Define Source repudiation and Destination repudiation Source repudiation is the Denial of transmission of message by source. Destination repudiation is the Denial of receipt of message by destination..
Define Masquerade. Masquerade is the insertion of messages into the network from a fraudulent source. This includes the creation of messages by an opponent that are purported to come from an authorized entity. Also included are fraudulent acknowledgments of message receipt or nonreceipt by someone other than the message recipient
Define Timing modification. Timing modification is the Delay or replay of messages. In a connection-oriented application, an entire session or sequence of messages could be a replay of some previous valid session, or individual messages in the sequence could be delayed or replayed. In a connectionless application, an individual message (e.g., datagram) could be delayed or replayed.
Define Hash function (APRIL/ MAY 2018) A function that maps a message of any length into a fixed length hash value, which serves as the authenticator
Differentiate Message Authentication Code and Hash function. (DEC 2016) In MAC, a public function of the message and a secret key are used to produce a fixed length authenticator. A hash function accepts a variable size
message as input and produces a fixed size output (hash code) which is similar to MAC. But hash code does not use a key.
What you meant by MAC? **MAC is Message Authentication Code. It is a function of message and secret key which produce a fixed length value called as MAC.** **T=MAC(K,M)** **where M is a variable-length message, K is a secret key shared only by sender and receiver, and MAC(K,M) is the fixed-length authenticator.**
List out the attack on MAC. • **Brute-force attacks** • **Cryptanalysis.**
What do you mean by one way property in hash function? (APR2011, NOV2012) **An algorithm that turns messages or text into a fixed string of digits, usually for security or data management purposes. The "one way" means that it's nearly impossible to derive the original text from the string. A one-way hash function is used to create digital signatures, which in turn identify and authenticate the sender and message of a digitally distributed message.**

Define Replay Attack. (NOV2011)
Replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IPpacket substitution

What is meant by Message Authentication?
Message Authentication is a mechanism or service used to verify the integrity of a message. Message authentication assures that data received are exactly as sent by (i.e., contain no modification, insertion, deletion, or replay) and that the purported identity of the sender is valid.

Define Digital signature.
A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. Typically the signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message

What are the properties of Digital Signature?
The digital signature must have the following properties:
It must verify the author and the date and time of the signature. It must authenticate the contents at the time of the signature. It must be verifiable by third parties, to resolve disputes

List out the attacks related to Digital Signature.
Key-only attack:

- **Known message attack**
- **Generic chosen message attack**
- **Directed chosen message attack**
- **Adaptive chosen message attack**

Mention the signature function in DSS ? (NOV/DEC2017)
The hash function used in the DSS standard is specified in the Secure Hash Standard (SHS), which are the specifications for the Secure Hash Algorithm (SHA).

Define Generic chosen message attack
If A is the sender and C is the attacker. Then C chooses a list of messages before attempting to breaks A's signature scheme, independent of A's public key. C then obtains from A valid signatures for the chosen messages. The attack is generic, because it does not depend on A's public key; the same attack is used against everyone.

Define Universal forgery
If A is the sender and C is the attacker. Then C finds an efficient signing algorithm that provides an equivalent way of constructing signatures on arbitrary messages.

Define Existential forgery
If A is the sender and C is the attacker. Then C forges a signature for at least one message. C has no control over the message. Consequently, this forgery may only be a minor nuisance to A.

What are the two approaches of Digital Signature? (NOV2012)

- **RSA Approach**
- **DSS Approach**

How is the security of MAC expressed? (NOV /DEC 2017)

MACs do not provide the property of non-repudiation offered by signatures specifically in the case of a network-wide shared secret key: any user who can verify a MAC is also capable of generating MACs for other messages. In contrast, a digital signature is generated using the private key of a key pair, which is public-key cryptography. Since this private key is only accessible to its holder, a digital signature proves that a document was signed by none other than that holder. Thus, digital signatures do offer non-repudiation

How Digital signature differs from authentication protocols? (APR/ MAY 2018)

A digital signature is a mathematical scheme for presenting the authenticity of digital messages or documents.

A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message, and that the message was not altered in transit.

An authentication protocol is a type of computer communications protocol or cryptographic protocol specifically designed for transfer of authentication data between two entities. It allows the receiving entity to authenticate the connecting entity (e.g. Client connecting to a Server) as well as authenticate itself to the connecting entity (Server to a client) by declaring the type of information needed for
authentication as well as syntax

List out some hash algorithm.

- **MD5 (Message Digest version 5) algorithm.**
- **SHA_1 (Secure Hash Algorithm).**
- **RIPEMD_160 algorithm**

What is the role of compression function in hash function? (APR 2017)

The hash algorithm involves repeated use of a compression function f, that takes two inputs and produce a n-bit output. At the start of hashing the chaining variable has an initial value that is specified as part of the algorithm. The final value of the chaining variable is the hash value usually b>n; hence the term compression