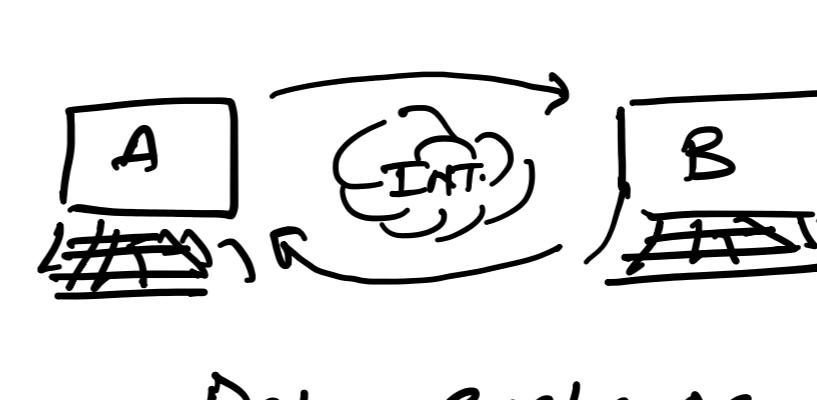


1.2.2 / 1.4

ZAFAR Plaintext
A B G B S Cipher text



Data exchange over Internet.

Plain text → Cipher text
Encryption (Public key)

Cipher text → Plain text
Decryption (Private key)

key terms:

Plaintext: The original text, document or message before it is put through an encryption algorithm.

Ciphertext: The product when plaintext is put through an encryption algo.

Encryption: It is encoding of plaintext into ciphertext.

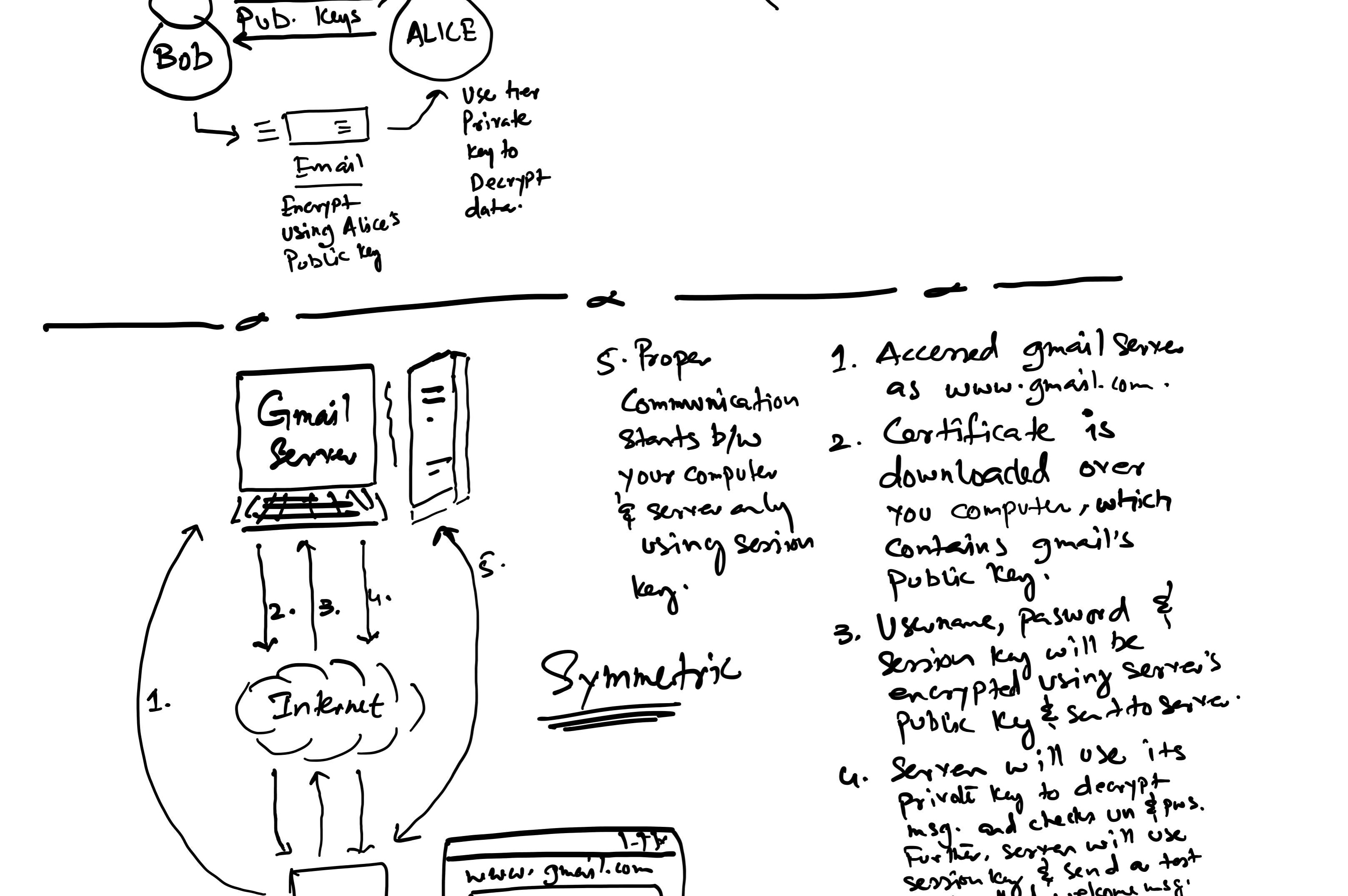
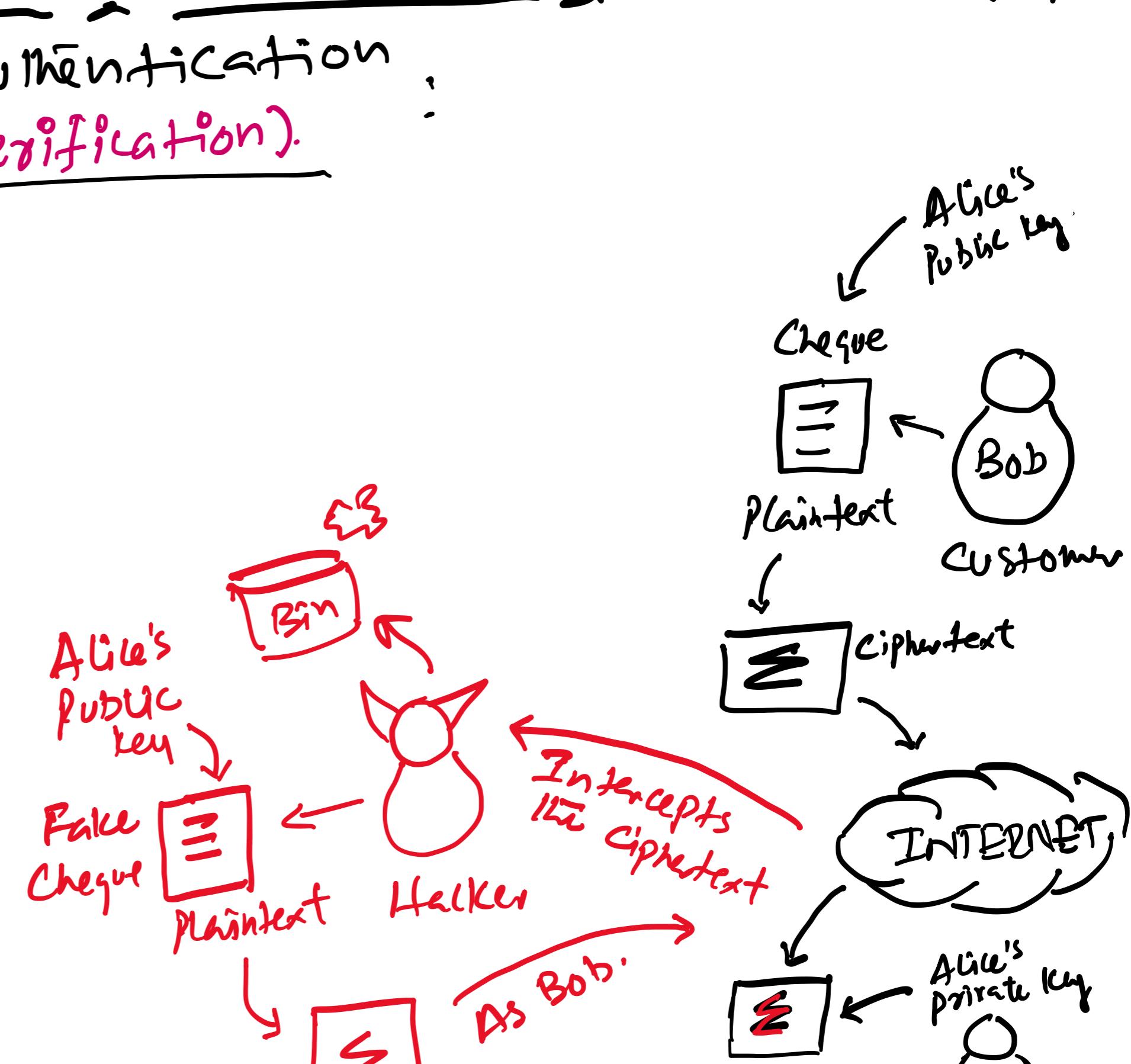
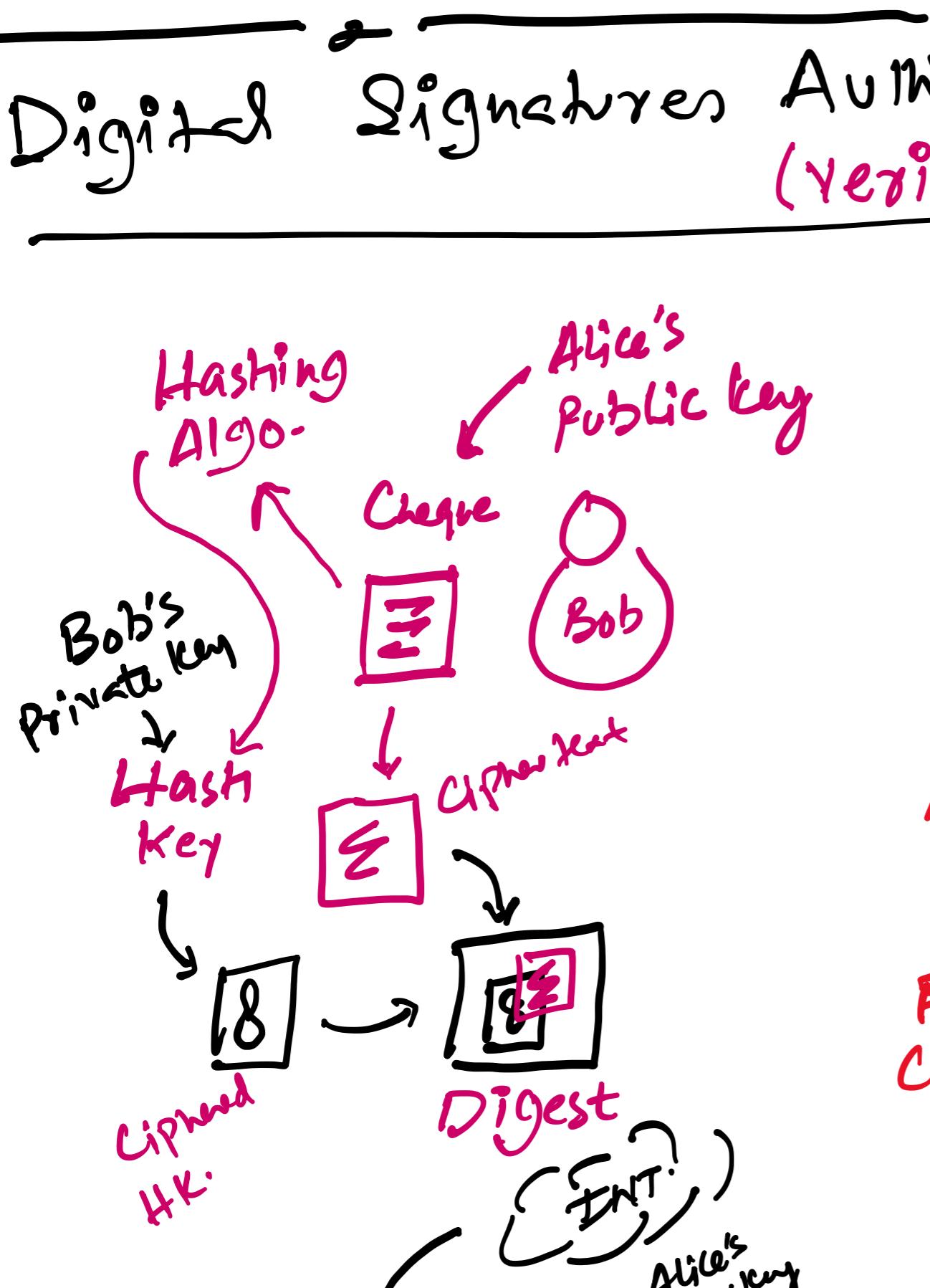
There are two types:

Symmetric encryption: It is encryption that uses same secret key to encrypt & decrypt.

Asymmetric encryption: It uses public keys and private keys.

Public key: Encryption/Decryption key known to all users.

Private key: Encryption/Decryption key known to a single user/computer that is owner.

Digital Signatures Authentication (Verification).Solution