Assignment-1

1) List of all symmetric algorithm.

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

- This encryption method differ from asymmetric encryption where a pair of keys, one public and one private is used to encrypt and decrypt message

- By using symmetric encryption algorithm data is converted to a form that can't be understood by anyone who does not Posses 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 or letter that have been generated by secure random number generator

→ Types of symmetric encryption algorithm.

1) Block algorithm :- set length of bits are encrypted in block of Electronic data with the use of a specific key.

2) stream algorithm :- Data is encrypted as it stream instead of being retained algorithm include:-

-> AES (Advanced encryption standard)

-> DES (Data Encryption Standard)

-> IDEA (International Data encryption algorithm)

-> Blowfish (Replacement for DES or IDEA)

-> RC4 (Rivest Cipher 4)

Q-2 List all assymmetric key algorithm

-> Assymmetric key algorithm work in a similar manner to symmetric ~~al~~ key algorithm, where plaintext is combined with a key, input to an algorithm, And output ciphertext

- The key pair is comerised of a private key and a public key. As the name imply, the public key is made available to everyone, whereas the private key is kept secret.

- The two main uses of asymmetric-key algorithm are public-key encryption and digital sym: signatures Public-key encryption is a method where anyone can send an encrypted message within a trusted network only receiver ~~and~~ can decrypt message using the own private key.

→ Types of asymmetric key algorithm

1) Diffie- Hellman key agreement.

2) Rivest Shamir Adleman.

3) Elliptic curve cryptography (ECC)

4) Digital signature Algorithm (DSA).

Q-3 List the algorithm for message digest

→ message digest algorithm 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 arbitory length and produces a unique value of a fixed length.

- Adding a unique symmetric key [illegible] shared between sender and receiver in order to compute message digest value provides confidentiality to [illegible] that the message ~~is the data~~ [illegible] cannot be easily changed if the [illegible] changed in an unauthorized or [illegible] manner.

List of message digest algorithm.

1) message Digest 5 (MD5)

2) Secure Hash Algorithm (SHA-I)

3) SHA 2 - 224

4) SHA 2 - 256

5) SHA2 - 512