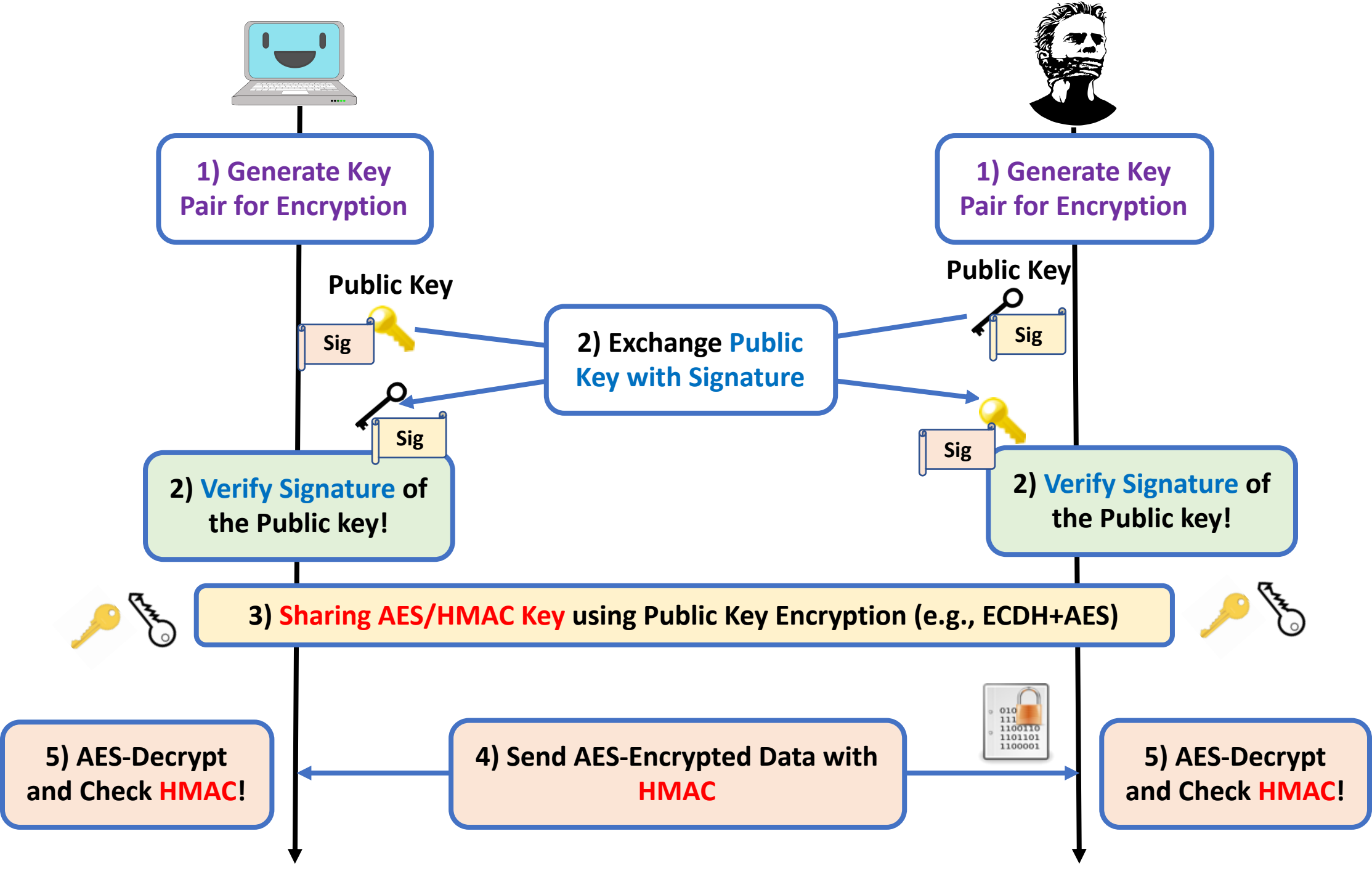
1) Generate Key Pair for Encryption
1) Generate Key Pair for Encryption
Public Key
Sig
2) Exchange Public Key with Signature
Public Key
Sig
Sig
Sig
2) Verify Signature of the Public key!
2) Verify Signature of the Public key!
3) Sharing AES/HMAC Key using Public Key Encryption (e.g., ECDH+AES)
5) AES-Decrypt and Check HMAC!
4) Send AES-Encrypted Data with HMAC
5) AES-Decrypt and Check HMAC!