DOI: http://dx.doi.org/10.26483/ijarcs.v11i5.6655

Volume 11, No. 5, September-October 2020

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

SIMULATION-BASED COMPARATIVE ANALYSIS OF SYMMETRIC ALGORITHMS

Rohit Verma
Department of Computer Science
Himachal Pradesh University
Shimla, India

Aman Kumar Sharma
Department of Computer Science
Himachal Pradesh University
Shimla, India

Abstract: Data security is one of the major problems faced by today's world. In actuality, the communication channel used to transmit data from one user to another is highly insecure. Any trespasser can easily get access to sensitive data which results in cybercrime. To resolve this problem of data security before transmission of data through any medium it gets changed to some codes which are human unreadable forms, this process is known as encryption of data and this leads to the term cryptography. Nowadays we have but many algorithms available that encrypt the data. Some of them use a single key for encryption as well as for decryption known as symmetric key algorithms. This paper contains the comparison of such symmetric algorithms namely: DES, TDES, AES, Blowfish, RC6 based on performance, and the avalanche effect. The main aim of this study is to find out the most secure algorithm and algorithm with high performance. Java programming language is used in this study for the implementation of the above algorithm. From results, it was concluded that the AES algorithm has good performance whereas RC6 has better security and DES requires disk space to store data.

Keywords: Avalanche effect, AES, Blowfish, cryptography algorithms, DES, encryption, RC6, TDES.

I. INTRODUCTION

In the current scenario, billions of peoples are using the internet per minute for various types of activities like communication, education, entertainment, banking, etc. One of the most used applications of the Internet is E-Commerce. 1000 of the things are being sold and purchased in a day and crores of money are traded. Maximum of these transactions are made using Internet Banking, UPI IDs, Debit cards, etc. These confidential and sensitive data should be kept secret from the intruders. Cryptography comes in existence here when there is a need to secure some sensitive and confidential data. Cryptography is derived from the Greek word: “cryptos” which means “secret” and “graphein” which means “writing” [1][2].

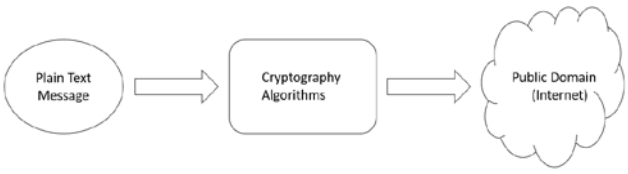

Fig 1: Overview of cryptography

Figure 1 shows that cryptography is a central part that secures the plain text message in the public domain i.e. internet from intruders.

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called intruders. More generally, it is about constructing and analyzing algorithms that overwhelmed the impact of intruders and are associated with various aspects of information security like confidentiality, integrity, authentication, and non-repudiation [3].

- Authentication: That verifies one entity towards permit them or not to permit accesses of resources.
- Confidentiality: it can be defined that the message cannot be changed by others except the approved receiver.
- Integrity: refers to maintaining and making sure that the data stays correct and reliable over its entire life cycle.
- Non-Repudiation: refers to the capability to make sure that a person or a party connected with a communiqué cannot deny the legitimacy of their signature over their document or the sending of a message.

Encryption and decryption are one way to achieve cryptography. Encryption is the process of converting a human-readable message into some secret codes and decryption is the reverse process of encryption. The unreadable form of the message is different from the original plain text message. For encryption, an algorithm and key are needed. The key is a string of bits that are used by the cryptographic algorithm to convert plain text messages into ciphertext. The key is a core part of the encryption process. The security of data depends upon the length of the key. If a weak key is used for encryption then it becomes very easy for intruder or attacker to decrypt data and read it.

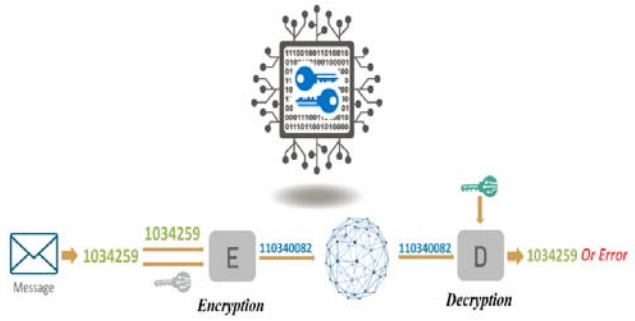

Fig 2: Encryption and Decryption [1]

Figure 2 represents how encryption and decryption are done.

In cryptography avalanche effect [4] is used to define some precise property of the encryption algorithm. Avalanche effect is defined as a slight change in plain text or even a bit of plain text gets changed then it should result in a significant change in the plain text or multiple bits of ciphertext should change. A good cryptography algorithm should always satisfy the following equation:

Avalanche > 50% [2]

This ensures that attackers should not easily predict the ciphertext from plain text or vice versa. The cryptography algorithm that does not satisfy the Avalanche effect equation and easily breached by the cryptanalyst.

A. Basic terms used in cryptography

- **Plain Text:** The human-readable message that Alice/sender wants to send to bob/receiver is called plain text. This can be a text, image, audio-video, etc.
- **Cipher Text:** The encoded message is called ciphertext. This is an inhuman unreadable form and may contain binary data, special character data, etc.
- **Algorithm or cipher:** It is a well-defined mathematical function that is used to apply cryptography.
- **Avalanche effect:** if a single bit of ciphertext gets altered then it should alteration multiple bits of a plain text message or vice versa.
- **Memory:** Memory is used to store plain text and ciphertext.

II. SYMMETRIC KEY CRYPTOGRAPHY ALGORITHMS

Cryptography algorithms have advanced over time along with the progression of computer systems and data. Symmetric key cryptography is also known as private key cryptography. It is known as a private key cryptography algorithm because a single key is used for both encryption and decryption [15]. So, there is a need to keep encryption and decryption key secret because if anyone gets access to the key, he/she can easily decrypt the data and read or alter it. Different mechanisms are used for a key generation like the Diffie-Hellman Key Exchange/Agreement algorithm which is based on some mathematical principles. Symmetric algorithms are of two types:

- **Block algorithms:** Block cipher is a method that applies to an algorithm along with a key to encrypt a block of text, rather than encrypting one bit at a time as in stream ciphers. Common block cipher algorithms are DES, TDES, AES, etc. Block cipher modes of operations have been established to remove the chances of encrypting identical blocks of plaintext the same way, the ciphertext generated from the previous block is applied to the next block as an input. A block of bits called an initialization vector (IV) is used by modes of operation to guarantee that ciphertexts remain distinct even when the same plaintext message is encrypted several times.

- **Stream cipher:** Stream Cipher is the type of encryption where the conversion of plain text is achieved by taking one byte of the plaintext at a time. In-Stream Cipher at most 8 bits could get encrypted at a time. It uses confusion principle for this conversion. The main example of a stream cipher is Vernam Cipher.

In this study, the man focus block is given in block cipher symmetric algorithms.

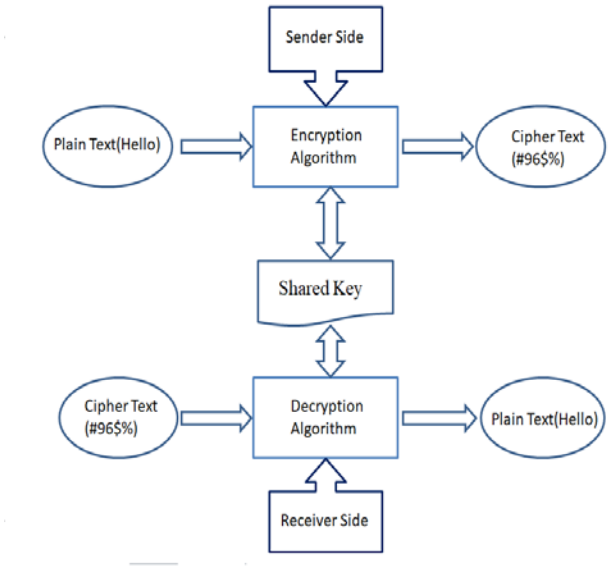

Fig 3: Encryption and Decryption process of symmetric key algorithms

Figure 3 shows how the encryption and decryption process is carried out in symmetric key algorithms. Some commonly used symmetric key encryption algorithms are shown in figure 4.

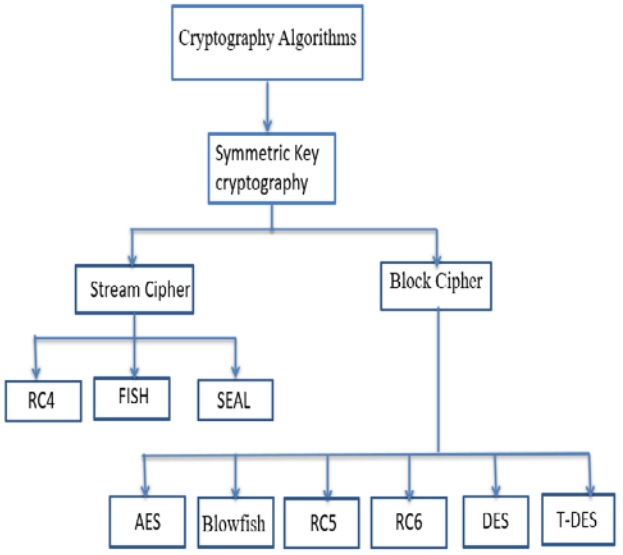

Fig 4: Types of symmetric key algorithms

Description of block ciphers symmetric algorithms are given below:

1) **DES (Data Encryption Standard**): DES was presented by Horst Feistel in IBM in the year 1972. DES is an implementation of a Feistel Cipher. It uses a 16 round Feistel structure. 64 bits of the plain text block is used. Key length is 64-bit since 8 of the 64 bits of the key are not used by the encryption algorithm, these 8 bits are reserved for parity checks which leave the key size of 56 bits.

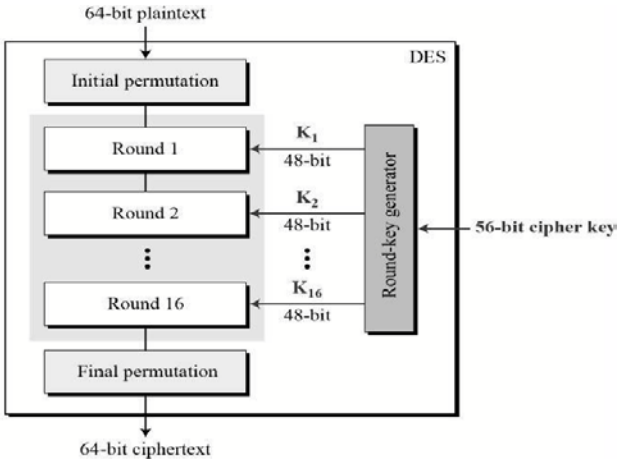

Fig 5: DES Structure [3]

Figure 5 shows the basic structure of the DES algorithm.

2) **TDES (Triple Data Encryption Standard):** In 1990 DES was very much prone to exhaustive key searches attacks which led to the existence of TDES and also known as 3DES. There are two variants of TDES known as 3-key TDES and 2-key TDES (2TDES). TDES consists of three different DES keys K1, K2, and K3. This means that the actual 3TDES key has a length of 3×56 = 168 bits [5]. The encryption-decryption process is as follows [6] −

- Encrypt the plaintext blocks key K1.
- Decrypt the output of step 1 using key K2.
- Finally, encrypt the output of step 2 using key K3.
- The output of step 3 is the ciphertext.
- The decryption of a ciphertext is an inverse process. User first decrypts using K3, then encrypt with K2, and finally decrypt with K1.

3) **AES (Advanced Encryption Standard):** it is also known as the Rijndael algorithm [7]. AES is a symmetric block cipher technique developed by NIST (National Institute of Standards and Technology) to substitute DES in 2001. It uses 10, 12 and 14 rounds of encryption depend upon key size used [8]. AES uses 128 bits of plain text block that can be split into 4 fundamental blocks of data. These parts are dealt with a line of bytes and combine a 4*4 matrix.

4) **Blowfish:** it was designed by Bruce Schneier in 1993 [9] [10]. Blowfish is a symmetric algorithm that uses a 64-bit plain text block and a variable key length of 128-448 bits. Blowfish is a free open source algorithm.

5) **RC6:** RC6 was introduced in 1997. It as a symmetric block cipher algorithm that uses a 128-bit block of plain data and it uses 3 variants of key i.e. 128, 192, and 256 bits. It uses four registers and needless rounds of encryption and decryption as compare to AES [11]. RC6 was designed to meet the expectations of AES.

III. RELATED WORK

In this section, various literature reviews of different researchers are presented.

Nadeem [12] discussed the popular secret key algorithms DES, 3DES, AES, Blowfish, and their performance was compared by encrypting input files. Java is the programing language for the implementation of these algorithms and was tested on different hardware platforms. It was concluded that Blowfish had an advantage over other algorithms. Also, it showed that AES has better performance than DES and 3DES.

Singh et al. [13] performed a comparison between the most common encryption algorithms; AES, DES, 3DES, and Blowfish in terms of security and power consumption. Experimental results of the comparison were carried out over different data types. The simulation results showed that AES has a better performance than other algorithms. AES is supposed to be a better algorithm that was compared to the original Blowfish Algorithm.

Another study carried out by **Pankaj et al. [14]**, three Algorithms like DES, AES, and BLOWFISH was compared for video encryption and decryption. Three parameters were such as time and file size. Based on experimental results it was concluded that the Blowfish algorithm consumes the least encryption time and DES consumes maximum encryption time. they also detected that the Decryption of

Blowfish and AES algorithms is better than the DES algorithm.

IV. EXPERIMENTAL METHODOLOGY AND ENVIRONMENT

For the implementation of symmetric algorithms, Java 8.0 was used because it contains inbuilt java classes for cryptography. The system used in this experiment was Intel® Core (TM) i7-7700 HQ CPU @ 2.80 GHz with 8 GB of RAM and 1TB HDD. These algorithms are evaluated according to their performance (encryption + decryption time) and security (avalanche effect) and memory need to store plaintext as well as ciphertext.

Table 1: Algorithm setting

Algorithms	Key Size	Plain text Size	No. of Rounds
DES	56	64	16
TDES	3 keys = 168	64	16
AES	256	128	14
Blowfish	448	64	N/A
RC6	256	128	N/A

Table 1 shows the key size used; block size of plain text used in the experiment. The plain text used in the experiment is the same for all the algorithms.

V. EXPERIMENTAL RESULTS AND ANALYSIS

This section shows the experimental results in the form of tables as well as graphs. Based on experimental results we will get the ideal cryptographic algorithm.

Table 2: Performance of symmetric algorithms

Algorithms	Encryption + Decryption Time (in sec)
DES	9.10
TDES	22.26
AES	3.33
Blowfish	4.97
RC6	5.21

From table 2 it is clear that AES has a better performance than other algorithms. Performance time is the execution time needed by the algorithm to perform encryption and decryption.

This performance time is static means after every iteration all algorithms need the same execution time to complete their encryption and decryption process.

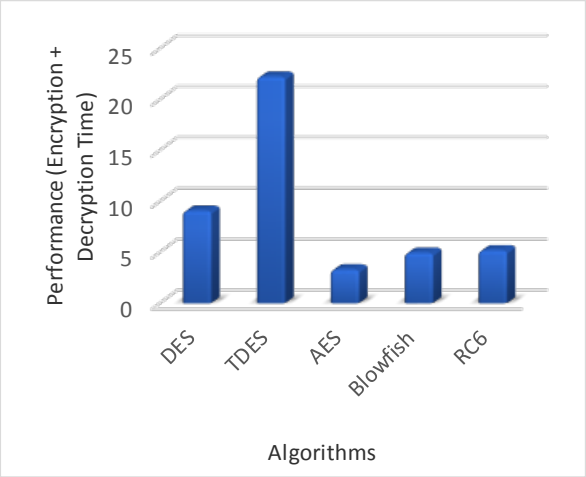

Fig 6: Performance

Figure 6 shows that AES requires less execution time (encryption + decryption time) to perform operations (encryption and decryption) whereas TDES performs very poorly as it require large time to perform its operations.

Table 3: Avalanche effect

Algorithms	Avalanche effect
DES	34.6
TDES	38.7
AES	40
Blowfish	48.35
RC6	55

Table 3 shows the Avalanche Effect when the bit of the plaintext is changed before being charted in binary codes. Avalanche Effect is calculated by counting the number of flipped bits in the ciphertext due to a 1-bit change in the original plaintext. It is clear from table 3 that the RC6 has the highest avalanche effect hence it is more secure for communication. Blowfish also have quite a satisfactory avalanche effect but not suitable for use. Formulae used to calculate the avalanche effect is:

Avalanche effect = Number of bits changed / Total number of bits (1)

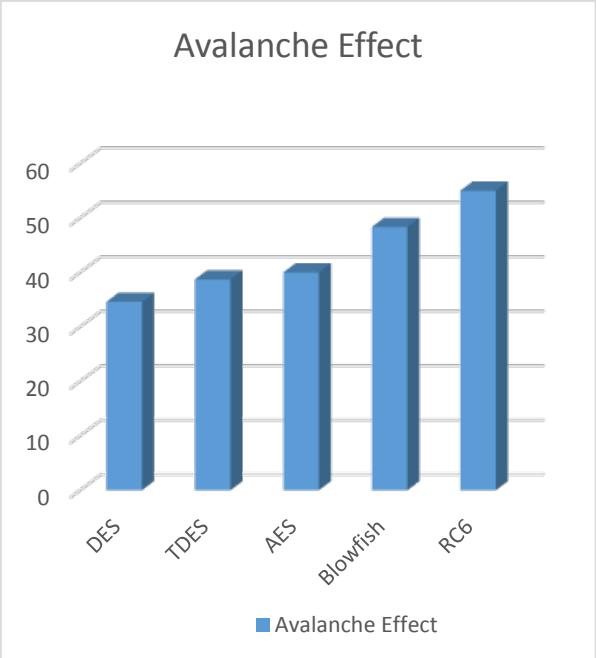

Fig 7: Avalanche effect

Figure 7 shows the analysis of the Avalanche Effect due to a one-bit change in plaintext when the key is constant. it is clear from the figure that RC6 is an ideal algorithm if security, because it has, highest avalanche effect is the main concern followed by Blowfish. The avalanche effect is calculated based on the same plaintext message by just changing one letter in the plaintext.

Table 4: Storage area used

Algorithms	Plaintext (in Bytes)	Ciphertext (in Bytes)
DES	16	16
TDES	16	48
AES	16	32
Blowfish	16	32
RC6	16	32

Table 4 presents the memory used for operations for all cryptographic techniques that we studied. It shows the disk space used by symmetric algorithms to store plaintext and ciphertext. The size of plain text is fixed i.e. 16 bytes because the same plaintext was used in each algorithm but their ciphertext size varies.

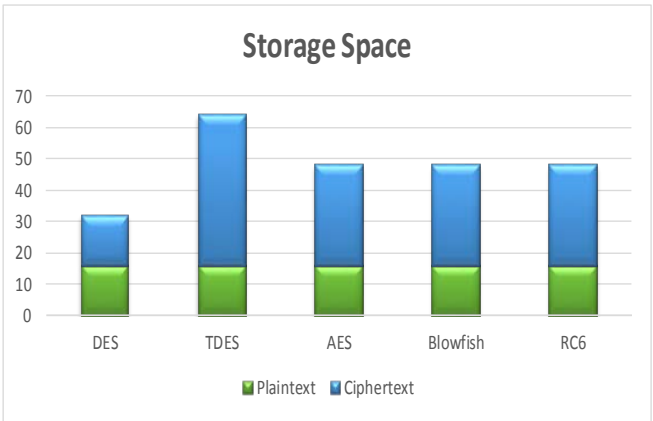

Fig 8: Disk space need to store data

From figure 8 it was clear that DES requires less storage are compared to other algorithms and TDES requires more storage area. On the other hand, AES, Blowfish, and RC6 require nearly the same storage.

VI. CONCLUSIONS AND FUTURE SCOPE

The security of data is the main concern in today's world. This work presents the comparative study of symmetric algorithms based on performance and security. The experimental results show that AES has better performance in terms of encryption and decryption time than all other algorithms. Whereas the RC6 algorithm has a better avalanche effect than other algorithms hence make it an ideal algorithm for public use. DES requires less disk space to store plaintext and ciphertext and on the other hand, Whereas TDES needs the most storage space.

In this experiment, Java is used as a programming language but in the future, one can also implement these algorithms on different programming languages like python, ruby, R, etc. While implementing in other programming languages their performance and avalanche effect values might change because the performance of algorithms can depend on various other factors.

VII. REFERENCES

[1] A. Khate, "Cryptography and Network Security," Tata McGraw Hill Education Private Limited, pp. 14-16, 2003.
[2] T. Limbong and P. D. P. Silitonga, "Testing the Classic Caesar Cipher Cryptography using MATLAB," International Journal of Engineering Research & Technology, Vol. 6, No. 2, Feb 2017.
[3] N. Tyagi and A. Ganpati, "Comparative Analysis of Symmetric Key Encryption Algorithms," International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 8, No. 4, Aug 2014.
[4] A. Kumar and N. Tiwari, "Effective Implementation and Avalanche Effect of AES", International Journal of Security, Privacy and Trust Management, Vol. 1, No. ¾, pp. 31-34, 2012.
[5] O. G. Abood and S. K. Guirguis, "A Survey on Cryptography Algorithms," International Journal of Scientific and Research Publications, Vol. 8, No. 7, July 2018.
[6] S. Pavithra and E. Ramadevi, "Study and Performance Analysis of Cryptography Algorithm," International Journal of Advanced Research in Computer Engineering & Technology, Vol. 1, No. 5, July 2012.
[7] J. Daemon and V. Rijmen, "AES Proposal: Rijndael," 1999.
[8] G. Kaur and M. Mahajan, "Analyzing Data Security for Cloud Computing Using Cryptographic Algorithms," International Journal of Engineering Research and Applications, Vol. 3, No. 5, Sept 2013.
[9] J. Thakur and N. Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis," International Journal of Emerging Technology and Advanced Engineering, Vol. 1, No. 2, Dec 2011.
[10] P. C. Mandal, "Superiority of Blowfish Algorithm," International Journal of Advanced Research in Computer Science and Software Engineering, Cryptography, Vol. 2, No. 9, Sept 2012.
[11] S. Charbhathia and S. Sharma, "A Comparative study of Rivest Cipher Algorithms," International Journal of Information and Computational Technology, Vol. 4, pp. 1831-1838, 2014.

[12] N. Aamer, "Performance Comparison of Data Encryption Algorithms", Oct 2008.
[13] G. Singh, A. Kumar and K. S. Sandha, "A Study of New Trends in Blowfish Algorithm," International Journal of Engineering Research and Applications, Vol. 1, No. 2, pp.321-326.
[14] P. Kumari, M. Bala and A. Sharma, "A Comparative Study of Symmetric Key Algorithm DES, AES and Blowfish for Video Encryption and Decryption," International Journal of Advance Engineering and Research Development, Vol. 4, No. 5, May 17.
[15] M. Marwaha, R. Bedi, A. Singh and T. Singh, "Comparative Analysis of Cryptographic Algorithms," International Journal of Advanced Engineering Technology, Vol. 4, No. 3, Sept 2013.

Web References

[1] edureka.co/blog/what-is-cryptography
Accessed on 14/08/2020 at 12:15 am
[2] Accessed on 03/03/2020 at 12:13 AM. [Online]. Available: https://www.geeksforgeeks.org/avalanche-effect-in-cryptography/
[3] https://www.tutorialspoint.com/cryptography/data_encryption_standard.html
Available Online: Accessed on 16/08/2020 at 3:30 pm