# Identification and authentication

* Identification: the ability to identify uniquely a user of a system or an application that is running in the system.
* Authentication: the ability to prove that a user or application is genuinely who that person or what that application claims to be.

## Non-repudiation

To prove that a particular message is associated with a particular individual

Can provide proof of origin and proof of delivery components.

## Authorization

Limiting access to only authorized users and their applications. Preventing the unauthorized use of a resource.

## Auditing

Auditing is the process of recording and checking events to detect whether any unexpected or unauthorized activity has taken place or attempts to perform such activity.

## Confidentiality

Protects sensitive information from unauthorized disclosure. When sensitive data is stored locally, access control mechanisms may be sufficient to protect it. If greater security is required, the data can be encrypted.

## Data integrity

Checks whether there has been unauthorized modification of data.

## Cryptography

The process of converting readable plaintext into unreadable ciphertext form.

Process of encrypting the message from the sender (encipherment), transmitting the ciphertext to the receiver, and converting the ciphertext back to its plaintext form (decryption).

* Cipher algorithm used to encrypt and decrypt text.
* Key – parameters that guide a cipher
* Cryptanalysis – process of decrypting a message without knowing the cipher or key
* DES, 3DES, AES, public/private keys
* Hash functions

## Message Digest

A fixed size numeric representation of the contents of a message, computed by a hash function. A message digest can be encrypted, forming a digital signature. Hash function must meet two criteria: The hash function must be one way, it must not be possible to reverse the function. Also, it must be computationally infeasible to find two messages that hash to the same digest.

A message digest created using a secret symmetric key is known as a Message Authentication Code (MAC), because it can provide assurance that the message has not been modified

## Digital Certificate

* Owner’s public key
* Owner’s distinguished name
* The distinguished name of the CA that issued the certificate
* The date from which the certificate is valid
* The expiry date of the certificate
* The version number of the certificate data format
* A serial number

## Public Key Infrastructure

PKI typically comprises certificate authorities (CAs) and registration authorities (RAs). CAs provide the following services:

* Issuing digital certificates
* Validating digital certificates
* Revoking digital certificates
* Distributing public keys

## SSL and TLS concepts

The SSL and TLS protocols enable two parties to identify and authenticate each other and communicate with confidentiality and data integrity.

## Firewalls

* Effective means of protecting LANs.
* Inserted between the premises network and the internet to establish a controlled link
* Used as a perimeter defence. Choke point to impose security and auditing. Insulates the internal systems from external networks.
* All traffic from inside to outside and vice versa must pass through the firewall.
* Firewall should be immune to penetration

## IDS & IPS

* Intrusion detection systems, detection and monitoring tools.
* Do not act
* Requires another system to look at results
* Intrusion Prevention Systems, control systems
* Accepts and rejects a packet based on the ruleset
* Requires the database to be regularly updated with new threat data

## Passwords

* Hash functions
* MD5, SHA-1, SHA 256, SHA3

Two Factor Authentication