Name : Tandel Bindiyaben Vasantbhai

Roll No : 42

Subject : ION

class : MCI - I

Assignment : I

*** Assignment - I ***

① List of all symetric key algorithms :

Ans. There are two types of symetric algorithms :
① Block algorithms
② Stream algorithms.

→ The list of symetric algorithm is following :

- AES (Advanced Encryption standard)
- DES (Data Encryption standard)
- IDEA (International data Encryption Algorithm)
- Blowfish (Drop-in replacement for DES or IDEA)
- RC4 (Rivest Cipher 4)
- RC5 (Rivest Cipher 5)
- RC6 (Rivest Cipher 6)

→ AES, DES, IDEA, Blowfish, RC5 and RC6 are Block ciphers.

→ RC4 is stream cipher.

② List of all asymmetric key Algorithms.

Ans. Encryption with asymmetric cryptography works in a slightly different way from symmetric key. encryption. someone with the public key is able to encrypt a message, providing confidentiality, and then only the person in possession of the private key is able to decrypt it.

→ Here the list of asymmetric key :

- Ed25519 singning
- x25519 key exchange
- Xd448 signing

- Elliptic curve cryptography
- RSA
- Diffie - Hellman key exchange
- DSA
- Key serialization
- Asymmetric Utilities

③ list of algorithms for message digest.

Ans. The list of algorithms for message digest is below.

- SHA3 - 512
- SHA - 384
- SHA
- SHA3 - 384
- SHA - 512/256
- SHA - 256
- MD2
- SHA - 512/224
- SHA3 - 256
- SHA - 512
- MD5
- SHA3 - 224

*** Assignment - 2 ***

⇒ briefly discussion of following topics :-

(a) PII (Personally Identifiable Information)

→ Personally Identifiable Information (PII) refers to data that can directly or indirectly identify individuals

① Direct Identification :-

The following PII directly identify an individual:

- Name, social security number, Biometric data

② Indirect information :-

- phone number it's not that always straight forward. which is Indirect information.

(b) US Privacy act of 1974

→ The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, established a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

(c) FOIA - Freedom of Information Act

→ Since 1967, the freedom of information Act (FOIA) has provided the public the right to request access to records from any federal agency. It is often described as the law that keeps citizens in the know about the government.

(d) FERPA

→ FERPA was enacted by congress to protect the privacy of student and their parents. The act is designed to ensure that students and parents of

coverage for workers who lose or change their job and the ultimately reduce the cost of healthcare by standarding the electronic transmission of administractive and financial transactions.

(i) COLBA

→ The Gramm-Leach-Bliley Act (GLBA).

→ It's also known as the financial modernization Act of 1999. It is United states federal law that requires financial institutions to explain how they share and protect their customes' private information.

(j) PCI DSS

→ Payment card Industry Data Security Standard

→ It stands for payment card industry data security standard. This global security standard for information is designed to enhance control over credit card data to prevent fraud. All businesses. regardless of size must follow PCI DSS requirment if they accept credit card payments from the five major brands.

(k) FCRA - Foregin Contribution Regulation Act

→ The FCRA was enacted with the primary purpose of regulating the inflow of foreign contributions and ensuring that the received foreign contributions are not utilized for purposes other than those specified under the legisation. All charitable organization in India recieving foreign contribution come under the purview of this Act.

vision

(1) FACTA

→ The foreign Account Tax compliance Act

→ It is a tax law that compels U.S. citizens at home and abroad to file annual reports on any foreign holdings. FACTA was endorsed in 2010 as part of the Hiring Incentives to Restore Employment (HIRE) Act to promote transparency in the global financial services sector.