Name = Soni Varshil R

Roll No = 40 class = MCA-1

Subject : ION Dr. Hardik Joshi sir

Assignment = 1

1 List of all symmetric algorithms.

Ans. Symmetric encryption is a type of encryption where only one key is used to both encrypt and decrypt electronic information.

* This encryption method differs from asymmetric encryption where a pair of keys, one public and one private, is used to encrypt and decrypt messages.

* By using symmetric encryption algorithm data is converted to a form that can not be understood by anyone who does not possess the secret key to decrypt it.

* The secret key that the sender and recipient both use could be a specific password/code or it can be random string of letter that have been generated by a secure random

number generator (RNG).

→ There are mainly Two type of symmetric encryption algorithms.

1. Block algorithms :- Set lengths of bits are encrypted in block of electronic data with the use of a specific key.

2. Stream algorithms :- Data is encrypted as it stream instead of being retained in the system's memory.

* Some examples of symmetric encryption algorithm include :-

→ AES (Advanced Encryption Standard)

→ DES (Data Encryption standard)

→ IDEA (International Data Encryption Algorithm)

→ Blowfish (Replacement for DES or IDEA)

→ ~~RC4~~ RC4 (Rivest cipher 4)

Q-2. List all asymmetric key algorithms.

Ans. Asymmetric key algorithms work in a similar manner to symmetric key algorithm, where plaintext is combined with a key, input to an algorithm, and outputs ciphertext.

* The key pair is comprised of a private key and a public key. As the name imply, the public key is made available to everyone, where as the private key is kept secret.

* The two main uses of asymmetric-key algorithms are public-key encryption and digital signatures. public-key encryption is a method where anyone can send an encrypted message within a trusted network. only receiver can decrypte the message using the own private key.

Types of asymmetric key algorithm

1. Diffie-Hellman key agreement.

2. Rivest Shamir Adleman.

3. Elliptic curve cyptography (ECC)

4. Digital signature Algorithm (DSA)

Que-3. List the algorithms for message digest

Ans. Message digest algorithms rely on cryptographic hash functions to generate a unique value that is computed from data and a unique symmetric key

* A cryptographic has function inputs data of albitrary length and produces a unique value of a fixed length.

* Adding a unique symmetric key that is shared between a sender and receiver in order to compute message digest value provides confidentiality to ensure that the message digest can not be easily changed if the data is changed in an unauthorized or other manner.

list of message digest algorithms.

(1.) Message Digest 5 (MD5)

(2.) Secure Hash Algorithm (SHA-1)

(3.) SHA2-224 (4.) SHA2-256

(5) SHA2-512