Name — Prajwal Rai

Roll no - 31

Subject - ION

-> Mca - I

Assignment - 1

1- List all symmetric key algorithms:

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

- The entities communicationg via symmetric encryption must exchange the key so that it can be used in decryption process.
- This encroption method differs from asymmetric encryption where a pair of keys, one public and one private, is used to encrypt and decrypt messages.

⇒ There are two types of symmetric encryption algorithms:-

1. - Block algorithms
2. - Stream algorithms.

⇒ List of Symmetric key Algorithms:-

- Advanced Encryption Standard
- Data Encryption Standard
- International Data Encryption Standard.

- Blowfish
- Rivest cipher 5.
- Rivest cipher 6

- Block cipher

- Stream cipher - Rivest cipher 4.

2- List all assymmetric key algorithms :-

⇒ Asymmetric key algorithms work in a simmilar to symmetric - key algorithm where plain text is combined with key, input to an algorithm, and outputs chiphertext.

- Asymmetric cryptography is branch of cryptography where a secret key can be divided into two ~~Project~~ parts, a public key and a private key.

⇒ List of Asymmetric key Algorithm.

Ed25519 signing.
- X25519 - key exchange
- Xd448 signing
- Elliptic curve cryptography
- RSA

- Differ - Hellman key exchange
- DSA
- Key Serialization
- Asymmetric utilities.

3 - <u>List of algorithms for message digest.</u>

-> The MD5 Message - digest algorithm is a widely used hash function Producing a 128 - bit hash value. Although MD5 was initally design to Be used as a cryptographic hash function.

-> list of Message digest Algorithm

- MD2 - ~~The MD2 message digest Algorithm~~
- MD5 ~~as define in RF~~
- SHA-1 , SHA - 224, SHA -256, SHA -384, SHA - 512 / 224 , SHA 512/256.
- SHA 3 - 224 , SHA3 - 256 , SHA3 - 384, SHA3 - 512 .

Assignment - 2

(4)=) Discuss briefly :-

(a) PII (Personally Identifiable Information):-

- Personally identifiable information (PII) is any data that could Potentially identify a specific individual. Any information that can used to distinguish one person from another and can be used for deanonymizing Previously anonymous data can be considered PII. Protecting PII is essential for Personal Privacy, data Privacy, data Protection, information Privacy and information Security.

(b) Us Privacy Act of 1974 :-

- The Privacy Act of 1974 is a united States federal law, establishes a code of fair Information Practice that governs the collection, maintenance, use and dissemination of Personally identifiable information about individual that is maintained in systems of records by federal agencies.

- The Privacy Act Prohibits the disclosure of information from a System of records absent of the written consent of the Subject individual, unless the disclosure is Pursuant to one of twelve Statutory exceptions.

(C) FOIA :- (Freedom of Information Act)

- The freedom of Information Act is a federal freedom of information law that requires the full or Partial disclosure of Previously unreleased information and documents controlled by the United States government upon request.

(D) FERPA :-

- The Family Educational Rights and Privacy Act is a federal law that affords Parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of Personally identifiable information from the education records.

- When a Student turns 18 Yrs old, or enters a Post Secondary institution at any age, the rights under FERPA transfer from Parents to the Students.

(E) CFAA :-

- The Computer Fraud and Abuse Act is a united States cybersecurity bill that was enacted in 1986 as an amendment to existing Computer fraud law, which had been included in the comprehensive Crime Control Act of 1984.
- The law Prohibits accessing a computer without authorization, or in excess of authorization.

(F) COPAA :-

The Council of Parent Attorneys and Advocates is an independent national American Association of Parent's of Children with disabilities, attorneys, Advocates, and related Professionals who Protect the legal and civilrights of Students with disabilities and their families.

(G).- VPPA :-

The video Privacy Protection Act was a bill Passed by the united States Congress to Prevent what it refers to as "wrongful disclosure of video tape rental or Sale records".

(H) HIPAA :-

Health Insurance Portability and Accountability Act was created Primarily to modernize the flow of healthcare information, Stipulate how Personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance Coverage.

(I)- GLBA :-

- The Gramm - Leach - Bliley Act also known as the Financial Servies modernization Act of 1999.
- It created to enhance competition in the financial Services industry by Providing a Prudential framework for the affilation of banks, Securities firms, and other financial Service Provides, and for other Purpose.

(J) PCI DSS :-

- The Payment card industry Data Security Standard is a set of Security Standards formed in 2004 by Visa, Mastercard, Discover Financial Services, JCB international.
- Governed by the Payment Card industry Security Standards Council. The Compliance Scheme aime to Secure credit and debit card transaction against data theft and fraud.

(k) FCRA :-

The Fair Credit Reparting Act, was intended to Protect consumers from the willful and negligent inclusion of inaccurate information in their credit reports.

(L) FACTA :-

The Fair and Accurate credit Trandactions Act to amend the fair credit Reporting Act, to Prevent identity thef, improve resolution of consumer disputes improve the accuracy of consumer disputes, improve the accuracy of consumer records, make improvements in the use of and consumer access to credit information and for other Purpose.