**INSTITUTE OF TECHNOLOGY**

**Department of Information Technology**

**Subject: IAS & IASL**

**Class: BE [IT]**

**Important questions for oral and theory**

1. What are different IT laws for India?

2. Cryptography vs Steganography vs Data hiding?

3. What is Joint ownership? Explain secret splitting and secret sharing.

4. Compare and contrast Stream Ciphers vs Block Ciphers.

5. Differentiate between Symmetric Key Algorithms and Asymmetric Key Algorithms

6. What is the difference in DES & AES.

7. Use of BLOWFISH? Describe Blowfish.

8. Attacks on DES.

9. Explain different modes of Operations.

10. Differentiate between Linear Cryptanalysis and Differential Cryptanalysis.

11. What do you mean by Public Key Algorithms?

12. What is RSA? Explain Key Generation and Usage.

13. Explain Elliptic Curve Cryptography.

14. What is the output of Hash Algorithms

15. Differentiate between SHA-1 & MD5.

16. What are the different ways of Key Generation and Distribution?

17. What is a Digital Certificate?

18. What is Digital Signature?

19. What is revocation? When is it required to be done?

20. What do you mean by PKI? Explain.

21. Explain Diffie Hellman Key Exchange.

22. How is authentication done? Explain One Way Authentication, Mutual Authentication?

23. Explain Neeham Schroeder Protocol.

24. What is IPSEC? Explain AH and ESP in Tunnel Mode and Transport Mode?

25. What are Security Associations?

26. Explain SSL?

27. Describe Handshake Protocol and Record Layer Protocol.

28. What is IKE- Internet Key Exchange Protocol?

29. What is the necessity of Intrusion Detection Systems?

30. Explain Anomaly Based, Signature Based, Host Based, Network Based Systems?

31. Using the Extended Euclidean algorithm, find the multiplicative inverse of

* 1. 1234 mod 4321
  2. 24140 mod 40902
  3. 550 mod 1796
  4. 550 mod 1796

1. Explain the OSI security architecture in detail.
2. Describe the transposition techniques in detail.
3. Explain the Monoalphabetic ciphers in detail with suitable example.
4. Explain the concept of secret splitting and secret sharing.
5. What is the CRT?
6. What is Computer Forensics?
7. Why do individuals and organizations need to pay attention to Computer Forensics?
8. What is digital data?
9. Why knowledge of Computer Forensics so important?
10. What does a Computer Forensics specialist do?
11. What should a company do if an incident occurs?
12. Explain the concept of industrial espionage through social engineering.
13. What are different methods of Industrial Epsionage?
14. How can we prevent Industrial Epsionage?
15. What are the risk factors due to Industrial Epsionage? Give the impact of Loss.
16. Discuss on Internet Scams and some easy ways to protect yourselves.
17. What are Investment Scams? What are its different types?
18. How E-mail Scams Work? Discuss on how to report and avoid them?
19. Spam mail - 'Nigerian fraud 419', Discuss.
20. What are Corporate Epsionage Techniques? Which are high risk industries?
21. What is phishing scam? How does it work?
22. What is the Indian IT Act? Give the Scope and Coverage of the Indian IT Act.
23. Write notes on following
    1. Laws of intellectual property Rights (IPR)
    2. Patent Law
    3. Copyright Law
24. What are benefits of ISO 27001certification?
25. Write a note on Payment types.
26. Explain the concept of Mobile Payments.
27. What are the possible attacks on the E-Transaction using cards?
28. Discuss the issues and concerns for Payment over the Internet.
29. Write a note on Electronic Cash.