Enhanced Avalanche Effect using SecuredCryptography

Priya Shah
Assistant Professor
Department of Computer Application
Patel Group of Institutions, GTU Mehsana
(Gujarat, India)

Vikash Katariya
Assistant Professor
Department of Computer Application
Patel Group of Institutions, GTU Mehsana
(Gujarat, India)

Abstract

This survey is presenting the study of data security using cryptography technique. This is describing cryptography technique in detail. After the survey of security using cryptography, thesis presenting some flaws of existing system as well as cryptography algorithms and how can remove theses with the help of propose work. This survey is dividing in four sections. Section-I, presenting introduction of cryptography, Section-II, presenting detailed description of cryptography algorithms and study of research papers, and presenting problem in existing algorithm, Section-III, presenting proposed idea, Section-IV, presenting expected out come of proposed idea and references.

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. An important concept in security is that virtually any security system can and will be compromised eventually; it simply takes time. For example, the Japanese never broke the code employed with great success by the Navajo code talkers in the Pacific theatre during World War II, but their code was only employed for a few years [1]. The success of that code was the use of words in a foreign and little-known language to represent military messages. Had the Japanese efforts to decrypt the Navajo code focused more on linguistics than cryptography, it would have likely been just another broken security scheme in a long line of others. 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. 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 [2].

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. 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.

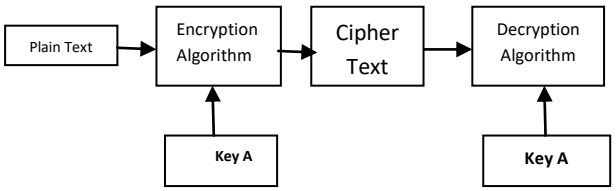

Figure1.1 Simple Encryption and Decryption of symmetric key

Public-key cryptography (also known as asymmetric algorithms) use 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.

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 [22]

Literature Survey

Here we are discussing previous research to calculate avalanche effect. In [25] I have analyzed that this research is based on comparisons of existing algorithm. Basically in [25] 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. In [26] I have observed that this research is the study of classical and modern encryption technique which is 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. Furthermore I have also observed that this research is the comparisons between classical and modern technique. In [26] they have suggested building the basics of classical encryption and modern techniques and comparison has been done between each of them. In [11] I have study on different-different type of encryption technique where 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. Here in [11] they have suggested an encryption technique that is a blend of both classical encryption as well as modern technique, according to him that suggested hybrid technique have superior in terms of security than average Classical ciphers. In [28] I have observed that in this they are comparing different-different encryption technique on the basis of execution time. According to researches they have suggested timing evaluation model based on random number generating mechanism 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. Here RSA is used which is not include in my research due to its public cryptography in nature. In [28] I have observed that this research is also based on comparisons between classical and modern encryption technique to calculate and analyze to avalanche effect. One serious drawback with classical method is that it is prone to brute force attack. Modern methods are less affected by brute force attack because of the usage of keys. Basically here they have designed an algorithm that combines the process of scrambling of bits and substitution boxes resulting in high avalanche effect.

Problem Formulation:

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 algorithm 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 I 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:

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.

Proposed Concept:

In proposed symmetric cryptography algorithm which will be 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 algorithm. At the time of encryption or decryption same key will use because symmetric in nature. Proposed Key length will 256 bits long so that security of proposed algorithm will be very high. Proposed algorithm is highly efficiently due to its simplicity. Here proposed algorithm will take less amount of time in execution as compare other algorithms 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.

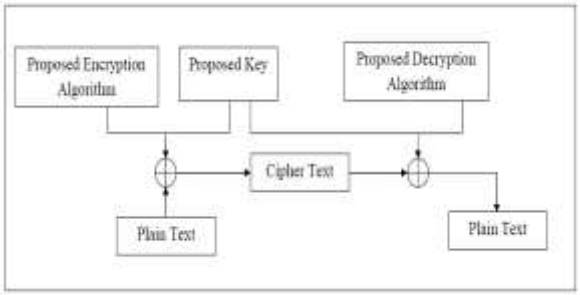

Figure 1: Block Diagram of Proposed Concept

Figure 2 is showing architecture of proposed system. In this figure proposed system will start with the help of start function then it will execute random function, in this function is divided in to two function, one is random number function and second is encryption number function: where random number function will help to produced key value when key function will execute and encryption number function and key function will help in proposed algorithm when it will execute. After executing all function, final result will produced in terms of cipher text. Finally stop function will execute to terminate system.

Expected Outcome

Proposed research will present performance evaluation of selected symmetric encryption algorithms. The selected algorithms will be AES, DES, DJSA symmetric key algorithm and NJJSAA symmetric key algorithm. Several points will include in the simulation results. First; there will no significant difference when the results will display either in hexadecimal base encoding or in base 64 encoding. Secondly; in the case of changing packet size, it will concluded that proposed algorithm will be produce better performance than other common encryption algorithms used. Third; in the case of changing data type such as image, audio or video instead of text, it will found proposed algorithm will be produce better performance than other common encryption algorithms used in terms of time consumption. Finally in the case of changing key size it will denote that higher key size leads to clear change in the battery and time consumption.

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] 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

[12] 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 .

[13] 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

[14] M. S. Hwang and C. Y. Liu, “Authenticated encryption schemes: current status and key issues," International Journal of Network Security, vol. 1, no. 2, pp. 61-73, 2005.

[15] M. H. Ibrahim, “A method for obtaining deniable public key encryption," International Journal of Network Security, vol. 8, no. 1, pp. 1-9, 2009.

[16] D. Wagner, L. Simpson, E. Dawson, J. Kelsey, W. Millan, and B. Schneier, Cryptanalysis of ORYX, Fifth Annual Workshop on Selected Areas in Cryptography, Springer Verlag, August 1998,

[17] Scott R. Fluhrer, Itsik Mantin and Adi Shamir, Weaknesses in the Key Scheduling Algorithm of RC4. Selected Areas in Cryptography 2001

[18] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone . "Handbook of Applied Cryptography". 1996

[19] Shiho Moriai, Yiqun Lisa Yin. "Cryptanalysis of Twofish (II)". 2000

[20] C.M. Adams. "Constructing Symmetric Ciphers Using the CAST Design Procedure", 1997.

[21] Garfunkel, Simson "PGP: Pretty Good Privacy, O'Reilly Media, 1997

[22] A. F. Webster and Stafford E. Tavares, "On the design of S-boxes", Advances in Cryptology vol. 219, pp. 523-534, 1985.

[23]Ralph Merkle, Martin Hellman: "On the Security of Multiple Encryption", July 1981

[24] N. Ferguson; B. Schneier "Practical Cryptography",2003

[U1]http://upload.wikimedia.org/wikipedia/commons/6/6a/CAST-128-large.png

[U2]http://commons.wikimedia.org/wiki/File:International_Data_Encryption_Algorithm_InfoBox_Diagram.png

[25] Himani Agrawal and Monisha Sharma "Implementation and analysis of various symmetric cryptosystems" Indian Journal of Science and Technology Vol. 3 No. 12 (Dec 2010) ISSN: 0974- 6846

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

[27] Yan Wang Ming Hu "Timing evaluation of the known cryptographic algorithms" IEEE International Conference on Computational Intelligence and Security 2009

[28] 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.