BE-1431

Total No. of Printed Pages:03

B.E - (Computer) (Sem-VIII)(Revised Course 2019-2020)
EXAMINATION MAY 2024
Cryptography Techniques For Network Security

[Time: 3:00 Hours] **[Max. Marks:100]**

Instructions:
1) Answer any two questions from Part-A.
2) Answer any two questions from Part-B.
3) Answer any one question from Part-C.
4) Make suitable assumption only if required.

Part-A

Q1 a) Consider the initial values of RSA technique as follows: p-11, q=17 and e = 7. Calculate private key of RSA algorithm using Extended Euclidean Algorithm. Generate cipher text for given original message as "Destroy 100 targets" using RSA technique for above RSA configuration. **(10)**

b) Explain AES technique with neat diagram. Compare the performance of AES technique with DES technique. **(08)**

c) Explain Monoalphabtic Ciphers with help of example? **(02)**

Q2 a) Consider the statement as "It is said that Diffie Hellman algorithm is strong and secure algorithm to share keys". Is this statement is true? If yes, provide proper justification in support of the statement. Using Diffie Hellman algorithm demonstrate how to share key =20 between sender and receiver. **(10)**

b) Explain different transposition techniques with help of example. **(05)**

c) What is the difference between Stegnography and Cryptography? What are the strength and weakness of Stegnography techniques? Discuss. **(05)**

Q3 a) Discuss the performance of DES algorithm. Explain Permutation Matrix, Expansion Matrix and S - Box of DES algorithm with help of example. Design S-Box for DES Architecture with input string of length 20 bits and output string of length 10 bits. Consider content of input string as "1001101011 0111011011". **(13)**

b) Explain in detail the block cipher design principles. **(07)**

Part-B

Q4 a) Explain the steps of Elgamal Digital Signature with help of example. User X has generated hash value of m=30 using hashing algorithm for some input text. Explain how X is generating signature for hash value of m=30 and explain how user Y is performing verification process. Make suitable assumption for various parameters of Elgamal Digital Signature algorithm. **(09)**

b) Explain Message authentication code based on Hash Functions. **(06)**

c) Explain X.509 Certificate. **(05)**

Q5 a) Is RSA algorithm is used in digital signature? If yes, then what is significance of RSA algorithm in Digital Signature? Discuss the performance of digital signature algorithm. **(07)**

b) With the help of neat diagram, explain the elements of 802.11i wireless protocol **(07)**

c) Explain Pubic Key Infrastructure in Cryptography and challenges faced by PKI. **(06)**

Q6 a) Generate Hash value at the end of Second Round using SHA algorithm for given message "Attack X Immediately". The SHA configuration is as follows:- The maximum size of A, B, C D and E blocks is 15 bits. The size of message and key is 10 bits. Initial values of A=10101 10110, B=11001 11010, C=10101 01110, D=01010 01100 and E=10011 10111. Let K1= 11001 11101 and K2=10111 01011 be two keys. The left rotate for A is 2 and left rotate for B is 4. The F function is same as that of SHA technique. **(13)**

b) Explain Message Authentification Functions in Cryptography. **(07)**

Part-C

Q7 a) Generate cipher text using Polyalphabetic Cipher for given input message =”Target X is Powerful". Assume suitable key. Compare Polyalphabet cipher technique with Playfair cipher Technique for performance. **(06)**

b) Explain Cipher Feedback Mode and Output feedback mode. **(07)**

c) Explain Triple DES with help of example. **(07)**

Q8 a) Generate Cipher Text for the given input message="Transfer 100CR" using Playfair Cipher with key="Diamond". Discuss the performance of Playfair Cipher Techniques. **(07)**

b) Why HTTPS protocol is said to be Strong and Secured Protocol? Discuss. **(07)**

c) List and explain the applications of Cipher Hash Functions. **(06)**