The Design of advanced High Performance Encryption Algorithm by using Symmetric Cryptography

Prof Surbhi R.Khare
Asst.Prof.DEPT.OF CSE/IT
PIGCE,NAGPUR,INDIA
e-mail: surbhikhare06@gmail.com

Prof.Syaed Rehan
Asst.Prof:Dept.of CSE
ACET,NAGPUR,INDIA
email: sayedrehan1@yahoo.com

Prof .P.N.Vithalkar
Asst.Prof.DEPT.OF CSE/IT
PIGCE,NAGPUR,INDIA
e-mail: Pshendekar@yahoo.com

Abstract—This paper presents a new approach towards cryptography. There are many methods for acquiring security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential and important aspect for secure conversion of the information is cryptography, But it is important to note that cryptography is necessary for secure conversion of information, it is not fulfill required security. In this Paper, we are showing a new encryption key model as well as encryption algorithm model which will improving avalanche effect as compare various encryption algorithm. The proposed models will secures information from all the attack which is constantly follow-up peculiarity over public network. It significantly simplifies model written as security purpose while improving the efficiency of cryptography algorithm.

Keywords*- High Performance, secure commerce, encryption algorithm, conversion, peculiarity, avalanche effect (key words)*

*****

I. INTRODUCTION

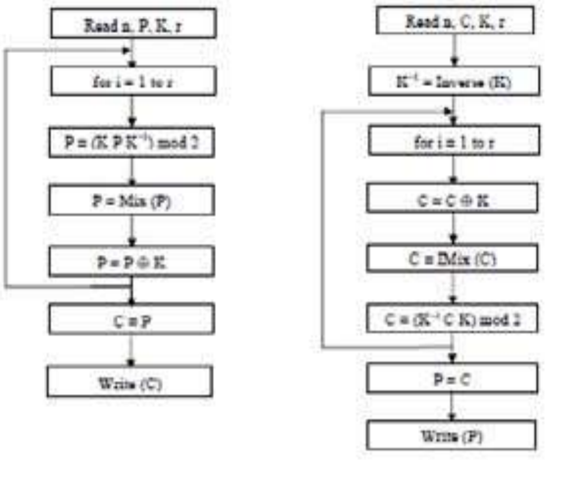
In an open networked systems, information is being received and misused by adversaries by means of facilitating attacks at various levels in the communication [4].Data encryption is sought to be the most effective means to counteract the attacks [5].There are two type of encryption in use, which are referred to as i) Symmetric-key encryption and ii) Asymmetric-key encryption. Asymmetric encryption algorithms are slow, whereas Symmetric-encryption algorithms generally run 1000 times faster [3]. Symmetric-encryption has been - and - still is extensively used to solve the traditional problem of communication over an insecure channel [2].In public 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[5]. A Cipher is something that is used to change the actual data into a format that cannot be recognized by anyone except the sender and receiver. One of the important considerations for measuring the strength of any cryptographic algorithm is its Avalanche Effect [2].

II. LITERATURE SURVEY

In this section basically we are presenting study of two algorithms which is following:

- A Block Cipher Having a Key on One Side of the Plain Text Matrix and its Inverse on the Other Side[1]
- A Modified Hill Cipher Involving a Pair of Keys and a Permutation

Here a newly developed technique named, “A Block Cipher Having a Key on One Side of the Plain Text Matrix and its Inverse on the Other Side” [6] is discussed. At first, consider a plain text P which can be represented in the form of a square matrix given by P = [Pij], i = 1 to n, j = 1 to n, where each Pij is equal to 0 or 1. Let us choose a key k. Let it be represented in the form of a matrix given by K = [Kij], i = 1 to n, j = 1 to n, where each Kij is a binary number. Let C = [Cij], i = 1 to n, j = 1 to n be the Corresponding cipher text matrix. The process of encryption and the process of decryption adopted in this analysis are given in Fig. 1. Here r denotes the number of rounds in the iteration process. In the process of encryption, we have the iteration scheme[4]. which includes the relations P = (KPK^{-1}) mod 2, (2.4) P = Mix (P), and P = P ⊕ K. (2.6) The relation (2.4) is used to achieve diffusion, while the relations (2.5) and (2.6) are used to acquire confusion. The function Mix (P) mixes the plain text at every stage of the iteration. In the process of decryption, the function I Mix represents the reverse process of Mix[3].



(a) Process of Encryption (b) Process of Decryption

Figure1: process of encryption and Decryption (CIPHER)

Another newly developed technique named “A modified hill cipher involving a pair of keys and a permutation” [7] is discussed. in the recent years, several modifications of hill cipher have appeared in the literature of cryptography. in all these investigations, modular arithmetic inverse of a key matrix plays a vital role in the processes of encryption and decryption. it is well known that the hill cipher containing the key matrix on the left side of the plaintext as multiplicand can be broken by the known plaintext attack[2]. in a recent paper, to overcome this drawback, have developed a block cipher which includes a key matrix on both the sides of the plaintext matrix. in this analysis they have discussed the avalanche effect and cryptanalysis, and have shown that[3].

The cipher is a strong one. In the present algorithm, our objective is to modify the Hill Cipher by including a pair of key matrices, one on the left side of the plaintext matrix and another one on the right side of the plaintext matrix as multiplicands, so that the strength of the cipher becomes highly significant. In this we represent each character of the plaintext under consideration in terms of EBCDIC code and use mod 256 as a fundamental operation[4]. Here the security of the cipher is expected to be more as we have two keys. This is on account of the fact that, in some untoward circumstances, though one key is known to the hackers, other remains as a secret one and it protects the secrecy of the cipher. The process of encryption, which is in the form of iteration, is governed by the relations,

P = (K P L) mod 256, and P = Permute(P).

The process of decryption is governed by the relations,

C= I Permute(C) and C= (K¯¯1 C L¯¯1) mod 256,

This contains m (=n2) rows and eight columns. Assuming that n is an even number, the above matrix is divided into two halves. The upper half contains m/2 rows and eight columns, and similarly the lower half. Then the upper half is mapped into a matrix containing m rows and Four columns[5]. In the process of mapping we start with the last element of the upper half and place it as the first row, first column element of a new matrix. Then we place the last But one element of the upper half as the element in the second row and first column.

We continue this process of placing the remaining elements of the upper half, one after another, till we get m rows and four columns of the new matrix[3]. Then we place the elements of the lower half from the beginning to the end, such that they occupy four more columns and m rows. Thus we again get a matrix of size mx8. This process of permutation is expected to thoroughly permute the binary bits of the elements. The clear picture of this permutation can be seen later in illustration. It may be noted here that IPermute () in decryption is a reverse process of Permute () used in encryption[4]. The process of encryption and the process of decryption are described by the flow charts given in Figure 2.

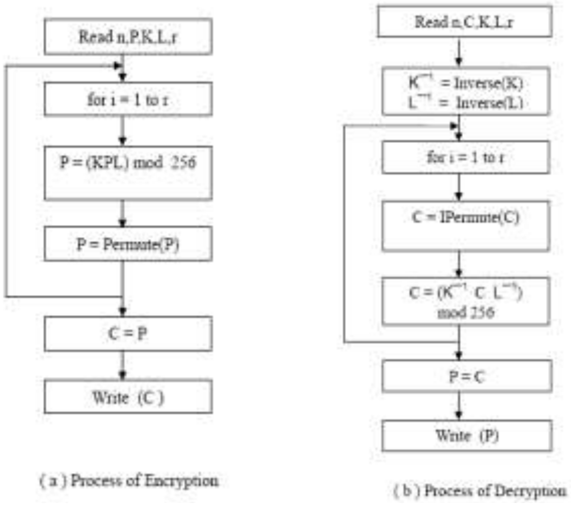


Figure 2. Flow Charts of the Cipher

III. Problem Analysis of Paper

A. Selecting a Template (Heading 2)

Each of the above specified techniques is having their own strong and weak points. In order to apply an appropriate technique in a particular application we are required to know these strong and weak points. Therefore the comparison of these techniques based on several features is necessary. Some of these points under which the cryptosystems[4] can be compared are described below:

1. Avalanche effect: A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the cipher text. In, particular a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the cipher texts.

2. Memory required for implementation: Different encryption techniques require different memory size for implementation. This memory requirement depends on the number of operations to be done by the algorithm. It is desirable that the memory required should be as small as possible.

3. Simulation time: The time required by the algorithm for processing completely a particular length of data is called the simulation time. It depends on the processor speed, complexity of the algorithm etc. The smallest value of simulation time is desired.

4. Inverse Zero: - Because determinant of key K can be zero that by it is time consuming process.

IV. Proposed Model

Encryption Approach used:- Symmetric-key algorithms are a class of algorithms for cryptography that use trivially related, often identical, cryptographic keys for both decryption and encryption. An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. Contrast this with public-key cryptology, which utilizes two keys **-** a public key to encrypt messages and a private key to decrypt them.

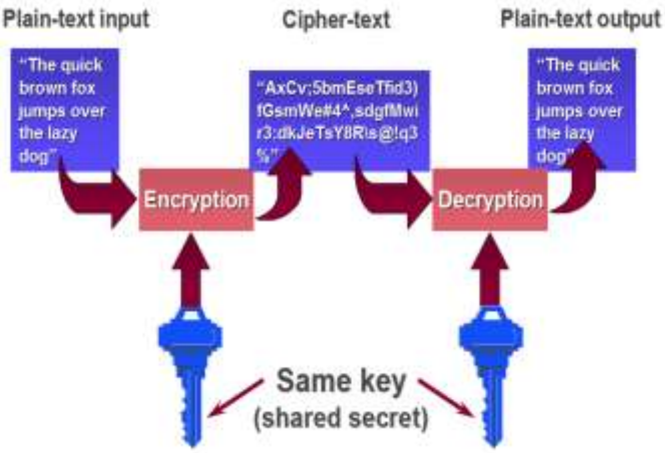

Plain-text input
Cipher-text
Plain-text output
"The quick brown fox jumps over the lazy dog"
"AxCv;5bmEseTfid3)fGsmWe#4^,sdgfMwir3:dkJeTsY8R\s@!q3%"
"The quick brown fox jumps over the lazy dog"
Encryption
Decryption
Same key
(shared secret)

Figure-3: Symmetric Key Cryptography

Other terms for symmetric-key encryption are secret-key, single-key, shared-key, one-key and eventually private-key encryption. Use of the latter term does conflict with the term private key in public key cryptography. Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way. Public-key encryption avoids this problem because the public key can be distributed in a non-secure way, and the private key is never transmitted. Symmetric-key cryptography is sometimes called secret-key cryptography. The most popular symmetric-key system is the Data Encryption Standard (DES).

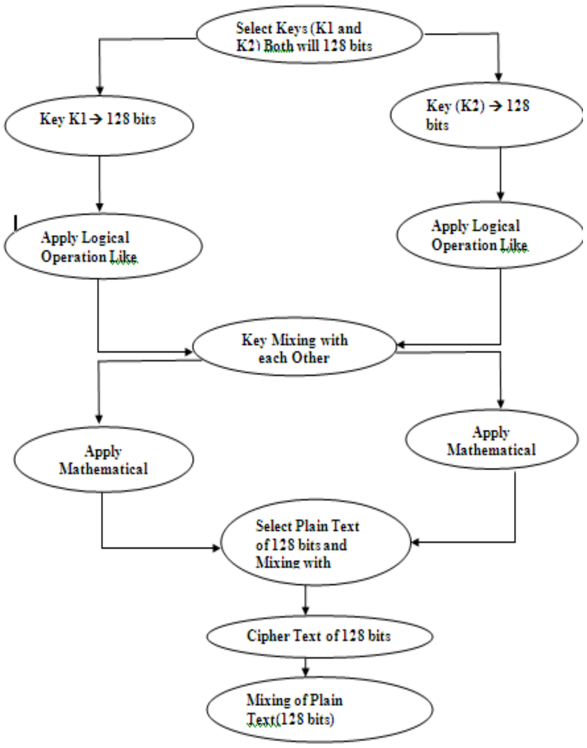

Select Keys (K1 and K2) Both will 128 bits
Key K1→ 128 bits
Key (K2) → 128 bits
Apply Logical Operation Like
Apply Logical Operation Like
Key Mixing with each Other
Apply Mathematical
Apply Mathematical
Select Plain Text of 128 bits and Mixing with
Cipher Text of 128 bits
Mixing of Plain Text(128 bits)

Figure 4 :proposed model

V. Advantage of Proposed Model

1] Our Proposed Model will generate key of 128 bits which is larger than other algorithm key length, this will enhance the security aspect of this algorithm and make them more secure than other encryption Algorithms.

2] This Algorithm is much smaller with comparing algorithms and easy to understand and implement.

3] It does not contain complex structure, control flow is well defined and looping structure is minimized. Due to the following facts it takes very less time for execution.

4] Our Proposed Model using symmetric key for avalanche effect which is 1000 time faster then asymmetric encryption algorithms.

VI. Algorithm Steps:

1) Define Variable P as a Plain Text, K1 as a Key1, K2 as a Key2, R as a Number of Round, N as a 1 to 16 Numeric Value.
2) Assign Value to P = 128bits, K1 = 128 bits, K2 = 128 bits, N = 16.
3) For R = 1 to 16.
4) Select K1 & K2.
5) Divide K1 into K11→ 64 bits & K12→ 64 bits.
6) Divide K2 into K21→ 64 bits & K22→ 64 bits.
7) Apply Mix (K1o1, K21)→ K1→128bits and Mix (K12, K22)→ K2→ 128 bits.
8)Apply LeftCircularShift (K1) and RightCircularShift (K2).
9) Again K1 will divided into two parts of equal bits, 64 bits for K11 and 64 bits for K12. Similarly K2 will also divided into two parts of equal bits. 64 bits for K21 and 64 bits for K22.
10) Select K12 & K21
11) Apply M-Box(K12, K21)
12) Select K11 & K22 Separately.
13) Apply P-Box (K11) and P-Box (K22).
14) Apply Con-Cat(Output of P-Box(K11) & Output of M-Box(K12,K21))→ K1 and Con-Cat(Output of P-Box(K22) & Output of M-Box(K12,K21))→ K2.
15) Select Plain Text P→128 bits and K1→128 bits.
16) Apply Mod Function on K1 & P

$$\phi P = (K1\ P\ K1^{-1}) \bmod 2$$

17) Apply Mod Function on 21 & ϕP

$$\Psi P = (K2\ \phi P\ K2^{-1}) \bmod 2$$

18) Cipher Text will be produce in the form of ΨP.
19) Exit.

VI.[A]. Algorithm Steps of M-Box

1) Select 64 bits Key K12 and K21 Separately.
2) Select K12→ 64 bits & divided into 8-8 bits blocks. Total 8 blocks will be generating. Similarly select K21→ 64 bits & divided into 8-8 bits blocks. Total 8 blocks will be generating.
3) Apply Mix (K12, K21).
4) After Mixing of K12 and K21 with each other total 64 bits will be generating. This will become output of M-Box function.
5) Exit.

VI.[B]. Algorithm Steps of P-Box

1) Select 64 bit key -k11 64 bit –Array 8-8 bit Block. Like-

1 0 1 0 1 1 0 1	1st Row
1 1 0 1 1 0 1 1	2nd Row
1 1 1 1 0 0 1 1	3rd Row
1 0 0 0 0 1 1 0	4th row
1 1 0 0 1 1 0 1	5th Row
1 0 0 1 1 1 1 1	6th Row
1 1 1 0 0 1 1 1	7th Row
1 0 1 0 1 0 1 0	8rt Row

2) Select 4th Row & Arrange all entry of that Row in 1st Column .Similarly 3rd Row entry in 2nd Column, 2nd Row in 3rd Column & 1st Row in 4th Column.

1 1 1 1 1 1 1 1
0 1 1 0 0 1 0 1
0 1 0 1 1 1 0 0
0 1 1 0 0 0 1 0
0 0 1 1 1 0 1 1
1 0 0 1 0 1 1 1
1 1 1 0 1 1 1 0
0 1 1 1 0 1 1 1

3) Select 8th row in 5th column, 7th row in 6th column, 6th row in 7th column & 5th Row in 8th column.

4) Now combine out 8 bit – 8 bit value in 64 bit

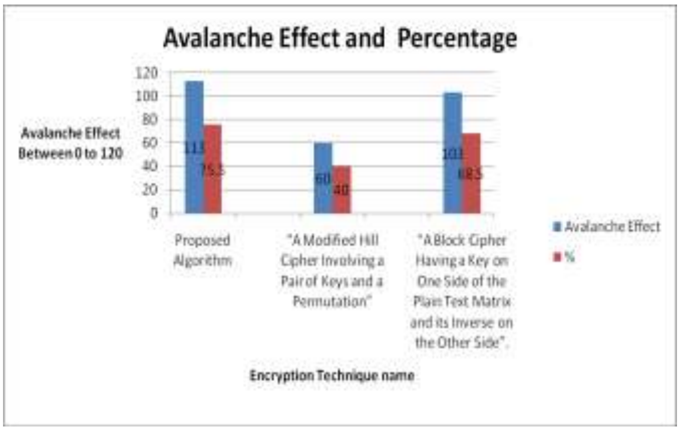
5) Same Permutation Process we will apply on key k22 & we will get 64 bit key k22.

VII. SUMMARY OF RESULT AND COMPARISON

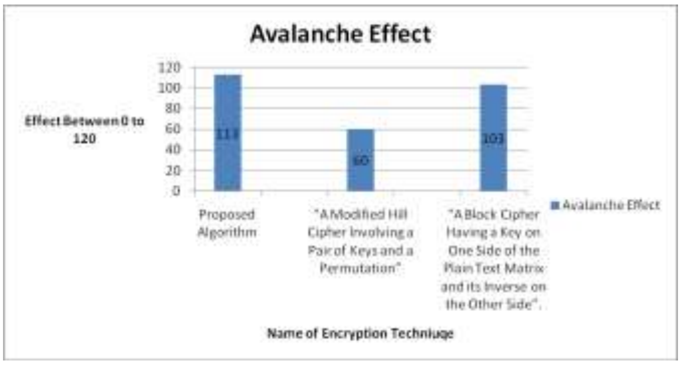
Comparison the results that were obtained can be well represented in form of table that describes the avalanche effect in the above discussed algorithms.

Table-1:- Avalanche Comparison of various Encryption Algorithm

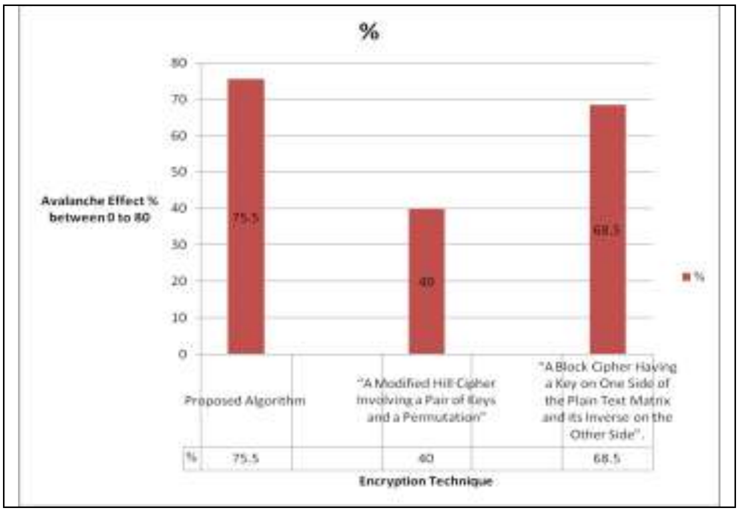
Encryption Technique	Avalanche Effect	%
Proposed Algorithm	**113**	**75.5**
“A Modified Hill Cipher Involving a Pair of Keys and a Permutation”	**60**	**40**
“A Block Cipher Having a Key on One Side of the Plain Text Matrix and its Inverse on the Other Side”.	**103**	**68.5**



Graph-1:- Avalanche Effects and there percentage results of various algorithm.



Graph-2:- Only Avalanche Effects of various algorithm



Graph-3:- Avalanche Effects results in % of various algorithm

VIII. CONCLUSION

Design of High Performance Encryption Algorithm Security point of view our in proposed working model will be very effective, efficient and it will give better performance in terms of avalanche effect than other encryption algorithms used in the other model. Since it does not have any known security weak points so far, this makes it an excellent candidate to be considered as a standard encryption working model. Some typical results obtained by the evaluation system can be found in Tab. I can produce more results here but these results are sufficient to differentiate between proposed algorithm and comparing algorithm.

In conclusion, this evaluation model based technique in this research paper is a new quantitative analysis method about cryptographic algorithm, further manifests a new conclusion that the cryptographic algorithm may be have some data dependence. Future security mechanism must have a more effective cryptographic algorithm to keep information confidential, and that is the reason why always searching for more effective algorithm. Analyzing the avalanche effect of each algorithm can lay a foundation for evaluating other more secure method in future, Also the evaluation model based technique may be useful for analyzing new and more effective algorithm to reduce.

References

[1] 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.

[2] 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.

[3] [7]. V. U. K. Sastry, V. Janaki, “A Modified Hill Cipher with Multiple Keys”, International Journal of Computational Science, Vol. 2, No. 6, 815 – 826, Dec. 2008.

[4] V. U. K. Sastry, D. S. R. Murthy, S. Durga Bhavani, “A Block Cipher Involving a Key Applied on Both the Sides of the Plain Text”, International Journal of Computer and Network Security (IJCNS), Vol. 1, No. 1, pp. 27 -30, Oct. 2009

[5] Lecture Notes on "Computer and Network Security" by Avi Kak.Pdf http://junichol l.org/Cryptanalysis/Data/EnglishData.php.

[6] William Stallings, "Network Security Essentials (Applications and Standards)" Pearson Education, 2004, pp.2-80.

[7] Charles P. Pfleeger, Shari Lawrence Pfleeger. "Security in computing" Pearson Education 2004 -pp. 642-666