

NAME :- ANKIT VIPULBHAI PRAJAPATI

ROLL No. : 29

CLASS : MCA-I

SUBJECT : ION (Dr HARDIK JOSHI SIR)

ASSIGNMENT - 1

1) List all Symmetric key Algorithms
Ans:

⇒ Symmetric-key algorithms are algorithms for cryptography that use the same ~~cryptographic~~ cryptographic keys for both encryption of plaintext and decryption of ciphertext.

⇒ Here is list of Symmetric key Algorithms :-

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
- Triple Data Encryption standard (Triple DES)
- Rivest Cipher 4 (RC4)
- International Data Encryption Algorithm (IDEA)
- Blowfish (Replacement for DES or IDEA)

2) List all Asymmetric Key Algorithms

Ans:

→ Asymmetric Algorithms are Algorithms for cryptography that uses a pair of related keys (one public key and one private key) to encrypt and a message and decrypt a message and protect it from unauthorized access or use.

→ Here is list of Asymmetric Key Algorithms:-

- Rivest Shamir Adleman (RSA)
- Diffie - Hellman Agreement
- Elliptic curve cryptography (ECC)
- Digital Signature Algorithm (DSA)
- El Gamal Encryption Algorithm

3) List the algorithms for Message digest

Ans:-

→ A Message digest is a cryptographic hash function containing a string of digits created by a one-way hashing formula.

→ Message digests are designed to protect the integrity of a piece of Data or media to detect changes and alterations to any part of a message.

→ Here is list of algorithms for Message digest

÷ Message Digest 5 (MD5)

÷ Secure Hash Algorithm 1 (SHA-1)

÷ SHA - 256

÷ SHA - 512

÷ SHA - 224