

Name - Harsh Mishra

Subject - ITW

Roll No - 20

Class - MCA-1

Assignment - I

Q1) 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 keys, i.e. one public and one private is used to encrypt and decrypt messages.

- The secret key that the sender and recipient both use could be a specific password/code or it can be random string of letters that have been generated by a secure random number generator (RNG).

- There are mainly two types 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 or stream it 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 (Rivest cipher 4)

Q2) list all asymmetric key algorithm.

Ans Asymmetric key algorithm 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, public key is made available to everyone where 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 while anyone can send an encrypted message within a trusted network only receiver can decrypt the message using the own private key:

- Type of Asymmetric key algorithm.

1) Diff - Hellman key agreement.

2) Rivest Shamir Adleman

3) Elliptic curve cryptography (ECC)

4) Digital signature Algorithm (DSA)

Q3) 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 hash function inputs data of arbitrary 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 cannot be easily changed if the data is changed in an unauthorized or other manner.

List of message digest algorithms.

1) Message Digests (MD5)

2) Secure Hash Algorithm (SHA-1)

3) SHA2-224

4) SHA2-256

5) SHA2-512

Name - Harsh Mishra

Subject - IOW

Roll no - 20

Class: MCA-I

Assignment - 2

Q) Discuss briefly in one-two sentences.

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

b) US Privacy Act of 1974:

This act was prepared by The Department of Justice of, privacy and civil liberties (DOJ), is a discussion of privacy Act's disclosure prohibition its amendment provisions, its access and its agency record keeping requirements.

c) FOIA:

FOIA stands for Freedom of Information Act.

It is a united states federal law that grants public access info. processed by government agencies.

d) FERPA: (Family Educational Rights and Privacy Act of 1974)

This is a federal legislation in US that protects privacy of students personally. This 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 protects the legal and civil rights of students with disabilities and their families.

(G) VPPA: - Video Privacy Protection Act (VPPA) of 1998 generally prohibits the disclosure of a consumer's video rental or purchase records to third parties.

(H) HIPAA: - The health insurance portability and Accountability Act (HIPAA) is an act created by US Congress in 1996 that amends both Employee Retirement Income Security Act (ERISA) and Public Health Service Act (PHSA).

(I) GLBA: - The Gramm-Leach-Bliley Act is also known as the financial modernization act of 1999. It is a United States federal law that requires financial institutions to explain how they share and protect their customers' private information.

(J) PCI DSS :- The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements 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 is a federal law that regulates the collection of consumers credit information and access to their credit reports.

(L) FACTA :- Fair and Accurate Credit Transaction Act is an Amendment to FCRA that has added primarily to protect consumers from identity theft.