ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 10, October 2014

A COMPARATIVE ANALYSIS OF CRYPTOGRAPHY ALGORITHMS

M.B.Nivetha[1], Mr.S.Sivaramakrishnan[2]

Department of Electronics and Communication, United Institute of Technology, Coimbatore, India[1,2]

Abstract: This paper is based on the analysis of the various algorithms in cryptography technique. With the fast changing technologies in today, more data are generated and transmitted. If the confidentiality of the information is very high, it should be protected. Cryptography is used to protect the personal or important data from the unauthorized people who try to access it. Cryptography is widely used by government and intelligence agencies around the world for the transmission of information. It can be either online offline. In this paper various cryptography algorithms are studied and compared.

Keywords: Cryptography, Hashing, symmetric key.

I.INTRODUCTION

Cryptography is the essential part of encrypting the important information and decrypting it to its original form. Encryption is the technique of changing the data so that it is not recognized by an unauthorized person. The encrypted information is then called cipher text. Decryption is changing cipher text back to its normal form. In addition to securing private data, it performs the security requirements for data integrity, confidentiality and authentication [8].

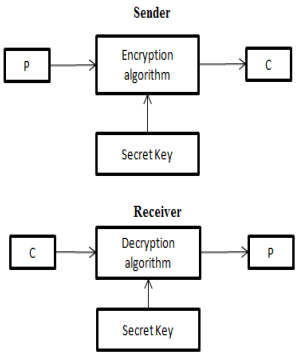
There are various cryptographic algorithms and most of all fall into two categories. They are public key system and secret key system. A shared key performs encryption and decryption in the symmetric key algorithm. The success of algorithm depends on the factors such as secret key and the distribution of the key as encryption and decryption are done using the same key. In asymmetric algorithm, private and public keys are used for encryption and decryption and it is alternatively known as public key algorithm.

Hashing is the topic in the cryptograph technique. A hash function maps a variable length message into fixed length hash value. In the recent years the mostly used hash function has been Secure Hash Algorithm (SHA). This algorithm is used in digital certificate and data integrity. Secure Hash Algorithm is a fingerprint that particulars the data and was developed as a U.S. Federal Information Processing Standard by N.I.S.T [1]. It is mainly intended for the use with digital signature applications.

II.SYMMETRIC KEY CRYTOSYSTEM

In symmetric key algorithms for cryptography, single key is present which is used for encryption and decryption. The key represents shared secret between parties which can maintain private information [7].

This mode of operation is used to encrypt longer messages than the block size. Block ciphers and stream ciphers can be contrasted. Stream cipher works on one digit at a time. The transformation varies during the encryption. A cipher block is a symmetric key cipher that operates on blocks that are the fixed length groups of bits and with an unvarying transformation.



2.1. Data Encryption Standard (DES)

The most of the encryption techniques are based on the DES. It is a block cipher text. It encrypts data in 64 bits blocks of size each. The input of DES is 64 bits of plain text, which produces cipher text of 64

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 10, October 2014

bits. 56 bit key is used in DES. By permuting 56 bit key, 48 bit sub keys are formed [9]. There are three modes of DES encryption, Electronic Code Book mode, Chain Block Coding and Cipher Feedback. In ECB mode, each 64 bit block is encrypted individually [13].

2.2. Triple DES

As the name implies, in the Triple DES key size of DES is extended by applying the algorithm three times in series with three different keys. So the combined key size is 168 bits that is 3 times of 56, beyond the reach of brute-force. Triple DES takes a data of 64 bit and performs encryption, decryption and again encryption.

2.3. Advanced Encryption Standard (AES)

AES is the approved standard replacing DES for wide range of applications. It is a symmetric block of cipher. AES uses symmetric keys of 128,192 or 256 bits to encrypt data of 128 bits [11]. The only effective attack known against this algorithm is the Brute force attack [2]. AES encryption is fast and flexible.

2.4. BLOWFISH

It is also a symmetric block cipher. It can be effectively used for encryption and protection of data. Blowfish is a variable length key and block cipher of 64 bit. The variable length key with the size from 32 bits to 448 bits is taken for securing data [3]. The size of the block is 64 bits and the key can be any length but up to 448 bits. There are two parts. They are key expansion part and data encryption part. It is one of the fastest block ciphers and it is unpatented and license free. It is available free for all users. Blowfish suffers from weak keys problem [10].

2.5. RC2

RC2 is a symmetric block cipher and operates on 64 bit quantities. RC2 uses variable size key. But the best key size is 128 bit. It can be used in all modes that DES can be used. RC2 encrypts data in blocks of 64 bits and this expands single message by up to 8 bytes.

2.6. RC6

RC6 has the same structure as that of the RC5. RC6 uses XOR operations, data dependent rotations and modular addition [2]. The block size is of 128 bits and supports three different key sizes of 128,192 and 256 bits. RC6 is the interweaving of two parallel RC5 encryption processes. RC6 uses an extra multiplication operation that is not present in RC5. This helps to produce the dependency of the rotation on every bit of the word.

III. HASH FUNCTION CRYPTOSYSTEM

For computing a strong representation of electronic data the Secure Hash Standard specifies four secure hash algorithms. They are SHA-1, SHA-256, SHA-384 and SHA-512. When the input for SHA-1 and SHA-256 is given as the data less than 2^{64} bits and for SHA-384 and SHA-512 the data is less than 2^{128} bits, the result is called as a message digest. Depending on the algorithm the length of the message digests varies from160 to 512 bits. These algorithms are used with digital signature algorithms and keyed-hash message authentication codes or generation of random numbers. There are three uses of hashes used in cryptography.

Digital signature:

The hash is transmitted along with the message. Thus recipient can compare outputs by hashing the message. The message that is send to the recipient can be proved to be not tampered by signing the hash before sending [4].

Storage of passwords:

Instead of storing the user's password, the system will store the hash of the password. When a user enters his password, the hash is generated and hash match test is performed by comparing the stored and generated hash. If the hash match test is positive and both the hash matches, then there exists a match of passwords match.

Integrity checking:

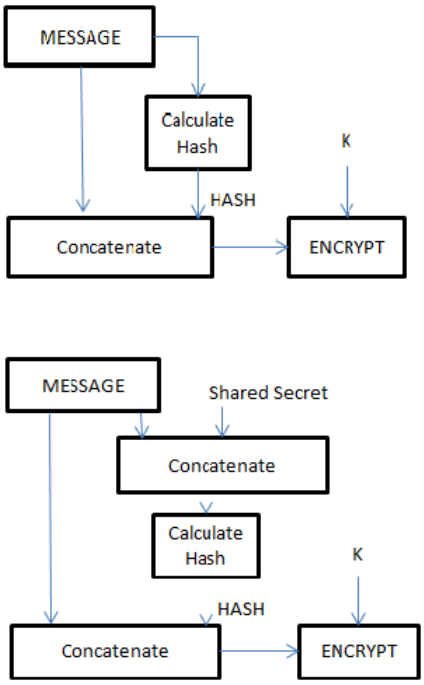
The sender can hash the file before the file has been send to the recipient. Then the received file is hashed

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 10, October 2014

and checked by the recipient. This is done to ensure that the files have not been corrupted or modified.

The four hash algorithms are called secure because, it is infeasible to produce a message for the given message digest. They also sound to be more secure because it is tedious to find the two different messages with the same message digest. Different message digest computed as any changes occurs in message with high probability. When both digital signature and the secure hash algorithm are used together or keyed-hash message authentication algorithm this will result in a verification failure. Algorithms can be explained as the following two stages such as preprocessing and hash computation.



Preprocessing have the following steps: the message is padded, the padded message is parsed into m bit blocks and then the hash is computed by setting initialization values [5]. The hash computation

V.SHA 256

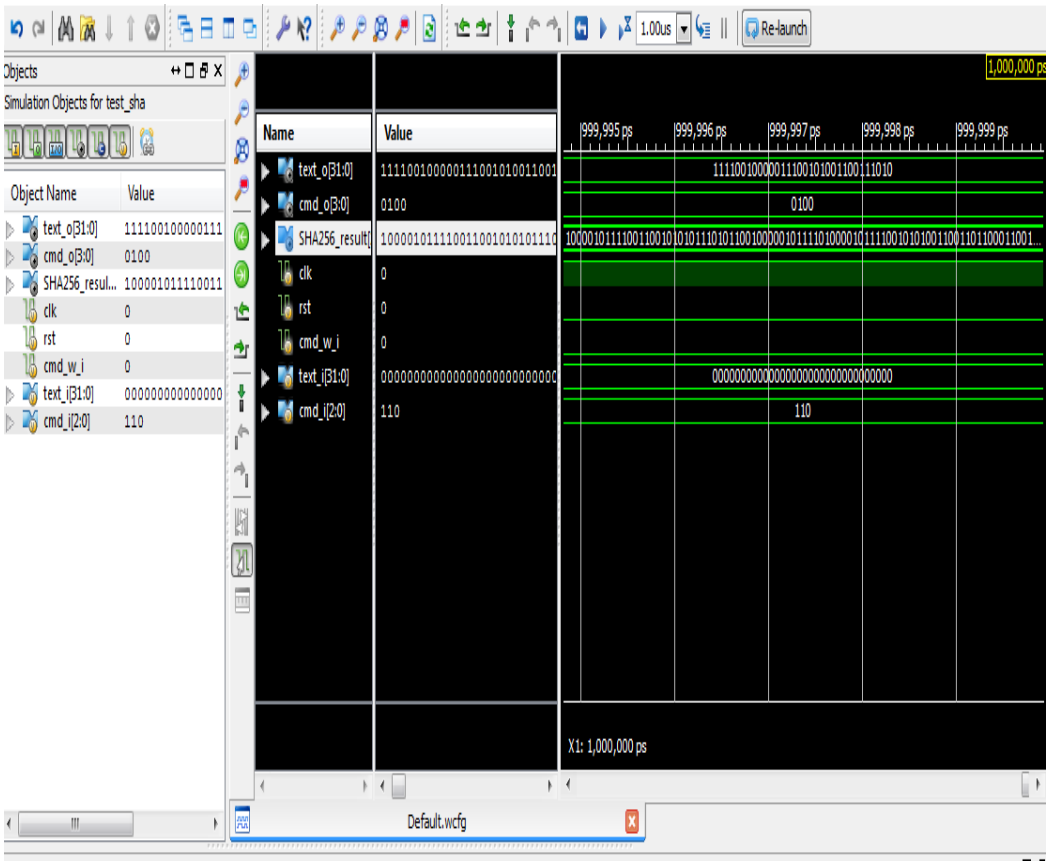
computes a message schedule from the padded message. This can be used to generate the series of hash values by using the functions, constants and word operations along with it. This value is used to determine the message digest [15].

IV.COMPARISION OF ALGORITHMS

The commonly used block ciphers are Advance Encryption Standard (AES) and Triple DES. DES encrypts data in 64 bit block size using 56 bit key. It can have 72 quadrillion possibilities. Considering today's technology it is not vulnerable to brute force attack. DES is no longer appropriate for security. At that time, 3DES was introduced which is more secure as compared with DES. 3DES has three different key and this has key length of 168 bits [14]. Another type of 3DES called two-key is less secure with key size of 112 bits. This is mainly used in electronic payments industry. The disadvantage of this method is that it takes three times as much CPU power as compare with its predecessor. AES outperforms 3DES both in software and hardware and this replace the 3DES algorithm. AES is the modified version of Rijndael algorithm. AES have larger block size and longer keys. This ensures more security. The block size is fixed that is 128 bit and key size is 128, 192 and 256 [6]. This algorithm is more flexible. The size of the key and block varies from 128 bits to 256 bits. To overcome this RC6 was introduced. The design of RC6 is developed over RC5 [13]. Depending on the number of bits provided for the data being hashed the four SHA algorithms are differed. This is related to the message digest length. The algorithm also depends on the size of blocks and words used during hashing. SHA-1 uses a sequence of 32 bit words - K0, K1 up to K63. SHA-384 and SHA-512 uses the eighty constant 64 bit words from K0, K1 up to K79. Hash computation is performed to get the hash value.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 10, October 2014



The algorithms have been analyzed and the operation is seen in detail. From the analysis it has been found that SHA 256 is the more secure one when compared to other algorithm. The operation of the SHA 256 is executed and the result is obtained as shown above. The text is given as input and the SHA 256 result is examined. The result consists of 256 bits which undergoes 64 rounds. When compared with the other SHA algorithms it has reduced number of rounds and increased number of output bits. This reduces the complexity by reducing the number of rounds and increases the security by increasing the number of output bits.

VI.CONCLUSION

This paper presents an analysis of selected encryption algorithms. The output of the SHA256 has been given. The various algorithms analyzed are AES, DES, 3DES, RC6, Blowfish, RC2 and SHA. Here the algorithms are studied in depth and they are analyzed with the key parameters. The output of the SHA 256 is obtained and analyzed to have the output bits of length 256 which provides high security with less complexity due to reduced rounds.

REFERENCES

[1] Piyush Gupta et al, "A Comparative Analysis of SHA and MD5 Algorithm", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014, 4492-4495.
[2] Milind Mathur, Ayush Kesarwani, "Comparison between Des, 3des, Rc2, Rc6, Blowfish And Aes" Proceedings of National Conference on New Horizons in IT - NCNHIT 2013.
[3]http://pocketbrief.net/related/BlowfishEncryption.pdf, "Blowfish Algorithm".
[4]http://www.asd.gov.au/publications/csocprotect/sha-1_deprecated.htm, "Information security for government levels".
[5]http://luizfirmino.blogspot.com/2011/04/secure-hash-algorithm-sha-1.html, "Cyber defence : Secure Hash Algorithm".
[6]http://blogs.msdn.com/b/ace_team/archive/2007/
[7] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall , 2005,PP. 58-309 .
[8] Atul Kahate, "Cryptography and Network Security", Tata McGraw-Hill publishing company,New Delhi,2008.
[9] "A Performance Comparison of Data Encryption Algorithms," IEEE [Information and Communication Technologies, 2005. ICICT 2005. First International Conference ,2006-02-27, PP.84- 89.
[10]S.Z.S.Idrus,S.A.Aljunid,S.M.Asi, "Performance Analysis of Encryption Algorithms Text Length Size on Web Browsers," IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, January 2008 ,PP 20-25.
[11] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard,"Dr. Dobb's Journal, March 2001,PP. 137-139.
[12] Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength Against Attacks. "IBM Journal of Research and Development, May 1994.
[13] Hardjono, "Security In Wireless LANS And MANS," Artech House Publishers 2005.
[14] How-Shen Chang, "International Data Encryption Algorithm",2004
[15] Shasi Mehlrotra seth, Rajan Mishra — Comparative Analysis of Encryption Algorithms For Data Communication‖, IJCST Vol. 2, Issue 2, June 2011.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 10, October 2014

BIOGRAPHIES

M.B.Nivetha received Bachelor of Engineering degree in Electronics and Communication Engineering from Sri Shakthi Institute of Engineering and Technology, Coimbatore. Currently she is doing Master of Engineering degree in VLSI Design at United Institute of Technology, Coimbatore. Her area of interest lies in the field of Networking and VLSI Design.

Mr.S.Sivaramakrishnan received Bachelor of Engineering degree in Electronics and Communication Engineering from Coimbatore Institute of Engineering and Technology. He received Masters in Communication Systems from Kumaraguru College of Technology. Currently he is an Assistant Professor at United Institute of Technology, Coimbatore and doing PhD at PSG College of Technology, Coimbatore. His area of interest lies in the field of Wireless networks, Embedded System and VLSI Design.