IJCSN - International Journal of Computer Science and Network, Volume 6, Issue 3, June 2017
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

A Literature Survey on Efficiency and Security of Symmetric Cryptography

[1] Mayank Kumar Rusia; [2] Mohit Rusia

[1] Lecturer (Senior Scale), Department of Technical Education, RGPV - Bhopal,
Sagar, Madhya Pradesh, India

[2] Senior Information Security Analyst,
National Capital Region - New Delhi, New Delhi, India

Abstract - Data encryption is widely used to assure security in open networks such as the internet. Each kind of data has its own features; therefore, different techniques should be used to protect confidential data from unauthorized access. Currently, most of the available encryption algorithms are used for text data. However, due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data. This Paper is a literature survey about block ciphers encryption algorithm(triple-DES, DES,AES, Blow-Fish).In this Paper I have concentrates on providing a starting point for designing strong, secure, and efficient cryptosystems. Various design issues and algorithms have been described in the paper. Paper explains a new timing evaluation model based on random number generating mechanism is proposed here to analyze the time-consuming of the known block cipher symmetric cryptographic algorithms. In this model for evaluation, there is one evaluating mode, which is different plaintexts in the same key (DPSK). As the basis of the evaluating model, the plaintext and the corresponding key, both generated by random numbers. The theoretical results shows that under the same key length and for the same size of the processed data, Triple-DES is about several hundred times slower than our proposed working model, AES, DES, Blow-Fish and IDEA. And there are other runtime characteristics which further highlight the difference between these three cryptographic algorithms and provide a reference value of for people's rational using.

Keywords - *Time-Consuming; Triple-DES; AES; Blow-Fish; IDEA; Random Number.*

1. Introduction

Many encryption algorithms are broadly available and used in information security. They can be categorized into Symmetric and Asymmetric key encryption, i.e. private and public key encryption respectively.

1.1 Symmetric Encryption

In symmetric encryption also known as the Private Key Method or encryption, a single key is used for encrypting and decrypting the data. This type of encryption is fast, but has a severe problem. The inherent weakness of this method is mostly the requirement of a key exchange between communications partners. In other words, in order to share a secret with someone, they have to know your key. This implies a very high level of trust between people sharing secrets, if an unscrupulous person has your key or if your key is intercepted by a spy they can decrypt all the messages you send using that key. However, Asymmetric encryption solves the trust problem inherent in symmetric encryption by using two different keys: a public key for encrypting the messages, and a private key for decrypting the messages. This makes it possible to communicate in secrecy. If your public key is known to others, then too your message is protected. The public key is only good for encryption; it's useless for decryption. Nobody can decrypt the messages unless they have private key. However, asymmetric encryption is very slow. It's not recommended for use on more than roughly 1 kilobyte of data [7].

1.2 Asymmetric Methods

In Asymmetric encryption also known as the Public Key Method, it uses two different keys: the private key and public key. The public key is distributed freely and the private key is known only to the owner of a key. The two keys have a (mathematical) relationship. However, for obvious reasons, calculation of a private key on the basis of the public key must be impossible or at least not

feasible. Both keys have different functions depending on the application at hand. In the case of data encryption, data is encoded using the public key. The private key is required in order to decrypt the message. The private key can also be used to generate digital signatures, which can later be verified using the public key [7].

2. Literature Survey

Cipher plays a significant role in camouflaging the true nature of data; this is achieved by inducing the factor of confusion through a series of shift and other mathematical functions. In the field of cryptography there exist several techniques for encryption/decryption these techniques can be generally classified in to two major groups Conventional and Public key Cryptography, Conventional encryption is marked by its usage of single key for both the process of encryption and decryption whereas in public key cryptography separate keys are used. Further on conventional techniques are further broken in to Classical and Modern techniques Public key cryptography is also an option when it comes to encryption but it requires excessive communication and processing resources. Our Proposed methods to some extent deals with some of the drawbacks of existing techniques that includes usage of key as it is without inducing any confusion in the primary key we changed that by generating many sub-parts of key from the primary key, similarly the key size of proposed concept may be varies from 4character or 32bits to onwards it can be 64-bits ,128-bits and so on (but here I am using 128 bits standard key size) whereas on the other hand we have example of DES, AES and triple-DES, Blow-Fish that have fixed key structure[9]. The variation in key introduces the aspect of uncertainty which is a positive aspect when it comes to encryption, time complexity is the phenomenon that describes the effect in the output cipher text if a large text data are changed in the file. This change that occurs at the output should be sufficient if we want to create a secure algorithm.

In this paper we are studying of two research paper name "A new timing evaluation model based on random number generating mechanism [9]" and "Performance Evaluation of Symmetric Encryption Algorithms [4]" is proposed here to analyze the time-consuming of the known cryptographic algorithms: triple-DES, AES and Blow-Fish and IDEA. In this model for evaluation, there is one evaluating modes: different plaintexts in the same key (DPSK). As the basis of the evaluating model, the plaintext and the corresponding key are both generated by random numbers" is discussed.

2.1 Evaluation Model Based on Random Number Generation Mechanism

Typically speaking, evaluating one algorithm usually need to consider time complexity and space complexity, which must be quite clear of algorithm. However, on the premise of unknown algorithm description, theoretical analysis becomes infeasible. The evaluation model based on the random number generating mechanism that this paper proposes can simulate the generation of plaintexts and keys that occur actually in existence, and the number of evaluating tests do not witnesses exponential growth according to the input scale. Because if we do not use the random number, then the tests should according to the size of data (from a few bytes to several megabytes) and the content of data (from 0 to its maximum number) to carry out. For example, a test of n-bit data, generating 2n data sequentially will be completed and suitable. Of course, according to the principles of the statistics, the larger the number of evaluated data generated is, the more evident the statistical effect of this evaluation model is.

A. The Generation and processing of Plaintext

In this evaluation model, the plaintext consists of a packet which is written by the random number. There are two parameters for generating a packet: the pointer for the array to store the packet data and the packet size, where the array is used for storing the generating message of a packet randomly and its every element is a random number with the range from 0 to 65535. Usually, random numbers are generated as part of the simulation, so they should closely approximate the ideal statistical properties of uniformity and independence. A packet is associated with the simulation of a file data, so, in this evaluated system, we define six kinds of the size of evaluated packets in order to measure the time-consuming of each algorithm that encrypt different size of plaintexts. These are 4KB, 8KB, 16KB, 32KB, 64KB and 128KB. For triple-DES, because it is a block cipher, so without the loss of generality, the processed plaintext is split into many blocks and a block size is 64 bits (i.e. the algorithm operates on the successive 64 bit blocks of the generated plaintext). The key length of triple-DES is 192-bit, given a plaintext P and three encryption keys K1, K2 and K3 and is defined as follows: C = EK3[DK2[EK1[P]]]. The generated plaintext do the following five functions: an initial permutation (IP); a complex function labeled fk, which involves both permutation and substitution operations and depends on a key input; a simple permutation function that switches (SW) the two halves of the data; the function fk again, and finally a permutation

function that is the inverse of the initial permutation (IP-1)..

For AES, its block-cipher length and key length are variable, and it was limited to 128-bit block-cipher and with three cipher key strengths of it: a 128-bit, 192-bit and 256-bit encryption key, but the corresponding number of iterative rounds is 10, 12 or 14.

B. The Generation of Keys

A key is a value that causes a cryptographic algorithm to run in a specific manner and produce a specific cipher text as an output. In this evaluation model, random numbers play an important role in the use of encryption. In fact, sources of true numbers are hard to come by, we use the function of "rand()" to simulate the random numbers generation and set the current time as the seed of random number here.

For other two algorithms, the function of "rand()" selects the specified median of random number to simulate the keys generation. So in this evaluation system, the key length of AES can be chosen at will.

In second research paper there are many examples of strong and weak keys of cryptography algorithms like RC2, DES, 3DES, RC6, Blowfish, and AES. RC2 uses one 64-bit key .DES uses one 64-bits key. Triple DES (3DES) uses three 64- bits keys while AES uses various (128,192,256) bits keys. Blowfish uses various (32-448); default 128bits while RC6 is used various (128,192,256) bits keys. But we are working only four block symmetric algorithms like DES, Triple-DES, AES, and Blow-Fish. Due to stream cipher I am not including RC2 and RC6 in my literature survey, here I am working only block cipher encryption algorithm.

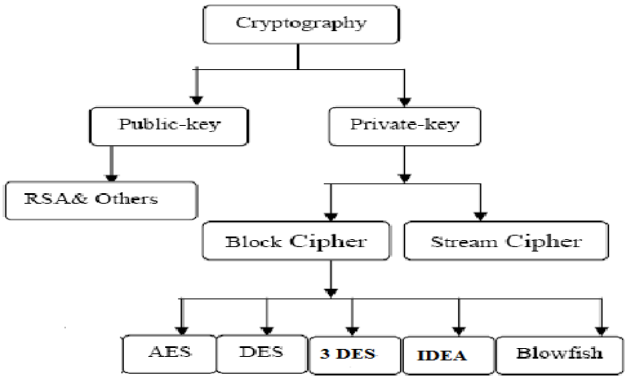

Fig. 1 Overview of the field of cryptography

Asymmetric key encryption or public key encryption is used to solve the problem of key distribution. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption. Because users tend to use two keys: public key, which is known to the public and private key which is known only to the user. There is no need for distributing them prior to transmission.

However, public key encryption is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices [1]. Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power. The most common classification of encryption techniques can be shown in Fig. 1 [4].

3. Proposed Evaluation Method

With the help of literature survey I have analyzed that I can improve efficiency and security of block cipher encryption. In this Paper I have study of two research paper which define above and found that everybody is trying to comparing time of known cryptography algorithm but nobody is trying for improvement of time efficiency of known cryptography algorithm, one more thing we have found in the survey that the key size of various algorithm is not fixed which is cause of poor efficiency.

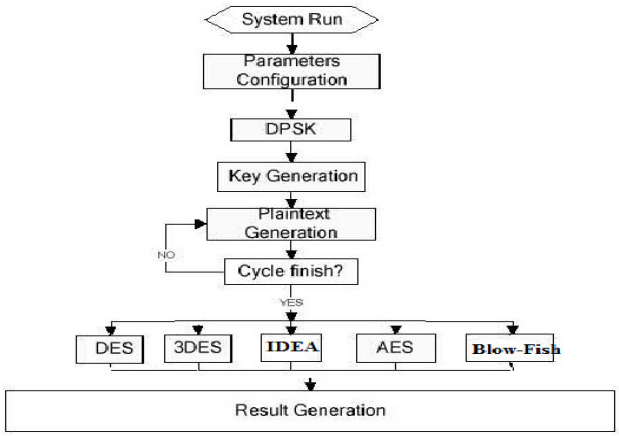

Fig. 2 Evaluation Method.

Here I am presenting only theory concept of working model. For timing evaluation of the known cryptographic algorithm, it is necessary to describe the detailed evaluation method, as illustrated in Fig.2. We defining one evaluating modes to find whether the key and the plaintext have impact on time consuming of cryptographic algorithms: DPSK (different

plaintexts in the same key).

This evaluation method will compare time-consuming of encrypting plaintext with different cryptographic algorithms. During processing, the content of the plaintext and the key will be both written by the random number. For DPSK evaluation mode, there are two parameters: the number of evaluated plaintexts and the size of evaluated plaintext, where the number of evaluated plaintexts is the number of plaintexts that are generated randomly and the size of evaluated plaintext can be chosen from six kinds that mention above. In this mode, we do n cycles (that is, the number of the evaluated plaintexts). In each cycle, three same plaintexts are respectively encrypted by triple-DES, IDEA, Blow-Fish and AES by copying them. In fact, the larger the number of keys generated is, the more evident the statistical effect of evaluation is. Finally, the outputs of the evaluation system will be the average time-consuming (AVT) and the maximum (MAX) and the minimum one (MIN), where AVT is n divide by the total time-consuming and MAX or MIN is the max or min value of the encrypting time-consuming, and the time consuming will be measured in seconds. Actually, for an encryption algorithm, the time-consuming of encryption not only depends on the algorithm's complexity, but also the key and the plaintext have certain impact.

4. Impacting Factors in Proposed Evaluation Method

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. The major factors responsible for efficiency of the encryption algorithm are as below:

- Encryption Time
- CPU Process Time
- CPU Clock Cycles and Battery Power.
- Memory,

The encryption time [4] is considered the time that an encryption algorithm takes to produce a cipher text from a plaintext. Encryption 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 encryption 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 [4-5].

The CPU clock cycles are a metric, reflecting the energy consumption of the CPU while operating on encryption operations. Each cycle of CPU will consume a small amount of energy [4-5].

The memory deals with the amount of memory space it takes for the whole process of encryption and decryption. The memory utilized for encryption and decryption should be taken care to reduce the overload of application.

5. Conclusion and Future Work

That is what most theoretical analysis cannot achieve, even though quite familiar with the algorithm. When the number of the evaluated plaintexts is bigger, their effect is more obvious. Finally, it is not difficult to find that, in contrast with training data, the larger the key length is, the bigger AVT is, especially for Triple-DES. This is also indicating that Blow-Fish is the most effective algorithm except proposed working model due to fixed key size and the value of MAX or MIN is not the same in evaluation mode. Besides, in contrast with training data, it is not difficult to find that the increasing key length can lead to the significant increment of AVT. In fact, different value of MAX and MIN further manifest that not only the resulting cipher text depends on the key; the content of key also effects the time consuming of algorithm. This means that an eavesdropper can have a complete copy of the algorithm in use, but without the specific key used to encrypt that message, it is useless. Generally speaking, the time-consuming of cryptographic algorithm usually depends on the size of plaintexts and keys, while the evaluation model based on random number generating mechanism that can verify that the time-consuming of cryptographic algorithm not only depends on the size of plaintexts and keys, but also their context will affect the time-consuming of algorithm to some degree. Due to stream cipher nature of RC2 and RC6 encryption algorithm I have not included in my literature survey because we have already know that stream cipher work on individual character and I am working on block cipher where encryption is done on block of character which also provide efficiency to algorithm. In Future I will implement my proposed working model and all the point will also cover which I have discussed above. I will display graphical as well as tabular comparisons of known cryptography algorithm with our proposed

working model and we will try to prove better efficiency of our proposed implementation.

References

[1] Onwutalobi Anthony-Claret, *"Using Encryption Technique",* Department of Computer Science,University of Wollongong Australia, Anthony.claret@ieee.org

[2] Prof. Mrinmoy Ghosh and Prof. Pranam Paul, *"An Application to ensure Security through Bit-level Encryption",* IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.11, November 2009.

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

[4] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, *"Performance Evaluation of Symmetric Encryption Algorithms",* IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008.

[5] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud, "*Evaluating The Performance of Symmetric Encryption Algorithms",* International Journal of Network Security, Vol.10, No.3, PP.213-219, May 2010.

[6] Diaa Salama Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud, *"Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types",* International Journal of Network Security, Vol.11, No.2, PP.78-87, Sept. 2010.

[7] William stallings, *"Cryptography and Network Security: Principles & Practices"*, second edition,

[8] Hardjono, "Security In Wireless LANS And MANS," Artech House Publishers, 2005.

[9] Yan Wang and Ming Hu, "Timing evaluation of the known cryptographic algorithms", published in 2009 International Conference on Computational Intelligence and Security978-0-7695-3931-7/09 IEEE DOI 10.1109/CIS .2009.81

Mayank Kumar Rusia, holds Master of Technology degree specialization in Artificial Intelligence in the Department of Information Technology awarded in the year 2011. He has done Bachelor of Engineering in Information Technology, awarded in the year 2005. The author is presently working as a Lecturer (Senior Scale), being the in-charge Head of Department for Computer Science and Engineering Department at S.R. Government Polytechnic College, Sagar, Madhya Pradesh, governed by Directorate of Technical Education, Government of Madhya Pradesh, India.

Mohit Rusia, being the Master of Engineer in Information Security in the branch of Information Technology awarded in the year 2014 and Bachelor of Engineer in Computer Science and Engineering stream, awarded in year 2012, works in a MNC as a Senior Information Security Analyst at National Capital Region, New Delhi, India.