Important Viva Questions

General Questions on Cryptography

1. **What is cryptography, and why is it important?**
2. **What are the main types of cryptographic algorithms?**
3. **Explain the difference between symmetric and asymmetric encryption.**

XOR and AND Operations

4. **What is an XOR operation, and where is it commonly used in cryptography?**
5. **How does the XOR operation work with binary data?**
6. **What is the difference between XOR and AND operations in terms of encryption?**

Caesar Cipher

7. **What is the Caesar Cipher, and how does it work?**
8. **What are the limitations of the Caesar Cipher?**
9. **How would you decrypt a message encrypted with the Caesar Cipher?**
10. **Why is the Caesar Cipher considered insecure for modern applications?**

Substitution Cipher

11. **What is a substitution cipher, and how does it differ from the Caesar Cipher?**
12. **Can you explain how a key is used in a substitution cipher?**
13. **What are some vulnerabilities of substitution ciphers?**

Hill Cipher

14. **Explain the basic working of the Hill Cipher.**
15. **What is the role of the key matrix in the Hill Cipher?**
16. **Why must the key matrix be invertible in the Hill Cipher?**
17. **How would you perform decryption in the Hill Cipher?**

Data Encryption Standard (DES)

18. **What is the DES algorithm, and how does it work?**
19. **Explain the concept of permutations and substitutions in DES.**
20. **What are S-boxes, and what role do they play in DES?**
21. **What are the key limitations of DES that led to the development of newer algorithms?**

RSA Algorithm

22. **How does the RSA algorithm work?**
23. **What are the steps involved in generating RSA keys?**
24. **What is the importance of prime numbers in RSA?**
25. **Why is RSA considered secure?**
26. **Explain how encryption and decryption are performed in RSA.**

Diffie-Hellman Key Exchange

27. **What is the Diffie-Hellman Key Exchange, and what problem does it solve?**
28. **How do users generate a shared key in the Diffie-Hellman method?**
29. **What are the security concerns with Diffie-Hellman Key Exchange?**

Hash Functions

30. **What is a hash function, and what are its applications?**
31. **Explain the MD5 hashing algorithm.**
32. **What are the key properties of a secure hash function?**
33. **Why are hash functions useful in digital signatures?**

Blowfish Algorithm

34. **What is the Blowfish algorithm, and what type of cipher is it?**
35. **How does Blowfish differ from DES and AES?**
36. **What is a key advantage of using Blowfish for encryption?**

RC4 Algorithm

37. **What is the RC4 algorithm, and how does it work?**
38. **What is a stream cipher, and how is it different from a block cipher?**
39. **Why is RC4 no longer widely recommended for secure communications?**

Digital Signature

40. **What is a digital signature, and how does it ensure authenticity?**
41. **How are public and private keys used in digital signatures?**
42. **What steps are involved in verifying a digital signature?**
43. **What is the significance of the hash function in digital signatures?**

Additional Practical Questions

44. **How would you choose a suitable cryptographic algorithm for securing sensitive data?**
45. **Explain how you would implement basic error handling in cryptographic programs.**
46. **What challenges might arise when implementing encryption algorithms in C or Java?**
47. **Why is it necessary to handle padding in block cipher algorithms?**
48. **How do you ensure that an encryption key is kept secure?**