1. **Hash functions** are mathematical algorithms that generate a message summary or digest (sometimes called a fingerprint) to confirm the identity of a specific message and to confirm that there have not been any changes to the content.

Because they are used in password verification systems to confirm the identity of the user.

2. A sender is an entity in a two-party communication which is the legitimatem transmitter of information.

A receiver is an entity in a two-party communication which is the intended recipient of information.

An adversary is an entity in a two-party communication which is neither the sender nor receiver, and which tries to defeat the information security service being provided between the sender and receiver.

3. An encryption scheme consists of a set $\{Ee : e \in K\}$ of encryption transformations and a corresponding set $\{Dd : d \in K\}$ of decryption transformations with the property that for each e K there is a unique key $d \in K$ such that $Dd = E_2^{-1}$; that is, $Dd (Ee (m)) = m$ for all $m \in M$. An encryption scheme is sometimes referred to as a cipher.

To construct an encryption scheme requires one to select a message space *M*, a ciphertext space *C*, a key space *K*, a set of encryption transformations $\{Ee : e \in K\}$ and a corresponding set of decryption transformations $\{Dd : d \in K\}$

4. MAC: Message Authentication Code

DES: Data Encryption Standard

PKI: Public Key Infrastructure

UDP: User Datagram Protocol

DSS: Digital Signature Standard

SHS: Secure Hash Standard