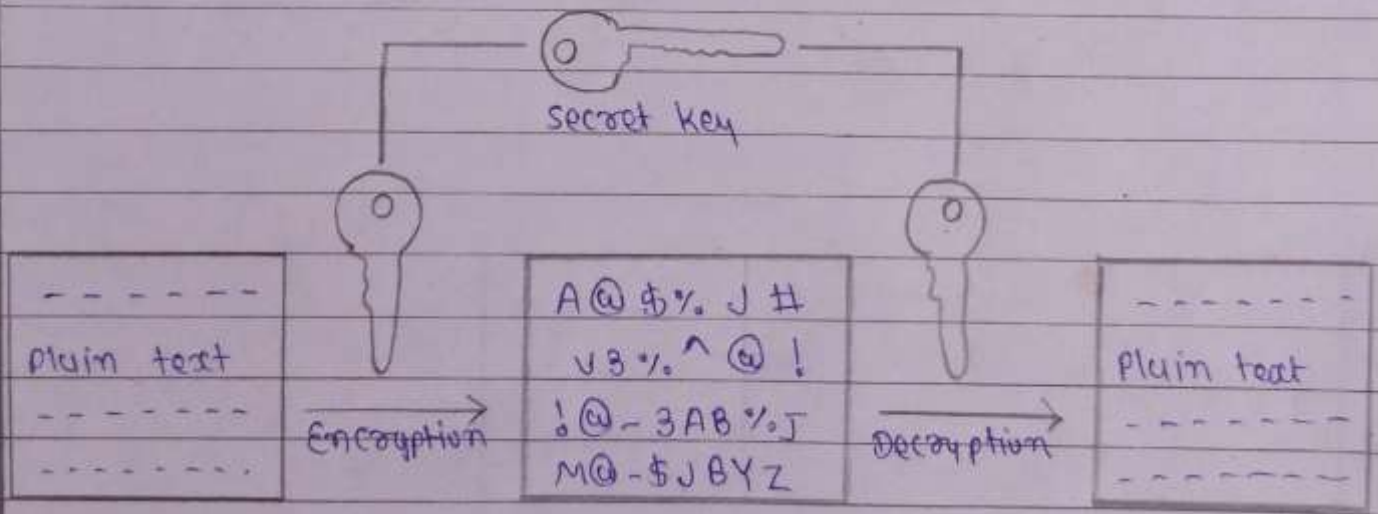
+ Assignment - 1

1 List all Symmetric Key Algorithms.

Ans. Symmetric key algorithms are algorithms for cryptography that use the same cryptographic keys of both encryption of plaintext and decryption of ciphertext. the key may be identical or there may be a simple transformation to go between the two keys. The key, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of Symmetric key encryption, in comparison to public-key encryption (also known as asymmetric key encryption).

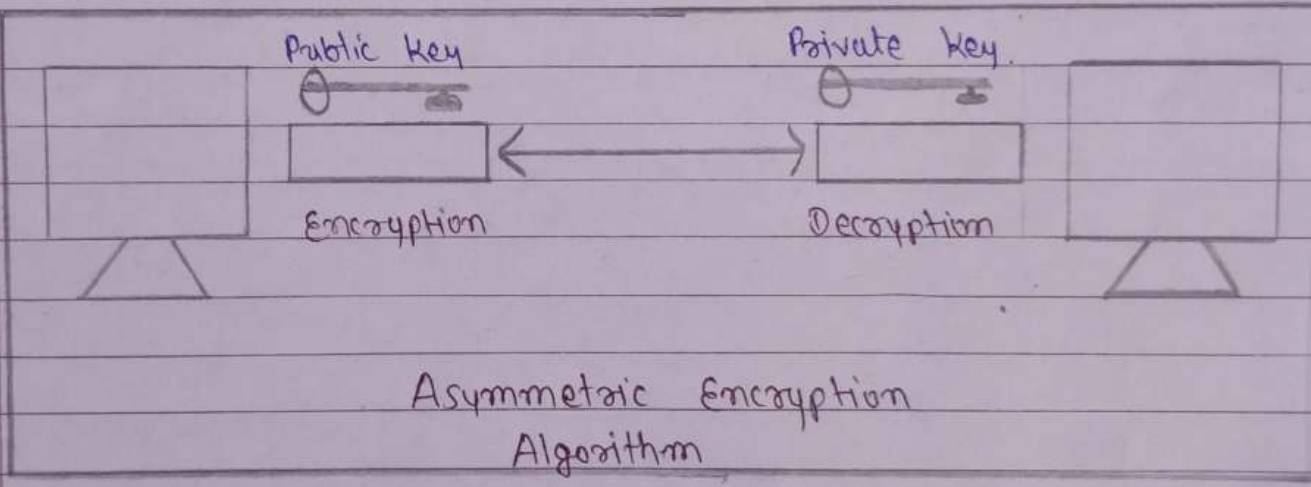


Cipher Text

- Some of the Symmetric Encryption Algorithms
  - AES (Advance Encryption standard)
  - DES (Data Encryption Standard)
  - IDEA (International Data Encryption Algorithm)
  - Blowfish (Drop-in replacement for DES or IDEA)
  - RC4 (Rivest Cipher 4)
  - RC5 (Rivest Cipher 5)
  - 3 DES
  - RC6 (Rivest cipher 6)

Q List All Asymmetric Key Algorithms.

Ans. Asymmetric Key Algorithms are Algorithms for Public-Key cryptography or asymmetric cryptography, is a cryptography system that uses pairs of key: Public Key, which may be disseminated widely, and private keys, which are known only to the owner. The generation of such key depends on cryptographic algorithms based on mathematical problems to produce one-way functions. Effective security only requires keeping the private key private; the private key; the public key can be openly distributed without compromising security.



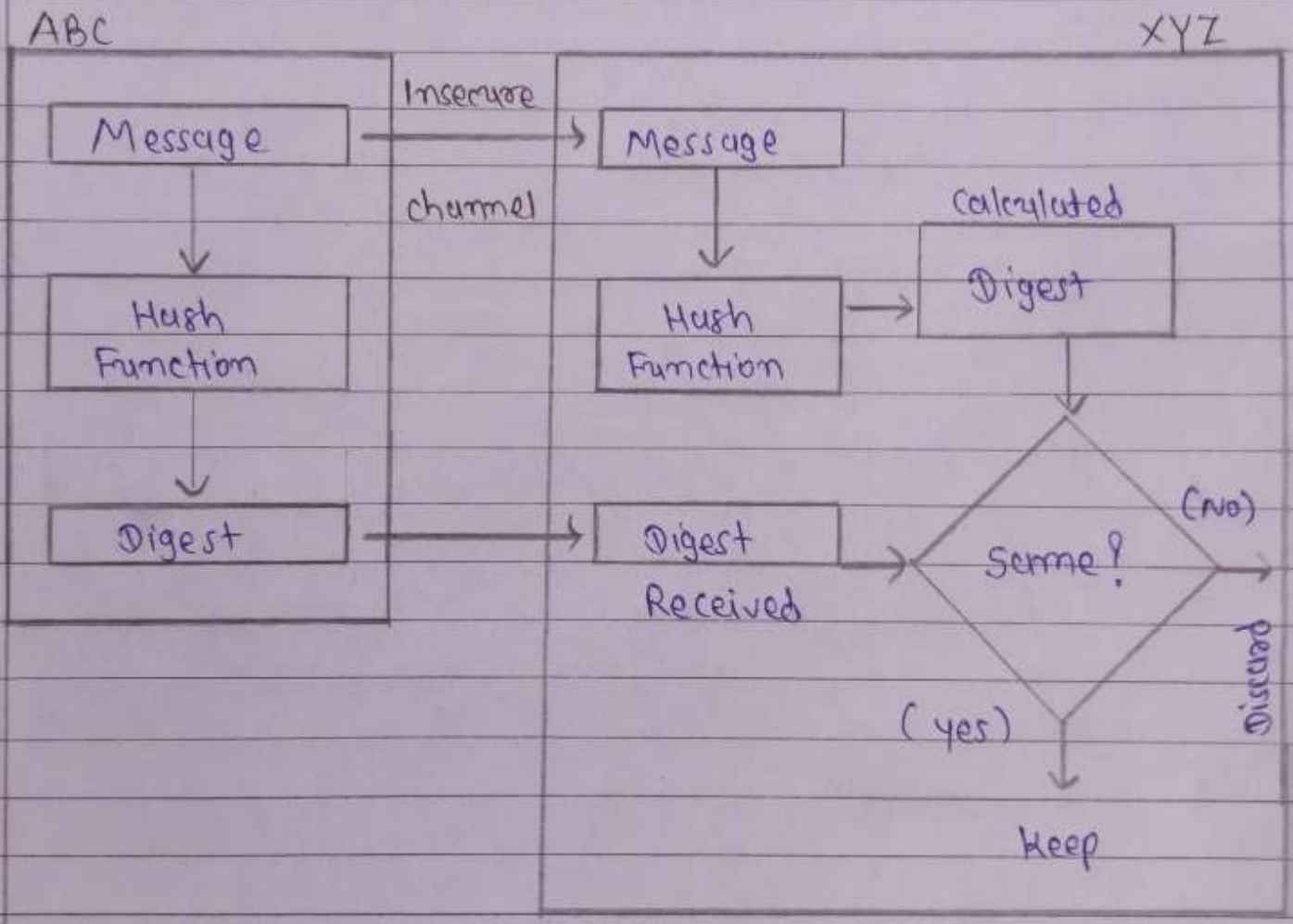
Asymmetric Encryption Algorithm

- Some of the Asymmetric Encryption Algorithms

- Diffie-Hellman Key exchange Protocol
- DSS - Digital Signature Algorithm
  Digital Signature Standard
- ElGamal
- RSA - encryption algorithm (PKCS #1)
- Paillier Cryptosystem
- YAK authenticated key agreement protocol.

3 List the Algorithms for message Digest.

Ans. Message Digest is used to ensure the integrity of a message transmitted over an insecure channel (where the content of the message can be changed). the message is passed through a Cryptographic hash function. This function creates a compressed image of the message called Digest.



- Message Digest Hash Algorithm (SHA) (secure)
  - MD2
  - MD5
  - SHA-1
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512

SHA - Secure Hash Algorithm.