Design and Development of New Cryptography Protocol

[1] Gajendra Singh, [2] Preeti Shukla

[1] C.S (Department) SSSIST Sehore (M.P), R.G.P.V, Bhopal, M.P, India

[2] M.Tech. Scholar SSSIST Sehore (M.P), R.G.P.V, Bhopal, M.P, India

Abstract - The world it knows today would be impossible without cryptography. This Paper is 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 stream cipher concept where it will be encrypt and decrypt any type of data file in bit wise way. 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.

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

1. Introduction

Cryptography is the practice and study of techniques for secure communication in the presence of adversaries'. Typically, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. There are different types of cryptography. There is a sender, receiver, intruder of information and cryptographic tool that prevents intruder from trespass the sensitive information [18]. Cryptography provides four types of services such as confidentiality, integrity, authentication, non-repudiation. A service that enhances the security of the data processing systems and the information transfers of an organization. Confidentiality is protection of data from unauthorized disclosure. Integrity provides assurance that the information received are exactly as sent by an authorized entity i.e., information contain no modification, deletion, etc. Authentication ensures that the identity of the sender and receiver of the information. It provides assurance that the communicating entity is the one that it claims to be. Non- repudiation refers to the ability to ensure that the sender or receiver cannot deny the authenticity of their signature on the sending information that they originated [19]. The Plaintexts are processed in two ways; one is the stream cipher and the other is the block cipher [18-19]. A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher key stream. In a stream cipher each plaintext digit is encrypted one at a time (encrypt the information by individual bits) with the corresponding digit of the key stream, to give a digit of the cipher text stream. A block cipher is another symmetric key cipher operating on fixed-length groups of bits, called blocks, with an unvarying transformation [19].

For example block cipher encryption algorithm take a 128-bit block of plaintext as input, and output a corresponding 128- bit block of cipher text. Block ciphers uses modes of operation to provide an information services such as confidentiality or authenticity. Many modes of operation have been defined some of these are Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter mode. A mode of operation describes how to repeatedly apply a cipher's single-bloc. Cryptography systems can be classified into three types as symmetric key cryptography, asymmetric key cryptography and hash functions. Figure 1 illustrates types of cryptographic techniques.

- Symmetric Encryption (Private Key Encryption): In this type of encryption same key is used at the time of encryption and decryption. The key distribution has to be made before the transmission of the information starts. The key plays a very important role in this type of encryption. Example: DES, 3DES, BLOWFISH, AES etc. A symmetric key cryptography uses same secret key by sender and receiver for encryption and decryption respectively for example DES, etc [5]. In these techniques the plaintext and key are processed as stream cipher or block cipher.

- Asymmetric Encryption (Public Key Encryption): In this type of encryption different key is being used for encryption and decryption process. Two different key is generated at once and one key is distributed to other side before the transmission starts. Example: RSA algorithm.. Asymmetric or public key cryptography uses public key by sender for encryption which is known to all and private key which known by the receiver for decryption for example RSA, etc. Mostly this kind of techniques uses block ciphers for processing plaintext with key.

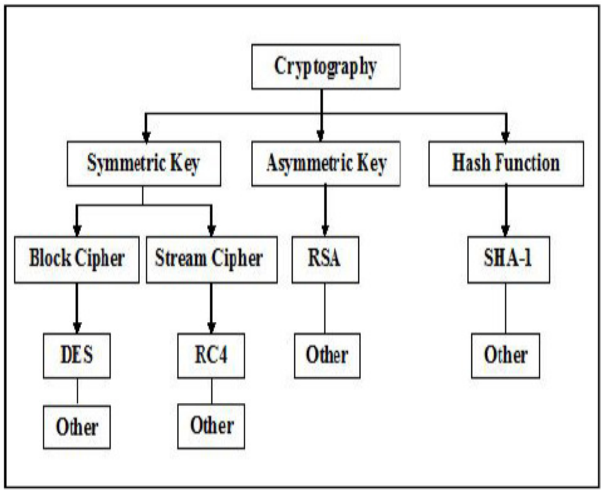


Figure 1 is showing the cryptography techniques view.

Hash Function: The hash function uses mathematical transformation to irreversibly encrypt information for example MD5, etc. It has no keys since the plaintext is not recoverable from the cipher text.

2. Related Work

Related Work and Issues: In [1], a technique which is the combination of stream ciphering and symmetric ciphering technique has presented. Lots of work has been done in the area of cryptography. Presented encryption algorithm work's by user defined dynamic key. Dynamic key is a concept in which key is decided at encryption of any message. It also provides the facility to increase the level of security through the encryption key. Encryption key Kei.C can be shifted 'n' number of times towards the right. In [2] presents hybrid encryption algorithm. First, write an initial encryption algorithm, second, add in the famous Vigenere encryption Algorithm and the Base64 encryption algorithm, then, improve the Vigenere encryption algorithm, finally, using the algorithm to encrypt the data processing in a specific sequence. In [3] extends the data set of the TSFS encryption algorithm to special characters as well, and corrects substitution and shifting processes by providing more than one modulo factor and four 16-arrays respectively in order to avoid the error that occurs in decryption steps. In [4] proposing Circular Design Pattern (CDP) which serves as a template for generating Dynamic Symmetric Encryption Frameworks (DSEF). The layout of a DSEF remains the same but the underlying algorithms may vary during run time. We illustrate how the proposed CDP can be used to create new DSEF from the set of existing algorithms.

They propose a modified version of conventional cryptosystem model to deploy the DSEF. In [5] three encryption algorithms namely DES, AES and Blowfish are analyzed by considering certain performance metrics such as execution time, memory required for implementation and throughput. In [6] introduced a symmetric key cryptographic method called Modern encryption Standard (MES) Version-II. Nath et. al already published Modern Encryption Standard version-I(MES-I). In the present method the authors have used Modified generalized Vernam cipher method with feedback with different block size from left to right and after that entire content is divided into two files and then combine them by taking 2nd half first and the 1st block. The generalized modified Vernam Cipher method again applied from left to right with different block sizes. In [7] Modified Vigenere Encryption Algorithm (MVEA) has been presented and also Hybrid encryption algorithm have been used which integrates MVEA, Base64 and AES algorithm. In [8] presented system highlights a method for performing encryption over the multimedia contents by using recurrence relation of degree 2 and evolutionary algorithm. The system uses recurrence relation for the preliminary encryption and the evolutionary algorithm is deployed to strength then encryption process in P2P network.

3. Issues

From the study of various presented papers we have observed that presented concept is based on classical encryption algorithm like mono alphabetic substitution due to this reason security of the algorithm is degrading. Another issue in this concept is time consuming process because the uses of random number generator. In some presented concept used mathematical operation during encryption and decryption which is provide sufficient security but it’s also time consuming process where each equation take some amount of time to execute which is causes of poor efficiency. In another paper we have observed hybrid encryption cocnept, in these various types of encryption algorithms are combining, on this basis, we can add several well-known encryption algorithms or design a new algorithm, there is no strict requirements about the numbers of the used encryption algorithm. But this is not a good approach because efficiency is the prime issues during encryption and decryption. Some of the presented concept not for large data set. It will required large memory space during encryption and decryption process. Practically it is not feasible such type of concept in practical use. Furthermore we have observed some encryption/ Decryption concept used large file size then total number of bits to be transmitted is more hence wastage of transmission bandwidth and also communication become slow.

4. Proposed Work

The objective of this paper is to design an architecture that will provide high security on transmitted data: In this we proposed a new encryption model which will provide confidentiality.

Key Features of Proposed Architecture are:

1) Will be Time efficient then Encryption/Decryption algorithm earlier proposed and other standard algorithms like AES and DES.
2) Highly secure (Will be proved by Avalanche Effect)
3) Suitable for any type of network.
4) Cryptanalysis will near to impossible.
5) Battery consumption will be less.
6) Can use for fast communication

In this work, we proposed an architecture shown in figure 3 and reverse architecture used in receiver end is shown in figure 4.

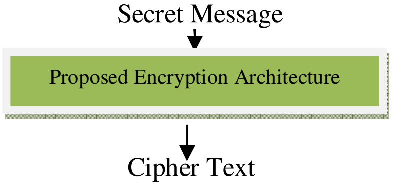


Figure 3: Proposed Architecture at sender end.

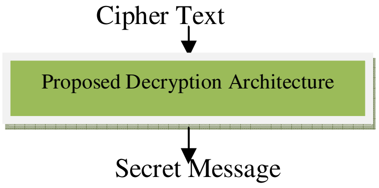


Figure 4: Proposed Architecture at Receiver end.

5. Expected Outcome

Performance parameter: In this section, the performance of the proposed two algorithms is analyzed in detail. 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 [10] 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 [10].

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 [10, 11]. The Proposed Encrption/ Decryption Algorithm will be highly secure. That this thesis will show with the help of avalanche effect. According to avalanche effect changing a single bit of key will change the 50% cipher text bits. The algorithm which is more close to avalanche effect is more secure. So we will compare the avalanche effect of base paper, standard algorithms and proposed algorithm. It will be highly time efficient and will be fit in any kind of network. 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.

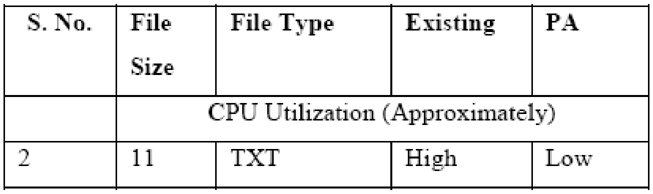
Table 1: Expected Avalanche Effect Comparison between Proposed and Existing Encryption Model

S. No.	File Size	File Type	Existing	PA
		Avalanche Effect (Approximately		
1	N KB	TXT	Low	High

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

S. No.	File Size	File Type	Existing	PA
	Execution Time (Approximately)			
2	11	TXT	High	Low

Table 3: Expected CPU Utilization Comparison between Proposed and Existing Encryption Model



S. No.	File Size	File Type	Existing	PA
	CPU Utilization (Approximately)			
2	11	TXT	High	Low

6. 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 will significantly better than other 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] Aasifhasan, Neeraj Sharma “A New Method Towards Encryption Schemes (N Ame-Based-Encryption Algorithm)” Published In IEEE International Conference On Reliability, Optimization And Information Technology -ICROIT 2014, India, PP 310-313 Feb 6-8 2014

[2] Xinqiang Li, Lili Yu, Lihuan Wei “The Application Of Hybrid Encryption Algorithm In Software Security” Published In IEEE International Conference PP 669-672, 2013

[3] Hanan A. Al-Souly, Abeer S. Al-Sheddi, Heba A. Kurdi “Enhanced TSFS Algorithm For Secure Database Encryption” Published In IEEE Science And Information Conference October 7-9, 2013 | London, UK PP 328-334

[4] Yash Bharadwaj, Shampa Chakraverty “A Design Pattern For Symmetric Encryption” Published In IEEE International Conference On Control, Computing, Communication And Materials (ICCCCM)2013 Pp 1-6

[5] A.Ramesh, Dr.A.Suruliandi “Performance Analysis Of Encryption Algorithms For Information Security” Published In IEEE International Conference On Circuits, Power And Computing Technologies [ICCPCT-2013] Pp 840-844

[6] Rahul Deep Sircar, Gunjan Sekhon, Asoke Nath “Modern Ecryption Standard (MES) : Version-II” IEEE International Conference on Communication Systems and Network Technologies 2013PP 506-511

[7] Gurpreet Singh, Supriya “Modified Vigenere Encryption Algorithm and its Hybrid Implementation with Base64 and AES” published in Second IEEE International Conference on Advanced Computing, Networking and Security 2013 PP 232-237

[8] Mr. Ramesh Shahabadkar, Dr. Ramachandra V. Pujeri “Optimization of Encryption Technique using Evolutionary Algorithm for Protecting Multimedia Contents in P2P System” published in 4th IEEE ICCCNT - July 4-6, 2013, Tiruchengode, India PP 256-261

[9] Songsheng Tang, Fuqiang Liu Nath “A one-time pad encryption algorithm based on oneway hash and conventional block cipher” published IEEE, June 2012.

[10] 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

[11] 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

[12] An Integrated Symmetric key Cryptography Algorithm using Generalised modified Vernam Cipher method and DJSA method: DJMNA symmetric key algorithm : Debanjan Das, Joyshree Nath, Megholova Mukherjee, Neha Choudhary, Asoke Nath: Communicated for publication in IEEE International conference WICT 2011 to be held at Mumbai Dec 11-14, 2011.

[13] Symmetric Key Cryptography using Random Key generator : Asoke Nath, Saima Ghosh, Meheboob Alam Mallik: “Proceedings of International conference on security and management(SAM’10” held at Las Vegas, USA Jul 12-15, 2010), P-Vol-2, 239-244(2010).

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

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

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

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

[18] Shivangi Goyal “A Survey on the Applications of Cryptography” published in International Journal of Science and Technology Volume 1 No. 3, March , 2012 PP 137-140 available at http://www.journalofsciences-technology.org/archive/2012/march_vol_1_no_3/9685431326187 843.pdf

[19] Saranya K, Mohanapriya R, Udhayan J “A Review on Symmetric Key Encryption Techniques in Cryptography” published in International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, March 2014 539 ISSN: 2278 – 7798 PP 539-544 available at http://ijsetr.org/wp-content/uploads/2014/03/IJSETR-VOL-3-ISSUE-3-539-544.pdf