

(ION)  
Assignment - I

ROLL NO:- 6

PAGE NO. 1

DATE: KARAN  
(CHHATLANI)

Q.1 List all Symmetric Key algorithms.

Ans. (1) ADVANCED ENCRYPTION STANDARD (AES)

(2) DATA ENCRYPTION STANDARD (DES)

(3) INTERNATIONAL DATA ENCRYPTION  
ALGORITHM (IDEA)

(4) BLOWFISH

Q.2 LIST OF ALL ASYMMETRIC KEY ALGORITHMS

- Ans.
- (1) RIVEST SHAMIR ADLEMAN (RSA)
  - (2) ELLIPTIC CURVE CRYPTOGRAPHY (ECC)
  - (3) DIGITAL SIGNATURE ALGORITHM (DSA)

Q.3 LIST THE ALGORITHMS FOR MESSAGE-DIGEST.

Ans.

(1) "MD2"

(2) "MD4"

(3) "MD5"

(4) "SHA-1"

(5) "SHA-256"

(6) "SHA-512"

(7) "SKEIN"

(8) "TIGER"

(9) "WHIRLPOOL"

(ION)

ROLL NO:- 6

PAGE NO.

4

DATE:

(NAME: KARAN

CHHATLANI)

Discuss briefly (one-two sentences)

(a) PII (Personally Identifiable Information)

⇒ Personally Identifiable Information (PII) is any data that can be used to identify a specific individual.

- For instance, social security numbers, mailing or email address, and phone numbers have most commonly been considered PII, but by the times technology has expanded the scope of PII considerably.

(b) US PRIVACY ACT OF 1974

⇒ The Privacy Act of 1974, establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.

### (C) FOIA

⇒ The Freedom of Information Act (FOIA), is a federal law that requires the full or partial disclosure of previously unreleased information and documents controlled by the United States Government upon request.

- This Act was effective from July 5, 1967.

### (D) FERPA

⇒ The Family Educational Rights and Privacy Act (FERPA) is a federal law enacted in 1974.

- This Act protects the privacy of student education records.

### (E) 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. The Law prohibits accessing a computer without authorization, or in excess of authorization.

## (F) COPAA

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

## (G) VPPA

⇒ The Video Privacy Protection Act (VPPA) was a bill passed by the United States Congress in 1988 as Publication. It was created to prevent what it refers to as "wrongful disclosure of video tape rentals or sale records."

## (H) 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.

## (I) GLBA

⇒ Owing to the sensitive nature of financial information, the U.S. Congress passed the Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, to protect consumer financial privacy.

## (J) PCI DSS

⇒ The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements intended to ensure that all companies that process, store or transmit credit card information maintain a secure environment.

## (K) FCRA

⇒ The Foreign Contribution Regulation Act, 1976 casts certain obligation on banks in regard to acceptance of foreign inward remittances for onward credit to the accounts of associations in India.

## (L) FACTA

⇒ The Fair and Accurate Credit Transaction Act (FACTA) is a federal law enacted by the United States Congress in 2003. Its stated purpose was to enhance consumer protections, particularly in relation to identity theft.



