1. List all symmetric key algorithm.

→ Advanced Encryption standard.
→ Data Encryption model.
→ International Data Encryption Algorithm.
→ Blowfish
→ Rivest Cipher 4   (RC4)
→ Rivest Cipher 5   (RC5)
→ Rivest Cipher 6   (RC7)

2. List all asymmetric key algorithm.

→ RSA
→ Diffie- Hellman
→ Elgermal
→ ECC

3. List all algorithms for message digest

→ MD5
→ SHA-1

a. P II :-

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 pratices that governs the collections maintenance use and dissemination of information about individual that is maintained in system of by federal agencies.

c. FOIA :-

It requires the full or partial disclosure of previously unreleased information and documents controlled by united states goverment upon request.

d. FERA :-

It governs the access to educational information and records by public entities such as potential employers public funded educational institutes

and foreign goverments.

e. CFAA :-

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

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 GLBA :-

It requires financial institutions companies that offer consumers financial ~~or~~ products or services like loans financial or investment advice or insurance – to explain their information sharing pratices to their customer.

i FCRA :-

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

k FACTA :-

FACTA is principally known for its provisions against identity theft.

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.
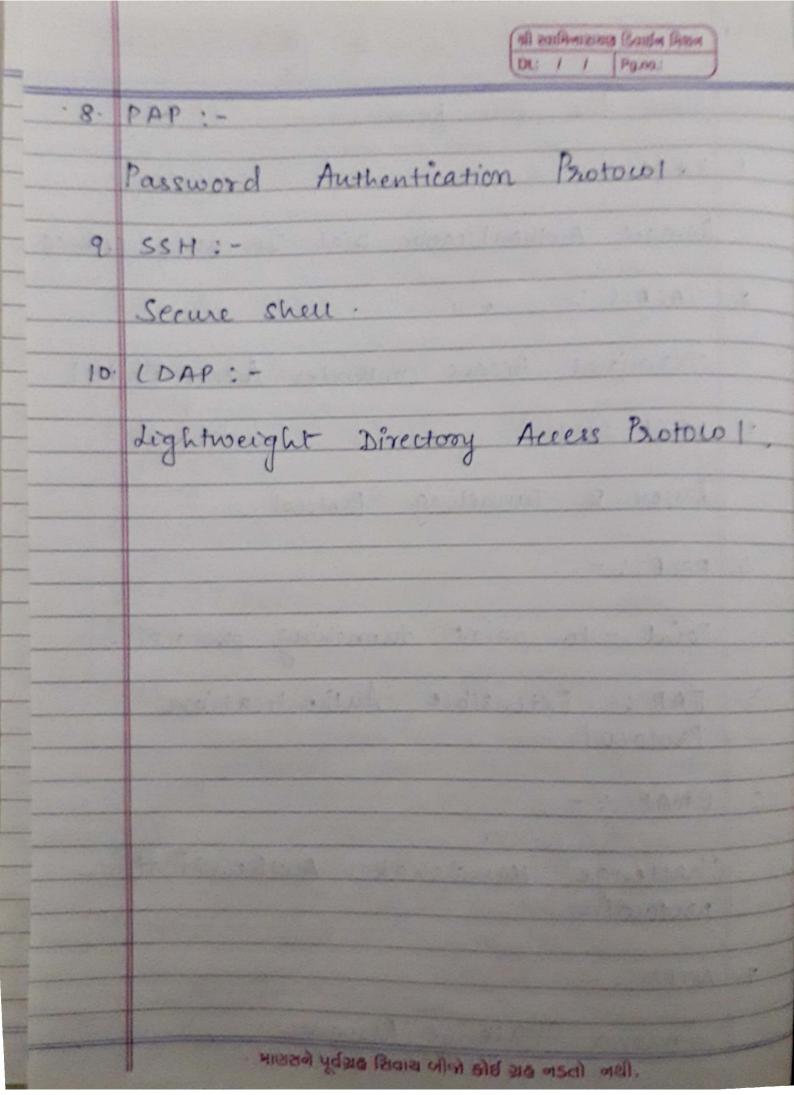
4. PPTP : -

   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.

1. List names of software :-

1. Firewall :-

   Fortigate
   Sophos xa firewall
   watch Guard Network Security
   Sonicwall
   Cisco
   Glass wine firewall

2. Intrusion Detection & prevention :-

   O.SSEC
   Snort
   surrates
   Security Onion

3. Anti virus :-

   Bitdefender
   Norton Antivirus.
   Avira Antivirus
   Trend Micro
   kaspersky Antivirus.

4. Packet Sniffing :-

Wireshark
Steel Central Packet Analyzer
NetworkMiner
Kismet.

2. State any 10 security software used by so ethical hacker

Metasploit framework.
Nmap
OpenSSH
Wireshark
Nerus
Aircracking
Snort
John the Ripper
Lophtcrack

3. what is the role of CERT.

CERT primary role is to noise 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 ten.

Injection
Broken Authentication
Sensitive Data Exposure
XML External Entities
Broken Access Control
Security misconfigurations
Cross site scripting
Insecure deserilization.
Insufficient logging and monitoring.