Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 5, May -2017

A Comparative Study of Symmetric Key Algorithm DES, AES and Blowfish for Video Encryption and Decryption

[1]Pankaj Kumari, [2]Manju Bala, [3]Ankush Sharma

[1]M.Tech Student , Computer science Engineering, Career Point University, Hamirpur(H.P)
[2]M.Tech Student, Computer science Engineering, Career Point University, Hamirpur(H.P)
[3]Assistant Professor, Computer science Engineering, Career Point University, Hamirpur(H.P)

Abstract- *Cryptography is "The science of protecting data" & Network security "Keeping information private and secure from unauthorized users". In cryptography encryption decryption of data is done by using secret key provide data confidentiality, data integrity and authentication[3]. The process of transforming plaintext into ciphertext is called encipherment or encryption; the reverse process of transforming ciphertext into plaintext is called decipherment or decryption. Both encipherment and decipherment are controlled by a cryptographic key.This paper performs comparative analysis of three Algorithms like DES, AES and BLOWFISH for video encryption and decryption considering certain parameters such as time and file size.*

Keywords: *Cryptography, Encryption, Decryption, DES, AES, BLOWFISH*

I. INTRODUCTION

Cryptography techniques often used to secure the data transmission and storing between user and cloud storage services. For secure communication over the public network data can be protected by the method of encryption[1]. Encryption converts that data using an encryption algorithm using the key in scrambled form. 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.

Cryptography is derived from Greek word. It has 2 parts: 'crypto' means "hidden secret" and 'graphy' means "writing". It is a study of techniques for secure communication in the presence of third parties to maintain information securities such as data integrity, confidentiality, authentication, and non-repudiation[7]. The original message, before being transformed, is called plain text. After the message is transformed, is called cipher text. An encryption algorithm transforms the plaintext into cipher text; a decryption algorithm transforms the cipher text back into plaintext. The sender uses an encryption algorithm, and the receiver uses a decryption algorithm. A cryptosystem is a collection of algorithms and associated procedures for hiding and revealing information.

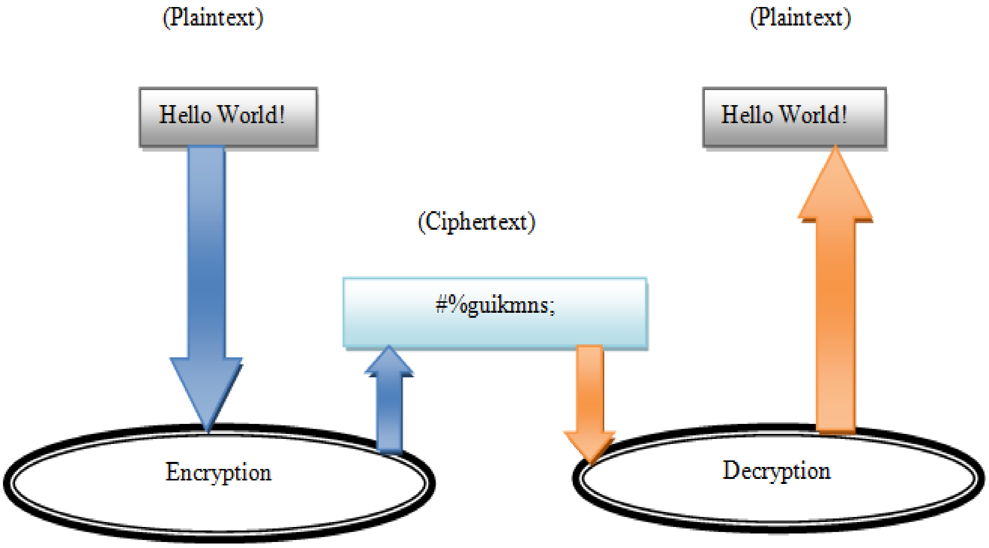

Figure1: Encryption Decryption process

A. Types of cryptography

- Symmetric Key or Secret Key Cryptography
- Asymmetric Key or Public Key Cryptography

Symmetric Key or Secret Key Cryptography

In symmetric-key cryptography, the same key is used by both parties. Sometimes is also called as single key or secret-key cryptography. It uses a single key. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and an decryption algorithm to decrypt the data [5].

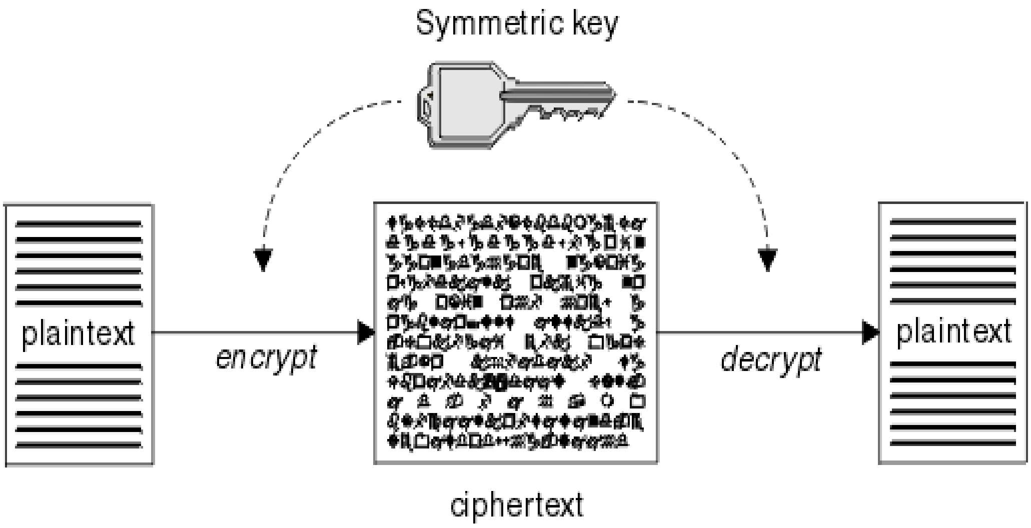

Figure 2: Symmetric Key Cryptography

Asymmetric Key Cryptography

Public key cryptography or Asymmetric-key cryptography: Asymmetric key (public key) encryption is used to solve the problem of key distribution[2]. In asymmetric key cryptography different keys are used for encryption and decryption. The two keys are used; private key and public key. For encryption public key is used and for decryption private key is used. Public key is known to public and private key is known to the user. The sender uses the public key for encryption and the receiver uses his private key for decryption [5]. The public key is available to the public; the private is available only to an individual.

Imagine sender wants to send a message to receiver. Sender uses the public key to encrypt the message. When the message is received by the receiver, the private key is used to decrypt the message.

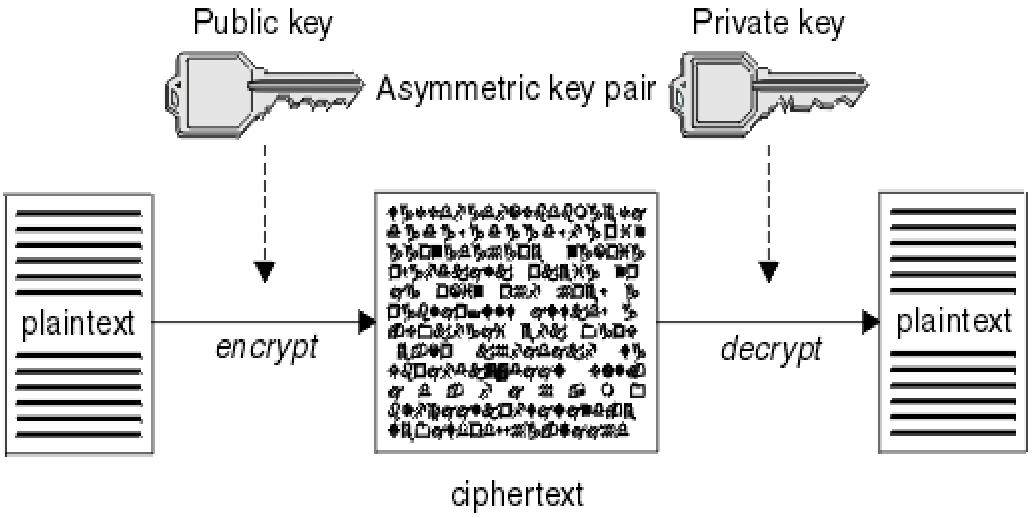

Figure 3: Asymmetric Key Cryptography

B. Need of cryptography

In today’s world cryptography has become a necessity for all the organizations. Data security is an essential component of an organization in order to keep the information safe from various competitors. It also helps to ensure the privacy of a user from others. These days passwords are not considered as reliable for this task because it is easy to guess passwords due to its short range. Moreover, if the range of password is small a brute force search can be applied to crack it. So, as to protect our data various algorithms have been designed. It helps us to securely access bank accounts, electronic transfer of funds and many more daily life applications.

II. CRYPTOGRAPHY ALGORITHMS

DES (Data Encryption Standard)

Data Encryption Standard (DES) is a symmetric key block cipher. The key length is 56 bits and block size is 64 bit length. It is vulnerable to key attack when a weak key is used. DES was found in 1972 by IBM using the data encryption algorithm. It was adopted by the government of USA as standard encryption algorithm. It began with a 64 bit key and then the NSA put a restriction to use of DES with a 56- bit key length, hence DES discards 8 bits of the 64 bit key and then uses the compressed 56 bit key derived from 64 bit key to encrypt data in block size of 64-bits .To encrypt a plaintext message, DES groups it into 64-bit blocks.DES is considering to be insecure for many applications, due to the 56-bit key size being too small. It uses the same keys for both encryption and decryption, and only operates 64 bit blocks of data at a time[4].

AES (Advance Encryption Standard)

AES is the new encryption standard recommended by NIST (National Institute of Standards and Technology) to replace DES. It was originally called Rijndael. It was selected in 1997 after a competition to select the best encryption standard.AES is a block cipher with a block length of 128 bits. The variable key length of 128,192 or 256 bits; default 256. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices brute force attack is the only effective attack known against it, in which attackers tries to test all the characters combinations to unblock the encryption[6]. It encrypts data blocks of 128 bits in 10, 12, or 14 rounds depends on the key size. It was found at least six times faster than triple DES.A replacement for DES was needed as its key size was too small, with increasing computing power, it was consider vulnerable against exhaustive key search attacks. Triple DES was designed to overcome this drawback but it was found slow.

Blowfish Algorithm

It is one of the most public domain encryption algorithms. Blowfish was designed in 1993 by Bruce Schneider as a fast alternative to existing encryption algorithms. Blowfish is a symmetric key block cipher that uses a 64 bit block size and variable key length from 32 bits to 448 bits. Blowfish has 16 rounds or less. Blowfish is a very secure cipher and to use encryption free of patents and copyrights. No attack is successful against Blowfish, although it suffers from weak keys problem. Blowfish security lies in its variable key size (32-448) providing high level of security, attempts to cryptanalysis blowfish started soon after its publication. However less cryptanalysis attempts were made on blowfish than other algorithms.

III RESULT AND ANALYSIS

The three video file of different size are used to conduct three experiments, where a comparison of three algorithms DES, AES and Blowfish is performed.

A. Evaluation Parameters

Performance of encryption algorithm is evaluated considering the following parameters.

- Encryption Time
- Decryption Time

Encryption Time

Encryption is the conversion of data into another form, called ciphertext, which cannot be easily understood by anyone except authorized parties. It may also be performed with a set of keys or passwords. The time taken to encrypt any file is called Encryption Time. Here, Encryption Time is measured in milliseconds (ms).

Evaluation of encryption time: The encryption simulation was performed on DES, AES and Blowfish algorithms had been carried on NetBeans IDE 7.1.2.The encryption simulation is probably the most fundamental type of cryptographic analysis that can be performed on the algorithms under study. This simulation is simple and standardized. In this work, the encryption simulation values are obtained for various algorithms, are shown in Figure given below:

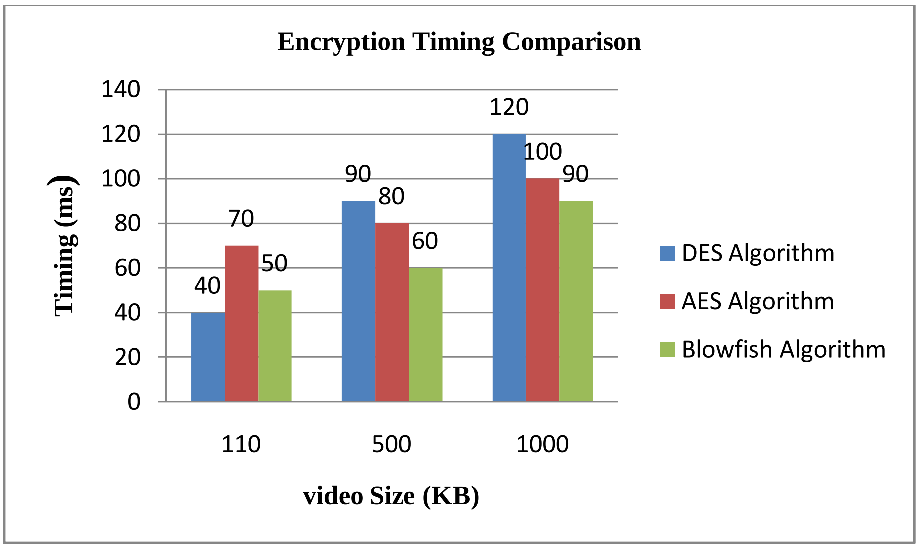

Figure 4: Shows the comparison of encryption timing in DES, AES, Blowfish algorithm and the encryption time of the Blowfish algorithm is lesser than AES and DES algorithm.

Decryption Time

Decryption is the process of transforming data that have been rendered unreadable through encryption back to its unencrypted form. During decryption, the system extracts and converts the cipher data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. It may also be performed with a set of keys or passwords. The time taken to decrypt any file is called Decryption Time. Here, Encryption Time is measured in milliseconds (ms).

Evaluation of decryption time: - The decryption simulation was performed on DES, AES and Blowfish algorithms had been carried on NetBeans IDE 7.1.2.The decryption simulation is probably the most fundamental type of cryptographic analysis that can be performed on the algorithms under study. This simulation is simple and standardized. In this work, the decryption simulation values are obtained for various algorithms, are shown in Figure given below:

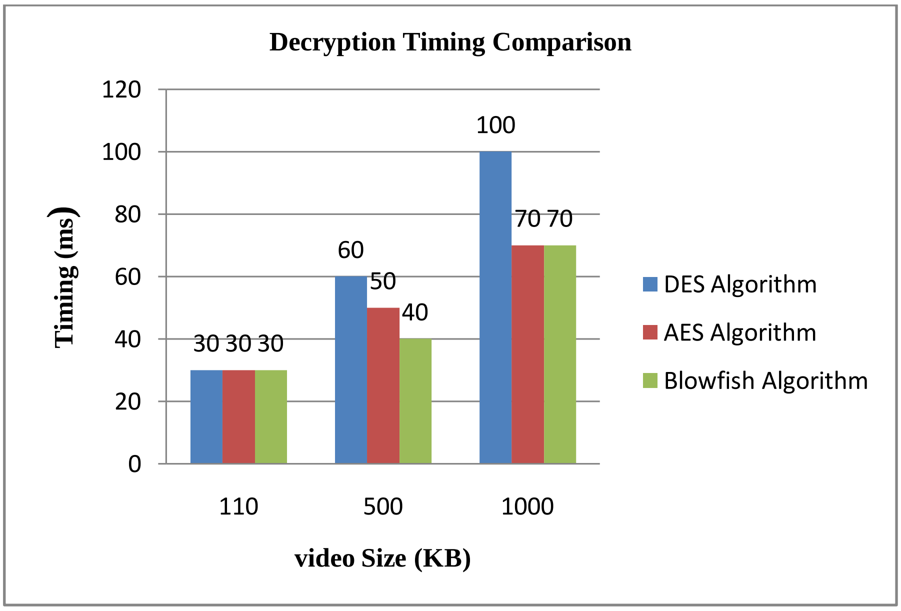

Figure 5: Shows the comparison of decryption timing in DES, AES, Blowfish algorithm and the decryption time of the Blowfish algorithm is lesser than DES algorithm.

IV. Conclusion

In cryptography, encryption and decryption algorithms plays important role in network security. In our research work, we analyzed the comparison of existing encryption techniques like DES, AES and Blowfish algorithms. Based on the video files used and the experimental result it was concluded that Blowfish algorithm consumes least encryption time and DES consume maximum encryption time. We also observed that Decryption of Blowfish and AES algorithms is better than DES algorithm. From our research work, it concluded that Blowfish algorithm is better than AES and DES algorithms.

REFERENCES

[1] *Kalyani P. Karule, and Neha V. Nagrale, "Comparative Analysis of Encryption Algorithms", International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-2, February 2016.*

[2] *Yogesh Kumar, Rajiv Munjal, and Harsh Sharma, "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures," International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.*

[3] *Nivedita Bisht, and Sapna Singh, "A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 3, March 2015, ISSN(Online) : 2319 – 8753*

[4] *M. Meena, and A. Komathi , " A Study and Comparative Analysis of Cryptographic Algorithms for Various File Format", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064*

[5] *Behrouz A. Forouzan, "Data Communication and Networking", McGraw-Hill Forouzan Networking Series, 2007.*

[6] *Simar Preet Singh, and Raman Maini, "COMPARISON OF DATA ENCRYPTION ALGORITHMS", international Journal of Computer Science and Communication ,Vol. 2, No. 1, January-June 2011, pp. 125-127*

[7] *Anjula Gupta, and Navpreet Kaur Walia, "Cryptography Algorithms", Sri Guru Granth Sahib World University, Fatehgarh Sahib, India.*