Model questions CNS-1

[Each question from Q.1 to Q.10 carries 2 mark , from Q.11 to Q.15 carries 6 marks and from Q.16 to Q.18 carries 10 marks]

1. Explain why challenge response identification systems are used.
2. Give the typical requirements of a secure communicated system.
3. Write down different types of attacks.
4. What is cryptology?
5. Define digital signature.
6. Suppose you decide to use a 10-bit key. How many combinations are there?
7. Draw a diagram to show where IPSec fits in the TCP/IP model.
8. Does a digital signature ensure the entire message is encrypted?
9. Name the security measures has taken for email in addition to digital signatures.
10. What is password audit?
11. Give a real life example where both confidentiality and integrity is needed. Explain why encryption alone does not provide integrity of information.
12. What is certificate based authentication? Explain.
13. Write down different substitution techniques in cryptography and network security.
14. Write short notes on SHTTP, SSL.
15. Describe encryption and decryption process with neat diagram.
16. Describe RSA algorithm with example.
17. Describe DES algorithm with neat diagram.
18. Briefly describe different layers and it's functions in TCP/IP protocol suite.