* **Key clustering: different encryption keys generate the same ciphertext from the same plaintext message**
* **Synchronous: encryption or decryption request is performed immediately**
* **Asynchronous: Encrypt/Decrypt requests are processed in queues**
* **Hash function: a one-way mathematical operation that reduces a message or data file into a smaller fixed length output, or hash value**
* **Digital signatures: provide authentication of a sender and integrity of a sender’s message. A message is input into a hash function. Then the hash value is encrypted using the private key of the sender. The result of these two steps yields a digital signature**
* **Symmetric**: **one key is used to encrypt and decrypt (private key)**
* **Asymmetric: two different but mathematically related keys are used where one key is used to encrypt and another is used to decrypt (public/private)**
* **Digital certificate: used to identify the certificate holder when conducting electronic transactions**
* **Certificate authority (CA): an entity trusted by one or more users as an authority in a network that issues, revokes, and manages digital certificates**
* **Registration authority (RA): responsible for the accuracy of the information contained in a certificate request. The RA is also expected to perform user validation before issuing a certificate request**
* **Plaintext or cleartext**
* **Ciphertext or cryptogram**
* **Cryptosystem: This represents the entire cryptographic operation. This includes the algorithm, key, and key management functions.**
* **Encryption**
* **Decryption**
* **Key or Cryptovariable: The input that controls the operation of the cryptographic algorithm**
* **Non-repudiation**
* **Algorithm**
* **Cryptanalysis: study of techniques for attempting to defeat cryptographic techniques and information security services**
* **Cryptology: the science that deals with hidden, disguised, or encrypted communications**
* **Collision: occurs when a hash function generates the same output for different inputs**
* **Key space: represents the total number of possible values of keys in a cryptographic algorithm or other security measure, such as a password**
* **Work factor: the time and effort required to break a protective measure**
* **Initialization vector (IV): A non-secret binary vector used as the initializing input algorithm for the encryption of a plaintext block sequence to increase security by introducing additional cryptographic variance**
* **Encoding: The action of changing a message into another format through the use of a code**
* **Decoding: The reverse process from encoding – converting the encoded message back into its plaintext format**
* **Transposition or permutation**
* **Substitution**
* **SP-network: substitution and permutation (transposition) most block ciphers do a series of repeated substitutions and permutations to add confusion and diffusion to the encryption process**
* **Confusion: provided by mixing (changing) the key values used during the repeated rounds of encryption**
* **Diffusion: provided by mixing up the location of the plaintext throughout the ciphertext**
* **Avalanche effect: where a minor change in either the key or the plaintext will have a significant change in the resulting ciphertext**