

- A. to find some insecurity in a cryptographic scheme
- B. to increase the speed
- C. to encrypt the data
- D. none of the mentioned

Ans: A

7. ----- is one of the cryptographic protocol used to secure HTTP connection?

- A. stream control transmission protocol (SCTP)
- B. transport layer security (TSL)
- C. explicit congestion notification (ECN)
- D. resource reservation protocol

Ans: B

8. Voice privacy in GSM cellular telephone protocol is provided by

- A. A5/2 cipher
- B. b5/4 cipher
- C. b5/6 cipher
- D. b5/8 cipher

Ans: A

9. ElGamal encryption system is-----

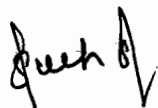
- A. symmetric key encryption algorithm
- B. asymmetric key encryption algorithm
- C. not an encryption algorithm
- D. none of the mentioned

Ans: B

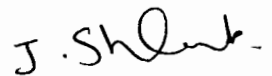
10. Cryptographic hash function takes an arbitrary block of data and returns

- A. fixed size bit string
- B. variable size bit string
- C. both fixed size bit string and variable size bit string
- D. none of the mentioned

Ans: A

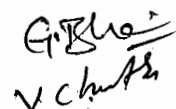


Faculty In-charge



Students





Subject Name: Computer Network and Security

Q.1 In cryptography, what is cipher?

- A. Algorithm for performing encryption and decryption
- B. Encrypted message
- C. Both algorithm for performing encryption and decryption and encrypted message
- D. None of the mentioned

Ans: A

Q.2 In asymmetric key cryptography, the private key is kept by

- A. Sender
- B. Receiver
- C. Sender and receiver
- D. All the connected devices to the network

Ans: B

Q.3 Which one of the following algorithm is not used in asymmetric-key cryptography?

- A. rsa algorithm
- B. diffie-hellman algorithm
- C. electronic code book algorithm
- D. none of the mentioned

Ans: C

Q.4 In cryptography, the order of the letters in a message is rearranged by

- A. transpositional ciphers
- B. substitution ciphers
- C. both transpositional ciphers and substitution ciphers
- D. none of the mentioned

Ans: A

Q.5 What is data encryption standard (DES)?

- A. block cipher
- B. stream cipher
- C. bit cipher
- D. none of the mentioned

Ans: A

Q.6. Cryptanalysis is used