Self-assessment questions - Cryptology etc.

1. What is meant by encryption and decryption of messages?

2. What is the difference between steganography and cryptology?

3. What is meant by a substitution cipher?

4. What is the difference between simple substitution and polyalphabetic substitution?

5. What is the difference between monogram and polygram substitution?

6. Briefly describe four types of simple substitution ciphers.

7. What is meant by a brute force attack?

8. How can simple substitution ciphers be broken? (two alternatives)

9. Briefly describe how the Vigenere cipher works.

10. How can the Vigenere cipher be broken?

11. Explain the difference between symmetric and asymmetric cryptography.

12. What is the difference between stream ciphers and block ciphers? Give one example of each.

13. Briefly explain what is meant by a product cipher and list its advantages.

14. List the main characteristics of the DES cipher.

15. Why is DES considered obsolete?

16. Describe how to use DES with multiple keys in order to increase the keyspace.

17. What is meant by message padding and why is it necessary?

18. What is meant by block cipher modes of operation?

19. Briefly describe ECB and CBC mode, advantages and disadvantages of each.

20. What is meant by Initialization Vector and when is it used?

21. List the main characteristics of the AES cipher.

22. What is pseudo-randomness? How can it be used to encrypt data?

23. Describe the synchronization problem in stream ciphers and a possible solution to it.

24. How can one user send a confidential message to

another user with the help of asymmetric cryptography?

25. Briefly describe the process of key creation in the RSA algorithm.

26. Why is it difficult for an attacker to calculate the private key in RSA if they only have the public key?

27. What are the disadvantages of the RSA algorithm?

28. What are the problems with asymmetric key distribution compared to symmetric key distribution?

29. List three methods for asymmetric key distribution.

30. What is a public key certificate and why is it necessary?

31. Why may certificate revocation be required? How is it accomplished?

32. What is a public key infrastructure (PKI)? Why is it useful?

33. Describe how one user in one certification domain can communicate securely with another user in a different certification domain (both domains part of the same PKI).

34. What is meant by message integrity and why is it necessary?

35. What is a Message Authenticity Code (MAC)?

36. How is the integrity of a message verified using a MAC?

37. Briefly describe how the MAC can be protected during transfer. Why is it necessary to protect it?

38. What is a digital signature? Explain what is achieved by adding a digital signature to a message.

39. Explain how a digital signature is produced and verified.

40. In the case of user authentication based on a secret, explain the difference between direct presentation, result of a challenge and implicit authentication.

41. List the steps necessary to access an application server using the Kerberos system.

42. What is meant by a Distinguished Name?

43. Describe the challenge/response authentication based on asymmetric cryptography.

Last modified: Monday, 14 February 2022, 10:41