NAME: MANSI BHAT CLASS: MCA-1
ROLLNO: 02 SUBJECT: ION
(Dr. Hardik Joshi Sir)

ASSIGNMENT-1

1. List all Symmetric Key Algorithms.

Symmetric Key Algorithms: Symmetric Key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.

- Symmetric Key algorithms are sometimes referred to as 'Secret Key' algorithms. This is because these types of algorithms generally use one key that is kept secret by the systems engaged in encryption and decryption processes.

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

- Symmetric-Key encryption can use either stream ciphers or block ciphers.

List of Symmetric Key algorithms :-

- **AES**: The most commonly used symmetric algorithm is Advanced Encryption Standard (AES), which was originally known as Rijndael. It was approved by NIST (National Institute of standards and Technology) in Dec-2001. Under NIST, AES cipher has a block size of 128 bits.

- **DES**: In modern computing, DES was first standardized cipher for securing electronic communications and is used in variations (eg- 2-key or 3-key 3DES).

- **IDEA** :- International Data Encryption algorithm (IDEA) uses Block Ciphers.

- **Blowfish** :- Blowfish uses Block ciphers. It is Drop-in replacement for DES or IDEA.

- **RC4**: RC4 was designed by Rivest in 1987. It is a Stream cipher that has been very widely used (eg- in SSL/TLS protocol and early wi-fi security standards).

- **RC5**: RC5 is a block cipher with a variable block size (32, 64 or 128 bits), variable key length (upto 2040 bits)

& variable number of rounds (upto 255).

- RC6 :- RC5 was modified to produced RC6 with a fixed block size of 128 bits.
  However, RC5 & RC6 are not widely used as they are patented.

2. List all Asymmetric Key Algorithms.

Asymmetric Key Algorithm: Asymmetric key algorithms are algorithms for cryptography where a secret key can be ~~given to one~~ divided into two parts, a public key and a private key.

- Public key can be given to anyone, trusted or not, while the private key must be kept secret (just like in symmetric cryptography).
- Asymmetric cryptography has two primary cases: authentication and confidentiality.
- Encryption with asymmetric cryptography works in slightly different way from symmetric encryption. Someone

with public key is able to encrypt a message, providing confidentiality, and then only the person in possession of private key is able to decrypt it.

Some Asymmetric Key algorithms are;-

1) Diffie-Hellman Key agreement
It is a method that allows two parties to jointly agree on a shared secret using an insecure channel.

2) RSA (Rivest Shamir Adleman)
RSA is a public key algorithm for encrypting and signing messages. RSA keys have a complex internal structure with specific mathematical properties.

3) Elliptic Curve Cryptography (ECC)
It provides similar functionality to RSA. ECC is being implemented in smaller devices like cell phones.

4) Digital Signature Algorithm (DSA):- Can be used only for signing data & it cannot be used for encryption.

5) El Gamal: It is an Algorithm used for transmitting digital signatures and key exchanges.

3. List the Algorithms for message digest.

Message digest: Message digest is used to ensure the integrity of a message transmitted over an insecure channel. The message is passed through a cryptographic hash function. This function creates a compressed image of the message called Digest.

- The cryptographic hash function takes a message of variable length as input and creates a digest / hash / fingerprint of fixed length, which is used to verify integrity of message.
- Message digest ensures integrity. To provide authenticity of the message, digest is encrypted with sender's private key. Now this digest is called digital signature, which can be only decrypted by receiver who has sender's public key.

List of Message digest algorithms:

1) **Message Digest 5 (MD5) :-**
It divides message into blocks of 512 bits and creates a 128 bit digest (typically, 32 Hexadecimal). It is no longer considered reliable.

2) **Secure Hash Algorithm (SHA) :-**
In response to insecurities of MD5, the Secure Hash Algorithm was invented. SHA is the name of series of hash algorithms.

   (a) **SHA-1** : Creates a 160-bit hash value.

   (b) **SHA-2** includes SHA-224, SHA-256, SHA-384, & SHA-512

3) **HAVAL (Hash of variable length) :**
is a hash algorithm that creates message digest of 128, 160, 192, 224 or 256 bits in length, using 3, 4 or 5 rounds.

ASSIGNMENT-2

Q Discuss briefly in one-two sentences.

(a) PIL: Personally Identifable information (PIL) is any data that can be used to identify a specific individual. Social Security no's, mailings, phone no's have most commonly considered as PIL.

(b) Us Privacy Act of 1974:
This Act was prepared by the Department of Justice's office of privacy and civil liberties (OPCL), is a discussion of Privacy Act's disclausre prohibition, its amendment provisions, its accers & its agency record keeping requirements.

(c) FOIA: FOIA stands for 'Freedom of Information Act. It is a United states federal law that grants public Accers to info. prossessed by government agencies.

(d) FERPA: (Family Educational Rights and Privacy Act of 1974) is federal legislation in U.S that protects privacy of students' personally PIL. the act applies to all educational institutions that receive federal funds.

(e) CFAA : The Computer Fraud and Abuse Act (CFAA) was enacted in 1986, as an amendment to the first federal Computer fraud law, to address hacking.

(f) COPAA : The Council of Parent Attorneys and Advocates (COPAA) is an independent national American association of parents of children with disabilities, attorneys, advocates and related professionals who protect the legal & civil rights of students with disabilities & their families.

(g) VPPA :- Video Privacy Protection Act (VPPA) of 1988 generally prohibits the disclosure of a Consumer's video rental or purchase records to third parties.

(h) HIPAA :- The Health Insurance ~~Pro~~portibility and Accountability Act (HIPAA) is an act created by U.S Congress in 1996 that amends both Employee retirement Income Security Act (ERISA) & Public Health Service Act (PHSA).

(i) GLBA :- The Graamm - Leach - Bliley Act (GLBA) is also k/a Financial modernization Act of 1999. It is a United States

federal law that requires financial institutions to explain how they share and protect their customer's private information.

(j) PCI DSS : The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirement intended to ensure that all companies that process, store or transmit credit card info. maintain a secure environment.

(k) FCRA :- The Fair Credit Reporting Act (FCRA) is a federal law that regulates the collection of consumers credit information and access to their credit reports.

(l) FACTA :- Fair and Accurate Credit Transactions Act is an Amendment to FCRA (Fair Credit Reporting Act) that was added, primarily to protect consumers from identity theft.