Comparative Study of Hash and MAC Algorithms for Cryptography

Premanand Patel*, Manisha Yadav**, Deepika Verma**,
* Research Scholar and** Assistant Professor
Department of Electronics and Communication Engineering
Institute of Engineering and Technology, Dr. Ram Manohar Lohia Avadh University, Ayodhya,U.P.

Abstract –Multicast is a type of group communication that plays very vital role in present communication technologies. Multicasting is a kind of group communication where the security is main concern. Cryptography is basically oriented from computer science which is used Encryption and Decryption techniques for securing messages that are sent via insecure channel from sender and receiver. In internet era, security is very much necessary for group communication aspects. A number of cryptographic techniques are developed for achieving secure communication. we have initially survey some of the more popular and interesting algorithms currently in use. Some techniques use key and some are the keyless techniques. So, it is the good area of the research for comparative study of key and keyless techniques that are to be used. This paper focuses mainly on the comparative study of the Hash and MAC algorithms used for encryption in cryptography.

Index Terms – Cryptography, Multicast,Hash function, Algorithm, Key, keyless, MAC algorithm, Encryption

1. INTRODUCTION

Cryptography plays very important rule in today's era of group communication over internet. If someone is sending any message to other person there should be assurance that right message is delivering to the receiver side.

According to William Stallings *"Cryptography is branch of cryptology dealing with the design of algorithms for encryption and decryption, intended to ensure the secrecy and/or authenticity of messages".*

Cryptography came because of the four fundamental problems that are exists during communication process. They are Integrity Control, Security, Non-Repudiation and Authentication[1].

Multicasting is a very necessary for the present-day scenario because all work done is going through the group of peoples. Main example is the video conferencing of any informative session via online platform like Zoom, google meet, Microsoft Teams etc. There are different cryptographic techniques that are to be used for such kind of secure communication.

Many more algorithms are to be developed and are in developing phase for the secure group communication aspects. We have to see the different algorithms with respect to the different parameter that are based on the cryptographic goals. In this paper our main focus is based on the different Hash function algorithm that are to be used for secure multicasting communication.

2. GOAL OF CRYPTOGRAPHY

We have to main concern with the different goal of the cryptography that are to be used. In short it is called the CIA (Confidentiality, Integrity and Availability).

1. **Confidentiality-** It is related to following two points-
   1a. Privacy: Users will control the related information with them and stored and collected by whom and to whom that message can be disclosed.
   1b. Data Confidentiality: It is assured that the personal data is unavailable to unapproved candidates/users.
2. **Integrity-** Integrity will cover following two points-
   2a. System Integrity: We have to assure that our system done its purposeful function in an unaltered way.
   2b. Data Integrity: It ensure that programs and related information are modified in defined and authorized way.
3. **Availability-** It ensure that systems work quickly and service is not opposed to authorized users.

3. *DIFFERENT ENCRPTION TECHNIQUES*

Cryptographic techniques are to be categorized in different types. Some are based on the key and some are type of keyless techniques that are to be used. In fig. we can see the different classification for the cryptographic techniques. Mainly we will focus on the hash function that are to be used via key and keyless too.

Cryptography

1. **Symmetric 2. Asymmetric 3. Hash function**
   1. **Symmetric- Classical (Transposition and Substitution) and Modern (Stream and Block)**
   2. **Asymmetric**
   3. **Hash function (3a. Keyless Hash 3b. Keyed Hash (MAC))**

The different examples of the algorithms are to be mentioned in the below table.

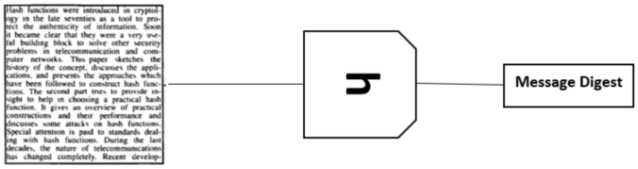
Table 1: Different types of Cryptography

Cryptography						
Symmetric (Example: DES, AES, RC2, RC4, RC6, Blowfish etc)				**Asymmetric (Ex: RSA, DH, ECC etc)**	**Hash (Whirlpool, SHA, MD5 etc)**	
Classical		**Modern**			**Keyless Hash function**	**MAC (with symmetric key)**
Transposition	**Substitution**	**Stream**	**Block**			

4. HASHING FUNCTION

Hash function is used for making short length code for some input data. The short length code also called fingerprints are unique. The other name for fingerprints is Message digest. The 160 bits are common choice for this code.

The input of hash function is message and it produce an output called as hash code, hash value, hash-result or simply hash. In other words, we can say that the hash function H converts input file of different length to specified length. This process of applying hash function is called hashing [2].



Hash functions were introduced in cryptology in the late seventies as a tool to protect the authenticity of information. Soon it became clear that they were a very useful building block to solve other security problems in telecommunication and computer networks. This paper sketches the history of the concept, discusses the applications, and presents the approaches which have been followed to construct hash functions. The second part tries to provide insight to help in choosing a practical hash function. It gives an overview of practical constructions and their performance and discusses some attacks on hash functions. Special attention is paid to standards dealing with hash functions. During the last decades, the nature of telecommunications has changed completely. Recent develop-

Fig 1: Basic Hash function

A hash function is of four different aspects (X,Y,K,h) where the following condition are met-

1. X is a group of possible strings
2. Y is finite group of possible message combination (message digests)
3. K is the keyset, is a finite combination of possible key used
4. For each keyset there can be a hash function h_K [3].

An excellent hash function has following characteristics-

1. Predetermined in nature meaning that the same input combination gives the same hash value.
2. The hash function is fast for any message.
3. One sided means it is computationally impractical to produce a specific input combination from its hash value except by testing all possible combinations in the allotted message sets.
4. The hash value should change for a little modification to a message. Generated new and old message digests are uncorrelated.
5. This property is called Collision property, it said that it is not solvable by calculation to get different combination of messages with alike hash values [4].

A hash function accepts random input combinations and produces definite size of output. Hash function is a basis for cryptographic explanation. MD family and SHA families are the most commonly used hash functions. It is also called message digest and it is one way type of encryption technique. It is a keyless encryption technique and produce the fixed length of hash value or message digest. It is generally used to ensure that the input file has not been altered by an unauthorized user or virus. This function has commonly used by many operating systems to encrypt passwords. Specially, Hash functions provide a measure of the integrity of an input data. [5].

In present day, families of MD and SHA are main cryptographic hash functions. MD is basically Message Digest and SHA is Secure Hash Algorithm [6].

4.1. Different Hash function

Secure Hash Algorithm (SHA)

SHA is basically used for the federal purpose. It is mentioned in National Institute of Standards and Technology (NIST), article number FIPS 180-4. It recognizes seven cryptographic functions [7-8].

Initial discovered SHA are called SHA version 0 (SHA-0). After SHA-0, in 1995, SHA-1 introduced. SHA-1 characteristics and design is similar to MD-4. The length of message digest for SHA-1 is 160 bits. Different hash values are introduced in the year 2002 with 256,384 and 512. These algorithms are collectively called SHA-2. SHA-2 is introduced by National Security Agency. The version of SHA-2 with 224 bits are introduced in 2008. SHA-3 was introduced by NIST in year 2007 with updated algorithmic features [9].

MD family

MD stands Message Digest. MD4 is discovered by Ronald Rivest of MIT, MD5 is improved variety of MD4. In MD5, the input file is length of 512 bit that is ahead converted into sixteen, 32-bit sub block sizes. The output is a group of four, 32-bits blocks that makes hash value of 128-bits [12-13].

MD2 is also designed by Ronald Rivest with 128 bits hash value. It is used for PEM protocols [14].

Table 2: Comparative study for SHA2 vs SHA 3 [10-11]

Different Variant of SHA	Parameters		
	Different Versions	Size of the Block	Operation performed
SHA 2	SHA 512	1024	And, Xor, Rot, Add, Or, Shr
SHA 2	SHA 384	1024	And, Xor, Rot, Add, Or, Shr
SHA 2	SHA 256	512	And, Xor, Rot, Add, Or, Shr
SHA 2	SHA 224	512	And, Xor, Rot, Add, Or, Shr
SHA 3	SHA 512	576	And, Xor, Rot, Not
SHA 3	SHA 384	832	And, Xor, Rot, Not
SHA 3	SHA 256	1088	And, Xor, Rot, Not
SHA 3	SHA 224	1152	And, Xor, Rot, Not

HAVAL

HAVAL is mainly one way hash function that will transform the random length of input combination to definite length of message digest. HAVAL is basically revised of MD5 with some modification. The message digest length is 128,160,192, 224 and 256-bits combinations. It has 3 to 5 rounds and each of which are 16 steps. For a comparative purpose with MD5 the HAVAL is 60% faster with 3 round and 15% faster with 4 rounds [15].

Whirlpool

The hash function whirlpool, designed by Belgian born Voncent Rijmen and a Brazilian based cryptographer Paulo Barreto. Whirlpool was accredited by NESSIE (New Europeon Schemes for Signatures, Integrity and Encryption). It uses the block cipher for compression scheme. Block cipher is basically based on the cipher text, key and some algorithms [16].

Whirlpool has 512-bits hash code length. Block cipher is used for both hardware and software implementation. AES algorithm is used for block cipher [17-18].

Table 3: Comparative study for MD4 and MD5

Parameters	MD4	MD5
Year	1990 by Ronald Rivest of MIT	1991 by Ronald Rivest of MIT, Strengthen version of MD4
Rounds	Three round Compress function	Four round Compress function
Hash value	128 bit	128 bits
Speed	Fast	Slow
Design	Less Conservative	More Conservative
Constant used	Fixed constant in each round	Additive constant in each round

5. MAC ALGORITHM

This technique is based on the concept that if there are two parties that are communicating, let as assume X and Y, both will share a key, say K, that is common. Whenever X will send the message to Y, it figures out the MAC of the message and key K.

MAC = F (K, G)

where-

G = Combination of Input messages
F = MAC function
K = secret key
MAC = Message Authentication Code

The input combination of message sent with MAC function from X to Y, the receiver Y perform the same function that is performed by the sender X using key K and produce the newly MAC. The derived MAC will be done comparison with the calculated MAC. If the derived MAC and calculated MAC is same, we can conclude that there is no modification in the input message and message is coming from so called sender. If m bit MAC is used then there are 2^m possible MAC functions and using a k bit key we have 2^k combination of keys. We will get 2^{10} combinations of keys with 10-bit key.

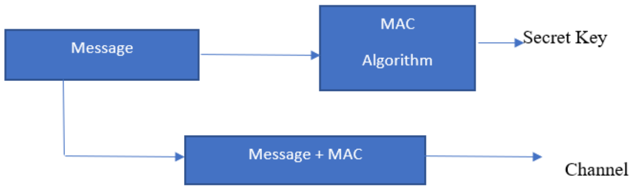


Fig 2: Message Authentication Code (MAC)

Different types of MACs are available. MAC based on Hash function is called HMAC. CMAC (Cipher Based Message Authentication Code), GMAC (Galois/Counter Mode) and DAA (Data Authentication Algorithms) are based on block ciphers. MAC is based on symmetric key algorithm means it uses only one key for encryption and decryption process. Other terms used include "Integrity Check Value" or "cryptographic checksum". For MAC function we will take the message and add some MAC with algorithms that are to be used with cryptographic secret key [20].

5.1. DIFFERENT MAC ALGORITHMS

HMAC

To find out MACs different types of algorithms are used. For calculation of the MAC, the Hash-based Message Authentication Code (HMAC) uses hash function [21].

Data Authentication Algorithm (DAA)

DAA is basically use AES algorithm. It is widely used from years. It is based on both FIPS (Federal Information Processing Standards) publication and an ANSI (American National Standards Institute) standard. The DAA algorithm is described with the help of Cipher Block Chaining (CBC) mode of operation [22].

Cipher Based Message Authentication Code (CMAC)

CMAC is validated by NIST (National Institute of standards and Technology). It uses Cipher Block Chaining (CBC) mode for symmetric block cipher. CMAC uses block cipher algorithm [23]

GMAC

Basically, GMAC is one of the forms of GCM (Galois/Counter Mode) algorithm. Its construction involves GHASH hash function. It is used for data encryption with additional data authentication. With only authenticity of data this model is called GMAC [24]. Fastest MAC algorithms are based on universal hashing UMAC-VMAC. In this, key is used mostly once.

6. COMPARATIVE STUDY OF HASH FUNCTION AND MAC ALGORITHM

As we have seen the different Hash and MAC cryptographic algorithms with various versions. We have seen the different properties for the covered algorithms. Every type has its own advantages and drawbacks that we have seen. We have also done the comparative study of some hash algorithms that have discovered. As a comparative sense we have to see the different parameters that are to be the basics for the cryptography in the modern-day multicast communication aspects.

Cryptographic parameters can be compared by the security goals they fulfil-

- **Integrity-** Receiver must be confident that the input message is not altered?
- **Authentication-** Receiver must assure that the message came from the sender end?
- **Non-repudiation-** If the message is sending from receiver to any third user, then the third user must assure that the input is came from the sender end?

The hash function is used to assurance of the integrity of data and MAC gives assurance of integrity and authentication. Hash function is generated from the input file without external input, we will get the something that can be applied to check if the message got any alter during the process of sending. A MAC uses the cryptographic key and hash is keyless.

Basically, the implementation of hash function is based on the definite length code called message digest or hash code that is converted from block of data can say any document, file and program etc. Hash code will alter with any modification in input message. Hash function is mainly used for data integrity.

Table 4: Comparative study for Hash function and MAC

Parameters	Hash function	MAC
Integrity	Yes	Yes
Keys Used	None	Yes (Cryptographic Symmetric Keys)
Non-Repudiation	No	No
Authentication	No	Yes
Different Examples	SHA and variants, MD and variants, HAVAL, Whirlpool etc	HMAC, DAA, CMAC, GMAC etc

7. CONCLUSION

In this paper we have discussed the different cryptographic aspect that are to be used for multicast communication perspectives. We have seen the different categorization of the Hash function with added to MAC algorithm. We have also done a comparative study of the Hash function that is keyless and MAC algorithm that are based on the symmetric key and part of hash function. The comparison is done on the basis of different cryptographic parameters.

Many more different cryptographic algorithms are also invented for the modern era of IoT, basically they all are called light weight cryptographic algorithm. There is more space for research related to the modern cryptography.

REFERENCES

[1] William Stallings, "Cryptography and Network Security, Principles and Practice", Global Edition (2017, Pearson)

[2] B Preneel, "Cryptographic Hash function", in European Transactions on Telecommunications, Wiley Online Library, 1994, pp. 431-448

[3] Douglas R. Stinson, "Discrete Mathematics and Its Applications" Cryptography, Theory and Practice (2005, Chapman and Hall_CRC)

[4] John F. Dooley, "History of Cryptography and Cryptanalysis, Codes, Ciphers, and Their Algorithms" (2018, Springer)

[5] Prashant P. Pittalia, "A Comparative Study of Hash Algorithms in Cryptography", International Journal of Computer Science and Mobile Computing, Vol.8, Issue.6, June- 2019, pp. 147-152

[6] Kleppmann, Martin, Designing Data-Intensive Applications: The Big Ideas Behind Reliable, Scalable, and Maintainable Systems (1 ed.). O'Reilly Media.

[7] "NIST releases SHA-3 cryptographic hash standard," 2018. Accessed: Jan. 13, 2018. [Online]. Available: https://www.nist.gov/news-events/news/ 2015/08/nist-releases-sha-3-crypt%ographic-hash-standard

[8] "Secure hash standard (SHS)," 2017. Accessed: Oct. 4, 2018. [Online]. Available: https://csrc.nist.gov/publications/detail/fips/180/4/final

[9] "NSA," 2018. Accessed: Jan. 13, 2018. [Online]. Available: https://www. nsa.gov/

[10] Fuqin Wang, Yijiang Chen, Ruochen Wang, Akindipe Olusegun Francis, Bugingo Emmanuel, Wei Zhengand Jinjun Chen, "An Experimental Investigation Into the Hash Functions Used in Blockchains" IEEE Transactions on Engineering Management, vol 67, Issue.4, pp. 1404-1424.

[11] P.S. Murvay and B. Groza, "Performance evaluation of SHA-2 standard vs. SHA-3 finalists on two freescale platforms," Int. J. Secur. Softw. Eng., Oct. 2013, vol. 4, no. 4, pp. 1–24.

[12] H. Dobbertin, "Cryptanalysis of MD4", Fast Software Encryption, LNCS 1039, D., Springer-Verlag, 1996, pp. 53-69.

[13] H. Dobbertin, "Cryptanalysis of MD5 compress", rump session of EurocrZpt'96.

[14] M. Stevens, "Fast Collision Attacks on MD5", IACR crptology ePrint Archieve, 2006, p. 104.

[15] Y. Zheng, J. Pieprzyk, and J. Seberry, "HAVAL—A One–Way Hashing Algorithm with Variable Length of Output," Advances in Crytology—AUSCRYPT '92 Proceedings, Springer–Verlag, 1993, pp. 83–104.

[16] William Stallings, "The Whirlpool Secure Hash Function", Taylor and Francis Group, 2006

[17] Black, J., P. Rogaway, and T. Shrimpton, "Black-Box Analysis of the Block-Cipher Based Hash Function Constructions from PGV", Proceedings, Advances in Cryptology— CRYPTO 002, New York: Springer-Verlag, pp. 320–335.

[18] Preneel, B., R. Govaerta, and J. Vandewalle, "Hash Functions Based on Block Ciphers: A Synthetic Approach", Proceedings, Advances in Cryptology—CRYPTO 093. New York: Springer-Verlag, pp. 368–378.

[19] Bruce Schneier, "Applied Cryptography, Protocols, Algorithms, and Source Code in C" (1995, Wiley)

[20] Menezes A.J., Oorschot P.C., Vanstone S.A, "Handbook of Applied Cryptography" 1996.

[21] NIST, "Federal Information Processing Standards Publication (FIPS 198-1). The Keyed-Hash Message Authentication Code (HMAC)," http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1 final.pdf, July 2008.

[22] Bellare, M.; Kilian, J.; and Rogaway, P., "The Security of the Cipher Block Chaining Message Authentication Code" Journal of Computer and System Sciences, December 2000, vol 61, issue 3, pp. 362-399

[23] NIST, "NIST Special Publication 800-38B - Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication," http://csrc.nist.gov/publications/nistpubs/800-38B/SP 800-38B.pdf, May 2005.

[24] NIST, "NIST Special Publication 800-38D - Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," http://csrc.nist.gov/publications/nistpubs/800- 38D/SP-800-38D.pdf, November 2007.

Authors

Premanand Patel, born in Raigarh, Chhattisgarh, India, in 1987. He received the B.E. degree in Electronics & Telecommunication from the Kirodimal Institute of Technology, Raigarh, India, in 2009. Presently he is working as Lecturer, Electronics Engineering, SBP GP Azamgarh comes under Department of Technical Education Uttar Pradesh.Currently pursuing his M.Tech degree from IET Ayodhya, Dr. Ram Manohar Lohia Avadh University, Ayodhya. His research interest includes Cryptography, Multicast Communication and IoT.

Manisha Yadav is working as an assistant professor in department of ECE, IETAyodhya. She has diploma in Electronics(2009), India, in 2009. B.Tech in ECE(2012), M.Tech in Wireless Communication (2014) and currently pursuing Ph.D from Dr. APJAl Abdul Kalam Technical University,Lucknow.Her researchinterestincludesWirelessMulticastCommunication Communication, Network Security and sensornetwork etc.**(CORRESPONDING AUTHOR)**

Deepika Verma is a Ph.D candidate in Physics and Electronics department of Dr.RML Avadh University, Ayodhya. She has a B.tech degree in ECE from BBDNITM,Lucknow and M.tech in ECE from I.E.T Dr. RMLAU Ayodhya. Her research interest includes 5G, Wireless Communication, IoT based Biomedical Applications and AI.