

Symmetric Key

- + Computationally inexpensive in comparison with public key
- + Ciphertexts are not significantly longer for short plaintexts

- Keys have to be exchanged among sender and receiver before starting the communication
- Can't be used to produce digital signature which can be verified by anyone

Public Key

- + No key exchange required
- + Anyone can encrypt
- + Anyone can verify integrity
- + Private key is only at one place

- Computationally expensive
- Longer ciphertexts even for short plaintexts
- Compromised key revocation is complex

IBC

- + Secret key of PKG can be destroyed at certain point
- + Authenticity of public key is guaranteed by PKG
- + No certificate
- + Public private key pair can not be created by any one

- Credential/public-key of an ID can not be revoked
- Too much trust on PKG

Certificate Based

- + Distributed trust network
- + Harder revocation, but still possible

- Long certificate chain increases communication overhead
- Network of CA required

Root-key Based

- + Easy key management
- + No trust hierarchy
- + No certificate required
- + Less communication overhead
- + Easier revocation

- Only trusted roots can decrypt the message which creates pressure of computation at a single point