Public Key Cryptography —

Public key cryptography is also known as assymetric cryptography.

Its a class of cryptographic protocols based on algorithms.

The method requires two different keys

The first key is private and the second key is public.

Public key cryptography uses two separate keys to encrypt and decrypt data to protect against unauthorized access.

When somebody wants to send a message, they look up a persons public key to encrypt the data which can then be decrypted using a private key.

The message can only be decrypted with private key that nobody should have access to.

RSA algorithm is a cryptography solution that allows sending secure data along an insecure channel. RSA allows both public and private keys to encrypt messages.

Challenges of Public Key Cryptography

- Speed
- Compromised Authority attacks

Benefits of Public Key Cryptography

- Increased Security
- No repudiation since there is a usage of digital signature

Symettric Encryption

Symettric encryption is the theory where only one key is used to encrypt and decrypt messages.

Private key encryption relies on mathematical functions to encrypt and decrypt messages.

A symetric key is a random string of binary digits or bits created specifically to encrypt or decrypt data.

- A key's length and randomness are factors in determining the strength of the encryption

Private key cryptography is based on the fact that private key CANNOT BE LEAKED.