Department of Computer Science and Engineering
Cryptography and Network Security
CSE-S510

Q1. What do you understand by sniffing and spoofing? Explain.

Q2. What is masquerade? Which principle of security is breached because of that?

Q3. What is the difference between monoalphabetic cipher and polyalphabetic cipher?

Q4. Distinguish between passive and active security attack. Name some passive attacks. Name some active attacks. Explain ?

Q5. Explain the Avalanche Effect.

Q6. What do you understand by DES? Explain the working of DES.

Q7. What is double DES? What kind of attack on double DES makes it useless?

Q8. Explain the principles of the IDEA Algorithm.

Q9. Distinguish between differential and linear cryptanalysis.

Q10. What is the difference between session key and master key?

Q11. List four general categories of schemes for the distribution of public keys.

Q12. What is the position of SSL in TCP/IP protocol suite and Why?

Q13. Show that in DES the first 24 bits of each subkey come from the same subset of 28 bits of the initial key and the second 24 bits of each sub key come from a disjoint subset of 28 bits of the initial key.

Q14. What is HMAC. Explain with suitable diagram.

Q15. Explain Diffie-Hellman key exchange algorithm.

Q16. Given two prime numbers p=13 and q=19 find out N, E and D in RSA encryption process.

Q17. Given two prime numbers P=17 and Q=29, find out N, E and D in an RSA encryption process.

Q18. List some common type of hijacking attacks. How can replay attacks be prevented?

Q19. In the Diffie –Hellman protocol, what happens if x and y have the same value, that is Alice and Bob have accidentally chosen the same number? Are R1 and R2 the same? Do the session keys calculated by Alice and Bob have the same value? Use an example to prove your claims.

Q20. List the security services provided by a digital signature. Compare and contrast a conventional signature and a digital signature.

Q21. Show an Example of the vulnerability of RSA to selective forgery when the values of p and q are small. Use p = 19 and q = 3.

Q22. What do you understand by Message Authentication code? Explain the Disadvantages of HMAC.

Q23. Define CFB and list its advantages and disadvantages. Show why CFB mode creates a nonsynchronous stream cipher, but OFB mode creates a synchronous one?

Q24. In an electronic mail system, what are roles of User Agent, Message Transfer Agent and Message Access Agent?

Q25. Explain the following.

i) Why the SSL Layer positioned between the application layer and the transport Layer?
ii) What is the purpose of SSL Alert protocol?
iii) How SHTTP different from SSL?
iv) What is the significance of the time stamping protocol?
v) Describe how master secret is created from pre-master secret in SSL?

Q26. How does SET protect payment information from the merchant? What is the difference between SSL and SET?

Q27. What is firewalls .Explain Types of firewalls.
A) Packet filters

B) Application gatways

Q28. What is Biometric Authentication? How does biometric works?

Q29. What is Digital Signature? Explain in the reference of key principal of security.

Q30. What is message Digest? Explain MD5 Algorithm and compare this with SHA-1 Algorithm.

Q31. Explain Playfair cipher with suitable Example.

Q32. Explain Hill cipher with suitable example.

Q33. Explain the difference between substitution and transposition techniques.

Q34. What do you understand by algorithm types and algorithm modes? Explain.

Q35. Explain Secure Socket Layer. And Also Explain the Working of SSL.

Q36. What do you understand by public key cryptography?

Q37. What is the difference between phishing and pharming?

Q38. What is stegnography?

Q39. Give a Brief Introduction to TCP/IP.

Q40. Writes short notes.

i) Firewall
ii) VPN
iii) WAP
iv) S/MIME
v) IP security
vi) SMTP
vii) IEEE 802.11 security

****