18/11/24

CE 810

Total No. of Printed Pages: 2

B.E - (Computer) (Sem-VIII)(Revised Course 2019-2020)

Cryptography Techniques For Network Security

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

Instructions: i) Answer any two full questions from Part-A, any two full questions from Part-B, and any one full question from Part-C.
ii) Draw neat diagrams wherever necessary.
iii) Assume suitable data if required.

PART A

Q1 a) Explain the layers of Advanced Encryption Standard algorithm with the block diagram **(6)**

b) Give the key "MONARCHY" apply Playfair cipher to plaintext "FACTIONALISM" and find cipher text. Also decrypt the ciphertext at destination to get original plaintext. **(7)**

c) Explain the Rivest, Shamir and Adleman Encryption algorithm. Using RSA perform encryption and decryption on the following: Alice wants to send message (M=15) to Bob with value of p=13, q=17 and she chooses the public component e=35 **(7)**

Q2 a) Explain in detail single round of DES with the help of necessary diagrams. **(8)**

(b)In the ElGamal cryptosystem, Alice and Bob use q=19 and α = 10. Alice chooses her public key to be 5. Bob chooses the random integer k= 6. Alice wants to send Bob a message M-17. Determine the ciphertext. Perform encryption and decryption. **(6)**

c) With a suitable diagram explain the model of symmetric cryptosystem. Also explain five ingredients of symmetric encryption scheme. **(6)**

Q3 a) What is steganography? Explain various techniques used in it. **(6)**

b) Illustrate RC4 algorithm **(6)**

c) State and explain Diffie-Hellman key exchange algorithm, prove the same if User A and User B want to exchange a key and they agree on this key exchange technique with a common prime q=353 and a primitive root α =3 **(8)**

i) If user A has private key X_A-97. What is A's public key Y_A?
ii) If user B has private key X_B-223. What is B's public key Y_B?
iii) What is the shared secret key?

PART B

Q4 a) Write a short note on S/MIME functionality (6)

b) Explain various properties of hash function. (6)

c) Explain different services provided by PGP with the help of neat diagrams. (8)

Q5 a) Explain in detail SHA-512 algorithm with the help of neat diagrams. (8)

b) State and explain different methods to distribute public keys. (6)

c) Explain the ElGamal Signature Scheme. (6)

Q6 a) What is the difference between MAC and one-way hash function? (4)

b) Explain overview of Kerberos with necessary diagram. (8)

c) Explain in detail about the message generation and reception in Pretty Good privacy with neat diagram. (8)

PART C

Q7 a) Give the structure of Output Feedback Mode? Explain the advantages and disadvantages of OFB. (6)

b) Explain the working of SSL Handshake protocol with neat diagram. (8)

c) Use Caesar cipher to encrypt and decrypt the plaintext "hello" using key=18. Show the steps of encryption and decryption in detail. (6)

Q8 a) Draw and explain X.509 format of digital certificate. (6)

b) Describe the various applications of cryptographic hash functions. Support your answer with example and neat diagrams wherever required. (8)

c) Encrypt the plaintext "attack" using Hill cipher for the given key $=\begin{bmatrix}2 & 3\\ 3 & 6\end{bmatrix}$ (6)