

# Assignment - 1

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

1) List all symmetric key algorithm.

- > Advanced Encryption Standard
- > Data encryption model.
- > International Data encryption.
- > Blowfish
- > Rivest Cipher 4 (RC4)
- > Rivest Cipher 5 (RC5)
- > Rivest Cipher 6 (RC6)

2 List all asymmetric key algorithm

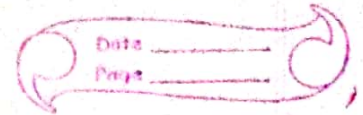
- > RSA
- > Diffie-Hellman
- > ElGamal
- > ECC.

3. List all algorithm for message digest

- > MD5
- > SHA-1



## Assignment - 2



a) PII :-

Personal Identifiable Information is any data 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 by 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 of to educational information and records by public entities such as potential employers public funded educational institutes and foreign government.

e) CFAA :-

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



3  
f) COPAA :-

The children online privacy protection act.

g) VPPA :-

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

h) HIPAA :-

Ensures that individual health care plans are accessible, portable and renewable.

i) FCRA :-

The FCRA regulates foreign denotations and ensures that such contributions do not adversely affect internal security.

k) FALTA :-

FALTA is principally known for its provisions against identity theft.



4

## Assignment - 3

1) state the full form :-

① RADIUS :-

Remote Authentication Dial - In user service

② TACACS :-

Terminal Access controller Access control

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

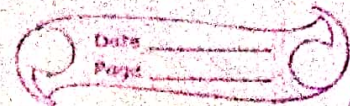


(9) SSH :-  
Secure shell :-

(10) LDAP :-  
Lightweight Directory Access protocol.



## Assignment - 4



1. List Names of Software :-

1) Firewall :-

Fortigate.

Sophos Xc firewall

Watch guard Network Security

Sonicwall

Cisco

Glasswire firewall.

2. Intrusion Detection & prevention

OSSEC

Snopt

Suricata

Security onion.

3. Anti Virus.

Bitdefender.

Norton Antivirus

Avira Antivirus

Trend Micro

Kaspersky Antivirus



#### (4) Packet sniffing:-

wireshark

Stel central Packet Analyzer.

Network Mines

Kismet.

#### 2. State any 10 Security Software used by ethical hacker.

Metasploit framework

Nmap.

openssh.

wireshark.

Netcat

Aircrackng

Shor.

John the Ripper.

Lophcrack.

#### 3. What is the role of CERT

CERT primary role is to raise security awareness among Indian cyber community and to provide technical assistance and advice them to help them recover from computer security incidents.



#### 4. List OWASP top 10

##### - Injection

Broken Authentication

Sensitive Data Exposure

XML External Entities

Broken Access Control

Security Misconfigurations

Cross Site Scripting

Insecure deserialization

Insufficient logging and monitoring