Comparative Study of Hash and MAC Algorithms for Cryptography

Premanand Patel*, Mantsha Yadav**, Deeptka Verma**,
* Research Scholar and** Assistant Professor
Department of Electronics and Communitcation 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 rule 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. COAL 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.