Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Analysis on Different Parameters of Encryption Algorithms for Information Security

[1]Manju Rani, [2]Dr. Sudesh Kumar
[1]M.Tech Scholar, BRCMCET, Bahal Bhiwani, Haryana, India
[2]Associate Professor, BRCMCET Bahal, Bhiwani, Haryana, India

Abstract— With the fast evolution of digital data exchange, security information is very important in data storage and transmission. Data encryption is widely used to ensure security in open networks such as the internet. Security is a very important factor in every field such as Government Agencies (CBI, FBI), Research Organization, E-commerce and etc. where internet is being used. Each type of data has its own features, therefore, different techniques should be used to protect confidential image data from unauthorized access. Cryptography is a technique to secure data on the network from unauthorized user. There are different types of a cryptography algorithm (a) symmetric and (b) asymmetric has been designed. To secure data it is necessary to know which algorithm provides better security, efficiency, accuracy and effectiveness. This paper presents the complete analysis of various symmetric key encryption algorithms (DES, 3DES, AES, and RC4) based on different parameters.

Index Terms— Cryptography, Symmetric Key, Information Security, Performance Matrices, Encryption, AES, DES, 3DES, and RC4

I. INTRODUCTION

The development of information technology and the rapid growth of computer networks allowed large files, such as digital images, to be easily transmitted in open networks such as the internet [1]. Each type of data has its own aspects, and different techniques should be used to protect confidential image data from unauthorized access [2]. Encryption is the process of transforming the information to ensure its security. Although data encryption is widely used to ensure security, most of the available encryption algorithms are used for text data. Due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data. Even though Triple-DES and IDEA can achieve high security, it may not be suitable for multimedia applications and therefore encryption algorithms such as DES, AES, RSA and IDEA were built for textual data. These algorithms are used perfectly to secure textual data. However, digital images are different from texts in many aspects and thus requiring different encryption algorithms. In most of the natural images, the values of the neighboring pixels are strongly correlated. This means that the value of any given pixel can be reasonably predicted from the values of its neighbors [3]-[5]. In order to dissipate the high correlation among pixels and increase the entropy value, we propose a permutation process based on the combination of the image permutation and a well known encryption algorithm called RijnDael.

CRYPTOGRAPHY

The many schemes used for enciphering constitute the area of study known as cryptography. There are three types of cryptography:

Secret Key Cryptography:

This type of cryptography technique uses just a single key. The sender applies a key to encrypt a message while the receiver applies the same key to decrypt the message. Since only single key is used so we say that this is a symmetric encryption. The biggest problem with this technique is the distribution of key as this algorithm makes use of single key for encryption or decryption.

Public Key Cryptography:

This type of cryptography technique involves two key crypto systems in which a secure communication can take place between receiver and sender over insecure communication channel. Since a pair of keys is applied here so this technique is also known as asymmetric encryption. In this method, each party has a private key and a public key. The private is secret and is not revealed while the public key is shared with all those whom you want to communicate with. If Alice wants to send a message to bob, then Alice will encrypt it with Bob's public key and Bob can decrypt the message with its private key.

Hash Functions:

This technique does not involve any key. Rather it uses a fixed length hash value that is computed on the basis of the plain text message. Hash functions are used to check the integrity of the message to ensure that the message has not be altered, compromised or affected by virus. Cryptography technique needs some algorithm for encryption of data. Nowadays when more and more sensitive information is stored on computers and transmitted over the Internet, we need to ensure information security and safety.

Cryptography Goals:

There are some goals of cryptography that are given below:

1) Authentication: Sender and data receiver must be authenticated before sending and receiving data.
2) Confidentiality: The user who is authenticated, can access the messages.
3) Integrity: Data is free from any kind of modification between sender and receiver.
4) Non-Repudiation: The sender the receiver cannot deny that they had sent a message.
5) Service Reliability: Attackers can attack on secure systems, which may affect the service of the user.

II. RELATED WORKS

Many authors have compared these algorithms either on a single parameter or two parameters. But generally they have published their paper based on time complexity of these algorithms. In [6], the authors have compared AES and DES based on their performance, generally comparison has done for time complexity but they could not find which algorithm is better. In [7], the author compared some symmetric key algorithm on the basis of space complexity, In this paper, we conduct with different statistical analyses, an analysis of the sensitivity to secret key, differential analysis, an analysis of the key space and the encryption speed, etc... .

Generally, in this paper author compared Various algorithms and focused on encryption and decryption Time analysis, key analysis and various factors[8]-[9]. On the base of encryption and decryption time we cannot say that the which algorithm is efficient and effective. For this, we need to compare all the parameters of the algorithm and then we can easily decide which algorithm is efficient and secure. So, in this paper, I compared various symmetric key encryption algorithms based on different features.

III. DESCRIPTION

1. BASED ON ARCHITECTURE:

In this section, algorithms are discussed on their architecture (Basically structure, key size, block size and number of processing rounds).

1.1 DES (Data Encryption Standard):

DES designed by IBM in 1972 and it was adopted by the U.S. Government as standard encryption technique. It is a symmetric key block cipher encryption algorithm based on Feistel Network. DES uses 64 bit block of text and 56 bit key length, it performs total 16 rounds of processing to encrypt data [10]. In DES, the key was 64 bits but due to some restrictions from NSA (National Security Agency) IBM decided to use 56 bit key length for encryption and the remaining 8 bits is used as a parity bit for error detection, it also uses 8 boxes. DES divides the 64 bit block into two equal parts and then applies F - function on each part. Ffunction performs four different tasks- Expansion, Key_Mixing, Substitution and Permutation. Decryption is the same process of encryption in DES.[1]

1.2 3DES (Triple DES)

3DES is an enhancement of Data Encryption Standard. It uses 64 bit block size with 192 bits of key size. The encryption method is similar to the original DES but it applied 3 times to increase the safe time and encryption level. Triple DES is slower than other block encryption methods. It has the advantage of reliability and a longer key length that eliminates many shortcut attacks. 3DES can be used to reduce the amount of time to break DES.[10]

1.3 AES (Advanced Encryption Standard):

AES is a symmetric key block cipher encryption algorithm designed by Vincent Rijmen and Joan Daemen in 1998. It is based on Feistel network and support 128 bit block size and key length 128, 192 and 256 bits [1]. AES performs 10, 12 or 14 round and the number of rounds depends on the key. It means for 128 bit key length AES performs 10 rounds, for 192 bit key it performs 12 rounds and for 256 bit key it performs 14 rounds [14]. In AES each round performs some steps. Key-expansion, Initial-round, Rounds and Final-rounds. In Rounds step, Sub-byte generation, Shift-rows, Mix-columns and Add-round_key are performed whereas in Final-rounds step, same functions are performed except Mix-columns function.[11]

1.4 RC4

RC4 is a stream cipher, symmetric key encryption algorithm. The same algorithm is used for both encryption and decryption. The data stream is simply XORed with the series of generated keys. The key stream does not depend on plaintext used at all. RC4 use 256 bit key length, it performs total 256 rounds of processing to encrypt data. Vernam stream cipher is the most widely used stream cipher based on a variable key-size. It is popular due to its simplicity. It is often used in file encryption products and secure communications, such as within SSL. The WEP (Wireless Equivalent Privacy) protocol also used the RC4 algorithm for confidentiality. It was also used by many other email encryption products. The cipher can be expected to run very quickly in software. It was considered secure until it was vulnerable to the BEAST attack.[12]

2. BASED ON SCALABILITY:

In this section, analyze the scalability of various encryption algorithms on the basis of performance (key scheduling and encryption) and space required by the encryption algorithm. The memory required by any algorithm depends on the number of variables and functions executed by the encryption algorithm. Due to lack of memory to execute program there is a need to require less memory to execute the algorithm. If any algorithm requires less memory space provide better efficiency.

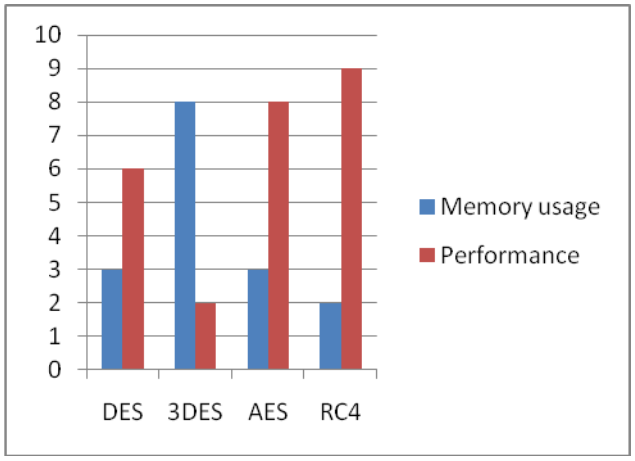

Figure1. Comparison of Algorithm based on scalability

3. AVALANCHE EFFECT:

A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the cipher text. In, particular a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the cipher texts.

Table 1.Comparison based on Avalanche effect

Technique	1 bit variation in key, keeping plaintext constant	1 bit variation in plaintext, keeping Key constant
DES	30	34
3DES	37	33
AES	64	71
RC4	0	1

4. ON THE BASIS OF FLEXIBILITY:

In this section, compared various algorithms base on their flexibility i.e. in the future according to the need the algorithm is able to modify or not.

Table2. Comparison of Algorithms based on Flexibility

Algorithms	**Flexibility**	**Modification**	**Remarks**
DES	NO	NO	Does not support any modification.
3DES	Yes	168 Bits	3DES performs DES operation
AES	Yes	128, 192 or 256 Bits	Its structure was flexible to the multiples of 64.
RC4	Yes	RC4C,2S-RC4 and many more	Supports key size from 8 bits to 256 bits and any size of input data.

5. SECURITY LEVEL:

In this section, I discussed about the security of these algorithms. It is the most important parameter of a cryptography algorithm because an algorithm is said to be better if they provide a strong security level.

5.1 DES:

Security is the main drawback of DES. DES does not provide strong security because of its key length 0f 56 bits.[13]

5.2 3DES (TDES):

3DES removes the security problem of DES. In 3DES, DES process is performed three times with three different keys to provide better security. It provides high level security in comparison to DES.[14]

5.3 AES:

AES is also provides a very high security level because of using variable length key i.e. 128, 192 or 256 bits. Different types of attack tried to crack AES like Square attack, Key attack, Differential attack and improved square attack but none of them is possible to crack this algorithm. So, AES is a highly secured encryption technique [6, 16].

5.4 RC4

RC4 failed to provide high level of security because of its poor key scheduling, biases in adjacent bytes in RC4 keystream, fixed single key or with a small keyspace and many more. When used in WEP RC4 failed to provide desired level of security because of its weak initial vector and small keyspace. Many modifications suggested by many researchers which are able to provide much more better level of security than the original RC4.

IV. CONCLUSION

1. DES is the most widely used encryption scheme, especially in financial applications.
2. In 3DES memory required for implementation is the highest means it is the slowest algorithm. This is the main drawback of 3DES.
3. In AES the avalanche effect is highest. AES is being considered by the US government as a replacement for DES. AES is ideal for encrypting messages sent between objects via chat-channels, and is useful for objects that are part of a game, or anything involving monetary transactions.
4. RC4 is the shortest algorithm means it requires minimum memory space for implementation. RC4 is used in many commercial software packages such as Lotus notes and Oracle secure SQL.

REFERENCES

[1] W. Lee, T. Chen and C. Chieh Lee,"Improvement of an encryption scheme for binary images," Pakistan Journal o f Information and Technology. Vol. 2, no. 2 , 2003, pp. 191-200,

[2] A. Mitra, Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science, vol. 1, no. 1, 2006, p.127,

[3] S. P. Nana'Vati and K. P. Prasanta, "Wavelets: Applications to Image Compression-I," Joined of the Scientific and Engineering Computing. Vol. 9 , No.3: 2004, PP. 4-10

[4] c. Ratael, gonzales, e. Richard, and woods, "Digital image processing," 2nd ed, Prentice hall, 2002.

[5] AL. Vitali, A. Borneo, M. Fumagalli and R. Rinaldo, "Video over IP using standard-compatible multiple description coding," Journal of Zhejiang University- Science A, vol. 7, no. 5 ,2006, pp. 668- 676.

[6] A. K. Mandal, C. Parakash and M. A. Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES", 2012 IEEE Student's Conference on Electrical, Electronics and Computer Science.

[7] V. Singh and S. K. Dubey, "Analyzing Space Complexity Of Various Encryption Algorithms", International Journal of Computer Engineering and Technology (IJCET), Volume 4, Issue 1, January- February (2013).

[8] Tingyuan Nie, Yansheng Li and Chuanwang Song, "Performance Evaluation for CAST and RC5 Encryption Algorithms", International Conference on Computing, Control and Industrial Engineering, IEEE, 2010.

[9] A.Ramesh and Dr.A.Suruliandi, "Performance Analysis of Encryption Algorithms for Information Security", International Conference on Circuits, Power and Computing Technologies [ICCPCT-2013], IEEE, 2013.

[10] Michal Halas, Ivan Bestak, Milos Orgon, and Adrian Kovac, "Performance Measurement of Encryption Algorithms and Their Effect on Real Running in PLC Networks", IEEE, 2012

[11] Fei Shao, Zinan Chang and Yi Zhang, "AES Encryption Algorithm Based on the High Performance Computing of GPU", Second International Conference on Communication Software and Networks DOI 10.1109/ICCSN.2010.124, IEEE, 2010

[12] Jian Xie, Xiaozhong Pan, "An Improved RC4 Stream Cipher", International Conference on Computer Application and System Modeling, ISBN 978-1-4244-7237-6, IEEE 2010

[13] Md Asif Mushtaque, H. Dhiman, S. Hussain and Shivangi Maheshwari,"Evaluation of DES, TDES, AES, Blowfish and Twofish Encryption Algorithm Based on Space Complexity", International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 4, April – 2014.

[14] Fei Shao, Zinan Chang and Yi Zhang, "AES Encryption Algorithm Based on the High Performance Computing of GPU", Second International Conference on Communication Software and Networks DOI 10.1109/ICCSN.2010.124, IEEE, 2010.

[15] Harmanpreet Singh, Amritpal Singh Danewalia, Deepak Chopra and Naveen Kumar N, "Randomly Generated Algorithms and Dynamic Connections", ISROSETInternational Journal of Scientific Research in Network Security and Communication, Volume-02, Issue-01, Page No (1-4), Jan -Feb 2014.

