International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

A Study of Encryption Algorithms (DES, 3DES and AES) for Information Security

R. Sivakumar[1], B. Balakumar[2], V. Arivu Pandeeswaran[3]

[1]*M.Tech II yr, CITE, Manonmaniam Sundaranar University, Triunelveli, Tamilnadu, India.*
[2]*Assistant Professor, CITE, Manonmaniam Sundaranar University, Triunelveli, Tamilnadu,India.*
[3]*M.Tech II yr, CITE, Manonmaniam Sundaranar University, Triunelveli, Tamilnadu, India.*

Abstract: *Encryption is the process of converting information into a code so that only the intended recipient can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. It can still be used to protect a user's identity and privacy. As more and more information is stored on computers or communicated via computers, the need of the hour is to ensure that this information is secure and to prevent from snooping / tampering becomes more relevant. Even if data does end up getting stolen, it will be unreadable and nearly useless if it's encrypted. With the fast progression of digital data exchange in electronic way, Encryption is essential for ensured and trusted delivery of sensitive information sent over the internet. Contemporary human being intelligence, lead to cryptography has become more complex in order to make information more secure. Mean while many encryption algorithms are being developed in the world of Cyber security society. In this paper, a survey of various Encryption Algorithms is presented.*

Keywords :- *Information Security, Encryption, DES, 3DES, AES*

1. INTRODUCTION

In this era of universal electronic connectivity, the possibility of data damage or stolen is very high that's why it is need of the time is to secure data from the those group .The tremendous growth in computer systems and inter connection with networks have increased depends on company or individual based on information stored and communicated using this system. There is need to protect the data from disclosure and to protect systems from network based attacks.

Cryptography is a technique which is intended to transform the data and can be used to provide various security related concepts such as confidentiality, data integrity, authentication, authorization and non-repudiation. Zaran et al[15]. Secure the information and other services is very important thing by using the security mechanism we have to protected from unintended or unauthorized access, change or destruction. Cryptography is the art of secret writing to hide information secret or keeping message secure. A secure network must have integrity, so that all of the information stored in always correct and protected without any redundant data . There are many techniques and tools which are used to reduce network threats . Basically encryption/decryption are the fundamental function of cryptography, which is used to hide the information from the unauthorized users so that chances of threats also reduced. The aim of many cryptosystems is to make their data computationally infeasible to crack by intruders. It can provide integrity as it can be used to detect any changes which may have happened to the data, and it can provide accountability as it can be used to verify the origin of the data.

In encryption simple message (the plaintext) converted into unreadable form called cipher text (scrambled message after encryption). While decryption the cipher text is converted into plain text(original form) Many encryption algorithms are widely available and used in information security[15]

Cryptosystems are used to encrypt the data using a cipher, and can be classified into following broad categories;

- Symmetric encryption
- Asymmetric encryption
- Physical encryption
- Hashing encryption
- Quantum encryption

These methods are specifically designed to meet some of the goals of cryptography such as confidentiality, integrity and accountability

Here we have some of the ciphers which is used by cryptosystems to encode data with different kind of calculation;

- Substitution cipher
- Transposition cipher
- Stegano graphic cipher
- Block cipher
- Stream cipher

The selection of key in Cryptography algorithm is core issue because the security of encryption algorithm depends directly on it.

2. RELATED WORKS

To give more prospective about the performance of the encryption algorithms, this subsection describes and examines previous work done in field of data encryption. The metrics taken into consideration are processing speed, security, block size, rounds, key length and cipher type. This subsection also discusses the results obtained for some of the algorithms.

Arora et al. [6] studied about the performance of different security algorithms on a cloud network and also on a single processor for different input sizes. This paper aims to provide the comparative analysis of the different algorithm such as AES, DES and 3DES which are used by businesses to encrypt large volumes of data.

Cyber security and protection is one of the most important issue. As relation between user and internet is increasing rapidly the chances of theft also increase, so there are more requirements to secure the data transmitted over different network using different services. To provide the security to the network and data different encryption methods are used. In this paper, a survey on the existing algorithms on the encryption techniques are useful for real time encryption .Each technique is unique in its own way , which might be suitable for different applications and services and has its own significance. According to research done and literature survey it can be found that the AES algorithm is most efficient in terms of speed, time, throughput, and etc. These parameters are the vital for any Encryption Algorithm to measure the standard. Experimental results show that DES algorithm consumes least encryption time and AES algorithm has least memory usage while encryption time difference is very minor in case of AES and DES algorithm. RSA consume longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm. Zaran et al. [14] studied about the performance of Symmetric Encryption and Asymmetric Algorithms. This paper provides evaluation of Symmetric key algorithms : AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6, TEA, MARS,IDEA,SERPENT,TWO FISH, BLOW FISH and Asymmetric key algorithms : DH, SSL, RSA, SSH. A comparison has been conducted at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. Experimental simulation shows following results. The analysis is based on the architecture of algorithm, the security aspects and the limitation they have. The comparison clearly states that though asymmetric algorithm s are superior in security, they take more time for processing and requires more memory. Faiqa et al. [15] compare the some of the symmetric algorithm such as DES, AES, RC5,Two fish and some asymmetric algorithm such as ECC and RSA, they observed AES works with less complexity and has high security level while compare to DES it taken time very less. Prerna et al. [12] compares the performance evaluation of various cryptographic algorithms. On the basis of parameter such as scalability, inherent vulnerability, power consumption and deposit keys. Study shows that AES is better than DES and 3DES. Rajadeep et al. [13] in this paper compared two most widely used symmetric encryption techniques i.e. data encryption standard (DES) and advanced encryption standard (AES) on the basis of key length, number of rounds, block size(bits), attack found, level of security and encryption speed, memory required for implementation and simulation time required for encryption.

AES provides a high security level since uses variable length key bits. It uses operations similar to the RSA modulo arithmetic operations but it can be mathematically inverted, DES is highly susceptible to linear crypto analysis attacks. It is exposed to brute force attack because of weak keys,3DES is vulnerable certain variation of meeting on the middle attacks. It is also exposed to differential and related key attacks. Zaran et al.[14] AES is ideal for encrypting messages sent between objects via chat-channels, and is useful for objects that involve monetary transactions. Studied the various techniques and algorithms used for the data security in MN (Multinode Network). It has been observed that the strength of system depends upon the key management, type of cryptography (public or private keys), number of keys, number of bits used in a key. Longer key length and data length consumes more power and results in more heat dissipation. Larger the number of bits used in a key, the more secure the transmission. All the keys are based upon the mathematical properties and their strength decreases with respect to time. The keys having more number of bits requires more computation time which simply indicates that the system takes more time to encrypt the data. To secure the communication key size is the most important parameter in symmetric and asymmetric cryptography. The key size of symmetric cryptography is less than the asymmetric cryptography which make symmetric cryptography less secure for more sensitive data. Faiqa et al [15].

3. DETAILED DESCRIPTION OF COMMON ENCRYPTION ALGORITHMS

The generation, modification and transportation of keys have been done by the encryption algorithm. It is also named as cryptographic algorithm. There are many cryptographic algorithms available in the market to encrypt the data. The strength of encryption algorithm heavily relies on the computer system used for the generation of keys. Some important encryption algorithms are discussed here:

3.1 Data Encryption Standard (DES)

The DES was once a predominant symmetric-key algorithm for the encryption of electronic data. But now it is an outdated symmetric key data encryption method. DES uses 56 bits key for encryption and decryption. It completes the 16 rounds of encryption on each 64 bits block of data. Data Encryption Standard is a symmetric encryption system that uses 64-bit blocks, 8 bits of which are used for parity checks.

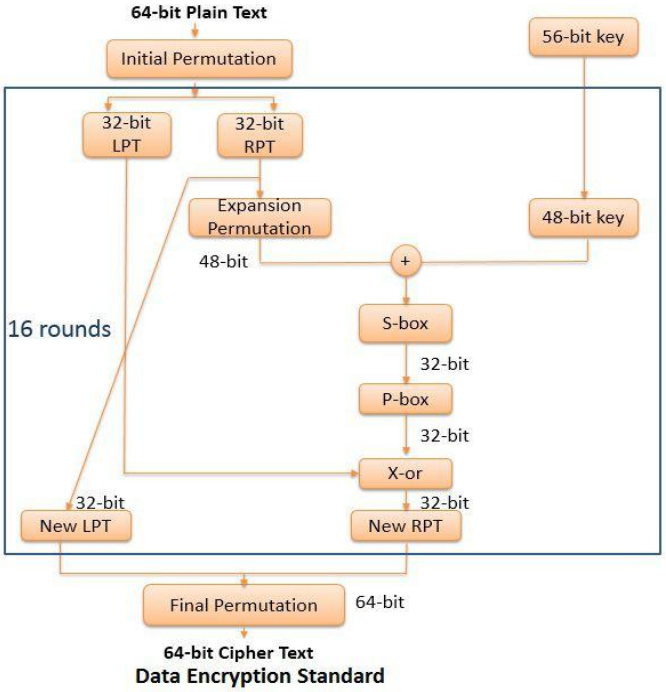

Fig 1: General Depiction of DES

Each of the keys parity bit is used to check one of the keys octets by odd parity, that is each of the parity bits is adjusted to have an odd number of 1s in the octet it belongs to. The key therefore has a real useful length of 56 three bits, which means that only 56 bits are actually used in the algorithm. So it would take a maximum of 72,057,594,037,927,936, attempts to find the correct key. The flow of DES Encryption algorithm is shown in Figure 1. The algorithm processes with an initial permutation, sixteen rounds block cipher and a final permutation (i.e. reverse initial permutation).The block of the message is divided into two halves. The right half is expanded from 32 to 48 bits using another fixed table. The result is combined with the sub key for that round using the XOR operation. Using the S-boxes the 48 resulting bits are then transformed again to 32 bits, which are subsequently permutated again using yet another fixed table. This by now thoroughly shuffled right half is now combined with the left half using the XOR operation. In the next round, this combination is used as the new left half. Encryption strength is directly tied to key size, and 56 bit key lengths have become too small relative to the processing power of modern computers.

3.2 Triple DES (3DES)

3DES is a symmetric-key block cipher, derived from the DES and it uses three different key that means which applies the Data Encryption Standard (DES) three times to each data block. uses a 56-bit key and is not deemed sufficient to encrypt sensitive data. 3-DES simply increase the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits because of 56 bit with three times. 3DES involves using three 64-bit DES keys (Key1, Key2, Key3) in Encrypt-Decrypt- Encrypt (EDE) mode, that is, the plain text is encrypted with K1, then decrypted with K2, and then encrypted again with K3. The 3DES is a trick to reuse DES encryption algorithm but with three distinct keys. Rajadeep et al[13].

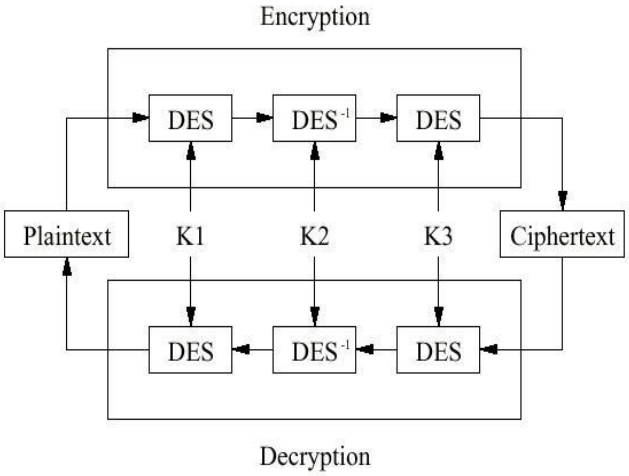

Fig 2: General Depiction of 3DES

Here data is encrypted two times more using DES .Hence, this makes the encryption stronger and more difficult to break. Triple DES is basically a block cipher which uses 48 rounds (three times DES) in its computation and has a key length of 168bits. There are following mode of operation.

EDE : Encrypt, Decrypt and Encrypt with unique keys as mentioned above.

EEE : A block of data is encrypted, and encrypted again with a different key finally encrypted once more with another key, using a total of three unique key.

EDE: First and last keys are same for encryption and for decryption using separate key.

In 3-DES the 3-times iteration is applied to increase the encryption level and average time. It is a known fact that 3DES is slower than other block cipher methods [11].3DES is believed to be secure up to at least two and half security , but it is slow especially in software computation. Rajadeep et al[13].

3.3 Advanced Encryption Standard (AES)

AES algorithm is not only security but also for great speed. Both hardware and software implementation are faster AES is also block cipher algorithm based on fiestel network, to replace DES in 2001. AES is actually, three block ciphers AES-128, AES-192, AES-256.Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128 bits, 192 bits, 256 bits respectively The AES is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world for sensitive data encryption. Rajadeep et al[13].. During encryption-decryption process, AES system there are 10 rounds for 128-bit keys, 12 round for 192-bit keys, and 14 round for 256-bits in order to deliver final cipher-text or to retrieve the original plain-text.

Usual Round : Execute the following operations which are 1).Sub Bytes 2).Shift Rows 3).Mix Columns 4).Add Round Key

Different type of attack to crack AES like square attack, key attack, differential attack were tried , but none of them cracked AES algorithm, and also consider as impervious to all attacks.

Each round consists of following four steps:

3.3.1 Substitute Byte

The first transformation, sub bytes is used at the encryption site. To substitute a byte, we interpret the byte as two hexa decimal digits.

3.3.2 Shift Rows

It is a simple byte transposition, the bytes in the last three rows of the state, depending upon the row location, are cyclically shifted. For 2nd row, 1 byte circular left shift is performed. For the 3rd and 4th row 2-byte and 3-byte left circular left shifts are performed respectively.

3.3.3 Mixcolumns

This mix columns transformation operates at the column level; it transforms each column of the state to a new column.

3.3.4 Addroundkey

Add Round Key. Proceeds one column at a time . Add key round adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition

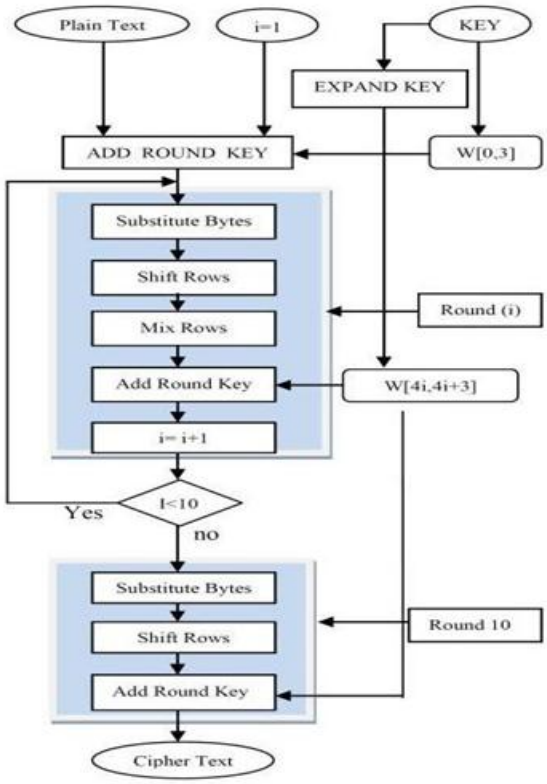

Fig 3: AES (Advanced Encryption Standard) process

4. COMPARITIVE STUDY OF SECURITY ALGORITHM

Factors	DES	3DES	AES
Created By	IBM in 1975	IBM IN 1978	Vincent Rijmen, Joan Daemen in 2001
Key Length	56 bits	168 bits (k1, k2 and k3) 112 bits (k1 and k2)	128, 192, or 256 bits
Round(s)	16	48	10 - 128 bit key,12 - 192 bit key,14 - 256 bit key
Block Size	64 bits	64 bits	128 bits
Cipher Type	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Speed	Slow	Very Slow	Fast
Security	Not Secure Enough	Adequate Security	Excellent Security

Table 1. Comparision of DES, 3DES and AES

5. CONCLUSION AND SCOPE OF FUTURE WORK

This paper depicted the popular Encryption Algorithms such as AES, DES and 3DES. The use of internet and network is growing rapidly. That's why more requirements to secure the data transmitted over internet using different services. To provide the security to the network and data different encryption methods are used. In this paper, a survey on the existing works on the Encryption techniques has been done. If we increase the key with minimum size, this techniques are more optimize 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. According to research done and literature survey it can be found that AES algorithm is best one in terms of speed, time, throughput , key length, rounds and block size . The Security provided by these algorithms can be enhanced further, if key size is reduced and complicated then the algorithm is most suitable for secure data. Our future work will explore this concept and based on the length of the key, to setup a more secure environment for data storage and retrieval.

6. REFERENCES

[1] Tingyuan Nie, Chuanwang Song and Xulong Zhi, "Performance Evaluation of DES and Blowfish Algorithms", IEEE International Conference on Biomedical Engineering and Computer Science (ICBECS- 2010), pp. 1-4, 23-25 Apr 2010.

[2] Behrouz A Forouzan, "Data Communications and networking", McGraw-Hill, 4th Edition.

[3] William Stallings, "Cryptography and etwork Security: Principles and Practice", Pearson Education/Prentice Hall, 5th Edition.

[4] E. Thambiraja, G. Ramesh and Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, pp. 226-233, July 2012.

[5] 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, pp. 280-286, December 2008.

[6] Priyanka Arora, Arun Singh and Himanshu Tiyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World of Computer Science and Information Technology Journal (WCSIT), Vol. 2, No. 5, pp. 179-183, 2012.

[7] S. Pavithra and Mrs. E. Ramadevi, "Performance Evaluation of Symmetric Algorithms", Journal of Global Research in Computer Science, Volume 3, No. 8, pp. 43-45, August 2012.

[8] 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, pp. 152-157, MARCH 2010.

[9] Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-5, 2012.

[10] Ajay Kakkar, M. L. Singh and P.K. Bansal, "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network", International Journal of Engineering and Technology, Volume 2 No. 1, pp. 87-92, January 2012.

[11] Aman Kumar, Dr. Sudesh Jakhar and Mr. Sunil Makkar, "Comparative Analysis between DES and RSA Algorithm's", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, pp. 386-391, July 2012.

[12] Dr.Prerna mahajan, Abhishek Sachdeva, "A study of Encryption Algorithms AES,DES ans RSA for Security" Global Journal of Computer Science and Technology Network and Web Security, Volume 13 issue 15, 2013.

[13] Rajadeep Bhanot, Rahul Hans, "A review and Comparative Analysis of various Encryption Algorithms", International Journal of Security and its Applications, volume 9,issue 4,2015.

[14] Zaran Hercigonja, Durga gimnazija Varazdin and Croatia," Comparative Analysis of Cryptographic Algorithms", International Journal of Digital Technology and Economy, volume 1, issue 2,2016

[15] Faiqa Maqsood, Muhammad Ahmad, Muhammad Mumtaz Ali, Munam Ali hah," Cryptography: A Comparative Analysis for Modern Techniques", International journal of Advanced Computer Science and Applications, volume 8, issue 6,2017