Topics Covered: Cryptography, Cipher, Public key, Private key, Digital Signature, Concept of Hashing and MD5

Question 1: Use the keyword “CHARLES” to encrypt the plaintext
MEETMEATHAMMERSMITHBRIDGETONIGHT
showing all the steps of the encryption.

Question 2: What are the different types of Ciphers?

Question 3: Explain briefly the disadvantages of symmetric key cryptography?

Question 4: Given the following input (4322, 1334, 1471, 9679, 1989, 6171, 6173, 4199) and the hash function x mod 10, which of the above elements will hash to the same values?

Question 5: What is the difference Between Block Cipher and Stream Cipher?

Question 6: List and briefly define types of cryptanalytic attacks based on what is known to the attacker.

Question 7: How many one-to-one affine Caesar ciphers are there?

Question 8: What requirements should a digital signature scheme satisfy?

Question 9: Differentiate between a message authentication code and a one-way hash function?

Question 10: A ciphertext has been generated with an affine cipher. The most frequent letter of the ciphertext is 'B', and the second most frequent letter of the ciphertext is 'U'. Break this code.

Question 11: What characteristics are needed in a secure hash function?

Question 12: Describe three broad categories of applications of public-key cryptosystems?

Question 13: In one of his cases, Sherlock Holmes was confronted with the following message. 534 C2 13 127 36 31 4 17 21 41 DOUGLAS 109 293 5 37 BIRLSTONE 26 BIRLSTONE 9 127 171 Although Watson was puzzled, Holmes was able immediately to deduce the type of cipher. Can you?

Question 14: Encrypt the message "meet me at the usual place at ten rather than eight oclock" using the Hill cipher with the key 9 4 5 7 . Show your calculations and the result.

Question 15: In what order should the signature function and the confidentiality function be applied to a message, and why?