Name :- LADANI TEJASKUMAR V.

Class :- MCA-I

Roll No. :- 14

Subject :- ION

College :- Rollwala Computer centre - GU.

Assignment-1

(1) List all Symmetric key Algorithms.

DES - (Data Encryption standard)

3DES - (3 data Encryption Standard)

AES - (Advanced Encryption Standard)

IDEA - (International Data Encryption Algorithm)

Blowfish (Drop-in replacement for DES or IDEA)

RC-4 (Rivest cipher 4)

RC-5 (Rivest Cipher 5)

RC-6 (Rivest Cipher 6)

(2) List all Asymmetric key Algorithms.

RSA - (Rivest Shamir Adleman)

ECC - (Elliptic Curve Cryptography)

Deffie - Hellman key exchange

DSA - (Digital signature Algorithm)

Key Serialization

Asymmetric utilites

(3) List the Algorithms for Message Digest.

MD-5 (Massage Digest -5)

SHA-1 (Simple Hash Algorithm)-1

SHA-2 (Simple Hash Algorithm-2)

SHA-256 (Simple Hash Algorithm-256)

SHA- 224 (Simple Hash Algorithm- 224)

HAVAL (Hash of Variable Length)

Assignment-2

* Brief Discussion.

(a) PII -- Personally identifiable information

⇒ Personally identifiable information is any information about an individual maintain by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, Birthdate, Biometric records, medical details, Educational as well financial detail etc.

(b) US Privacy Act of 1974

⇒ The Purpose of the Privacy Act is to balance the government's need to maintain information about individuals with the rights of individual to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, ~~maintain~~ maintence, use and disclosure of personal information.

⇒ The Privacy Act of 1974, as amended to establishes a code of fair information Practices that governs the collection, maintence, use and dissmination of information about individual.

(c) FOIA

⇒ FOIA Means Freedom of information Act

⇒ Since, 1967 the freedom of information Act has Provided the public the right to request access to records from any federal agency.

⇒ In India it is RTI (Right to info. Act-2005)

→ It is often described as the law that keeps citizens in the know about their government.

(d) ~~FERPA~~ FERPA

⇒ FERPA Means family Educational Rights and Privacy Act.

→ FERPA 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 ~~the~~ some control over the disclosure of Personally identifiable information from the education records.

→ when a student turns 18 Years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the Parents to the student.

(e) CFAA

⇒ CFAA Means Computer fraud and Abuse Act.

→ CFAA is the Federal anti-hacking statute that Prohibits ~~fraud~~ unauthorized access to computers and networks.

→ This Act was Passed in 1984.

(f) COPAA

⇒ COPPA means children's online Privacy Protection Act of 1998.

→ COPPA - 1998 to Protect the Privacy of children under the age of 13 by requesting Parental consent for the collection or use of any Personal information of web site users.

(g) VPPA

⇒ VPPA Means Video Privacy Protection Act.

→ ~~VPPA~~ VPPA that Prevents Wrongful disclosure of an individual's Personally identifiable information stemming from their rental or Purchase of audiovisual material, including videotapes, DVDs and video games.

(h) HIPPA

⇒ HIPPA means Health insurance Portability and Accountability Act - 1996.

→ HIPPA is a federal law that required the creation of national standards to Protect Sensitive Patient health information from being disclosed without the Patient's consent or knowledge.

(i) GLBA

⇒ GLBA means Gramm - Leach - Bliley Act.

→ GLBA requires financial institutions companies that offer consumers financial products or services like loans, financial or investment advice, or insurance - to explain their information sharing practices to their customers and to safeguard sensitive data.

(j) PCI DSS

⇒ PCI DSS stand for payment card industry Data security standard.

⇒ PCI DSS is an information security standard for organizations that handle branded credit

cards from the major card schemes. The PCI standard is mandated by the card brands but administered by the payment card industry security standards council.

(K) FCRA

→ FCRA stand for fair credit Reporting Act.

→ FCRA is federal law that regulates the collection of consumers' credit information and access to their credit reports.

→ It was passed in 1970 to address the fairness, accuracy and Privacy of the personal information contained in the files of the credit reporting agencies.

(L) FACTA

→ FACTA stand for fair and Accurate credit Transactions Act.

→ FACTA is 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.