DS What is public key and private key cryptosystem ?

Public Key Cryptography, also known as Asymmetric Key Cryptography, is a type of encryption system that uses two keys: a public key and a private key. The public key is used for encrypting messages and verifying digital signatures, while the private key is used for decrypting messages and creating digital signatures. The keys are generated as a pair, with the private key kept secret and the public key made public. The security of the system depends on the assumption that while the public key can be freely distributed, the private key is kept secret. This allows for secure communication as only the holder of the private key can decrypt messages encrypted with the public key.

DS What is private key cryptosystem

A private key cryptography system is a type of encryption method that uses a single key, known as the private key, to both encrypt and decrypt messages. The private key is kept secret by the owner and is used to encrypt messages that are meant to be kept confidential. When a recipient receives the encrypted message, they use their own copy of the private key to decrypt it and access the original message. This type of encryption is considered to be less secure than public key cryptography as there is only one key and if it is compromised, all past and future encrypted messages can be decrypted by the attacker. Additionally, private key cryptography systems can only be used for encrypting messages between two parties who have agreed on and securely exchanged the private key.