

BCS703 - Cryptography & Network Security

Important Question Bank

Module 1:

1. What is Cryptography? With neat diagram explain Symmetric cipher model & model for network security.
2. Explain Substitution Techniques with example (such as Caesar cipher, monoalphabetic ciphers, poly alphabetic cipher, vigenere cipher, vernam cipher, playfair cipher & OTP) with its advantage & disadvantages.
3. what is block cipher & stream cipher? With neat diagram explain Feistel cipher and algorithm (May ask Feistel Encryption & Decryption also)
4. With neat diagram Explain DES working & it's encryption algorithm with example.
5. What is cryptanalyst? Explain it's type of attacks.
6. Problems on Playfair cipher & caser cipher & hill cipher.
7. List and Explain block cipher principles.

Module 2:

8. What is pseudorandom number generators? With neat diagram Explain its types of algorithms for PRNGs (May ask Explain LCG &BBS generator)
9. What is Public key cryptosystems? Explain public key cryptosystems and its principles and applications with neat diagram (May ask Explain public key encryption and decryption with example)
10. Explain requirements for public key cryptography and public key cryptanalysis.
11. Explain RSA Algorithm and how is RSA key generation and security Explain and do it's problems
12. Explain secrecy and authentication in public key cryptosystem.
13. Explain encryption and decryption in ELGamal and cryptosystems with example.
14. Explain Diffie Hellman key exchange algorithm with example.
15. With a neat diagram explain Middle Man Attack with example.

Module 3:

16. Explain symmetric key distribution using symmetric and asymmetric encryption.
17. what are cryptographic hash functions? Explain its applications (May ask with diagram of explain man in middle attack in hash functions)
18. Explain two sample hash functions with neat diagram.
19. What is key management? With a neat diagram Explain KDC and KDS and explain KDC major issues.
20. With a neat diagram explain control vector encryption and decryption & explain how controlling key usage.
21. Explain the various techniques used in distribution of public key. (May ask explain categories of DPK or different ways)
22. With a neat diagram Explain decentralized key distribution

Module 4:

23. What is user authentication? How many steps involved in authentication? With a neat diagram explain NIST asap 800-63-2 E – Authentication.
24. Explain one way authentication and explain about authentication protocol and replay attacks with example.
25. Explain remote user authentication principles.
26. Explain remote user authentication using symmetric and asymmetric encryption.
27. what is Kerberos? Explain Kerberos authentication service with version 4 dialogue with message exchange.
28. With a neat diagram explain overview of Kerberos.
29. Explain web security consideration and TL security.

Module 5:

30. Briefly explain the concept of DKIM. With a neat diagram Explain DKIM functional flow & it's strategy.
31. Explain IP security architecture.
32. Explain the ESP format. Explain transport mode & tunnel mode of ESP.
33. Explain benefits, services, applications, documents and routing applications of IPsec.
34. Explain IPv4 and IPv6 (May ask difference between IPv4 & IPv6).
35. Explain security associations with SA parameters.
36. Explain transport mode & tunnel mode of IPsec.
37. With a neat diagram, Explain IKE v2 exchange.