International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 10 6024 - 6026

A Comparative Case study on Different Parameters of Blowfish Algorithm with other Cryptographic Algorithms

Vaibhav Poonia
Sri Balaji College Of Engineering & Technology
Jaipur, India
vaibhavpoonia007@gmail.com

Rahul Guha
Dr. Radhakrishnan Institute Of Technology
Jaipur, India
rahul24guha@yahoo.co.in

Jai Prakash Kumawat
Sri Balaji College Of Engineering & Technology
Jaipur, India
jai_kumawat@sbss.ac.in

***Abstract*—** As we use our data of high value or confidential one then we are in need of protection. An appropriate solution is always needed to maintain the significance, accuracy & sensitivity of data. So, now in this digital era security and privacy has become an important issue. So, throughout this paper we will have a comparative study cum analysis of cryptographic algorithms like Blowfish, DES, AES, and Diffie Hellman.

Keywords- *Blowfish ,f function, AES, DES, Symetric, Asymmetric.*

*****

I. INTRODUCTION

In the 21st century people are using internet on a wide range and everyday their dependency on the internet is rapidly increasing. Even the children are using it at a very early age. But most of them are still unaware of the increasing unauthorized access and security breaches, which leaves their data or information vulnerable. Whenever they try to communicate, these problems arises. There has been tremendous advances in the digital technology and electronic information used in various sectors like - business, industries, administrations, etc. Due to these advances the risks regarding the information security has also increased. Every individual wants to have a secure exchange of information whether he is a sender or a receiver. If their information does not remain secure then it would be a great loss to both the sender and the receiver. So in order to overcome these issues cryptography is used. It provides many security techniques which helps the user to secure and protect their valuable information[1].

II. ABOUT CRYPTOGRAPHY

Cryptography is a Greek word which means hidden or secret writing. It provides us confidentiality, security and protection from security breaches[3]. A simple example of cryptography can be: Say we want to send HELLO to a person, and if we use cryptography then instead of directly sending HELLO to that person, we would convert it into something that wouldn't be recognized as the same such as @H12#. This conversion is known as Encryption.(Here, HELLO is called the Plain Text and @H12# is called the Cipher text). Now after encryption the information is sent to the recipient. But that information is useless for the recipient if it could not be converted back to the original message i.e from @H12# to HELLO and this reconversion is known as Decryption. Every Cryptographic algorithm includes both of these processes.

III. COMPARISION OF ALGORITHMS

There are two types of cryptographic algorithms namely: Symmetric algorithms and Asymmetric algorithms. In both of these algorithms key/keys are used which acts as the piece of information in determining the output of the encryption/decryption.

A. Symmetric Algorithms

In symmetric algorithms same key is used in both encryption and decryption, i.e both the sender and the receiver of the information have the same piece of information to be used in cryptography. Furthermore, symmetric algorithms can be divided into stream ciphers and block cipher. A stream cipher is used to encrypt a single bit of information at a time whereas the block cipher is used to encrypt number of bits of information as one block. Few popular symmetric algorithms are: DES, Triple DES, AES/Rijndael, RC6, Blowfish, CAST5, TEA, IDEA, Serpent, Twofish and MARS.

3.1 Overview Of Symmetric Algorithms :

3.1.1 DES

DES or Digital Encryption Standard is a symmetric block cipher algorithm which has size of 64 bits and uses 56 bit key. It was made a standard by the United States in 1977[2]. DES uses the Feistel network where the algorithms complexity increased as the number of rounds increased. For many year it was considered safe and was used in cryptography, but later in 1998 it was cracked and this leaded the way to find other algorithms.

3.1.2 Triple-DES

Triple DES is used to encrypt data three times. It uses a different key for at least one of the three passes. Triple DES has a key size of 112-168 bits. Although the working of Triple DES remained the same as DES except the three phases, yet it proved to be much stronger than (single) DES. However it was slow and due to unsatisfactory results, AES evolved.

3.1.3 Blowfish

Blowfish algorithm was designed by Bruce Schneier in 1993[4]. He made it unpatented and licence free. It also uses 64 bit block cipher but the key size became variable i.e from 32 to 448 bits. It uses Feistel network in 16 rounds and a large key dependent S-box. This algorithm proven to be invulnerable to many different attacks. The only know attack are based on weak keys.

3.1.4 IDEA

IDEA in other word known as International Data Encryption Algorithm is an encryption algorithm developed at ETH in Zurich, Switzerland[7]. It uses block cipher with key size of 128 bits. It is considered as a secure algorithm as in years many tried to find vulnerability in it but so far it is secure to those attacks. IDEA is a patented algorithm by Ascom-Tech.

3.1.5 TEA

TEA or Tiny Encryption Algorithm (TEA) was designed by David Wheeler and Roger Needham. It is a block cipher which is known for its simplicity of description and implementation, typically a few lines of code. It uses 64 bit block size with the key size of 128 bits. Many simple attacks can be prevented in it as it is based on the symmetry of rounds.

3.1.6 CAST 5

CAST is named after its developers i.e Carlisle Adams and Stafford Tavares[5]. It uses 64 bit block cipher with variable key sizes ranging from 40 to 128 bits. It works on Feistel network with prefixed 8 S-boxes.

3.1.7 AES (Rijndael)

AES or Advanced Encryption Standard is a symmetric key encryption technique which was meant to replace DES algorithm issued by the US Government's National Institute of Standards and Technology (NIST) in 1997 and completed in 2000[7]. In AES many algorithms were analyzed and among them Rijndael algorithms was finally selected as it performed on various environments and in every mode[8].

This algorithm used variable key sizes i.e 128,192 and 256 bit. With the increase in sizes the complexity and the possibility to mix the data also increased. The principle of the algorithm uses a combination of both permutation and substitution on a 4X4 matrix of bytes[9]. And there would be a prefixed number of repetitions of converting the plain text into cipher text. It does not use Feistel network like DES algorithm did.

3.1.8 AES (RC6)

RC6 algorithm was designed by Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin. It was designed to meet the requirements of the Advanced Encryption Standard (AES) competition.

It is a block cipher derived from RC5 which uses block size of 128 bits and it uses variable key size i.e 128, 192 and 256 bits. RC6 can be understood as the blend of two parallel RC5 processes as RC6 uses an extra multiplication operation in order to make the rotation dependent on every bit.

3.1.9 AES (Serpent)

Serpent is a block cipher developed by Ross Anderson, Eli Biham and Lars Knudsen. Serpent is a block cipher with block size of 128 bits and the key size use by it can vary i.e, 128, 192 or 256 bits. It uses substitution-permutation network working in 32 rounds. Serpent was also selected among other five finalists to become the new federal Advanced Encryption Standard (AES). It was ranked second in that competition. Though Rijndael algorithm was selected to form AES but Serpent provides high security due to its 32 rounds against attacks.

3.1.10 AES (Two Fish)

Twofish algorithm was designed by Bruce Schneier, John Kelsey, Chris Hall, Niels Ferguson, David Wagner and Doug Whiting which is a block cipher[13]. It uses a single key with key size variable upto 256 bits. Like Blowfish algorithm it uses Fiestel network and remains unpatented. It provides high security and is faster when used with 256 bit keys. It was also a finalist to become the new federal AES.

3.1.11 AES (MARS)

MARS algorithm was developed by Don Coppersmith. He was the developer of the DES algorithm. He presented MARS in the 1999. MARS algorithm was the fifth algorithm in the competition among the five finalists to become the new federal Advanced Encryption Standard (AES). It uses block size of 128 bits along with a variable key size ranging from 128 to 448 bits. It uses Feistel network.

3.1.11 Modified Blowfish Algorithm

In the modified Blowfish algorithm i have enhanced the Blowfish algorithm by making changes in the ‘f’ function. I have modified it by mixing the XOR and addition operators used in the original algorithm. On the basis of different parameters like Encryption Quality, Correlation Coefficients, Key Sensitivity Test and Size of Output File the results of all the tests conducted on the cases lead to a common conclusion that the security of the modified algorithm with different cases makes the original Blowfish algorithm more compact and more secure than the earlier.

B. Asymmetric Algorithms

In asymmetric algorithms two different keys are used i.e, a private key and a public key in the process of encryption and decryption. The information is encrypted with a public key and then decrypted with the private key of the recipient. Few popular asymmetric algorithms: RSA, Diffie-Hellman, Digital Signature and ElGamal.

3.2 Overview Of Symmetric Algorithms :

3.2.1 RSA

RSA is an asymmetric algorithm developed by three mathematicians namely Ronald Rivest, Adi Shamir, and Leonard Adleman[14]. It was based on the calculating the product of two large prime numbers with a supplementary value chosen as public key. The major protection provided by this algorithm was that it can easily increase the key size where ever applicable and also any key whether it is private or public can be used to encrypt and the other one used by the recipient can decrypt the information.

3.2.2 Diffie-Hellman

Diffie-Hellman algorithm was developed by Whitfield Diffie and Martin Hellman in 1976[15]. It is mainly used to exchange the keys in an unsecure network.

3.2.3 Digital Signature

Digital Signature algorithm was developed by David W. Kravitz in 1991. This algorithm uses two phases to generate keys. The first phase give an option to choose algorithm parameters that will be shared among different users. The second phase calculates both the private and the public keys for one user. It forms the basis of the Secure Sockets Layer (SSL), Secure Shell (SSH) and IPsec protocols.

3.2.4 ElGamal

ElGamal algorithm was developed in by Tehar ElGamal in 1980s [16]. It is an extension of Diffie-Helman algorithm which specifically targets at the encryption of digital signatures. The algorithm comprises of three basic components i.e a key generator, an encryption algorithm and a decryption algorithm. The algorithm provides good security as a single plaintext can be encrypted to many possible cipher texts.

IV. COMPARATIVE ANALYSIS

After analyzing the various cryptographic algorithm including both the symmetric key cryptographic algorithm and the asymmetric key cryptographic algorithms we can make comparisons among them on the basis of their usability, scalability, security and methodology. There are some flaws in symmetric algorithms such as weak keys, insecure transmission of secret key, speed, flexibility, authentication and reliability i.e. in DES, four keys for which encryption is exactly the same as decryption. This means that Original plain text can be recovered, if the encryption is applied twice with one of these weak keys. DES is very slow when implemented in software; the algorithm is best suited to implementation in hardware. Similar is the case in IDEA that involves large class of weak keys facilitating the cryptanalysis for recovering the key. DES and IDEA have the same encryption speed on. Triple DES does not always provide the extra security that might be expected making use of double and triple encryption as well as it is very slow when implemented in software as it is derived from DES and DES on software is already slow, so Triple-DES might be considered safest but slowest. In Blowfish there are certain weak key that attacks its three-round version, further it is also exposed to a differential attack against its certain variants, it is also slow in speed but much more faster than DES and IDEA.

V. CONCLUSION

The main objective of this paper is to show the comparison of among different cryptographic algorithms on the basis of their usability, scalability, security and methodology. The modified Blowfish algorithm in different cases with different parameters like Encryption Quality, Correlation Coefficients, Key Sensitivity Test and Size of Output File. In all those case we find that we have improved the Original Blowfish algorithm to some extents. The comparison of all the tests conducted above lead to common conclusion that the security of the modified algorithm with different cases makes the original Blowfish algorithm more compact and more secure than the earlier. The flexibility of the modified Blowfish algorithm is much higher than the other algorithms given in the above table.

ACKNOWLEDGMENT

Our sincere thanks to Mr. Jaiprakash Kumawat who has guided us and shared his valuable knowledge with us for the completion of this paper. We also like to thank the rest of the participants who also contributed their knowledge with us.

REFERENCES

[1] Massey, J.L, "An Introduction to Contemporary Cryptology", Proceedings of the IEEE, Special Section on Cryptography, 533-549, May 1988.
[2] Data Encryption Standard, Federal Information Processing Standard (FIPS) Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington, DC (January 1977).
[3] Text Book: Cryptography and network security, Principles and practices by William Stalling, Retrieved on 8 December 2006
[4] Bruce Schneier, "The Blowfish encryption algorithm9", Dr. Dobb's Journal of Software Tools, 19(4), p. 38, 40, 98, 99, April 1994
[5] Heys, H.M.; Tavares, E. On the Security of the CAST Encryption Algorithm, Electrical & Computer Engg.
[6] X. Lai and J. Massey. A proposal for a new block encryption standard. In Proceedings of the EUROCRYPT 90 Conference, pp. 3 89-404, 1990.
[7] AES home page may be found via http://www.nist.gov/ CryptoToolkit.
[8] J. Daemen and V. Rijmen, AES Proposal: Rijndael, AES algorithm submission, September 3, 1999, available at [1]
[9] James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, and Edward Roback, Report on the Development of the Advanced Encryption Standard (AES), Volume 106 Number 3 May– June 2001
[10] Federal Register: January 2, 1997 (Volume 62, Number 93), available at [1].
[11] Federal Register: September 12, 1997 (Volume 62, Number 177), available at [1].
[12] Federal Register: September 14, 1998 (Volume 63, Number 177), available at [1].
[13] Schneier et al., Twofish: A 128 bit Block Cipher, AES algorithm submission, June 15, 1998, available at[1]
[14] Rivest, R.L., Shamir, A., Adleman, L. "A Method for Obtaining Digtal Signatures and Public Key Cryptosystems," Communications of the ACM, 21, No. 2, 120-126 (1978).
[15] Diffie, W. and Hellman,M.E., "New Directions in Cryptography,' IEEE Transactions on Information Theory, IT-22, No. 6, 644- 654 (1976).
[16] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In Proceedings of CRYPTO 84 on Advances in cryptology.
[17] Haiyong Xie, Li Zhou, and Laxmi Bhuyan, "Architectural Analysis of Cryptographic Applications