

Date \_\_\_\_\_  
Page \_\_\_\_\_

Name: Dheeraj M. Shrivastava  
Roll No.: 36 class - MCA - I  
Subject : ITN

## (1) List of all Symmetric Algorithms

→ Symmetric encryption is a type of encryption where only one key is used to both encrypt and decrypt electronic information.

- This encryption method differs from asymmetric encryption where a pair of keys one public and one private, is used to encrypt and decrypt message.

### - Examples

AES → Advanced Encryption Standard

DES → Data Encryption Standard

IDEA → International Data Encryption Algorithm

Blowfish

RC4 → River Cipher

## (2) List all asymmetric key algorithms

→ Asymmetric key algorithms work in a similar manner to symmetric key algorithm where plain text is combined with a key, input to an algorithm and output

ciphertext.

- The key pair is comprised of a private key and a public key as the name imply the public key is made available to everyone where as the private key is kept secret.

- Example:

Diffie

DSS  $\Rightarrow$  Digital Signature Standard

~~Eigamal~~

Elliptic - curve cryptography.

(3) List the algorithms for message digest.

$\rightarrow$  MD5  $\Rightarrow$  Message Digest 5.

SHA - 1  $\Rightarrow$  Secure hash Algorithms.



Name: Dhairya M. Shah  
Roll No: 36 Class - MCA-I  
Subject - IT

(1) PII

→ Personal Identifiable Information  
- PII is any data that could potentially identify a specific individual.

(2) US Privacy Act of 1974

→ Establishes a code of fair information practices that governs the collection, maintenance, use and dissemination of information about individual that is maintained in systems of records by federal agencies

(3) FOIA

→ Freedom of Information Act  
- FOIA, is a federal freedom of information law that requires the full or partial disclosure of previously unreleased information and documents controlled by the U.S. government upon request.



(4) FERPA

→ Family Educational Rights and Privacy Act.

- FERPA is a federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

(5) CFAA

→ Computer Fraud and Abuse Act.

- CFAA is a U.S. cybersecurity bill that was enacted in 1986 as an amendment to existing computer fraud laws, which had been included in the Comprehensive Crime Control Act of 1970.

(6) COPPA

→ Children's Online Privacy Protection Act.

- The COPPA of 1996 is a U.S. federal law, located at 15 U.S.C. 6501-6506.

(7) VPPA

→ Virtual Power Purchase Agreement.

- A VPPA is a purely financial contract that provides RECs from a specific renewable energy project located off your company's property.



(8) HIPAA

→ Health Information Privacy

- HIPAA is a federal law that required the creation of national standard to protect sensitive patient health information from being disclosed without the patients consent or knowledge.

(9) GLBA

→ The Gramm-Leach-Bliley Act is also known as the financial modernization Act of 1999.

(10) PCI DSS

→ 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.