Proposed Model of Encryption Technique using Block Cipher Concept to Enhance Avalanche Effect

[1]Aumreesh Saxena, [2]Sourabh Singh

[1] Sagar Institute of Research Technology and Science, Bhopal, Madhya Pradesh India

[2] Sagar Institute of Research Technology and Science, Bhopal, Madhya Pradesh India

Abstract - The world It know today would be impossible without cryptography. This Paper are presenting study of cryptography and problem associating with existing encryption model is also presented. Furthermore this is proposing encryption model. This encryption model is based on the block cipher concept where it will be encrypt and decrypt any type of data file. The primary goal of this paper is to improve level of security. The proposed encryption model will analyze by using a parameter called Avalanche effect. Plaintext and encryption key are mapped in binary code before encryption process. Avalanche Effect is calculated by changing one bit in plaintext keeping the key constant and by changing one bit in encryption key keeping the key constant. Expected experimental results shows that the proposed encryption model exhibit significant high. Avalanche Effect will improve the level of the security.

***Keyword* - Encryption, Decryption, Security, Model, Cryptography, Key.**

1. Introduction

A typical approach to security is to strike a balance between apparent risks to information and efforts to mitigate those risks. A common standard used to determine the level of security required is commercial impracticability, if it takes longer to access critical data than the timeframe within which its knowledge confers some benefit, practical security has been achieved. For example, if the credit card information is protected by a system that would take the most sophisticated hacker five years to unlock, but one may obtain new credit card numbers every two years on average, there will be little benefit to breaking the security scheme [1]. Encryption is the process of turning a clear-text message (Plaintext) into a data stream which looks like a meaningless and random sequence of bits (cipher-text). The process of turning cipher text back into plaintext is called decryption. Cryptography deals with making communications secure. Crypto-analysis deals with breaking cipher text that is, recovering plaintext without knowing the key. Cryptology is a branch of mathematics which deals with both cryptography and crypto-analysis. A cryptographic algorithm, also known as a cipher, is a mathematical function which uses plaintext as the input and produces cipher text as the output and vice versa [2]. All modern ciphers use keys together with plaintext as the input to produce cipher text. The same or a different key is supplied to the decryption function to recover plaintext from cipher text. The details of a cryptographic algorithm are usually made public. It is the key that the security of a modern cipher lies in, not the details of the cipher [3, 4].

Cryptography algorithms are divided into two families based on the key type: symmetric or secret key cryptography, and asymmetric or public key cryptography. In symmetric key cryptography both the sender (encrypter) and receiver (decrypter) use the same secret key, so named because the strength of the system relies on the key being known only to the sender and receiver. Symmetric algorithms use the same key for encryption and decryption. These algorithms require that both the sender and receiver agree on a key before they can exchange messages securely. Some symmetric algorithms operate on 1 bit (or sometimes 1 byte) of plaintext at a time. They are called stream ciphers [4]. Other algorithms operate on blocks of bits at a time. They are called block ciphers. Most modern block ciphers use the block size of 64 bits.

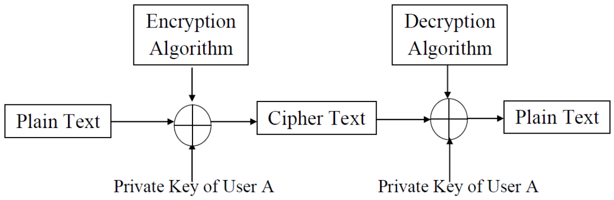

Figure1.1 Simple Encryption and Decryption of symmetric key

Public-key cryptography (also known as asymmetric algorithms) uses two different keys (a key pair) for encryption and decryption. The keys in a key pair are mathematically related, but it is computationally infeasible to deduce one key from the other. These algorithms are called "public-key" because the encryption key can be made public. . Anyone can use the public key to encrypt a message, but only the owner of the corresponding private key can decrypt it. Some public-key algorithms such as RSA allow the process to work in the opposite direction as well: a message can be encrypted with a private key and decrypted with the corresponding public key [5].

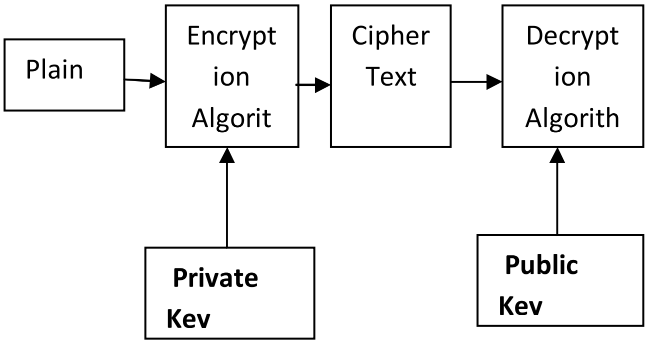

Figure1.2 Simple Encryption Decryption using Private & Public Key

Avalanche Effect: In cryptography, the avalanche effect is evident if, when an input is changed slightly (for example, flipping a single bit) the output changes significantly (e.g., half the output bits flip). In the case of quality block ciphers, such a small change in either the key or the plaintext should cause a drastic change in the cipher text. If a block cipher or cryptographic hash function does not exhibit the avalanche effect to a significant degree, then it has poor randomization, and thus a cryptanalyst can make predictions about the input, being given only the output. This may be sufficient to partially or completely break the algorithm. Thus, the avalanche effect is a desirable condition from the point of view of the designer of the cryptographic algorithm or device [5-6].

This survey is presenting the study of data security using cryptography technique. This paper is describing existing cryptography technique briefly. Rest of this paper is organized in following way, Section-II, Literature survey and presenting problem in existing algorithm, Section-III, presenting proposed idea, Section-IV, presenting expected outcome of proposed idea and conclusion.

2. Literature Survey

A Modified Playfair Cipher Involving Interweaving and Iteration 2009 [11]: In this investigation, they have generalized and modified the Playfair cipher into a block cipher. Here, they have introduced substitution, interweaving and iteration. The cryptanalysis and the avalanche effect carried out in this analysis markedly indicate that the cipher is a strong one, and it cannot be broken by any cryptanalytic attack. Timing evaluation of the known cryptographic algorithms 2009 [12]: A new timing evaluation model based on random number generating mechanism is presented to analyze the time-consuming of the known cryptographic algorithms: triple-DES, AES and RSA. In this model for evaluation, there are two evaluating modes: different plaintexts in the same key (DPSK), the same plaintext in different keys (SPDK). As the basis of the evaluating model, the plaintext and the corresponding key are both generated by random numbers. The results show that, under the same key length and for the same size of the processed data, RSA is about several hundred times slower than AES, triple-DES is about three times slower than AES, and there are other runtime characteristics which further highlights the difference between these three cryptographic algorithm and provides a reference value of for people's rational using. Integrating Classical Encryption with Modern Technique 2010 [13]: Alphabetical ciphers are being used since centuries for inducing confusion in messages, but there are some drawbacks that are associated with Classical alphabetic techniques like concealment of key and plaintext. In this they suggested an encryption technique that is a blend of both classical encryption as well as modern technique.

A Modified Hill Cipher Involving Interweaving and Iteration 2010 [14]: This paper deals with a modification of the Hill cipher. In this, they have presented interweaving in each step of the iteration. The interweaving of the resulting plaintext, at each stage of the iteration, and the multiplication with the key matrix leads to confusion and diffusion. Comparing Classical Encryption With Modern Techniques 2010 [15]: In this they presented building the basics of classical encryption and modern techniques. Implementation and analysis of various symmetric cryptosystems 2010 [16]: In this we have analyzed that this research is based on comparisons of existing algorithm. Basically in this they have implemented some of the widely used symmetric encryption techniques i.e. data encryption standard (DES), triple data encryption standard (3DES), advanced encryption standard (AES), BLOWFISH and RC4 in using software. After the implementation, these techniques have compared on some points. These points are avalanche effect due to one bit variation in plaintext keeping the key constant, memory required for implementation and simulation time required for different message lengths. Matrix based Key Generation to Enhance Key Avalanche in Advanced Encryption Standard 2011 [17]: In symmetric block ciphers, substitution and diffusion operations are performed in multiple rounds using sub-keys generated from a key generation procedure called key schedule. The key schedule plays a very important role in deciding the security of block ciphers. In this they presented a key generation procedure, based on matrix manipulations, which could be introduced in symmetric ciphers. As a case study, matrix based key generation procedure has been introduced in Advanced Encryption Standard (AES) by replacing the existing key schedule of AES. The key avalanche and differential key propagation produced in AES have been observed. The paper describes the matrix based key generation procedure and the enhanced key avalanche and differential key propagation produced in AES. It has been shown that, the key avalanche effect and differential key propagation characteristics of AES have improved by replacing the AES key schedule with the Matrix based key generation procedure. Analysis of Avalanche Effect in Plaintext of DES using Binary Codes 2012 [18]: With the fast progression of digital data exchange in electronic way, information security is becoming more important in data storage and transmission. Cryptography has come up as a solution which plays a vital role in information security system against malicious attacks. This security mechanism uses some algorithms to scramble data into unreadable text which can be only being decoded or decrypted by party those possesses the associated key. These algorithms consume a significant amount of computing resources such as CPU time, memory and computation time. In this a most widely used symmetric encryption technique i.e. Data Encryption Standard (DES) have been implemented. After the implementation, this encryption technique was analyzed based on a parameter called Avalanche effect, using binary codes.

Avalanche Effect due to one bit variation in plaintext keeping the key constant after mapping it in a binary code. Effective implementation and avalanche effect of AES 2012 [20]: Efficient implementation of block cipher is critical towards achieving high efficiency with good understandability. Numerous number of block cipher including Advance Encryption Standard have been implemented using different platform. However the understanding of the AES algorithm step by step is very typical. This paper presents the efficient implementation of AES algorithm and explains Avalanche effect. A Bit Level Session Based Encryption Technique to Enhance Information Security 2012 [21]: In this paper, a session based symmetric key cryptographic system has been presented and it is termed as Bit Shuffle Technique (BST). BST consider the plain text (i.e. the input file) as binary string with finite no. of bits. The input binary string is broken down into manageable-sized blocks to fit row-wise from left to right into a square matrix of suitable order. Bits are taken diagonally upward from the square matrix to form the encrypted binary string and from this string cipher text is formed. Combination of values of block length and no. of blocks of a session generates the session key for BST. For decryption the cipher text is considered as binary string. Using the session key information, this binary string is broken down into manageable-sized blocks to fit diagonally upward from left to right into a square matrix of suitable order. Bits are taken row-wise from left to right from the square matrix to form the decrypted binary string and from this string plain text is formed. Study of Avalanche Effect in AES Using Binary Codes 2012 [22]: With the fast progression of digital data exchange in electronic way, security of information is becoming more important in data storage and transmission. Cryptography has come up as a solution which plays a vital role in information security system against malicious attacks. This security system uses some algorithms to scramble data into scribbled text which can be only being decoded or decrypted by party those possesses the associated key. These algorithms consume a significant amount of computing resources such as CPU time, memory and computation time. In this paper a most widely used symmetric encryption techniques i.e. advanced encryption standard (AES) have been implemented using MATLAB software. After the implementing this encryption technique, analysis is done by using a parameter called Avalanche effect. Plaintext and encryption key are mapped in binary code before encryption process. Avalanche Effect is calculated by changing one bit in plaintext keeping the key constant and by changing one bit in encryption key keeping the key constant, Experimental results shows that the proposed algorithm exhibit significant high avalanche Effect which improves the level of the security.

This survey reviews some of the classical encryption and modern encryption 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 algorithms presented above is a simple, direct mapping algorithm using matrix and arrays. With the increasing importance of message security more enhanced better methods are required to improve security in a broad way. 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 required knowing 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 can be compared are described below:

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.

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.

Execution 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.

3. Proposed Work

Proposed Concept: In proposed encryption model is based on block cipher concept where data block will divide into sub blocks of equal length and then each sub block will encrypt using a special mathematical set of functions known as Key with the help of proposed encryption model. At the time of encryption or decryption same key will use because symmetric in nature. Proposed Key length will 128 bits long so that security of proposed encryption model will be very high. This is highly efficiently due to its simplicity. Here proposed encryption model will take less amount of time in execution as compare other encryption model because only one key will be work in whole process. Figure 1 is presenting basic block diagram of proposed concept. In this figure plain text will execute with proposed encryption algorithm and proposed encryption algorithm will call to proposed key to produce cipher text. In reverse cipher text will execute with proposed decryption algorithm and this proposed decryption algorithm will call same proposed key to produce plain text.

Table 1: Expected Avalanche Effect Comparison between Proposed and Existing Encryption Model

S. No.	*File Size*	*File Type*	*TDES*	*AES*	*BST*	*PA*
Avalanche Effect (Approximately)						
1	2	Image	Low	Low	Low	High
2	5	PDF	Low	Low	Low	High
3	7	XLX	Low	Low	Low	High
4	9	MP3	Low	Low	Low	High
5	11	TXT	Low	Low	Low	High

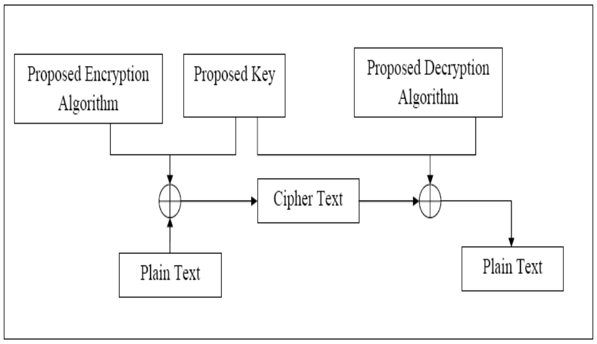

Figure 1: Block Diagram of Proposed Concept

4. Expected Outcome and Conclusion

Performance parameter: For an algorithm it is important to be efficient and secure. Efficiency of an algorithm is computed on the bases of time complexity and space complexity**.**

- Execution Time
- CPU Process Time
- Avalanche Effect

The execution time [21] is considered the time that an encryption algorithm takes to produce a cipher text from a plaintext. Execution time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated as the total plaintext in bytes encrypted divided by the execution time.

The CPU process time is the time that a CPU is committed only to the particular process of calculations. It reflects the load of the CPU. The more CPU time is used in the encryption process, the higher is the load of the CPU [21]. Avalanche effect is important characteristic for encryption algorithm. This property can be seen when changing one bit in plaintext and then watching the change in the outcome of at least half of the bits in the cipher text [20]. Hear we will evaluate proposed encryption model with existing encryption model on above mention parameter and expected results are shown in table 1 and table 2.

Table 2: Expected Execution Time Comparison between Proposed and Existing Encryption Model

S. No .	***File Size***	***File Type***	***TDES***	***AES***	***BST***	***PA***
Execution Time (Approximately)						
1	2	Image	High	High	High	Low
2	5	PDF	High	High	High	Low
3	7	XLX	High	High	High	Low
4	9	MP3	High	High	High	Low
5	11	TXT	High	High	High	Low

5. Conclusion

The proposed encryption model, presented in this paper is very simple to understand and it will easy to implement. The 128 bits key length for any particular file which will certainly enhance the security features. Expected outcome section indicates that the proposed encryption model is definitely comparable with existing encryption model. The performance of Proposed Encryption model is significantly better than existing encryption model. For large files, proposed encryption model will be very suitable. The proposed encryption model will be applicable to ensure high security in transmission of any file of any size.

References

[1] David Kahn, "The Code Breakers: The Story of Secret Writing," Simon & Schuster, 1996

[2] Simon Singh, "The Code Book," Anchor Books, 1999

[3] Robert Reynard “Secret Code Breaker II: A Cryptanalyst's Handbook.” , 1997

[4] David Mertz, “Introduction to cryptology, Part 1:” 2001

[5] Horst Feistel, "Cryptography and Computer Privacy." Scientific American, Vol. 228, No. 5, 1973.

[6] David Mertz, “Introduction to cryptology, Part 2:” 2002

[7] Bruce Schneier, Applied Cryptography published in 1999.

[8] An Introduction to Cryptography; released June 8, 2004 by PGP Corporation.

[9] T. Kohno, J. Kelsey, B. Schneier, “ Preliminary Cryptanalysis of Reduced-Round Serpent”,2000

[10] William stallings, “Cryptography and Network Security: Principles & Practices”, second edition, chapter 2 pg 29.

[11] V. Umakanta Sastry , N. Ravi Shanker and S.Durga Bhavani “A modified Playfair Cipher Involving Interweaving and Iteration” International journal of Computer theory and Engineering Vol.1,No. 5, December,2009 [12] Yan Wang Ming Hu “Timing evaluation of the known cryptographic algorithms” IEEE International Conference on Computational Intelligence and Security 2009

[13] Fauzan Saeed, Mustafa Rashid “Integrating Classical Encryption with Modern Technique”IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.5, May 2010

[14] V. Umakanta Sastry1, 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

[15] Mohit Kumar, Reena Mishra, Rakesh Kumar Pandey and Poonam Singh “Comparing Classical Encryption With Modern Techniques” S-JPSET, Vol. 1, Issue 1 2010

[16] Sriram Ramanujam and Marimuthu Karuppiah “Designing an algorithm with high Avalanche Effect” IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.1, January 2011

[17] Paul A.J., Mythili P., Paulose Jacob K. Matrix based Key Generation to Enhance Key Avalanche in Advanced Encryption Standard International Conference on VLSI, Communication & Instrumentation (ICVCI) 2011

[18] Akash Kumar Mandal, Mrs. Archana Tiwari, “Analysis of Avalanche Effect in Plaintext of DES using Binary Codes” IJETTCS Volume 1, Issue 3, September – October 2012 ISSN 2278-6856

[19] Chandra Prakash, Dewangan, Shashikant Agrawal “A Novel Approach to Improve Avalanche Effect of AES Algorithm” International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 8, October 2012 ISSN: 2278 – 1323

[20] Irfan.Landge, Burhanuddin Contractor, Aamna Patel and Rozina Choudhary “ Image encryption and decryption using blowfish algorithm” World Journal of Science and Technology 2012, 2(3):151-156 ISSN: 2231 – 2587

[21] Jyotsna Kumar Mandal, Manas Paul “A Bit Level Session Based Encryption Technique to Enhance Information Security”c International Journal on Computer Science and Engineering (IJCSE) ISSN : 0975-3397 Vol. 4 No. 02 February 2012

[22] Chandra Prakash Oewanganl ,Shashikant Agrawal,Akash Kumar Mandae,Mrs. Archana Tiwari “Study of Avalanche Effect in AES Using Binary Codes” 2012 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)