Assignment :- 1 :- Networking Communication

Page No.
Date / /

① List all symmetric key Algorithms.

=> Symmetric encryption is a type of encryption where only one key (a secret-key) is used to both encrypt and decrypt electronic information.

-> There are two types of symmetric encryption algorithms :-

(1) Block algorithms.
(2) Stream algorithms.

-> List of symmetric key Algorithms :-

* AES (Advanced Encryption standard)
* DES (Data Encryption Standard)
* IDES (International Data Encryption ~~Algorithm~~ Algorithm)
* Blowfish (Drop-in replacement for DES or IDEA).
* RC4 (Rivest Cipher 4)
* RC5 (Rivest cipher 5)
* RC6 (Rivest cipher 6)

Note :- AES, DES, IDEA, Blowfish, RC5 and RC6 are block ciphers.
RC4 is stream cipher.

(2) List all Asymmetric key Algorithm.

=> Asymmetric key algorithms work in a simmilar to symmetric-key algorithms, where plaintext is combined with key, input to an algorithm, and outputs chipher text.

=> Asymmetric cryptography is branch of cryptography where a seoreet key can be divided into two parts, a Public key and a private key.

=> List of Asymmetric key Algorithm

* Ed25519 signing
* X25519 key exchange
* Ed448 signing
* X448 key exchange
* Elliptic curve cryptography
* RSA
* Diffie-Hellman key exchange
* DSA
* key serialization
* Asymmetric utilities.

(3) List the Algorithms for message digest.

=> The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function.

=> List of message Digest Algorithms

* MD2 :- The MD2 message digest Algorithm as define in RFC 1319.

* MD5 :- The MD5 message digest Algorithm as define in RFC 1321

* SHA-1, SHA-224, SHA-256, SHA-384, SHA-512/224, SHA-512/256.
  => Has Algorithms defined in FIPS PUB 180-4
  => secure Has Algorithms (SHA)

* SHA3-224, SHA3-256, SHA3-384, SHA3-512.

Assignment - 2

Page No.
Date / /

* Discuss briefly (one-two sentences)

(A) PII (Personal identifiable information)

⇒ PII is often referenced by US government agencies and non-governmental organizations.

(B) US Privacy Act of 1974

⇒ The Privacy Act of 1974, As Amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use and dissemination of information about individuals that is maintained in system of record by federal agencies.

(C) FOIA (Freedom of information Act)

⇒ This includes print documents, Photographs, Videos, maps, e-mail, and electronic records. In additional to releasing information upon written request, Agencies are required to publish instructions on How to make a FOIA request and Automatically publish certain information in online 'reading rooms.

(D) FERPA (family Educational Rights and Privacy Act)

⇒ FERPA of 1974 is also commonly referred to as the "Buckley Amendment".

(E) CFAA (Computer fraud and Abuse Act)

⇒ Also known as the Cfaa, is the federal anti-hacking statute that prohibits unauthorized access to computers and networks.

(F) COPAA (council of Parent Attorneys and Advocates)

⇒ The COPAA is an independent national American Association of Parents of children with disabilities, attorneys, Advocates, and related Professionals who Protect the legal and civilrights of students with disabilities and their families.

(G) VPPA

⇒ A VPPA is purely financial contract that provides RECs from a specific renewable energy Project located off your Company's property.

(h) HIPAA (Health Insurance Portability and Accountability Act).

⇒ The HIPAA sets the standard for sensitive patient data protection.

(i) GLBA (Gramm Leach - Bliley Act)

⇒ The financial services modernization Act, better known as GLBA, requires that financial institutions ensure the security of customer data, protect data against known or anticipated risks and secure data to protect it from unauthorized Access.

(j) PCI DSS (Payment Card Industry Data security Standard)

⇒ The PCIDSS is a security standard developed and maintained by the PCI council.

(k) FCRA (Fair Credit Reporting Act)

⇒ The FCRA is US federal legislation that promotes accuracy, fairness and privacy for data used by consumer reporting Agencies ...

(L) FACTA (Fair and Accurate Credit Transactions Act)

=> The FACTA is a federal law passed in 2003 designed to enhance consumer protections. FACTA is principally known for its provisions against identity theft.