

## Assignment - 1

Q.1) List all Symmetric key algorithm.

- i) Advanced Encryption Standard
- ii) Data Encryption standard
- iii) International Data Encryption Algorithm.
- iv) Blowfish
- v) Rivest cipher 4 (RC4)
- vi) Rivest cipher 5 (RC5)
- vii) Rivest cipher 6 (RC6)

Q.2) List all asymmetric key Algorithm.

- i) RSA
- ii) Diffie - Hellman
- iii) ElGamal
- iv) ECD

Q.3) List all algorithms for message digest.

- i) MD5
- ii) SHA-1

## Assignment - 2.

(A) PII :-

Personal Identifiable Information is any information that could potentially identify a specific individual.

(B) 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 system of any Federal agency.

(C) FOIA :-

It requires the full or partial disclosure of previously unclassified information and documents controlled by United States government upon request.

(D) FERPA :-

It governs the access to educational information records by public entities such as potential employers, public funded educational institutions and foreign governments.

(E) CFAA :-

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

(F) COPPA :-

The Children Online Privacy Protection Act.

(G) UPPA :-

It regulates the disclosure of information about customer consumption of video content, imposing prescriptive requirement to obtain consumers consent to such disclosure.

(H) HIPPA :-

It ensures that individual health care plans are portable and transferable.

(I) CFPB :-

It requires financial institutions (Companies) that offer consumers financial products or services like loans financial or investment advice or insurance to explain their information sharing practices to their customers.

(J) FEPA :-

The FEPA regulates foreign donations and ensures that such contributions don't adversely affect internal security.

(K) FACTA :-

FACTA is principally known for its provisions against identity theft.

### Assignment - 3

Q.1)

State the Full Form :-

1) RADIUS :-

Remote Authentication Dial-In User Service

2) TACACS :-

Terminal Access Controlled Access Control Service

3) L2TP :-

Layer 2 Tunneling Protocol.

4) PPTP :-

Point-to-point Tunneling Protocol

5) EAP :-

Extensible Authentication Protocol.

6) CHAP :-

Challenge - Handshake Authentication Protocol

7) NTLM :-

Windows Challenge Response

8) PAP :-

Password Authentication protocol

9) SSH :-

Secure Shell

10) LDAP :-

Lightweight Directory Access Protocol

## Assignment - 4

Q. 1) List Names of Software :-

1) Firewall :-

- i) Fortigate
- ii) Sophos XE Firewall
- iii) Watchguard Network Security
- iv) Sonicwall
- v) Cisco
- vi) Ciscofire Firewall

2) Intrusion, Detection and Prevention :-

- i) OSSEC
- ii) Snort
- iii) Suricata
- iv) Security Onion.

3) Anti-virus :-

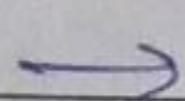
- i) BitDefender
- ii) Norton Antivirus
- iii) Avast! Antivirus
- iv) Trend Micro
- v) Kaspersky Antivirus

4) Packet Sniffing :-

- i) Wireshark
- ii) Steel Central packet Analyzer
- iii) NetworkMiner

Q.2)

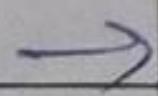
State any 10 security software used by ethical hackers.



- i) Metasploit Framework.
- ii) Nmap
- iii) Ophcrack
- iv) Netbeeshark
- v) Nessus
- vi) Aircrackng
- vii) Snort
- viii) John the Ripper
- ix) L0phtcrack.

Q.3)

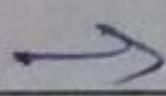
What is the role of CCERT.



CCERT primary role is to raise Security Awareness among Indian Cyber Community and to provide technical assistance and advise them to help them recover from Computer Security incidents.

Q.4)

List 8 ASP top 7.



- i) Injection
- ii) Broken Authentication
- iii) Sensitive Data Exposure
- iv) XML External Entities
- v) Broken Access Control
- vi) Security misconfigurations.

- vii) Cross site Scripting
- viii) Insecure Deserialization.
- ix) Insufficient logging
- x) Monitoring