1) Explain Let’s Encrypt

Let’s Encrypt is a free, automated, and open certificate authority. It is used to set up an HTTPS server and have it automatically obtain a browser-trusted certificate, without any human intervention. For this reason, a certificate management agent is placed in the server.

- **Domain validation:**

Let’s Encrypt identifies the server administrator by its public key.

The Let’s Encrypt agent in a server is set up as follows:

1. When the agent in the server interacts with the Let’s Encrypt certificate authority (CA) for the first time it asks the CA what it can to do to prove that the server controls some domain.
2. The CA looks up the domain and sends back to the agent a list of challenges which are ways to prove that the agent controls the domain.
3. Let’s Encrypt CA also provides a nonce that the agent must sign with its private key pair to prove that it controls the key pair.
4. When the agent completes one of the challenges and signs the given nonce with its private key, it tells the CA that it is ready for validation.
5. The CA then checks the challenges and verifies the signature on the nonce.
6. It the signature is valid and the challenges check out then the agent is authorized to do certificate management for the domain or server.

The key pair used by the agent is called the authorized key pair.

- **Certificate Issuance and Revocation:**

For issuing the certificate, the agent sends a certificate signing request (CSR) to the CA which includes a signature generated using the private key corresponding to the public key inside the CSR. The agent also signs the entire CSR with its authorized key to let the CA know that it is authorized. The CA checks both the signatures and if they are valid it issues the certificate with the public key inside the CSR and returns it to the agent. Revocation occurs in the same way. The agent signs the revocation request with the authorized key pair and after the CA verifies the request it publishes revocation information into the normal revocation channels.

2) Compare / Contrast Encrypt with the traditional PKI system

- The Public Key Infrastructure provides a certificate at some cost while the Let’s Encrypt software offers free service.
- Both PKI and Let’s Encrypt are trust based models.
- Let’s encrypt offers a 90 day valid certificate. PKI on the other hand does not have a fixed time. PKI provides the expiration time of a certificate based on the type of the certificate.

Type of certificate	Maximum validity period
Root CA	Specified during setup of Certificate Services
Subordinate CA, Internet Protocol Security, Enrollment Agent, Domain Controller	Up to 5 years, never more than the Root CA's validity period
All other certificates	1 year, never more than the Issuing CA's validity period

- Both PKI and Let’s encrypt can have a central or hierarchical structure.