Unit – 05: Cryptographic Hash Functions

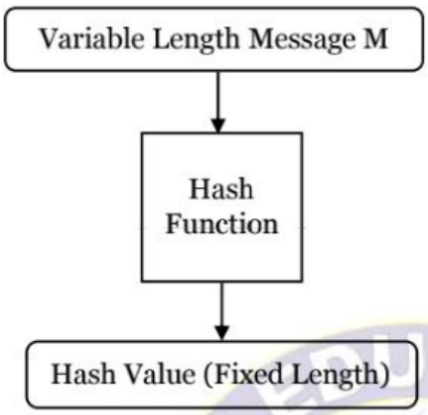
- Hashing schemes SHA- family,
- MAC,
- Digital Signature RSA El Gomel,
- DSS DSA,
- Authentication Protocols,
- applications Kerberos,
- X.509 Directory services

Questions to be discussed:

1. What are Cryptographic Hash Functions?
2. What is digital signature? What are the benefits of digital signatures?
3. Write the difference between RSA algorithm and DSA.
4. Write short notes on:
   a. Message Digest(MD)
   b. MAC
   c. Kerberos.

What are Cryptographic Hash Functions?

- A cryptographic hash function is a mathematical function used in cryptography.
- A hash functions take inputs of variable lengths to return outputs of a fixed length.
- It converts a numerical input value into another compressed numerical value.
- The values returned by a hash function are called message digest(MD) or simply hash values.
- The hash is much smaller than the input data, hence hash functions are called compression functions.



Popular Cryptographic Hash Function:

There are many cryptographic hash algorithms:

1. Message Digest (MD)
2. Secure Hash Algorithm (SHA)

Message Digest (MD):

- MD stands for message digest.
- It is a 128-bit hash function.
- It is a popular cryptographic hash function.
- The MD family comprises of hash functions MD2, MD4, MD5 and MD6.
- MD5 digests have been widely used in the software world to provide assurance about integrity of transferred file.

Secure Hash Algorithm (SHA):

- The SHA stands for "Secure Hash Algorithm".
- The SHA is a cryptographic hash function.
- Family of SHA comprise of four SHA algorithms; SHA-0, SHA-1, SHA-2, and SHA-3.
- The original version is SHA-0 is a 160-bit hash function.
- It was published by the National Institute of Standards and Technology (NIST) in 1993.
- It had few weaknesses and did not become very popular.
- Later in 1995, SHA-1 was designed to correct alleged weaknesses of SHA-0.

MAC:

- MAC stands for message authentication code.
- A MAC ensures the transmitted message was not modified during transmission.
- A MAC is sometimes referred to as a *tag* because of the way it is added to the message it is verifying.
- MAC is also referred to as Cryptographic Checksum.
- It is similar to Message Digest (MD) except that it uses the symmetric key cryptography process to authenticate a message.

MAC = C (K, M), where K is a shared secret key and M is a message to be authenticated.

What is a digital signature?

- A digital signature is an authentication mechanism that allows the sender to attach an electronic code with the message in order to ensure its authenticity and integrity.
- This electronic code acts as the signature of the sender and, hence, is named digital signature.
- In 1976, Whitfield Diffie and Martin Hellman first described the notion of a digital signature.
- The first instance of digital signature to be implemented In 1977, by RSA(Rivest - Shamir – Adleman).
- It is an electronic, encrypted, stamp of authentication for electronic documents.
- A signature confirms that the information originated from the signer and has not been altered.
- It is a mathematical technique used to validate the authenticity and integrity of a digital document.
- Digital signatures are based on public key cryptography, also known as asymmetric cryptography.

What are the benefits of digital signatures?

Digital signatures offer the following benefits:

- Security
- Timestamping.
- Globally accepted and legally compliant.
- Time savings.
- Cost savings.
- Traceability.

DSS:

- DSS stands for Digital Signature Standard.
- It was introduced by the National Institute of Standards and Technology (NIST) in 1994.
- It was first proposed in 1991 and revised in 1993.
- DSS used SHA to create digital signatures.

DSA:

- DSA stand for Digital Signature Algorithm.
- It is used for digital signature and its verification.
- It is based on mathematical concept of modular exponentiation and discrete logarithm.
- It was developed by National Institute of Standards and Technology (NIST) in 1991.

Difference between RSA algorithm and DSA:

RSA	DSA
It is a cryptosystem algorithm.	It is digital signature algorithm.
It is used for secure data transmission.	It is used for digital signature and its verification.
It was developed in 1977.	While it was developed in 1991.
It was developed by Rivest, Shamir & Adleman.	It was developed by NIST.
It is faster than DSA in encryption.	While it is slower in encryption.
It is slower in decryption.	While it is faster in decryption.
It is best suited for verification and encryption.	It is best suited for signing in and decryption.

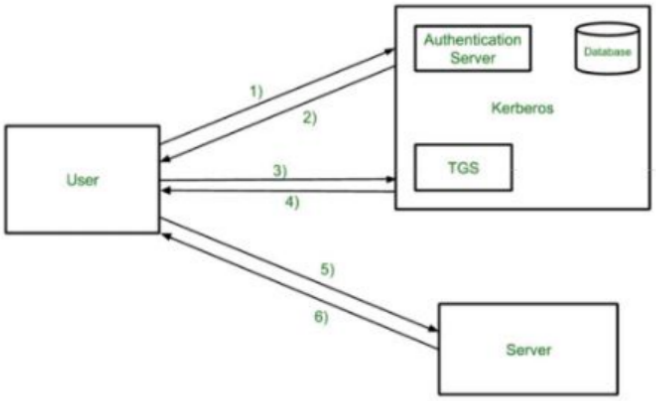
Authentication Protocols in Digital Signature:

Some authentication protocols are:

1. Kerberos.
2. LDAP (Lightweight Directory Access Protocol).
3. SAML (Security Assertion Markup Language)
4. RADIUS (Remote Authentication Dial-In User Service).

Kerberos:

- Kerberos is a protocol that helps in network authentication.
- It provides a centralized authentication server.
- Its main function is to authenticate users to servers and servers to users.
- In Kerberos Authentication server and database is used for client authentication.



Some advantages of Kerberos:

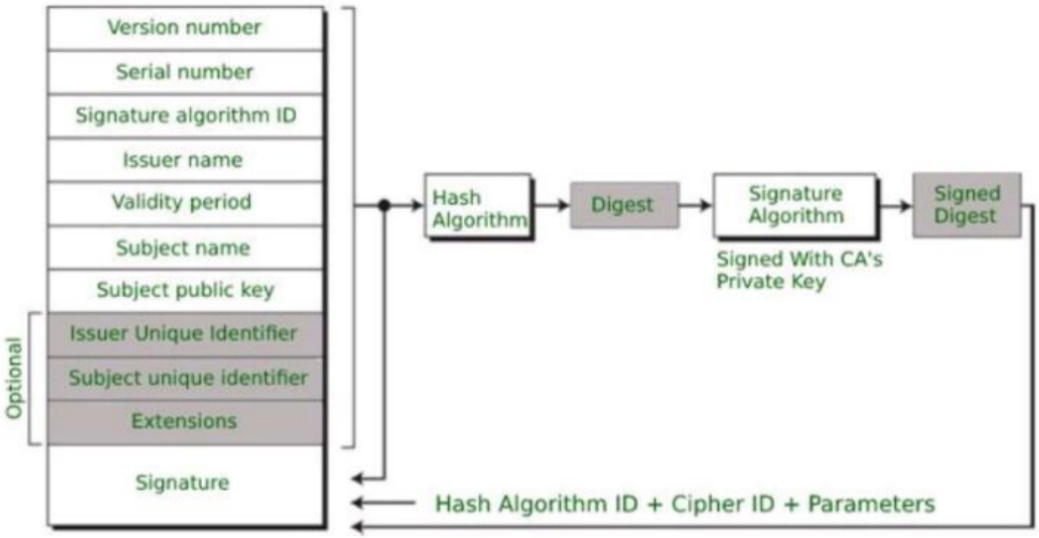
- It supports various operating systems.
- The authentication key is shared much efficiently than public sharing.

Some disadvantages of Kerberos:

- It is used only to authenticate clients and services used by them.
- It shows vulnerability to soft or weak passwords.

X.509 Authentication Service:

- X.509 is a digital certificate.
- It is built by widely trusted standard known as ITU(International Telecommunication Union).
- X.509 digital certificate is a certificate-based authentication security framework that can be used for providing secure transaction processing and private information.
- These are primarily used for handling the security and identity in computer networking and internet-based communications.



Applications of X.509 Authentication Service Certificate:

Many protocols depend on X.509 and it has many applications, some of them are given below:

- Document signing and Digital signature
- Web server security with the help of TLS/SSL certificates
- Email certificates
- Code signing
- Digital Identities