Comparative Study of MD5 and SHA Security Algorithm

ABHISHEK.B.N
STUDENT
JAIN DEEMED TO BE
UNIVERSITY
BANGALORE

UMARANI.C
ASSOCIATE PROFESSOR
JAIN DEEMED TO BE
UNIVERSITY
BANGALORE

Abstract

Security algorithms enables secure communication between two parties in the presence of a third-Party or a snooper. It guarantees the recipient of the message of the genuineness of the received message, protects the message against the unauthorized release of the message content by the third party, only authorized users can access the data. MD5 and (SHA), cryptographic hash algorithms are one-way hashing functions which are easier to compute/convert but are much harder to reverse and would take around millions of years to compute the authentic message content. This research paper analyses the two hash algorithms, MD5 and SHA, using various key features. Their features have also been highlighted in order to provide a better comparison picture so that they can understand which algorithm has superseded the other.

General Terms:

Security, cryptography, hash algorithm

Keywords:

MD5, SHA, hash

1. INTRODUCTION

In the current scenario, where the number of internet users is increasing, internet has become the primary medium of communication. In the field of data communication, a user's data gets the greatest priority. The network usage must be reliable, data integrity, data authentication, non- repudiation, data confidentiality should made available at all times. Encryption must be used for secure communication in the presence of third party or eavesdroppers. It provides all the aspects of information security such as data confidentiality, data integrity, authentication.
Cryptography is a process of making a piece of information indecipherable to attackers and available only to the intended recipients. So, the data can be easily transferred securely without the threat of information being compromised.

The popular methods of cryptography are:

1. ***Symmetric-key cryptosystem****, the same public key is used by both the sender to send and the receiver to retrieve the message, that is, the same key is used both for encryption and decryption.*

2. ***Asymmetric-key cryptosystem****, in which a private key and a public key is used for encryption and decryption. The message being sent uses the public key to encrypt the message and the message being received uses the private key to decrypt the message.*

*3. **Hybrid cryptosystem**:*

Combines both methods (symmetric and asymmetric-key cryptosystems). Asymmetric distributes a key, which is also known as a session key. Symmetric provides bulk encryption. SSL can be one of the examples for the hybrid cryptosystem.

The shortcomings of a symmetric-key algorithm:

- *Key-exchange becomes a problem.*
- *Problem occurs/will occur when someone gets their hands on a symmetric key because they can decrypt everything encrypted with the same key.*
- *As the number of users using the secret key increases, the consequences of this damage increases.*

The shortcomings of an asymmetric-key algorithm:

- *Since asymmetric-keys are many times longer than the secret-key in symmetric-key algorithm, asymmetric-keys are more computationally costly.*
- *They are susceptible to attacks.*
- *It is also vulnerable to Man in the middle attack (MITM).*
- *Public key systems use third parties to certify the reliability of public keys. The MD or message digest hash functions were proposed as an alternative to fulfill all the aspects of information security because of the following features:*
- *Calculating the hash of any message is very easy.*
- *Two different messages can never have the same hash.*

• Changes made in the message will also have changes in the hash value.
The two cryptographic hashing algorithms known are:

- *MD5*
- Security Hash Algorithm (SHA).

1.1 MD5

The message digest algorithm was given by Professor Ronald Rivest in 1991 to be a secure replacement for the MD4 algorithm.

- *Input: message of arbitrary length.*
- *Output: 128-bit hash code.*

The input is first broken up into chunks of 512-bit blocks in the MD5. If the message of the input does not meet the requirements, the message is padded so that its length is divisible by 512. The output is a hash value.

1.2 Secure Hash Algorithm (SHA)

- ***SHA-0**:*

SHA-0 was removed soon after publication as it had a flaw and was replaced by SHA-1.

- ***SHA-1***:

It produces a 160-bit message digest. This was developed by the National Security Agency (NSA) to be a component of the Digital Signature Algorithm.

- ***SHA-2***:

It was also formulated by the NSA. SHA-2 consists of similar hash functions, with different block sizes, SHA-256 and SHA-512, they only differ in the word size; SHA-256 uses 32-bit words where SHA-512 uses 64-bit words.

- ***SHA-3***:

It was proposed in 2012. SHA-3 supports the same hash lengths as SHA-2 and also has some improvements.

1.2.1 SHA-1

- *Input: message of arbitrary length.*
- *Output: 160-bit hash code.*
- *The input message is broken into chunks of 512-bit block's (sixteen 32-bitwords). If the input message is not an integer multiple of 512-bit blocks, the message is padded so that its length is divisible by 512.*
- *The padding: Pad the message with a 1 followed by 0's until the final block has 448 bits and append the size of the original message as an unsigned 64-bit integer.*

2. Why SHA is better than MD5?

MD5
MD5 normally processes smaller strings storing passwords and other sensitive data in databases.

Hash collisions*: These occur at any time when two given inputs produce the same hash output.*

- *Hash collisions are produced easily in MD5.*
- *MD5 provides no security against collisions.*

SHA

- *SHA algorithm collisions are not easy to produce.*
- *SHA-256, which has many more operations than SHA-1, with a similar structure, is currently still unbroken.*
- *MD5 cannot be implemented in existing technology at exceeding rates than the existing, i.e., at rates in excess of 256 Mbps in hardware, or 86 Mbps in software. SHA can be implemented in existing technology and is also feasible.*
- *SHA1 appears to be much more secure. Attacks on SHA1 are much less serious than the attacks on MD5.*

These days modern hash functions, like SHA256 is used rather than MD5 or SHA1 on which there are known attacks and is even better.

***Reverse hashing**: Validation of the data to check if it has been altered, a new hash is generated with the received data and is matched with the original hash. It is nearly not possible to generate a hash for an altered set of data that matches the hash of the original.*

3.CONCLUSION AND FUTURE SCOPE

This paper proposes that the SHA algorithms should be given more importance in comparison to MD5. SHA algorithms' performance surpasses the MD5 cryptographic hash algorithm functions.
In the near future, new researches would be propounded proposing the same conclusion and more information would be amassed which could be used as a driving factor in the technological testing of the cryptographic hashing algorithms. This would result in the ultimate approved superiority of SHA algorithms above all cryptographic hash algorithms.

4. References:

[1] Wikipedia, the free encyclopaedia.

[2] https://security.stackexchange.com/ questions/19705/is-sha1-better-than-md5-only-because-it-generates-a-hash-of-160-bits

[3] William Stalling7, Fourth Edition, Cryptography and Network Security (Various Hash Algorithms).

[4] http://science.opposingviews.com/ advantages-disadvantages-symmetric-key-encryption-2609.html

[5] https://techdifferences.net/difference-between-md5-and-sha-1/