Bridge Course

ION

Assignment - 1

Q1 List all Symmetric Key Algorithms

→ Following are the Symmetric Key algorithms:-

i) AES (i.e Advanced Encryption Standard)

ii) DES (i.e Data Encryption Standard

iii) IDEA (i.e International Data Encryption Algorithm

iv) Blowfish (Drop-in replacement for DES or IDEA)

v) RC4 (Rivest Cipher 4)

vi) RC5 (Rivest Cipher 5)

vii) RC6 (Rivest Cipher 6)

→ AES, DES, IDEA, Blowfish, RC5 & RC6 are block ciphers.

(Note: Block cipher: Set lengths of bits are encrypted in blocks of electronic data with the use of a specific secret key. As the data is being encrypted, the system holds the data in its memory as it waits for complete block.

→ RC4 is a stream cipher. Data is encrypted as it streams instead of being retained in the system's memory.

Q2 List all Asymmetric Key Algorithms

→ Following are the Asymmetric Key Algorithms:-

i) Ed25519 signing
ii) X25519 Key exchange
iii) Ed448 signing
iv) X448 Key exchange
v) Elliptic curve ~~cryptography~~ cryptography

vi) RSA (Rivest - Shamir - Adleman)
vii) Key Serialization
viii) Asymmetric Utilities
ix) Diffe - Hellman Key Exchange
x) DSA (Digital Signature Algorithm

Q3 List the algorithms for Message Digest.

→ Following are the Message Digest Algorithms

i) Message Digest 5 (MD5)
ii) Secure Hash Algorithm-1 (SHA-1)
iii) Secure Hash Algorithm-256 (SHA-25

Assignment - 2

Q1

1) PII (i.e Personally Identifiable Information):

→ Personally identifiable information (PII) is any data that could potentially identify a specific individual. It is essential for personal privacy, data privacy, data protection, information privacy & information security.

2) US Privacy Act of 1974:

→ The US Privacy Act of 1974 establishes 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.

→ This Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual.

3) FOIA:

→ FOIA stands for Freedom of Information Act.

→ Since 1967, FOIA has provided the public the right to request access to records from any federal agency.

4) FERPA:

→ FERPA stands for Family Educational Rights & Privacy Act.

→ The Act is also known as Buckley Amendment.

→ It is a United States Federal law that governs the access to educational information & records by public entities such as potential employers, publicly funded educational institutes & foreign governments.

5) CFAA:

→ CFAA stands for Computer Fraud and Abuse Act.

→ It is a United States cybersecurity bill that was enacted in 1986 as an amendment to existing Computer Fraud law.

→ The law prohibits accessing a computer without authorization or in excess of authorization

6) COPAA

→ The Council of Parent Attorneys and Advocates (COPAA) is an independent national American association of Parents of children with disabilities, attorneys, advocates, and related professional who protect the legal & civil rights of students with disabilities & their families.

7) VPAA :

→ VPAA stands for Vice President for Academic Affairs.

→ It works closely with the President, other Vice presidents, the Deans of colleges & Directors of units to set the academic priority for the University

8) HIPAA.

→ The Health Insurance Portability and Accountability Act of 1996 is a united states federal statue enacted by the 104th United States Congress & signed on August 21, 1996.

→ It was created primarily to modernize the flow of healthcare information, stipulate how PII maintained by the healthcare and healthcare insurance industry should be protected from fraud & theft, & address limitations on healthcare insurance coverage

9) GLBA:

→ The Gramm-Leach-Bliley Act is also known as the Financial Modernization Act of 1999. It is a United states Federal law that requires financial institutions to explain how they share and protect their customers private information.

10) PCI DSS:

→ The 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.

11) FCRA:

→ The Foreign Contribution (Regulation) Act, 2010 is an act of the Parliament of India, by the 42nd Act of 2010.

→ It is a consolidating act whose scope is to regulate the acceptance and utilisation of foreign contribution or foreign hospitality

12) FACTA:

→ Fair and Accurate Credit Transactions Act (FACTA) is an amendment to Fair Credit Reporting Act (FCRA) that was added, primarily, 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