

Ans:

## Assignment-1

- Q1 List all Symmetric Key Algorithm
- ↳ Digital Encryption Standard (DES)
  - ↳ Triple DES (3DES)
  - ↳ IDEA
  - ↳ BLOW FISH

- Q2 List all Asymmetric key algorithm
- ↳ RSA
  - ↳ DSA
  - ↳ ElGamal

- Q-3 List the algorithms for message digest
- ↳ SHA2
  - ↳ SHA1
  - ↳ MD5
  - ↳ HAVAL
  - ↳ SHA512
  - ↳ SHA3

## Assignment 2

- Q1 Discuss Briefly

- Q1) PII (Personally Identifiable Information)
- PII is any data that can be used to identify a specific or specific individual.

### (b) US Privacy Act of 1974

The Privacy Act 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practice that governs the collection, maintenance, use and dissemination of information about individuals that is maintained in system of records by federal agencies.

### (c) FOIA :

The Freedom of Information Act, 5 U.S.C. § 552 is a federal freedom of information law that requires the full or partial disclosure of previously unreleased information and documents controlled by the United States Government.

### (d) FERPA

The Family Educational Rights and Privacy Act is a federal law that affords parents the right to have access to their children's education records.



(e) CFAR

The Computer Fraud and Abuse Act is a US Cyber Security bill that was enacted in 1986 as an amendment to existing computer fraud law, which had been included in the Comprehensive CCC Act.

(f) COPAA

Council of Parent Attorneys and Advocates is an ~~idea~~ independent national American association of parent of children with disabilities, attorneys, advocates and related professionals who protects the legal and civil right of students

(g) VPPA

Virtual Power Purchase Agreement  
the contract, the corporate buyer does not own and is not responsible for the physical electricity generated by the power.  
The VPPA is purely a financial transaction

cn) HIPAA

The Health Insurance Portability and Accountability Act of 1996 is a United States federal statute enacted by the 104th US Congress and signed into law by President Bill Clinton.

ci) GLBA

The Gramm Leach Bliley Act is also known as the Financial Modernization Act of 1999. It is a US Federal law that requires financial institutions to explain how they share and protect their customer's private information.

cj) PCI DSS

The Payment Card Industry Data Security Standard is an information security standard of organization that handle branded credit card from the major card schemes.

ck) FCRA

The Foreign Contribution Act, 2010 is an act of the Parliament of India by the 16th act of 2010. It is a consolidating act whose scope is to



regulate the acceptance and utilization of foreign contribution.

## (1) FACTA

Fair and Accurate Credit Transaction Act is an amendment to FCRA that was added primarily to protect consumers from identity theft.

## Assignment-3

Q-1 State the full form for

(1) RADIUS :- Remote Authentication Dial-In User Service

(2) TACAS :- Tools and Algorithm for the Construction and Analysis

(3) L2TP & PPTP  
Layer 2 Tunneling Protocol  
Point-to-Point Tunneling Protocol

(4) PPP - Purchasing Power Parity

(5) EAP :- Extensible Authentication Protocol

- (6) CHAP :- Challenge Handshake Authentication Protocol.
- (7) NTLM:- New Technology LAN Manager
- (8) PAP:- Password Authenticate Protocol
- (9) SSH :- Secure Shell
- (10) LDAP:- Light Weight Directory Access Protocol.

### Assignment-4

- ① List all the names of Software
  - (i) Firewall
    - ↳ SolarWinds Network Firewall Security
    - ↳ System Mechanic Ultimate Defence
    - ↳ ZoneAlarm
    - ↳ Comodo Firewall
    - ↳ Tinywall
  - (ii) Intrusion Detection & Prevention
    - ↳ Snort
    - ↳ Suricata
    - ↳ McAfee HIP
    - ↳ Trend Micro Tipping Point.



↳ Hillstone NIPS    ↳ Huawei NIP

Civ) Anti-Virus

↳ Norton                      ↳ Kaspersky

↳ Eset                          ↳ AVG

↳ Avast                        ↳ Quick Heal

Civ) Packet Sniffing

↳ Solarwind                ↳ Pcapless PPTP

↳ ManageEngine NetFlow Analyzer

↳ Service Omnicast

↳ tcpdump                ↳ Wireshark

Q2 State any 10 security software used by ethical hackers

↳ Nmap                                ↳ Metasploit

↳ Intruder                          ↳ Armitage - Ng

↳ Metasparker                      ↳ Acunetix

↳ Acunetix                          ↳ Tenable Nessus

↳ Burp Suite                        ↳ Ettercap

Q3 What is role of CERT

The role of CERT 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.

Q4 List OWASP top ten example.

- ↳ Injection
- ↳ Broken authentication
- ↳ Sensitive data exposure
- ↳ Sensitive XML external entities
- ↳ Broken access control
- ↳ Security misconfiguration
- ↳ Cross-site scripting
- ↳ Insecure deserialization
- ↳ Using components with known vulnerabilities
- ↳ Insufficient logging and monitoring