Cryptography: Comparative Studies of Different Symmetric Algorithms

Vishal R. Pancholi[1], Dr. Bhadresh P. Patel[2]
[1] Research Scholar, Pacific University, Udaipur, Rajasthan, INDIA
vishal.pancholi@yahoo.com
[2] Principal (I/C), Matrushri L.J Gandhi (Bakorvala) BCA College, Modasa, Gujarat, INDIA
prof.bhadresh@gmail.com

Abstract — **Security is the prerequisite and the most challenging part in any technology domain or internet or any network application. The ratio of transmitting data over the internet is escalating day by day so there is a need to protect the transmitted data. For that cryptography is providing the best way to secure the data. It first encrypts the data at the sender side and at receiver side the data is decrypted. Cryptographic techniques are mainly allocated into two categories to secure the data, symmetric cryptography and asymmetric cryptography. This paper presents a relative study of various symmetric algorithms like AES, DES and Triple DES.**

Keywords - **Cryptography, Security, AES, DES, Triple DES**

I. Introduction

Security of data over the network is accomplished by encryption/decryption process. Cryptography is the art of writing in undisclosed code so that only those for whom it is offered can read and process it. Data cryptography mainly is the scrambling of the content of the data, such as text, image, audio, video and so forth to make the data unreadable, hidden or meaningless all the way through transmission or storage is termed Encryption [7]. The main determination of cryptography is to take care of data secured from attackers. The contrary procedure of getting back the original data from encrypted data is Decryption, which restores the original data.

The basic steps involved in encryption model are [1]:

- A sender wants to send a “Hello” message to a recipient.
- The original message, also called plaintext, is converted to random bits known as cipher text by using a key and an algorithm. The algorithm being used can produce a different output each time it is used, based on the value of the key.
- The cipher text is transmitted over the transmission medium.
- At the recipient end, the cipher text is converted back to the original text using the same algorithm and key that was used to encrypt the message. Figure 1 below shows the conventional cryptographic process.

Security goals of data cover three points namely: Availability, Confidentiality, and Integrity. Cryptographic algorithms are mainly divided into two categories:

(1) Symmetric-key Algorithms
(2) Asymmetric-key Algorithms

In symmetric key cryptography, same key is shared, i.e. the one key is used in both encryption and decryption, hence also known as single key or secret key encryption. Symmetric key cryptography algorithms are simple requiring lesser execution time. As a consequence, these are commonly used for long messages. There are two types of symmetric key encryption modes one as block ciphers and other as stream ciphers. Block ciphers operate on groups of bits called blocks and each block is processed multiple number of times. The key applied in each round is in a unique manner. A stream cipher operates on one bit at a time i.e. The data is divided as small as single bits and then the encryption is done. It contains algorithms like Data Encryption Standard (DES), Advanced Encryption Standard (AES), Ron's Code (RCn), and Triple DES.

In asymmetric key cryptography different keys are used for encryption and decryption, hence also known as public key encryption. The two keys are a private key and a public key. The public key is announced to the public; whereas the private key is kept by the receiver. The sender uses the public key of the receiver for encryption and the receiver uses his private key for decryption. Here the number of keys required is small but it is not efficient for long messages. It comprises various algorithms like Rivest, Shamir, & Adleman (RSA), DSA,Elliptic Curve(EC), Diffi-Hillman(DH),El Gamal.

II. LITERATURE REVIEW

In [2], the paper proposed by AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram, the summary of the classification of the types of the encryption techniques and the parameters like encryption ratio, speed, key length etc. are verified for the algorithms and the security issues are briefly placed.

In [3], the paper proposed by Ranjeet Masram, Vivek Shahare, Jibi Abraham, Rajni Moona, different symmetric key algorithm have been analyzed for various file features like different data type, data density, data size and key size, and analyzed the variation of encryption time for different selected cipher algorithms like AES, DES, Triple DES, RC2, Blowfish, Skipjack, RC4.

In [7], it is briefly described the theory of cryptography and its algorithms. There are different types of algorithms which are used to provide the security of the information.

In [9], a survey on the existing works on the Encryption techniques has been done. To sum up, all the techniques are useful for real-time

Encryption. Each technique is unique in its own way, which might be suitable for different applications and has its own pro's and con's. It can be found that AES algorithm is most efficient in terms of speed, time, and throughput and avalanche effect.

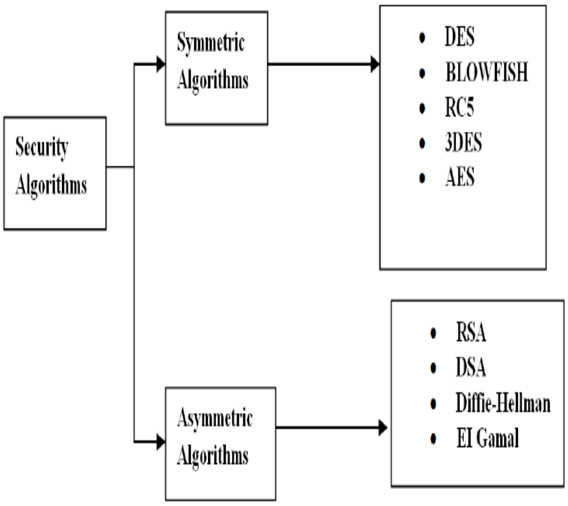

Figure 1: Security Algorithms

In [14], A comparative study of encryption techniques in terms of symmetric key and asymmetric key algorithms analyzed that symmetric key algorithms is viewed to be good in terms of speed and power consumption while asymmetric key algorithms in terms of tunability. In the symmetric key encryption AES algorithm is found to be better in terms of cost, security and implementation. In asymmetric key encryption RSA algorithm is better in terms of speed and security.

III. Overview Of Symmetric Algorithm

The overview of most common symmetric algorithms like AES, DES and Triple DES is as follows:

1. AES (Advanced Encryption Standard)

AES is a symmetric-key block cipher, developed by two Belgian cryptographers Joan Daemen and Vincent Rijmen, published by National Institute of Standards and Technology (NIST). It encrypts and decrypts a data block of 128 bits. It uses 10, 12 or 14 rounds. The key size which can be 128,192 or 256 bits depends on the number of rounds. If both block length and key length are 128 bits, AES will perform 9 processing rounds. If the block and key are 192 bits, AES will perform 11 processing rounds. If the block and key are 256 bits, then it performs 13 processing rounds. Final step is different in all the aspects that are 10th, 12th or 14th. Each processing rounds involves four steps:

1. **Substitute bytes**: Uses an S-box to perform a byte by byte substitution of the block.
2. **Shift rows**: A simple permutation.
3. **Mix column**: A substitution method where data in each column from the shift row is multiplied by the algorithm's matrix.
4. **Add round key**: The key for the processing round is XORed with the data.

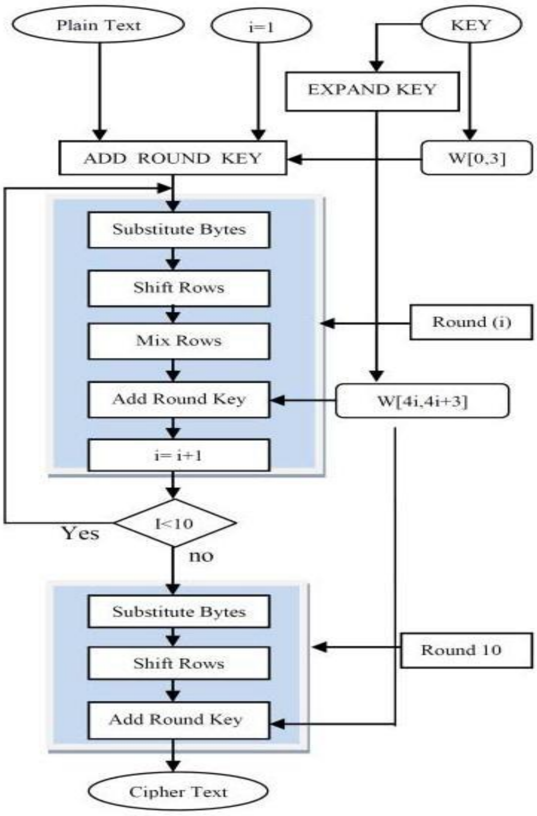

Figure 2: AES (Advanced Encryption Standard) process

The first three functions of an AES round are designed to prevent cryptanalysis via the Methods of "confusion" and "diffusion." The fourth function actually encrypts the data. AES formats plaintext into 16 byte (128-bit) blocks, and treats each block as a 4x4 State array. It then performs four operations in each round. The arrays contains row and column information used in the operations, especially MixColumns () and Shiftrows (). AES can be attacked using the Timing analysis Attack. This occurs when Malice (the malicious Alice) runs the Sub-Bytes method on different data and observes the time it takes for each execution.

A. *DES (Data Encryption Standard)*

Up until recently, the main standard for encrypting data was a symmetric algorithm known as the Data Encryption Standard (DES). DES is a 64 bit block cipher which means that it encrypts data 64 bits at a time. This is contrasted to a stream cipher in which only one bit at a time (or sometimes small groups of bits such as a byte) is encrypted.
Initially, 56 bits of the key are selected from the initial 64 by permuted choice; the remaining eight bits are either discarded or used as parity check bits. The 56 bits are then divided into two 28-bit halves; each half is thereafter treated separately. In successive rounds, both halves are rotated left by one or two bits and then 48 sub key bits are selected

by permuted choice, 24 bits from the left half and 24 from the right. The key schedule for decryption is similar; the sub keys are in reverse order compared to encryption [4].

Since the time DES was adopted (1977), it has been widely speculated that some kind of backdoor was designed into the cryptic S-boxes, allowing those "in the know" to effectively crack DES. Time has proven such speculation idle. Apart from any backdoors in the hash function, the rapid advances in the speed of electronic circuitry over the last 20 years, combined with the natural parallelism of Feistel ciphers and DES's relatively small key size, have rendered the algorithm obsolete. In 1998, the Electronic Frontier Foundation built a DES Cracker (full specifications available online) for less than $250,000 that can decode DES messages in less than a week.

A. Triple DES (Triple Data Encryption Standard)

It applies the Data Encryption Standard cipher algorithm three times to each data block. In Triple DES the data is encrypted with the first key, decrypted with the second key, and finally encrypted with the third key. It takes three 64-bit keys, for an overall key length of 192 bits. The original DES cipher’s key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible.

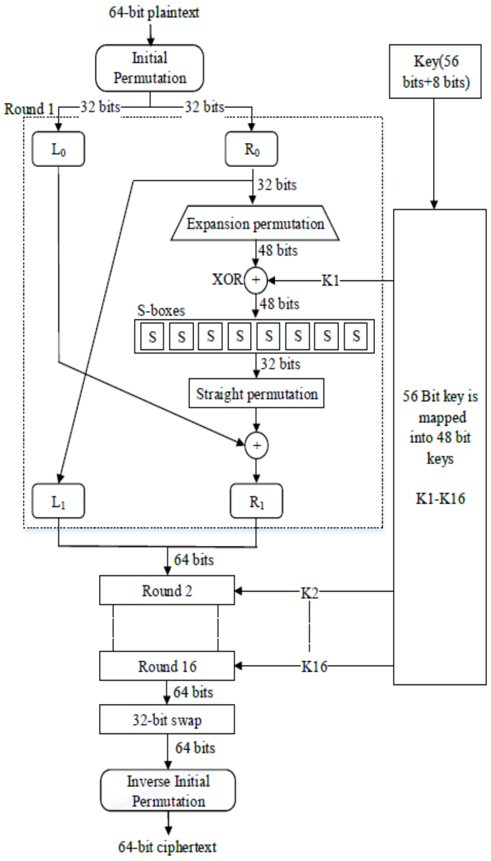

Figure 3: General Depiction of DES

Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks. Triple DES runs three times slower than DES, but it much more secure. The procedure for decrypting is the same as the procedure for encryption, except it is executed in reverse.

IV. Comparison of AES, DES, Triple DES Algorithms

Factors	AES	DES	Triple DES
Created by	Joan Daemen and Vincent Rijmen in 1998	IBM in 1975	IBM in 1978
Algorithm Structure	Substitution, permutation network	Feistel network	Feistel network
Cipher type	Block	Block	Block
Key size(bits)	128,192,256	56	K1,k2,k3 168 bits
Block size	128	64	64
Rounds	10,12,14	16	48
Effectiveness	Considered secure	Not enough secure	Adequate secure
Speed	Fast	Slow	Very slow
Encryption Time (Kbps)	0.3	0.3	0.8
Decryption Time (Kbps)	0.3	0.2	0.7
Memory Usage	Medium	High	Very High

Conclusion

In this paper, the concept of cryptography is explained. Cryptographic techniques are mainly of two types: Symmetric and Asymmetric. Symmetric algorithms use a same key for the encryption and decryption while asymmetric algorithms use different keys for encryption and decryption. It is concluded that AES is superior to the other algorithms DES and Triple DES for the various parameters like effectiveness, speed, encryption time, decryption time, memory usage. In terms of security and speed AES is better than DES and Triple DES. Future work may include different parameters to improve the encryption ratio.

References

[1] Jawahar Thakur, Nagesh Kumar, “DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 2, December 2011.

[2] AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram, “COMPARATIVE ANALYSIS OF PERFORMANCE EFFICIENCY AND SECURITY MEASURES OF SOME ENCRYPTION”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622,Vol. 2, Issue 3, May-Jun 2012.

[3] Ranjeet Masram, Vivek Shahare, Jibi Abraham, Rajni Moona, “ANALYSIS AND COMPARISON OF SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHMS

[4] BASED ON VARIOUS FILE FEATURES", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4, July 2014.

[5] E. Surya C.Diviya, "A Survey on Symmetric Key Encryption Algorithms", E Surya et al, International Journal of Computer Science & Communication Networks,Vol 2(4), 475-477.

[6] Gurpreet Kaur, Manish Mahajan, "Evaluation and Comparison of Symmetric key algorithms", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 2, Issue 10, October 2013.

[7] Gurvinder Singh Sandhu, Vinay Verma, "Comparing Popular Symmetric Key Algorithms Using Various Performance Metrics" , International Journal of Advance Research in Computer Science and Management Studies, Volume 1, Issue 7, December 2013.

[8] Disha Shah, "Digital Security Using Cryptographic Message Digest algorithm", International Journal of Advance Research in Computer Science and Management Studies, Volume 3, Issue 10, October 2015.

[9] 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.

[10] Gurpreet Singh, Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013.

[11] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors", JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010, ISSN 2151-9617.

[12] Pratap Chandra Mandal , "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES ,AES and Blowfish ", Journal of Global Research in Computer Science, Volume 3, No. 8, August 2012.

[13] Narender Tyagi Anita Ganpati, "Comparative Analysis of Symmetric Key Encryption Algorithms ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 8, August 2014 ISSN: 2277 128X.

[14] Nivedita Bisht, Sapna Singh," A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 3, March 2015.

[15] Mohit Marwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh, "COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS", Singh et al., International Journal of Advanced Engineering Technology E-ISSN 0976-3945.