Don Bosco Institute of Technology
Department of Information Technology

Security Lab (ITL502) Assignment : 2

Name : Lavena Babu   Roll No.: 29   Date: 15/10/22

Q1. Understand cryptographic hash function and its applications.

1.) HMAC

Definition :-

HMAC algorithm stands for Hashed or Hash-based Message Authentication Code. It is a result of work done on developing a MAC derived from cryptographic hash functions. HMAC is a great resistance towards cryptanalysis attacks as it uses the Hashing concept twice. HMAC consists of twin benefits of Hashing and MAC and thus is more secure than any other authentication code. RFC 2104 has issued HMAC, and HMAC has been made compulsory to implement in IP security. The FIPS 198 NIST standard has also issued HMAC.

2.) CMAC

Definition :-

Cipher-based message authentication codes (or CMACs) are a tool for calculating message authentication codes using a block cipher coupled with a secret key. You can use an CMAC to verify both the integrity and authenticity of a message

3.) MD5

Definition :-

The MD5 (message-digest algorithm) hashing algorithm is a one-way cryptographic function that accepts a message of any length as input and returns as output a fixed-length digest value to be used for authenticating the original message. The MD5 hash function was originally designed for use as a secure cryptographic hash algorithm for authenticating digital signatures. But MD5 has been deprecated for uses other than as a noncryptographic checksum to verify data integrity and detect unintentional data corruption.

4.) SHA256 AND SHA512

SHA 256

Definition :-
A cryptographic hash (sometimes called 'digest') is a kind of 'signature' for a text or a data file.SHA-2 (Secure Hash Algorithm 2), of which SHA-256 is a part, is one of the most popular hash algorithms around. A cryptographic hash, also often referred to as a "digest", "fingerprint" or "signature", is an almost perfectly unique string of characters that is generated from a separate piece of input text. SHA-256 generates a 256-bit (32-byte) signature.

Applications
SHA-256 is useful in so many circumstances! It's a fast and secure hash function, here are some of the most common ways that it's used:

SHA516

Definition :-
This algorithm is commonly used for email addresses hashing, password hashing, and digital record verification. SHA-512 is also used in blockchain technology, with the most notable example being the BitShares network.In this article, we explore the origins of SHA-512 and discuss how the algorithm has been used by BitShares as well other prominent blockchain projects. Lastly, we'll look at a few examples of non-blockchain applications and examine how SHA-512 compares to the SHA-256 algorithm.

References:
1. https://www.geeksforgeeks.org/hmac-algorithm-in-computer-network/
2. https://cryptography.io/en/latest/hazmat/primitives/mac/cmac/
3. https://www.geeksforgeeks.org/what-is-the-md5-algorithm/