Name :- Keyur Patel

Roll No. :- 26

Class :- MCA - I

Subject :- ION

Professor :- Dr. Hardik Joshi

Assignment :- I

① List of all symmetric algorithms.

→ AES (Advanced Encryption Standard)

DES (Data Encryption Standard)

IDEA (International Data Encryption Algorithm)

Blowfish

RC4 (Rivest Cipher 4)

RC5 (Rivest Cipher 5)

RC6 (Rivest Cipher 6)

CAST-128 (aka CAST5)

CAST-256

Twofish

Serpent

MARS

Rijndael

(Followed by Anubis, Grand Cru, Kalyna)

→ National Algorithms

Magma (aka GOST 28147-289) ]
Kuznyechik (aka GOST R 34.12-2015) ] → Russia

SM1 ]
SM4 ] → China

SEED ] → South Korea

BATON, JUNIPER, SKIPJACK and many others National Security Agency (NSA), U.S. Government.

② List all asymmetric key algorithms

→ Diffie - Hellman key exchange

→ RSA (Rivest Shamir Adleman)

→ ECC (Elliptic Curve Cryptography)

→ El Gamal Cryptosystem

→ DSA (Digital Signature Algorithm)

→ Paillier cryptosystem

→ Cramer - Shoup cryptosystem

→ YAK

→ NTRUEncrypt

→ McEliece

→ Merkle - Hellman knapsack cryptosystem

→ Protocols using asymmetric key algorithms include S/MIME, GPG, EMV, IPsec, PGP, ZRTP (a VoIP protocol), SILC, SSH, Bitcoin, Transport Layer Security, Secure Socket Layer

(3) List the algorithms for message digest

→ MD2 (Message Digest)

→ MD5

→ SHA - 1 (Secure Hash Algorithm)

→ SHA - 224

→ SHA - 256

→ SHA - 384

→ SHA - 512

→ SHA2

→ SHA3

(4) Discuss briefly (one - two sentences) :-

1. PII (Personally Identifiable Information)

→ PII is any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

2. 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 systems of records by federal agencies.

3. FOIA

→ The freedom ~~of~~ of Information Act, 5 U.S.C. § 552, 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~~ request.

4. FERPA

→ The Family Educational Rights and Privacy Act of 1974 is a United States federal law that governs the access to educational information and records by public entities such as potential employers, publicly funded educational institutions, and foreign governments.

5. 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.

6. COPAA

→ The Council of Parent Attorneys and Advocates is an independent national American association of parents of children with disabilities, attorneys, advocates, and related professionals who protect the legal and civil rights of students with disabilities and their families.

7. VPPA

→ A Virtual Power Purchase Agreement is a popular type of renewable energy contracting structure that provides a financial hedge against future energy fluctuations. It is a purely financial contract that provides RECs from a ~~specific~~ specific renewable energy project located off your company's property. In the U.S., each REC represents proof that 1 megawatt-hour (MWh) of electricity was generated from an eligible renewable energy resource.

8. HIPAA

→ The Health Insurance Portability and Accountability Act of 1996 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.

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 is a set of security standards formed in 2004 by Visa, MasterCard, Discover Financial Services, JCB International and American Express. Governed by the Payment Card Industry Security Standards Council (PCISSC) the compliance scheme aims to secure credit and debit card transactions against data theft and fraud.

11. FCRA

→ The Fair Credit Reporting Act is a 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.

12. FACTA

→ Fair and Accurate Credit Transactions Act is an amendment to FCRA (Fair Credit Reporting Act) 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.