A Survey on Generation and Evolution of Various Cryptographic Techniques

Shashi Gautam[1], Shubha Mishra[2], Dr. Manish Shrivastava[3]

[1]*PG Scholar in Information Technology, LNCT Bhopal, M.P, India*
[2]*Asst. Professor in Information Technology, LNCT Bhopal, M.P, India*
[3]*Professor and Head of Information Technology, LNCT Bhopal, M.P, India*

---***---

Abstract - *The evolution of wireless transmission in this modern era, daily touches the new heights of technology. There are so many eyes on the data transmitted over the network. This flow of data over the network requires some sort of security in terms of confidentiality, secrecy, authenticity etc. cryptography is one of the techniques used to provide security to the data flowing over the network by encryption and decryption. Till now, several cryptosystems have been designed and still they are introducing. So far, a large number of encryption/decryption techniques have been implemented and proposed. In this paper we have surveyed some symmetric key cryptographic techniques; we made study of analysis and basic comparison among them. This paper lists some basic features, advantages, disadvantages of various symmetric cryptographic algorithms.*

Key Words: Encryption, Decryption, Security, BCD, Binary Shifts, BLOWFISH, DES, 3DES

1. INTRODUCTION

This era's civilization is highly dependent upon the internet and its application for their part of life such as communication, transmission of data, files, videos etc. Hence these data are more vulnerable of duplicating of data and re-distribution of these data by unauthorized persons. Therefore these data must requires protection while flows over the networks. Cryptography is one of the techniques used to reach the some security essentials. In this era of communication, the encryption/decryption of data plays an important role for securing the data in mainly in wireless internet information systems. There are many cryptosystems have been introduced to provide protection and confidentiality from unauthorized use. Everyday new method for encryption/decryption techniques is discovered.

1.1 Purpose of cryptography:

- Authentication: An authentication is the cryptographic function of identifying the connecting entities by the internetwork. This is used when two or more entities try to start communication.
- Authorization: This function specifies the access rights to the resources.
- Integrity: This ensures the participants of communicator that their transmission will be intact and will not be modified on the air.
- Access Control: This function determines that who is permitted to access the restricted resources.
- Confidentiality: This principle specifies that only the participants of the communication must be able to access and receive the message.
- Non-Repudiation: Non-Repudiation principle does not allow the sender of the message to refute the claim of not sending the messages.

1.2 Types of Cryptography:

- Symmetric key cryptography: In symmetric cryptography a same key is used for both encryption and decryption, therefore it needs some mechanism to keep the key secret.
- Therefore this type of cryptography is also called secret key cryptography. DES, Triple DES, AES, RC5 and etc. are the exhibition of symmetric key cryptography.
- Asymmetric key cryptography: In the asymmetric key cryptography, there are two keys are used, one for encryption and other for decryption. Keeps encryption key public know to everyone but decryption key private. Therefore this type cryptography also known as public key cryptography. RSA, Elliptic Curve etc. are the exhibition of asymmetric key cryptography.

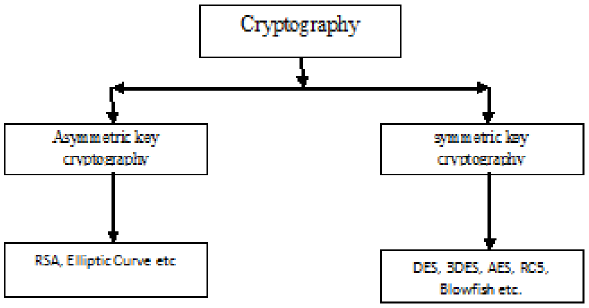
Cryptography
Asymmetric key cryptography
symmetric key cryptography
RSA, Elliptic Curve etc
DES, 3DES, AES, RC5, Blowfish etc.

Fig 1: Classification of Cryptography

This paper analyzes some of these recent existing encryption techniques and their security issues. The performance of all these techniques are studied and discussed in this paper.

2. BASIC TERMS IN CRYPTOGRAPHY

Plain text: Plaintext is those data written by user that are intelligible to everyone. This data needs security before sending to the intended recipients over internet. The input to the encryption function is called plain text.

Cipher text: In cryptography, ciphertext or cyphertext is the output of encryption function performed on plaintext using an algorithm, called a cipher. A cipher is a character -for-character or bit-for-bit transformation, without regard to the linguistic structure of the message. Ciphertext is a message after encryption or before decryption. In contrast a code replaces one word with another word or symbol. Ciphertext is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by human or computer without the proper cipher to decrypt it.

Encryption: The process of encryption is used to convert plaintext or clear text from intelligible form to an unintelligible form called cipher text. Encryption provides security and confidentiality to the communication. Encryption also used to provide authentication (i.e. the confirmation of identity of intended recipients).

Decryption: Decryption is the reverse process of encryption.

Cipher: In cryptosystem, a cipher (or cypher) is an algorithm for performing encryption or decryption---a series of well-defined steps that can be followed as a procedure. An alternative, less common term is encipherment. To encipher or encode is to convert information into cipher or code. In common parlance, 'cipher' is synonymous with 'code', as they are both a set of steps that encrypt a message.

Code: In cryptography, a code is a method used to encrypt a message that operates at the level of meaning; that is, words or phrase are converted into something else. A codebook is needed to encrypt, and decrypt the phrases or words.

Cryptanalysis: Cryptanalysis refers to the study of ciphers, ciphertext, or cryptosystems (that is, to secret code systems) with a view to finding a weaknesses in them that will permit retrieval of the plaintext from the ciphertext, without necessarily knowing the key or the algorithm. Breaking the cipher, ciphertext, or cryptosystem is called cryptanalysis.

Key: To perform encryption and decryption, one of the important parameter is a key. Key has its usual meaning to lock and unlock. But in some cryptosystem same key is used for encryption and decryption and in some other cryptosystem different keys are used for encryption and decryption.

3. PREVIOUS RELATED WORK

DES: DES is a symmetric key cryptographic algorithm described by Davis [1] which takes a fixed length input of plaintext, applied encryption process with the given series of key to output a cipher text of the same length. DES grouped plain text into block of 64 bits and makes use of 7 byte long key. From the plain text to cipher text, there are 16 rounds of encryption process. Additionally there is initial and final permutation of the plaintext which are inverse function of each other. In all rounds, there is an identical process of encryption.

Triple DES: IBM in early 1979 realized that the length of the key in DES is too short and introduced a new encryption technique called 3DES (triple DES) with the long key length. In the encryption, there are three stages of encryption which eats to keys.

- In the first stage 3DES encrypts the plaintext with k1 using the same process as the DES.
- The second stage decrypts the output of stage 1 with key k2. The process of decryption is identical to DES decryption.
- At the last step, the output of the stage 2 is re-encrypted with key k1 using the DES encryption.

$$C(t) = Ek1(Dk2(Ek3(t))) \quad [1]$$

Where C(t) is the chipher text, a final encryption output of the plaintext, Ek1 is the DES encryption using key k1, DK2 is the DES decryption using the key k2 and EK3 is the DES encryption using the key k1.
3DES makes the use of 3 times DES process, that's why it is called Triple DES. As the more number of key used, the possible combination also increased in power of 2. As the 3DES uses 2 keys, it requires 2112 possible combinations and with 3 key is requires 23*56 possible combinations. To try all these possible combination may take many decades with multiple processors; therefore this 3DES is the strongest encryption mechanism. But the disadvantage of this algorithm is its inefficiencies and memory, time consuming.

AES: The AES (Advanced Encryption Standard) [2] is a symmetric key algorithm. This algorithm makes use of the variable length key for encryption and decryption, which became the end of the DES. The number of encryption rounds depends on the length of the key, for 16-byte key it is 10. In DES half of the plaintext is encrypted in one round, whereas in AES all 16-bytes are encrypted in a single round. This is the biggest reason that the AES has small number of encryption rounds. AES encryption is fast and flexible. It can be implemented on various platforms especially in small devices.

Blowfish: In 1993 Bruce Schneier introduced the common public domain cryptographic algorithm named Blowfish [5].

It takes 64-bit block of plaintext as an input with variable length key. It has two steps:

- Sub-key generation: In this stage, the key is converted upto 56-bytes long to sub-keys to 521-bytes.
- Data encryption: 16 rounds of the encryption process make use of permutation dependent upon key and substitution dependent upon the combination of key-data.

The main drawback of the Blowfish is its rare key invariant i.e. it is used with the applications that do not require change of key for a long time, e.g. communication link encryption. It can't be used with the packet switching where key changes frequently switching).

4. SURVEY OF SYMMETRIC KEY CRYPTOGRAPHY

D. S. Abdul. Elminaam et.al [5] proposes a comparison of various cryptographic algorithms. The algorithms are evaluated on different video files; time is taken as an evaluation parameter. Different video and audio file extensions are processed with different speeds; also various sized audio/video files are taken in experiments. Time calculation for cryptography in various video as well as audio file formats is done with file size 1MB to 1100MB. Time calculation for encryption and decryption of files for various algorithms are compared. The experimental analysis shows that there was not much difference in time.

E. Thanbiraja [6] states that, symmetric key cryptography are widely used for huge data and link encryption. They made survey of some popular symmetric key cryptographic algorithms and study the comparison among them. In this paper, they chased out the different scenarios of the use of the cryptographic algorithms. They summed that the all the studied cryptographic algorithms are useful for real-time encryption. Each algorithm has their own significance and suitable for their different variable applications.

Challa Narasimham, Jayaram Pradhan [8] analyzes the performance characteristics of the various cryptographic system on the text files. The file used in experiments as input is variable in length. They showed the significant difference in time requirements for various cryptographic algorithms. Their experiments approximate that the DES decryption performance is very high as compared with others alternatives. To select appropriate cryptographic method they organize experiment with the computing running times for all methods.

Marwa Abd El-Wahed, Saleh Mesbah, and Amin Shoukry [13] proposes Image encryption algorithm for efficiency and security. They studied four encryption algorithms for images under the metrics encryption quality, memory consumption and the execution time for encryption. Additionally, analysis of security from the perspective of the cryptography, differential and statistical attacks Comparison of analytic results performed differently for each portions of image. Main criteria to evaluate cryptosystems are, ease of implementation, security levels, and efficiency. The optimal security level identification requires the comparison of the multimedia data cost to be secured and the cost of security itself.

Abdel-Karim Al Tamimi [9] evaluates the power consumption for different data types in secret key cryptographic algorithms. The simulation results that Blowfish outperformed than other alternatives as the Blowfish do not have any known security holes so far. AES performed poorly among other cryptographic algorithms since it requires more computing and processing powers. The CBC mode uses extra processing time, but if there is a security concern, this extra time can be avoided. The experimental result exhibits that Blowfish outperformed than the other algorithms. Also it showed that AES performed better than DES and 3DES. The performance of these algorithms reveals that triple DES has almost 1/3 throughput of DES i.e. it requires 3 times than DES to process the same amount of data since it has to perform 3 times the DES.

Prasithsangaree.P and Krishnamurthy.P [10] analyzes RC4 and AES algorithms with the parameter energy consumption in wireless LANs. The list of performance comparison parameters are throughput, energy cost, variable key size and CPU loads. For small packets, experiments exhibits that AES is fast and energy efficient and RC4 is fast and energy efficient for large packets. Hybrid method (combination of AES and RC4) provides encryption for any length packet that saves energy.

Nidhi Singhal1, J.P.S.Raina [11] analyzes the performance for RC4 and AES cryptographic algorithms. To analyze performance of these algorithms, the parameters are memory and time complexities, CPU utilization, throughput, and length of the key. To encrypt a packet of different sizes, RC4 consumes less time compared with AES. AES in Cipher Feedback and Cipher Block Chaining modes takes almost equal time but Electronic Code Block takes less time than both of these. Comparing on the basis of the length of the key uses three different length key are 16-byte, 24-byte and 32-byte, RC4 requires constant time for encryption which is less than the AES. Since RC4 has to work less therefore it consumes less power than AES.

Simar Preet Singh and Raman Maini [7] proposed a comparison among data encryption algorithms. They lists DES, 3DES, AES, Blowfish etc. algorithms and compare their performances. They showed that, among these algorithms Blowfish performs well and AES's performance was poor since it requires extra processing powers. In their first experiment using ECB mode, the Blowfish outperformed over all other algorithms within a time limit. This experiment also showed that the AES requires more resources with bigger data blocks. For 3DES, it is noticed that it requires more time and resources than DES since it has to perform 3 times of DES algorithms. With the longest key, Blowfish outperformed other cryptographic algorithms. DES and 3DES have worm holes in their security mechanism, but Blowfish and AES do not have any worm holes so far with the CBC mode which require more processing time slice than ECB. In their second experiment they showed that the extra quantum of time added is not important.

Dr. S.A.M Rizvi1 ,Dr. Syed Zeeshan Hussain2 and Neeta Wadhwa [14] compares the two symmetric encryption algorithms with different platforms Windows XP, Windows Vista, and Windows 7. On Windows XP, all algorithms executions are faster. For text AES runs faster than CAST. For image data, Blowfish performs image encryption faster on all the three platforms but CAST encryption process run faster on Windows XP. CAST and AES perform similarly on Windows 7 and Windows Vista. On Windows XP, for encrypting audio files, performance of CAST is better than AES and Blowfish. But on Windows 7 and Windows Vista, the difference in performance is almost acceptable for CAST and AES.

Turki Al-Somani ,Khalid Al-Zamil [15] evaluates the performance of the three cryptographic algorithms DES, Triple DES, and Blowfish on the two platforms Sun OS and Linux OS. They implemented all these algorithms using JAVA and JCA. The objective of this implementation is to evaluate their performance in terms of CPU time. They used a file of size 10MB to evaluate the performance of generating the secret key for encryption and decryption. Experimental analysis exhibits the orders of faster algorithms are:

BLOSFISH > DES > 3DES

i.e. Blowfish is faster than DES, which is faster than 3DES. Triple DES provides better security and complexity but its performance is slow because of complexity and security overhead.

Gurjeevan Singh, Ashwani Kumar Singla,K.S. Sandha [16] analyzes throughput of various encryption algorithms. The analysis performed, with the resources was Core-2 Dou Processor, CPU with 2.20GHz, 4GB RAM and Win7 (32-bits). In the experiments the file size included from 20KB to 99MB. They choose throughput to compare performance of all the implemented cryptographic algorithms. They perform experiments for encryption and decryption one by one. The competitor symmetric algorithms are AES, DES, BLOWFISH and 3DES. They concluded that the Blowfish outperformed well than other alternatives followed by the AES. 3DES has the least efficiency of all the algorithms studied.

5. CONCLUSION

In this wireless era of communication, the information security has become a very important issue. Everyone wants to high secure data transmission. So many researchers have trying to introduce a strong and full proof cryptographic algorithm that are efficient and perform well in all the scenarios. This paper tries to make a cryptography scenario from early to now. The all cryptographic techniques studied and analyzed have their own significance and are applicable in their own area of application. As the cryptanalyst continuously trying to find loop holes in all these security algorithms, researchers also continuously trying to evolve more secure algorithms.

REFERENCES

[1] Davis, R., “The Data Encryption Standard in Perspective,” Proceeding of Communication Society magazine, IEEE, Volume 16 No 6, pp. 5-6, Nov. 1978.

[2] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.

[3] Pratap Chnadra Mandal “Superiority of Blowfish Algorithm,” International Journal Of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, September 2012.

[4] R.L.Rivest, A.Shamir, and L.Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communication of the ACM, Volume 21 No. 2, Feb. 1978.

[5] 5. D. S. Abdul. Elminaam et.al,” Performance Evaluation of Symmetric Encryption Algorithms”, Communications of the IBIMA Volume 8, 2009 ISSN: 1943-7765,pp.58-64.

[6] E. Thanbiraja, G. Ramesh, Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques" IJARCSSE 2012

[7] Simar Preet Singh, and Raman Maini “COMPARISON OF DATA ENCRYPTION ALGORITHMS” International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127

[8] Challa Narasimham, Jayaram Pradhan,” EVALUATION OF PERFORMANCE CHARACTERISTICS OF CRYPTOSYSTEM USING TEXT FILES” Journal of Theoretical and Applied Information Technology,pp55-59 2008.

[9] Abdel-Karim Al Tamimi,” Performance Analysis of Data Encryption Algorithms “

[10] Prasithsangaree.P and Krishnamurthy.P(2003), “Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs,” in the Proceedings of the IEEE GLOBECOM 2003, pp. 1445-1449.

[11] Nidhi Singhal1, J.P.S.Raina2, Comparative Analysis of AES and RC4 Algorithms for Better Utilization”, International Journal of Computer Trends and Technology- July to Aug Issue 2011 pp177-181.

[12] 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.

[13] Marwa Abd El-Wahed, Saleh Mesbah, and Amin Shoukry,” Efficiency and Security of Some Image Encryption Algorithms”, Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008, July 2 - 4, 2008, London, U.K.

[14] Dr. S.A.M Rizvi1 ,Dr. Syed Zeeshan Hussain2 and Neeta Wadhwa” A Comparative Study Of Two Symmetric Encryption Algorithms Across Different Platforms”,

[15] Turki Al-Somani ,Khalid Al-Zamil “Performance Evaluation of Three Encryption/Decryption Algorithms on the SunOS and Linux Operating Systems”, Theses

[16] Gurjeevan Singh, Ashwani Kumar Singla,K.S. Sandha, ”ThroughPut Analysis Of Various Encryption Algorithms”, IJCST Vol. 2, Issue 3, September 2011.,” unpublished.