Comparative Analysis of Most Common Modern Symmetric Key Cryptographic Algorithms

Neetu Yadav, Dr. R.K. Kapoor, Dr. M.A. Rizvi
Department of Computer Engineering and Applications, NITTTR Bhopal, India

Abstract - The current era is an era of internet technology. Security of data has become one of the challenging issues. Hackers tries to gain access over the data being transferred . For an organization any loss to information can be great loss for it. Cryptography techniques come as a solution. These techniques ensures that the integrity, confidentiality, authentication, identity and availability of user data can be maintained as well as provide user the security and privacy of data. There are various cryptographic algorithms both symmetric and asymmetric that provide the required security for data. This paper provides comparative analysis of most common modern symmetric key cryptography algorithms like AES, DES, TDES, Blowfish,RC2,RC6 on different security parameters.

Keywords: Cryptography, Symmetric Key Encryption, DES, TDES, AES, Blowfish,RC2, RC6.

I. INTRODUCTION

The immense growth in computer systems and their interconnections via network has led a common culture for interchanging data among various users very significantly. Data security has become a prime concern while communicating over the network. Susceptible information like credit cards, social security numbers and banking transactions are required to be protected from intruders. Distinct encryption techniques are used to safeguard the confidential data from unauthorized person or entity. Encryption is a general technique for promoting the security of information. New methods of encryption techniques are evolved everyday. This paper proposed most common modern symmetric key cryptographic algorithms like AES, DES, TDES, Blowfish ,RC2, RC6 and comparing their security issues based on ten different parameters.

A. Cryptography

Cryptography is the art and science to safeguard the information from unauthorized person by transforming it into an unscrambled form making it unreadable. The main goal is to safeguard the data from the person who is not the intended recipient of it. The conversion of an original form of data into unintelligible form is commonly known as encryption process. The cipher text produced is an unintelligible form of data. The reverse process applied to get the original message back is known as decryption.

Cryptography algorithms are of two types- symmetric key cryptography algorithm and asymmetric key cryptography based on the keys used. The symmetric key cryptography algorithms use the same key for encrypting and decrypting the data. A key pair known as public key and private is used in asymmetric key cryptography algorithm. The data is encrypted by the sender using its public key. At the receiver end the private key is used to decrypt the data.

B. Purpose of Cryptography

Cryptography serves a number of security goals to safeguard the data from hackers. The different goals of cryptography are as follows:-

a. Confidentiality

The information cannot be read by anyone except the intended receiver. It is made available to the authorized persons during communication.

b. *Authentication*

It is a process of establishing one’s identity. The identity of the sender is checked whether the information is coming from an authorized person or an unauthorized person.

c. Integrity

It ensures that information has not been altered before reaching it to the intended receiver of the message. Only authorized party can alter the information during transmission.

d. Non Repudiation

It ensures that neither sender nor receiver can refute the acceptance or transmission of the message.

e. Access Control

Only authorized party can have access to the given information not to anyone.

C. Cryptanalysis attack

The purpose of cryptanalysis is to obtain the original message by using some cryptographic techniques. The types of cryptanalysis attack are :-

a. *Cipher text-only attack*

In this type of attack, an attacker has only part of the cipher text using available information and try to find out the original message by analyzing the cipher text.

b. *Known-plaintext attack*

In this attack, an attacker has plain text and its corresponding encrypted version (i.e. Cipher text). The attacker tries to find the relation between these two to obtain the key.

c. *Chosen-plain text attack*

The attacker has cipher text and associated plain text. The attacker chooses the plain text and tries to find it encryption in the cipher text messages to find out the key and the algorithm used to encrypt the message.

d. *Chosen-cipher text attack*

The attacker study the plain text produced by decrypting the chosen cipher text available to him.

e. *Chosen-text attack*

It is a combination of chosen plain text and chosen cipher text attacks[1] that an attacker tries to obtain the original message.

f. *Brute force attack*

Brute force attack is also called an exhaustive key search attack, in which an attacker tries all possible keys until correct key is obtained to decrypt the message.

g. *Man-in-the-Middle Attack*

It is the type of active attack which involves tricking individuals into conciliation their keys [2]. The cryptanalyst/attacker is in the communication channel between two parties and performs a key exchange with each party.

h. *Timing attack*

In this attack, the attacker by analyzing the time taken to execute cryptographic algorithm try to compromise the cryptosystem.

II. OVERVIEW OF CRYPTOGRAPHY ALGORITHMS

In this section overview of the most common modern symmetric key cryptography algorithms is briefly described as follows:

2.1 Data Encryption Standard[DES]

DES is a symmetric key encryption technique that uses 64-bit block size and 56 bit key length. It uses both permutations and substitutions in the algorithm and operates on blocks of equal size. It uses 16 rounds to encrypt each 64-bit plain text and to produce the encrypted text. The number of rounds in DES is exponentially proportional to the amount of time required to find a key by means of a brute-force attack. [2].The security of the algorithm increases exponentially with the increase in the number of rounds in DES.

2.2 Triple DES(TDES)

Triple DES [8] is same as the DES which performs three time encryption of the data. Three 64-bit keys and overall key length of 192 bits is used for three time encryption of the data. The plain text is encrypted with the first key then it encrypted with the second key and finally with the third key. All the Three keys are different from each other. The decryption process is the reverse of the encryptions in which keys are used in reverse order for decrypting the encrypted data.

2.3 Advanced Encryption Standard(AES)

AES is symmetric block encryption algorithm that uses 128-bit block size and key of sizes 128,192 and 256 bits. AES goes through different rounds based on the key length[9] .10 rounds for 128-bit keys, 12 round for 12 rounds for I92-bit keys, and 14 rounds for 256-bit keys to produce the cipher text. It is faster and flexible and can be implemented on various platform especially for small devices.

2.4 Blowfish

It is a symmetric key block cipher encryption algorithm that uses 64-bit block size and variable- key length from 32 bits to 448 bits to encrypt the data. Blowfish algorithm is a Feistel Network, a simple encryption function is repeated 16 times

[3].It is difficult to break the code because of the larger key size.

2.5 RC2

RC2 (RC stands for Rivest Cipher) is a symmetric-key block cipher encryption algorithm designed in 1987 by Ron Rivest. The algorithm uses 64-bit block size with a key of variable size. In RC2, the 18 rounds are organised as a source-heavy Feistel network consisting of 16 rounds of one type (known as MIXING) followed by two rounds of another type (known as MASHING)[4].The MIX transformation is used four times in MIXING round.

2.6 RC6

Rivest Cipher 6 (RC6) is a symmetric key block cipher encryption algorithm designed by Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin[4] which is derived from RC5 .It is very similar to RC5 in structure using data-dependent rotations, modular addition, and XOR operations but involves an extra multiplication operation .The multiplication operation make the rotation dependent on every bit in a word.

III. ANALYSIS

The comparative analysis of the algorithms DES, TDES, AES, Blowfish, and RC6 is shown in Table1.

On analysizing the algorithms based on the parameters used in the table. It is found that DES, TDES, Blowfish and RC2 encrypt a block size of 64-bit. Larger the bock size more secure is the code against cryptanalysis attack. Thus AES is secure among all the algorithms as it can encrypt data blocks of size 128,192 and 256-bits and RC6 is as secure as AES. But larger block size is costly to implement in terms of hardware. The strength of an algorithm depends on the resistance of key against brute force attack. Larger the key length more secure is the system .In this case, RC2 uses variable length key ranging from 8 bits to 1024 bit showing its superiority among all the algorithms.

The number of rounds increases the security of algorithm. In a Fiestel network, a single round does not provide sufficient security. DES, Blowfish and RC2 uses 16 rounds and RC6 uses 20 rounds. TDES uses 48 rounds as it encrypts the data three times. In AES the number of rounds depend on the key length. There are 9 rounds for key length 128-bit, 11 rounds for 192-bit key and 13 rounds for 256-bit key.

Throughput is one of the criteria to judge the efficiency of an algorithm. The throughput of an algorithm depends on its encryption speed. Faster the encryption speed higher the throughput thus resulting in lower power consumption. Form the table it can be seen that Blowfish has fast encryption speed whereas RC2 very slow encryption speed. The blowfish shows higher throughput thus it can be concluded that it has better efficiency and performance than all other algorithms: AES, DES, TDES, RC2, RC6.

Another criterion to select an algorithm is power consumption. Higher the throughput of an algorithm lower is the power consumption. The analysis shows that Blowfish consumes less power whereas RC2 consumes more power in comparison to all other algorithms because of key size changing up to 1024-bits.Thus it can also be conclude that the changing key size has effect on the throughput and power consumption. Hence, Blowfish is superior than all other algorithm making it preferable for devices that requires low power consumption.

An algorithm is said to be flexible if it can accept any modification according to the requirements thus making it suitable for hardware and software implementation. The analysis shows that DES is not flexible and effectively slow whereas AES is flexible and work effectively in software and hardware. Thus selection of an algorithm depends on the criteria how efficiently it can work on hardware and software.

IV. CONCLUSION

The algorithms DES, TDES, AES, Blowfish, RC2 and RC6 are analysed based on the parameters taken. The analysis shows that Blowfish has high throughput among all algorithms whereas RC2 has the lowest throughput. If throughput increases the power consumption decreases. The Blowfish consumes less power and is fastest among all the algorithms. The change in the key length also effect on the throughput, speed and power consumption of algorithm. The table shows that RC2 algorithm has maximum length of key of 1024 bits which is higher than among all the cryptographic algorithms but it has less throughput, more power consumption and slower in speed. All algorithms are flexible to accept modifications according to requirements except DES. The DES is not flexible to accept any modifications and also throughput decreases. The AES is effective in both hardware and software among all the algorithms. Thus Blowfish is better among all the algorithms in terms of security. The selection of an algorithm depends on the need of the application.

V. APPENDIX

The Comparison of the algorithms is shown in Table1.

TABLE 1.COMPARISON BETWEEN MOST COMMON MODERN SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHM

Parameters	**DES**	**TDES**	**AES**	**Blowfish**	**RC2**	**RC6**
Block Size	64bits	64 bits	128, 192, 256 bits	64- bits	64bits	128 bits
Key length	56 bits	112 -168 bits	128, 192, 256 bits	32–448 bits (128 by default)	8-1024 bits (64 by default	128, 192, 256 bits
Throughput	Lower than AES	Lower than DES	Lower than Blowfish	Very High	Low	Lower than Blowfish
Rounds	16	48	9, 11, 13	16	16	20
Network Structure	Fiestel Network	Fiestel Network	Substitution Permutation Network	Fiestel Network	Source Heavy Fiestel Network	Fiestel Network
Attacks	Brute force attack	Brute force, chosen-plaintext, known plaintext	Chosen plain, known plain tex	Dictionary Attacks	Related key attack, Chosen plaintext	Known plaintext, chosen cipher text
Speed	Slower than AES	Slower than DES	Slower than RC6	Very fast	Very Slow	Slower than Blowfish
Flexible	No	Yes	Yes	Yes	-	Yes
Power consumption	Higher than AES	Higher than DES	Higher than Blowfish and RC6	Very Low	Very high	Higher than blowfish
Effectiveness	Slow	Slow specially in Software	Effective in both Hardware & Software	Efficient in Software	Efficient in Software	Slow

REFERENCES

[1] Ritu Tripathi, Sanjay Agrawal" Comparative Study of Symmetric and Asymmetric Cryptography Techniques", International Journal of Advance Foundation and Research in Computer (IJAFRC)Volume 1, Issue 6, June 2014.

[2] AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram" Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms",International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 3, May-Jun 2012, pp.3033-3037.

[3] G. Muthukumar, Dr. E. George Dharma Prakash Raj "A Comparative Analysis on Symmetric Key Encryption Algorithms", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3, Issue 2, February2014.

[4] SSVR Kumar Addagarla , Babji Y,"A Comparative Security Study Review on Symmetric Key Cryptosystem Based Algorithms", International Journal of Computer Science and Mobile Computing , IJCSMC, Vol. 2, Issue. 7, July 2013, pg.146 – 151, ISSN 2320–088X.

[5] Saranya K, Mohanpriya R, Udhayan J, "A Review on Symmetric Key Encryption Techniques in Cryptography", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, March 2014, ISSN: 2278 – 7798.

[6] Kirti Aggarwal, Jaspal Kaur Saini, Harsh K. Verma, PhD" Performance Evaluation of RC6, Blowfish, DES, IDEA, CAST-128 Block Ciphers", International Journal of Computer Applications (0975 – 8887),Volume 68– No.25, April 2013.

[7] Srinivasarao D,Sushma Rani N, Ch.Panchamukesh and S.Neelima," Analyzing the Superlative Symmetric Cryptographic Encryption Algorithm(ASCEA)", Journal of Global Research in Computer Science, Volume 2, No. 7, July 2011.

[8] Harsh Kumar Verma , Ravindra Kumar Singh, "Performance Analysis of RC5, Blowfish andDES Block Cipher Algorithms", International Journal of Computer Applications, ISSN: 0975-8887, Volume 42– No.16, March 2012.

[9] 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.

[10] Sheetal Charbathia and Sandeep Sharma," A Comparative Study of Rivest Cipher Algorithms", International Journal of Information & Computation Technology,ISSN 0974-2239, Volume 4, Number 17 (2014), pp. 1831-1838.

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