IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

A Review: Text Data Encryption Technique using DES Algorithm with Random Key Generation and Comparative Study of Different Existing Technique's

Prashansa Shrivastava[1], Anita Katiyar[2], Neha Purohit[3], Chetan Gupta[4]

Department of CSE, SIRTS, Bhopal[1-4]

Abstract: With the progression of digital data exchange in electronic way, network security has become an important issue. Encryption algorithm plays a major role in the information security systems. The main objective of encryption algorithms is to protect data and information in order to achieve privacy. Encryption is the process of encoding plain text into cipher text. Encryption algorithms are mainly divided into two categories which are symmetric and asymmetric key encryption algorithm. In Symmetric key encryption, both sender and receiver uses the same key whereas, in asymmetric key encryption, both sender and receiver uses the different keys.DES is a strong block cipher encryption standard that operates on a 64-bits plain text block and returns a 64-bits cipher text. The DES algorithm provides security against various attacks in an effective, efficient and essential way by implementing security parameter counting Confidentiality, Authentication, accountability, and accuracy. In this paper we discussed about various encryption technique for secure data transmission and also compare different encryption techniques like AES, RSA, DES and Triple DES on the basis of various parameters, here we also suggested to encrypt text data using DES algorithm using random key generation to improve strength of encryption algorithm.

Keywords: Encryption, plain text, cipher text, confidentiality, accountability, accuracy, authenticity, DES, RSA, AES.

I. INTRODUCTION

With the rapid development of computer technology and progression of internet, the importance and value of data exchange is escalating. The wide usage of digital media for information conduction through secured and unsecured channels exposes messages sent through networks to third parties. Therefore to overcome this weakness, many researchers have come up with competent algorithms to encrypt information from plain text to cipher text. Cryptography is a key technology for achieving information security in the emerging information society. Cryptography is the process of transforming plain text or original information into an unreadable form (cipher text) so that intruders cannot access the information whenever sent over unsafe channels. As it is extremely difficult to recover the original plaintext without the key. The simplicity or complexity of encryption procedure depends on encryption algorithm and the key which is used in algorithm to encrypt or decrypt the data [1] [2]. Many encryption algorithms are widely available and used in information security. The first kind of encryption, called symmetric cryptography or shared secret cryptography.

In this form of encryption technique, sender uses a secret key, to scramble the data into incomprehensible form. The person on the other end needs the shared secret key to decrypt the data. It is called symmetric key cryptography because the same key is used on both ends for both encryption and decryption [3]. Another kind of encryption, called asymmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt and decrypt data. Public key can be shared with everyone. The private key is kept secret. Public key can be used to encrypt a message and the private key is used to decrypt the message. The shared between two parties is actually the secret information which needs to be transferred over the network. The use of secret key is sometimes known as symmetric key and that of an asymmetric key is known as public key. In asymmetric transformation the private or secret key is used to transform the original data into ciphered form, then at the other end the public key is used to convert the data into decrypted data again.

Some of the Basic terminologies used in cryptography are as follows:

Encryption: The process of encoding plain text (original text) into cipher text (unreadable text) to prevent unauthorized access is called encryption.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

Decryption: The reverse process of transforming the cipher text messages back to plain text messages is called decryption.

Plain text: plaintext is normal legible text before being encrypted into cipher text or after being decrypted. It is the input of an encryption procedure, and the output of a decryption procedure.

Cipher text: Cipher text is the unreadable output of an encryption procedure. It is not understandable until it has been converted into plain text using a key.

Key: A cryptographic key is a string of bits used by a encryption algorithm to convert plain text into cipher text and cipher text into plain text. This key ensures secure communication.

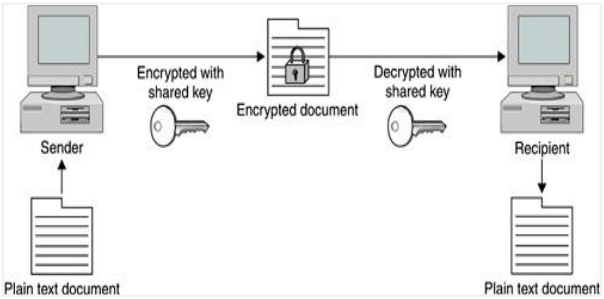

Figure1. Symmetric key cryptography

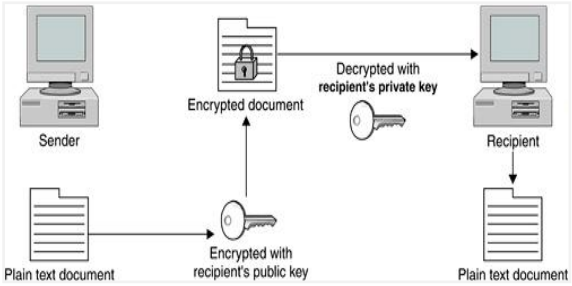

Figure2. Asymmetric key cryptography

II. LITERATURE SURVEY

In 2013, Dr. Prerna Mahajan & Abhishek Sachdeva implemented three encryption techniques (AES, DES and RSA algorithms) and compared their performance on the basis of its stimulated time of encryption and decryption. Based on the text files used and the experimental result they concluded that AES algorithm consumes least encryption time and RSA consume highest encryption time. They also observed that Decryption of AES algorithm is better than other algorithms. From the imitation result, they evaluated that AES algorithm is better than DES and RSA algorithm [3].

In 2016, Praveen Kumar B, Rajaanadan N.S had done a survey on the existing works on the Encryption techniques. All the techniques are useful for real-time Encryption. Each technique is exclusive in its own way and appropriate for different applications and has its own pro's and con's. In this paper they presented the performance valuation of selected symmetric encryption algorithms [4].

In 2013, Mansoor Ebrahimz, Shujaat Khan, Umer Bin Khalid presents a comprehensive comparative analysis of symmetric block encryption algorithms on the basis of different parameters such as Architecture, Security, Scalability, Reliability, Flexibility, Robustness and Limitations that are crucial for secure communication. The main aim was to examine the performance of the most popular symmetric key algorithms [5].

In 2016, Yashwant Kumar, Rajat Joshi, Tameshwar Mandavi, Simran Bharti, Miss Roshni Rathour presented a thorough study of the popular encryption and decryption algorithms such as DES, 2DES, 3DES and substitution technique. In this paper an analysis on the existing work on the encryption and decryption technique has been done. According to research done it has been found that the DES algorithm is most efficient in term of speed. The security provided by this algorithm can be improved further, if more than one algorithm is applied to data [6].

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 1, January 2018

III. EXISTING TECHNIQUES

RSA: RSA is a cryptosystem for public-key encryption, and is extensively used for securing sensitive data, particularly when being sent over an insecure network. RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology. It is the most broadly used asymmetric algorithm. It uses two dissimilar but mathematically related keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both the public and the private keys can encrypt a message and the opposite key is used to decrypt it.[

DES: DES is the typical block cipher algorithm that takes a fixed-length string of plaintext and transform it through a sequence of complex operations into another cipher text of the same length. The block size of DES is 64 bits. It is symmetric key encryption algorithm. It uses a key to modify the alteration, so that decryption can only be performed by those who know the specific key used to encrypt. The key apparently consists of 64 bits however, only 56 of these are really used by the algorithm. Eight bits are used exclusively for checking parity, and are thereafter discarded. Hence the useful key length is 56 bits.

Triple DES: 3DES or the Triple Data Encryption Algorithm (TDEA) was developed to address the evident flaws in DES without designing a entire new cryptosystem. Data Encryption Standard (DES) uses a 56-bit key and is not adequate to encrypt sensitive data. 3-DES merely extends the key size of DES by applying the algorithm three times in sequence with three different keys. The collective key size is thus 168 bits (3 times 56). [2].

AES: AES is the innovative encryption standard suggested by NIST to substitute DES in 2001. AES algorithm can sustain any permutation of data (128 bits) and key length of 128, 192, and 256 bits. The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length. During encryption and decryption course, AES system goes through 10 rounds for I28-bit keys, 12 rounds for I92-bit keys, and 14 rounds for 256-bit keys in order to bring final cipher-text or to regain the original plain-text. [2]. Table 1 shows the comparison between existing system the basis of different parameters:[12][13][14][15][16].

Comparison between RSA, DES, AES and Triple DES

Table 1: Comparison between Existing encryption System

PARAMETERS	RSA	DES	AES	Triple DES
Evolved In	1978	1977	2000	1998
Key Size	Less than 1024 bits	56 bits	128, 192, 256 bits	168, 112, 56 bits
Block Size	Minimum 512 bits	64 bits	128 bits	64 bit
Ciphering & Deciphering key	Different	Same	Same	Same
Key Used	Different key used for Encryption & Decryption	Same key used for Encryption & Decryption	Same key used for Encryption & Decryption	Same key used for Encryption & Decryption
Rounds	1	16	10 or12 or14	48 DES equivalent rounds
Algorithm	Asymmetric	Symmetric	Symmetric	Symmetric
Ciphering & Deciphering algorithm	Same	Different	Different	Different
Scalability	Not scalable	Scalable	Not scalable	scalable
Encryption & Decryption	Slower	Moderate	Faster	Slower than DES
Attacks	Brute force & Oracle attack	Brute force, differential cryptanalysis and linear attack	Brute forced attack	Meet-In-Middle attack
Security	Least secure	Not secure enough	Excellently secured	More secure than single DES
Hardware & Software Implementation	Not efficient	Better in hardware than software	Faster	Better in hardware & slower in software

IV. PROBLEM DOMAIN

After study of several proposed technique we can come with some problem which are following:

1. Hybrid combination is not used to encrypt data [7].
2. Random key not use in the round of encryption [8].
3. Information loss is very high in encryption and Decryption [9].
4. Proper XORed Function is not used[10][11].
5. In Text Data hiding techniques with bit shuffling cannot be used.

V. ADVANTAGES OF ENCRYPTION SCHEME

- ❖ More security archive.
- ❖ Information secrecy.
- ❖ Excellent encryption performance.
- ❖ High sensitivity to the security keys.
- ❖ Sufficiently large key space to resist the brute attack.

VI. CONCLUSION AND FUTURE WORK

There are so many technique to make an image secure. In general sense today's digital world where nothing is secure, the security of images over network is very important. In this survey we define so many techniques of image encryption. In this paper, we have surveyed different image encryption techniques from different research papers. We conclude that all techniques are good for data encryption and have their own advantages and disadvantages and they also gives better security at their level so that no unauthorized access can be done on images, which is in the open network. Each technique has its own suitability and its own limitations. But still lot more has to be done in this context. On the basis of above study we provide the following future direction:

1) The Powerful encryption technique like DES and MD5 can improve the security.
2) A large key size can be used to improve the image security and protect form bruit force attack.
3) We can work on Hybrid Encryption using random key generation for more strength in encryption algorithm.

REFERENCES

[1] Shipra Ravi kumar, Suman Avdhesh Yadav, Akanksha Singh, Smita Sharma, "Design and Implementation of Improved Data Encryption Standard" 2017.
[2] Gurpreet Singh, Supriya Kinger, "Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013
[3] Prerna Mahajan & Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security". Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013
[4] Praveen Kumar B, Rajaanadan N.S, "Data Encryption and Decryption Using By Triple DES Performance Efficiency Analysis of Cryptosystem". International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 3, March 2016
[5] Mansoor Ebrahimz, Shujaat Khan, Umer Bin Khalid, "Symmetric Algorithm Survey: A Comparative Analysis". International Journal of Computer Applications (0975 – 8887) Volume 61– No.20, January 2013
[6] Yashwant kumar, Rajat joshi, Tameshwar mandavi, Simran bharti, Miss Roshni Rathour, "Enhancing the Security of Data Using DES Algorithm along with Substitution Technique". International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 5 Issue 10 Oct. 2016, Page No. 18395-18398
[7] Alireza Jolfaei, Abdolrasoul Mirghadri, "Survey: Image Encryption Using Salsa20", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 5, September 2010 ISSN (Online): 1694-0814.
[8] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, 2003, 1-6. www.elsevier.com/ locate/optcom.
[9] Jui-Cheng Yen, Jiun-In Guo, "A new chaotic image encryption algorithm", Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China.
[10] Parameshachari B D, K M Sunjiv Soyjaudah, Chaitanyakumar M V, "A Study on Different Techniques for Security of an Image", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-6, January 2013.
[11] A.Masmoudi, M.S. Bouhlel, and W. Puech, "A new image cryptosystem based on chaotic map and continued fractions", 18th European signal processing conference (EUSIPCO-2010), Aaborg, Denmark, August 23-27,2010, ISSN 2076-1465.
[12] Jawad Ahmad, Fawad Ahmed, "Efficiency Analysis and Security Evaluation of Image Encryption Schemes", International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 12 No: 04.
[13] Abhinav Srivastava, "A survey report on Different Techniques of Image Encryption", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 6, June 2012).
[14] Sesha Pallavi Indrakanti and P.S.Avadhani, "Permutation based Image Encryption Technique", International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, August 2011.
[15] Yasaman Hashemi, "Design a new image encryption using fuzzy integral permutation with coupled chaotic maps", International Journal of Research in Computer Science eISSN 2249-8265 Volume 3 Issue 1 (2013) pp. 27- 34 www.ijorcs.org, A Unit of White Globe Publications doi: 10.7815/ijorcs. 31.2013.058.
[16] 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, July 2012 ISSN: 2277 128X.