Viva questions

q-1) What is difference between cryptography and steganography?

A-)



q-2) What is cryptosystem

A-2) A cryptosystem is a structure or scheme consisting of a set of algorithms that converts [plaintext](https://www.techtarget.com/searchsecurity/definition/plaintext) to [ciphertext](https://www.techtarget.com/searchsecurity/definition/cipher) to encode or decode messages securely.

**Components of cryptosystems**

A basic cryptosystem includes the following components:

* Plaintext- This is the data that needs to be protected.
* Encryption algorithm- This is the mathematical algorithm that takes plaintext as the input and returns ciphertext. It also produces the unique encryption key for that text.
* Ciphertext- This is the encrypted, or unreadable, version of the plaintext.
* Decryption algorithm- This is the mathematical algorithm that takes ciphertext as the input and decodes it into plaintext. It also uses the unique decryption key for that text.
* Encryption key- This is the value known to the sender that is used to compute the ciphertext for the given plaintext.
* Decryption key- This is the value known to the receiver that is used to decode the given ciphertext into plaintext.

q-3) What is cryptanalysis?

A-)Cryptanalysis is the study and process of analyzing and decrypting ciphers, codes, and encrypted text without using the real key. Alternately, we can say it’s the technique of accessing a communication’s plain text content when you don’t have access to the decryption key.

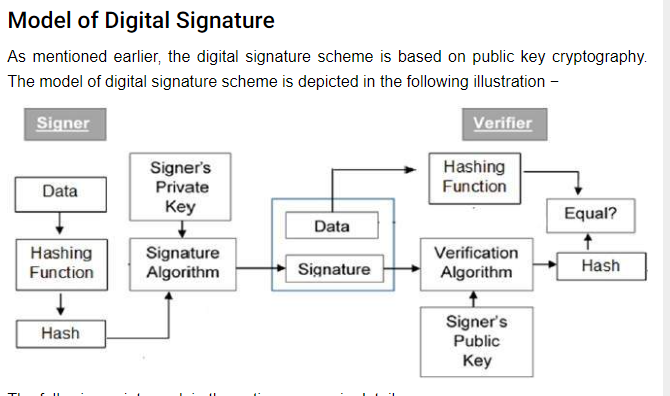
Put simply, [cryptanalysis](https://www.techtarget.com/searchsecurity/definition/cryptanalysis) is the practice, science, or art of decrypting encrypted messages.

Q-4) What is digital certificate in cryptography?

A-)

A [Digital Certificate](https://www.digicert.com/tls-ssl/digital-certificates) is an electronic file that is tied to a cryptographic key pair and authenticates the identity of a website, individual, organization, user, device or server. It is also known as a public key certificate or identity certificate. The certificate contains the subject, which is the identity piece, as well as a digital signature.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.



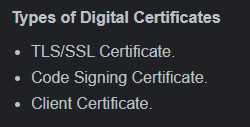
q-5) How is digital certificate created and what are its components?

When a web application requires digital certificates, an administrator typically creates digital certificates for each authorized user. The administrator digitally signs each certificate using the system CA certificate. These certificates, along with the public and private keys, are distributed to users.

Components:

* The date on which the certificate is issued.
* The date on which the certificate expires.
* The distinguished name of the issuing CA

q-) What are the types of certificates?

A-)

q-) What is Gpg4win used for?

Gpg4win **enables users to securely transport emails and files with the help of encryption and digital signatures**. Encryption protects the contents against an unwanted party reading it. Digital signatures make sure that it was not modified and comes from a specific sender

1. Why is 443 port secure?

Ans-HTTPS is secure and is on port 443, while HTTP is unsecured and available on port 80. Information that travels on the port 443 is encrypted using Secure Sockets Layer (SSL) or its new version, Transport Layer Security (TLS) and hence safer.

q-) Where is firewall placed?

A-)Firewalls can be placed **anywhere on a network** but are most commonly located between these components: Console and the Application Server. Application Server and the agents.