CPUH-Research Journal: **2017,** ***2(2),*** 114-116
ISSN (Online): 2455-6076
http://www.cpuh.in/academics/academic_journals.php

Comparative Study of Cryptography Algorithms

Pankaj Kumari* & Pratibha Sharma
School of Engineering and Technology, Career Point University Hamirpur (H.P.)-176041, India
E-mail: *sankhyanikusum@gmail.com*

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. The process of encoding plain text message into cipher text message is called as encryption. The reverse process of transforming cipher text message back to plain text message is called as decryption. This paper provide a comparative study of various cryptography Algorithms like DES, AES, BLOWFISH and DIFFIE-HELLMAN based on different factors like speed, security and cost in cryptography Algorithms.

Keywords: Cryptography; encryption; BLOWFISH and DIFFIE-HELLMAN.

INTRODUCTION: 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. The message to be sent through an unreliable medium is known as plaintext, which is encrypted before sending over the medium. The encrypted message is known as cipher text, which is received at the other end of the medium and decrypted to get back the original plaintext message.

Types of Cryptography:

Symmetric Key Cryptography: When the same key is used for both encryption and decryption, then that mechanism is known as symmetric key cryptography.

Asymmetric Key Cryptography: When two different keys are used, that is one key for encryption and another key for decryption, then that mechanism is known as asymmetric key cryptography.

PURPOSE OF CRYPTOGRAPHY:

Confidentiality: The principle of confidentiality Specifies that only the sender and the intended recipient should be able to access the contents of a message.

Authentication: Authentication mechanisms help to establish proof of identities. This process ensures that the origin of the message is correctly identified.

Integrity: The integrity mechanism ensures that the contents of the message remain the same when it reaches the intended recipient as sent by the sender.

Non-repudiation: Non-repudiation does not allow the sender of a message to refute the claim of not sending the message.

Access Control: Access Control specifies and controls who can access what.

Availability: The principle of availability states that resources should be available to authorized parties all the times.

CRYPTOGRAPHY APPLICATIONS: Cryptography has found its application in more than what one can imagine. Major sectors which use cryptographic techniques include defense, government and law enforcement agencies, banking, insurance, business and industry. It has even found its way into sectors like healthcare, education, tourism and social welfare. Cryptography could be applied to text, image, audio and video based scenarios including both real time and non-real time systems.

The use of embedded cryptographic processors has spread from low-cost crypto-processors, such as smart cards used for holding decryption keys, to more modern applications, such as user authentication, identity management, e-mail, mobile communication, electronic payment schemes, digital right management and trusted computing Initiative (TCI).

LITERATURE REVIEW: Agarwal et al., had a goal of guiding the design of any encryption algorithm against unauthorized attacks. This paper provided the performance comparison between four of the commonly used encryption algorithms such as DES, Triple DES, BLOWFISH and AES. The comparison had been conducted by running different sizes of the data blocks to evaluate the speed of the encryption and decryption algorithm. From the performance analysis of these algorithms, it had been concluded that the Blowfish was the best performing algorithm under the security against unauthorized attack and speed.

Gurjeevan Singh et al. tested the performance for the algorithms. The performance matrices were throughput. The throughput of encryption time and in the case of decryption scheme was calculated. This work presented the performance evaluation of selected symmetric algorithms such as AES, 3DES, Blowfish and DES that Blowfish had better performance than other algorithms followed by AES in terms of throughput.

Secondly 3DES had least efficient of all the studied algorithms.

Turki et al. evaluated the performance of these algorithms in terms of CPU execution time. The analyzed time was the CPU execution time for generating the secret key, encryption and decryption on a 10MB file. The results showed that the Blowfish algorithm was the fastest algorithm followed by the DES algorithm then the Triple-DES algorithm. The Triple-DES algorithm was slow in its performance due to the added complexity and security it had over the DES algorithm.

Saraf et al. 2014, fast evaluation of digital data exchange occurs in recent years. Due to that security of information is much important in data storage and transmission process. Security of internet banking account passwords, email accounts password etc. requires text protection in digital media. In the same way image transmission and storage during industrial and research processes requires image protection.

The National Institute of Standards and Technology (NIST) have initiated a process to develop Federal information Processing Standard (FIPS) which should be most flexible, secure, fast and which can replace Data Encryption standard. This new standard is recognized by name Advanced Encryption Standard (AES). Features of data are depends on its types. Therefore same encryption technique cannot be used for all types of data. Images have large data size and also has real time constrain problem hence similar method cannot be used to protect images as well as text from unauthorized access. However with few variations in method AES can be used to protect image as well as text. In this project I have implemented encryption and decryption for text and image using AES.

CRYPTOGRAPHY ALGORITHMS:

A. Data Encryption Standard (DES): DES is a block encryption algorithm. It was the first encryption standard published by NIST. It is a symmetric algorithm, means same key is used for encryption and decryption. It uses 64-bit key. Out of 64 bits, 56 bits make up the independent key; 8 bits are used for error detection. The main operations are bit permutations and substitution in one round of DES. Six different permutation operations are used both in key expansion part and cipher part. Decryption of DES algorithm is similar to encryption, only the round keys are in reverse order. The output is a 64-bit block. Many attacks and methods recorded weaknesses of DES, which has made it an insecure block encryption key.

B. **Advanced Encryption Standard (AES):** AES also known as the Rijndael's algorithm is a symmetric block cipher. It was recognized that DES was not secure because of advancement in computer processing power. It encrypts data blocks of 128 bits using symmetric keys. It has a variable key length of 128, 192 or 256 bits: by default 256 is used. AES encrypts 128 bits data block into 10, 12 and 14 round according to the key size. AES can be implemented on various platforms such as small devices encryption of AES is fast and flexible. AES has been tested for many security applications. The purpose of NIST was to define a replacement for DES that can be used in non-military information security applications by US government agencies.

C. Blowfish: 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.

D. DIFFIE-HELLMAN (DH) Algorithm: It is the public key algorithm which uses discrete logarithms in a finite field. It is also known as key exchange algorithm. In this the protocol allows two users to exchange a secret key over an insecure medium without any prior secrets. Hence this algorithm is vulnerable to a Man- in –the- middle attack. When an appropriate mathematical group is used then, only this protocol is considered to be secure.

CONCLUSIONS: Cryptography algorithm is the science in secret code. A comparative study of cryptography algorithms like AES, DES, Blowfish and Diffie-Hellman analyzed that algorithm is viewed to be good in terms of security and majorly deals the encryption and decryption process for protecting the text files using the cryptography algorithms.

REFERENCES:

1. Abdul D.S., Eliminaam, Kadar H.M.A. and Hadhoud M. (2008), " Performance Evaluation of symmetric Encryption Algorithms, "*International Journal of Computer Science and Network Security*" 8, 118-125.
2. Mandal P.C. (2012), "Evaluation of performance of the symmetric key algorithms: DES, 3DES, AES and Blowfish" *Journal of Global Research in Computer Science Department of Computer Application"* 3, 67-70.
3. Agrawal M. (2012) "A Comparative Survey on Symmetric Key Encryption Techniques*" International Journal on Computer Science and Engineering*, 4, 75-80.

4. Bhanot R. and Hans R. (2005) "A Review and Comparative Analysis of Various Encryption algorithms" *International Journal of Security and Its Applications*, 9, 289-306.
5. Seth S.M. and Mishra R. (2011) "Comparative analysis of encryption algorithms for data communication", *IJCST*, 2, 86-92.
6. Zhang T.N.T. (2009) "A study of DES and Blowfish encryption algorithm", Tencon IEEE Conference.
7. Stallings W. (2005) "Cryptography and network security principles and practices. Prentice Hall.
8. Agrawal H. and Sharma M. (2010) "Implementation and analysis of various symmetric cryptosystem" *Indian Journal of science and Technology*, 3, 150-157.