: DISASTER

0100010001001001010100110100000101010011010101000100010101010010

PLAIN TEXT 2: DISCSTER
0100010001001001010100110100010101010011010101000100010101010010



Playfair Cipher:

CIPHER TEXT 1: KDRMAOCA

0100101101000100010100100100110101000001010011110100000001101000001

CIPHER TEXT 2: KDRBAOCA

0100101101000100010100100100001001000001010011110100000001101000001

We can clearly see that the avalanche effect is 4 bits, that is, 6.25%.

Caesar Cipher:

CIPHER TEXT 1: GLVDVWHU

0100011101001100010101100100010001010110010101110100100101010101

CIPHER TEXT 2: GLVFVWHU

0100011101001100010101100100011001010110010101110100100101010101

The Avalanche Effect, in this case, is 1 bit only, that is, 1.56%.

DES:

CIPHER TEXT 1:

0100000011000110111110001011011101110110010010011010010111111111

CIPHER TEXT 2:

0110001000111110111010010100001110001110001111101000111000101000

After 16 Rounds of DES, there are 35-bits flipped. Hence the Avalanche Effect is 54.68%.

Proposed Technique:

CIPHER TEXT 1:

0100111101011100001001101001000000100000111000111111000001011111

CIPHER TEXT 2:

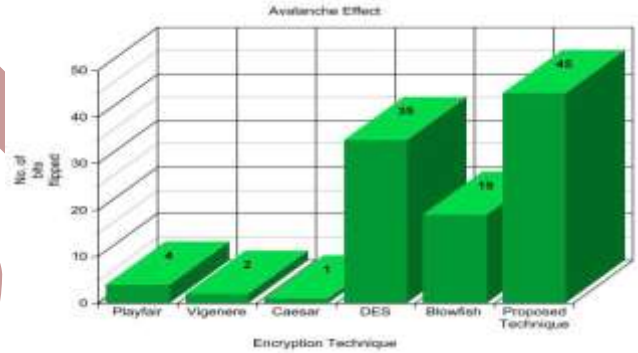
0000011000010011100110011010010110000100010101000001101001000101

We can clearly see that there is a difference of 45 bits. The Avalanche Effect is calculated as 70.31%.

Result

The following results are obtained after calculating the respective Avalanche Effects.

Encryption Technique	No. of bits flipped	%
Playfair Cipher	4	6.25
Vigenere Cipher	2	3.13
Caesar Cipher	1	1.56
DES	35	54.68
Blowfish	19	28.71
Proposed Technique	45	70.31



Conclusion

This paper reviews some of the encryption and modern techniques that are demanded in several fields nowadays. These techniques had already been applied in fields related to security in message communication, key management problem remote sensing satellite, video encryptions etc. The encryption algorithm used is a simple, direct mapping algorithm using matrix and arrays. The poly alphabetic cipher text generation provides a good strength to this encryption algorithm, while the combination of poly alphabetic substitution, translation and transposition makes the decryption extremely difficult in absence of a secret key. With the increasing importance of video security more enhanced better methods are required to improve security in a broad way. As such it is quite essential to improve our algorithms performance in future. From the above discussion we can clearly see that the proposed algorithm has better Avalanche Effect than any of the other existing algorithms and hence can

be incorporated in the process of encryption of any plain text. Also, we can see that the classical ciphers like Playfair cipher, Vigenere Cipher, Caesar Cipher etc. have very less Avalanche Effect and hence cannot be used for encryption of confidential messages. The modern encryption techniques are better than classical ciphers as they have higher Avalanche Effect. For Example, DES has an Avalanche Effect of 54.38%.

References

[1] William Stallings, "Network Security Essentials (Applications and Standards)" Pearson Education, 2004,pp.2-80.
[2] Charles P. Pfleeger, Shari Lawrence Pfleeger. "Security in computing" Pearson Education 2004 -pp. 642-666.
[3] Jose J. Amador, Robert W. Green, "Symmetric-key Block Ciphers for Image and Text Cryptography" , International Journal of imaging System Technology, Vol. 15 - pp. 178-188,2005.
[4] Dragos Trinica, "Sequential and Parallel Cascaded Convolution Encryption with Local Propagation: Toward future Directions in Cryptography", Proceedings of The third International Conference on information Technology-New Generations. (ITNG'06), 0-7695-2497- 4 / 2006, IEEE Computer Society.
[5] Lecture Notes on "Computer and Network Security" by Avi Kak.Pdf
h t t p: / / jun i ch ol l . or g/Cr ypt a na l ys i s /Da t a / EnglishData.php
[6] William Stallings, "Cryptography and Network Security", Fourth Edition, Prentice-Hall -pp.80-81.
[7] Fauzan Saeed 1, Mustafa Rashid 2, "Integrating Classical Encryption with Modern Technique", International Journal of Computer Science and Network Security, VOL. 10 No.5, {May 2010}.
[8] V. Umakanta Sastry 1, N.Ravi Shankar2, and S.Durga Bhavan "A Modified Hill Cipher Involving Interweaving and Iteration" International Journal of Network Security, Vol. 11, No. 1, PP.11 {16, July 2010}.
[9] Results of Comparing Tens of Encryption Algorithms Using Different Settings- Crypto++ Benchmark, Retrieved Oct.1, 2008, (http://www.eskimo.com/ wei-Dai/benchmarks.html).
[10] Y.C. Hu, A. Perrig and D.B. Johnson, "SEAD: Secure Efficient Distance Vector Routing for mobile wireless ad hoc networks", Proceeding of IEEE Workshop on Mobile Computing Systems and Applications, 2003.
[11] "Information Security: Theory and Practice", by Patel, Page 20.
[12] http://en.wikipedia.org/wiki/Data_Encryption_Standard.
[13] Janan Ateya Mahdi, "Design and Implementation of Proposed B-R Encryption Algorithm", IJCCCSE, Vol. 209, No.1.2009.
[14] http://www.cs.trincoll.edu/~crypto/historical/caesar.html.
[15] Schildt, "Java: The Complete Reference", 2006.
[16] http://en.wikipedia.org/wiki/Blowfish_(cipher).