

Roll No: 16

Class = MCA - I

Name : Luhur Prince

Date: / /20

Assignment - I

Page No.:

① List of all Symmetric Key Algorithms.

→ There are two type of Symmetric encryption Algorithm.

1) Block Algorithm.

→ Set lengths of bits are encrypted in blocks of electronic data with the use of Specific Secret Key.

2) Stream Algorithm

→ Data is encrypted as it Stream instead of being maintained in waits for Complete block.

→ Symmetric key Algorithms are

1) AES (Advanced Encryption Standard)

2) RC4 (Rivest Cipher 4)

3) DES (Data Encryption Standard)

~~4) 3DES~~

2) List of all asymmetric key Algorithms.

1) Diffie-Hellman Key agreement.

2) RSA (Rivest Shamir Adleman)

3) ECC (Elliptic Curve Cryptography)

4) ElGamal

5) DSA (Digital Signature Algorithm)

③ List of the algorithm for message digest

1) Message Digest 5 (MD 5)

2) Secure Hash Algorithm (SHA-1)

3) SHA2 - 224

4) SHA2 - 256

5) SHA2 - 512

Assignment - 2.

① PII (Personally Identifiable Information)

- PII is any data that can be used to identify a specific individual.
- mostly PII Consider by social security, email address and phone number

② US Privacy Act of 1974.

- This Act prepared by Department of Justice's office OPII
- This act establishes a code of fair Information Practices that govern the collection, maintenance, use and dissemination of information about individuals that is maintained in System records by federal agencies

③ FOIA

- FOIA → Freedom of Information Act
- This act is a US federal law that grants the public access to information possessed by government agencies

④ FERPA

- Family Educational Rights and Privacy Act (FERPA)
- This is a federal legislation in the United States that protects the privacy of students' PII.
- The act applies to all educational institutions that receive federal funds.

⑤ CFAA

- Computer Fraud and Abuse Act
- It act designed to protect computer system operated by US government and some financial institutions but expanded in scope after several amendments.

⑥ COPPA

- Children's online Privacy Protection Act
- It is for specially protect the privacy of children under the age of 13 by requesting parental consent for the collection or use of any personal information of website users.
- officially Take effect in April 2000

7) VPPA

- Video Privacy Protection Act.
- This Act refers to wrongful disclosure of video tape rental or sale records.

8) HIPAA

- Health Insurance Portability and Accountability Act.
- This Act provides data privacy and security for safe guarding medical information.

9) GLBA

- Gramm - Leach - Bliley Act (Financial Modernization Act)
- This Act aims to control the ways that financial Institutions deals with the Private Information of Individuals.
- The Act also requires financial institution to give customers written Privacy notices that explain their information sharing practices.

(10) PCIDSS

- Payment Card Industry Data Security Standard
- PCIDSS is a widely accepted set of Policies and Procedures intended to optimize the security of Credit, Debit and Cash Card transaction and Protect Cardholders against misuse of their Personal Information

(11) FCRA

- Fair Credit Reporting Act.
- This act Promotes accuracy, fairness and Privacy for data used by Consumer reporting agencies.

(12) FACTA

- Fair and Accurate Credit Transaction Act.
- This Act to Protect Consumers from identity theft.
- The Act stipulates requirements for Information Privacy accuracy and disposal and limits the ways Consumer Information can be Shared.