Public Key Infrastructure

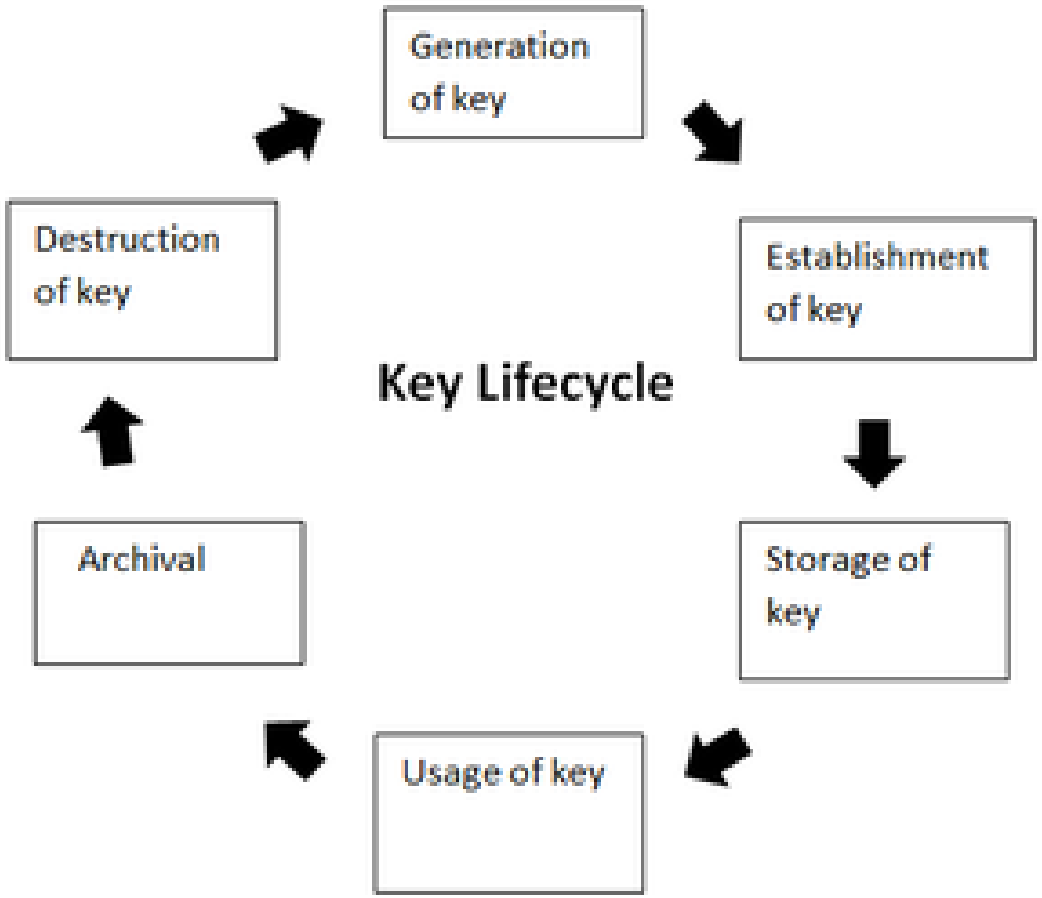
Public Key Infrastructure (PKI)

- PKI is the governing body behind issuing digital certificates
- It helps to protect confidential data and gives unique identities to users and systems.
- Thus, it ensures security in communications.
- PKI uses a pair of keys: the public key and the private key to achieve security.
- The public keys are prone to attacks and thus an intact infrastructure is needed to maintain them.

Managing Keys in the Cryptosystem:

- The security of a cryptosystem relies on its keys.
- Thus, it is important that we have a solid key management system in place.
- A cryptographic key is a piece of data that must be managed by secure administration.
- It involves managing the key life cycle which is as follows:

Managing Keys in the Cryptosystem:



Managing Keys in the Cryptosystem:

- Public key management further requires:

- **Keeping the private key secret:**

- Only the owner of a private key is authorized to use a private key.

- It should thus remain out of reach of any other person.

Managing Keys in the Cryptosystem:

- **Assuring the public key:**
- Public keys are in the open domain and can be publicly accessed.

- When this extent of public accessibility, it becomes hard to know if a key is correct and what it will be used for.

- The purpose of a public key must be explicitly defined.

Core components of public key infrastructure

A PKI generally consists of the following elements:

- **Digital certificate**—also known as a public key certificate, this PKI component cryptographically links a public key with the entity that owns it.
- **Certificate authority (CA)**—the trusted party or entity that issues a digital security certificate.
- **Registration authority (RA)**—also known as a subordinate certificate authority, this component authenticates requests for a digital certificate and then forwards those requests to the certificate authority to fulfill them.
- **Certificate database and/or certificate store**—a database or other storage system that contains information about keys and digital certificates that have been issued.