V SEMESTER B.TECH. (Computer and Communication Engineering) MAKEUP EXAMINATIONS, JAN 2022 SUBJECT: INFORMATION SECURITY [ICT 3172] REVISED CREDIT SYSTEM PART A 22/2/2022

Question Μ 1. What type of cipher relies upon changing the location of characters within a message to achieve confidentiality? A. Stream cipher **B.** Transposition cipher C. Block cipher D. Substitution cipher 2. Arya wishes to communicate a very secret message to Rehman. She uses the prime numbers 13 and 17 to generate her key pairs. If her public key is 35, what is her private key? a. b. c. d. 3. What kind of attack makes the Caesar cipher virtually unusable? A. Meet-in-the-middle attack B. Escrow attack **C. Frequency attack** D. Transposition attack 4. How many rounds does the AES-256 perform? a) 10 b) 12 c) 14 d) 16 5. Show the result of passing 111111 through S-box 4 (Figure 1) of Data Encryption Standard. n Figure 1: S-Box 4 a.1101 b.1001 c.1100 d. 1110 6. The main difference in MACs and digital signatures is that, in digital signatures the hash value of the message is encrypted with a user's public key. a. True

| 7. In SHA-512, the message is divided into blocks of size bits for the hash 1 computation. a) 1024 b) 512 c) 256 d) 1248 8. Which one of these is not a Whirlpool function? a) Add Key b) Substitute Bytes c) Mix Rows 9. On Encrypting "cryptography" using Vignere Cipher System using the keyword 1 "LUCKY" we get cipher text a) nlazeiibljii b) nlaeiibljii c) Adaeiibljki d) Bhit Rows 10. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes 1 the two numbers n and r to be 20 and 7 respectively. Encrypt the binary message "10. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes 1 the two numbers n and r to be 20 and 7 respectively. Encrypt the binary message 10. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes 1 c. 28 c. 27B, CFB c) | ilse | |
|---|---|---|
| computation.a) 1024b) 512:256c) 256:11a) Add Key:11b) Substitute Bytes:256c) Mix Rows:11a) Add Key:258b) Substitute Bytes:218c) Mix Rows:11a) Adarceiblji:218b) On Encrypting "cryptography" using Vignere Cipher System using the keyword1"LUCKY" we get cipher textinlazeiibljiic) olaaeiibljki:218d) mlaaeiibljki:21810. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializesit te two numbers n and r to be 20 and 7 respectively. Encrypt the binary message"1101". Display the cipher text in decimal.a. 16b. 18c. 28c. 28d. 2011. Which of the following modes does not implement chaining or "dependency on previous stage computations"?a) CTR, ECBb) CTR, CFBc) CFB, OFBc) CFB, OFBc) 2. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The Cipher text isa) 42b) 93c) 74d) 1213. In, a claimant proves her identity to the verifier.14. Munt Attenticationb. message authenticationc. message authenticationc. message integrity14. Mons dimension14. Mons dimensiona) 14. Mons dimensiona) 14. Mons dimensiona) 14. Mons dimensiona) 14. Mons dimensionb) 15. Cresc) 16. | 7. In SHA-512, the message is divided into blocks of size bits for the hash | 1 |
| a) 1024 b) 512 b) 512 c) 256 d) 1248 1 a) Add Key b) Substitute Bytes c) Mix Rows 1 a) Add Key b) Substitute Bytes c) Mix Rows 1 a) On Encrypting "cryptography" using Vignere Cipher System using the keyword 1 "LUCKY" we get cipher text a) nlazeiibljji b) nlazeiibljii c) olaaeiibljki d) mlaaeiibljki 1 d) Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes 1 intareiibljki 1 d) Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes 1 intareiibljki 1 10. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes 1 inthe onumbers n and r to be 20 and 7 respectively. Encrypt the binary message 1 i10!". Display the cipher text in decimal. 1 a. 16 b.18 1 b) CTR, ECB 1 1 b) CTR, CFB 1 1 c) CFB, OFB 1 1 d) 12 1 1 13. In | computation. | |
| b) 512 c) 256 d) 1248 8. Which one of these is not a Whirlpool function? a) Add Key b) Substitute Bytes c) Mix Rows d) Shift Rows 9. On Encrypting "cryptography" using Vignere Cipher System using the keyword 1 "LUCKY" we get cipher text a) nlazeiibljii c) olaaeiibljii d) mlaaeiibljii d) mlaaeiibljii d) mlaaeiibljii 10. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes the two numbers n and r to be 20 and 7 respectively. Encrypt the binary message "1101". Display the cipher text in decimal. a. 16 b. 18 c. 28 d. 20 11. Which of the following modes does not implement chaining or "dependency on previous stage computations"? a) CTR, ECB b) CTR, CFB c) CFB, OFB d) ECB, OFB 12. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The Cipher text is a) 42 b) 93 c) 74 d) 12 13. In, a claimant proves her identity to the verifier. a. entity authentication b. message authentication c. message confidentiality d. message integrity 14. Myna tries to exchange some confidential information with Sabrina in a meeting 1 | a) 1024 | |
| c) 256 d) 1248 8. Which one of these is not a Whirlpool function? 9. Add Key b) Substitute Bytes c) Mix Rows d) Shift Rows 9. On Encrypting "cryptography" using Vignere Cipher System using the keyword "LUCKY" we get cipher text a) nlazeiibljji b) nlazeiibljji 10. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes the two numbers n and r to be 20 and 7 respectively. Encrypt the binary message "1101". Display the cipher text in decimal. a. 16 b. 18 c. 28 d. 20 11. Which of the following modes does not implement chaining or "dependency on previous stage computations"? a) CTR, ECB b) CTR, CFB c) CFB, OFB d) ECB, OFB 12. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The Cipher text is a) 42 b) 93 c) 74 d) 12 13. In, a claimant proves her identity to the verifier. a. entity authentication c. message confidentiality d. message integrity 14. Myna tries to exchange some confidential information with Sabrina in a meeting. 15. Mich Sabrina in a meeting. 16. Mich Sabrina in a meeting. 17. Mich Sabrina in a meeting. 18. Mich Sabrina in a meeting. 19. Mich Sabrina in a meeting. 10. Mich Sabrina in a meeting. 10. Mich Sabrina in a meeting. 11. Mich Sabrina in a meeting. 12. Mich Sabrina in a meeting. 13. Mich Sabrina in a meeting. 14. Myna tries to exchange some confidential information with Sabrina in a meeting. 19. Mich Sabrina in a meeting. 10. Mich Sabrina in a meeting. 10. Mich Sabrina in a meeting. 11. Mich Sabrina in a meeting. 12. Mich Sabrina in a meeting. 13. Mich Sabrina in a meeting. 14. Mich Sabrina in a meeting. 15. Mich Sabrina in a meeting. 16. Mich Sabrina in a meeting. 17. Mich Sabrina in a meeting. 18. Mich Sabrina in a meeting. 19. Mich Sabrina in a meeting. 19. Mich Sabrina in a meeting. 10. Mich Sabrina in a meeting. | b) 512 | |
| d) 1248 1 8. Which one of these is not a Whirlpool function? 1 a) Add Key 1 b) Substitute Bytes 1 c) Mix Rows 1 0 . On Encrypting "cryptography" using Vignere Cipher System using the keyword 1 "LUCKY" we get cipher text 1 a) nlazeiibljii 1 c) olaaeiibljki 1 d) mlazeiibljki 1 10. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes 1 the two numbers n and r to be 20 and 7 respectively. Encrypt the binary message 1 "1101". Display the cipher text in decimal. 1 a. 16 b.18 1 c. 28 1 1 d. 20 1 1. Which of the following modes does not implement chaining or "dependency on previous stage computations"? 1 a) CTR, ECB 1 1 b) CTR, OFB 1 1 c) TR, OFB 1 1 d) 12 12. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The Cipher text is a) 42 1 b) 93 1 1 c) 74 1 1 <td>c) 256</td> <td></td> | c) 256 | |
| 8. Which one of these is not a Whirlpool function? 1 a) Add Key 1 b) Substitute Bytes 1 c) Mix Rows 1 d) Shift Rows 1 d) Mazeiiblji 1 b) nlazeiibljii 1 c) olaaeiibljki 1 10. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes 1 the two numbers n and r to be 20 and 7 respectively. Encrypt the binary message 1 "1101". Display the cipher text in decimal. 1 a. 16 1 1 b. 18 1 1 c. 28 1 1 d. 20 1 1 11. Which of the following modes does not implement chaining or "dependency on previous stage computations"? 1 a) CTR, CFB 1 1 c) CFB, OFB 1 1 d) ECB, OFB 1 1 12. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The pipe text is a) 42 | d) 1248 | |
| a) Add Key Image: state of the state | 8. Which one of these is not a Whirlpool function? | 1 |
| b) Substitute Bytes c) Mix Rows d) Shift Rows 9. On Encrypting "cryptography" using Vignere Cipher System using the keyword 1.UCKY" we get cipher text a) nlazeiibljii b) nlazeiibljii c) olaaeiibljki d) mlaaeiibljki 10. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes the two numbers n and r to be 20 and 7 respectively. Encrypt the binary message "1101". Display the cipher text in decimal. a. 16 b. 18 c. 28 d. 20 11. Which of the following modes does not implement chaining or "dependency on previous stage computations"? a) CTR, CCB b) CTR, CFB c) CFB, OFB d) ECB, OFB d) ECB, OFB d) ECB, OFB d) ECB, OFB d) 12 13. In, a claimant proves her identity to the verifier. a. entity authentication b. message authentication c. message confidentiality d. message integrity 14. Myna tries to exchange some confidential information with Sabrina in a meeting 14. Myna tries to exchange some confidential information with Sabrina in a meeting 14. Myna tries to exchange some confidential information with Sabrina in a meeting 14. Myna tries to exchange some confidential information with Sabrina in a meeting 14. Myna tries to exchange some confidential information with Sabrina in a meeting 14. Myna tries to exchange some confidential information with Sabrina in a meeting 14. Myna tries to exchange some confidential information with Sabrina in a meeting 14. Myna tries to exchange some confidential information with Sabrina in a meeting 14. Myna tries to exchange some confidential information with Sabrina in a meeting 14. Myna tries to exchange some confidential information with Sabrina in a meeting | a) Add Key | |
| c) Mix RowsImage: Cipher Rows9. On Encrypting "cryptography" using Vignere Cipher System using the keyword1"LUCKY" we get cipher text1a) nlazeiibljii1c) olaaeiibljki1(c) olaaeiibljki110. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes11. Who and r to be 20 and 7 respectively. Encrypt the binary message(c) 11. Display the cipher text in decimal.a. 16 b. 18 c. 28d. 2011. Which of the following modes does not implement chaining or "dependency on previous stage computations"?a) CTR, ECBb) CTR, CFBc) CFB, OFBd) ECB, OFB12. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The13. In, a claimant proves her identity to the verifier.14. Why a trites to exchange some confidential information with Sabrina in a meeting14. Wave tritegrity | b) Substitute Bytes | |
| d) Shift Rows19. On Encrypting "cryptography" using Vignere Cipher System using the keyword "LUCKY" we get cipher text a) nlazeiibljii b) nlazeiibljii c) olaaeiibljki110. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes the two numbers n and r to be 20 and 7 respectively. Encrypt the binary message "1101". Display the cipher text in decimal. a. 161 b. 18 c. 28 d. 20111. Which of the following modes does not implement chaining or "dependency on previous stage computations"? a) CTR, ECB b) CTR, CFB c) CFB, OFB112. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The Cipher text is a) 42 b) 93 c) 74 d) 12113. In, a claimant proves her identity to the verifier. a. entity authentication b. message authentication c. message confidentiality d. message integrity1 | c) Mix Rows | |
| 9. On Encrypting "cryptography" using Vignere Cipher System using the keyword 1 "LUCKY" we get cipher text 1 a) nlazeiibljii 1 b) nlazeiibljii 1 c) olaaeiibljii 1 10. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes 1 the two numbers n and r to be 20 and 7 respectively. Encrypt the binary message 1 11.01". Display the cipher text in decimal. 1 a. 16 1 b. 18 1 c. 28 1 d. 20 1 11. Which of the following modes does not implement chaining or "dependency on previous stage computations"? 1 a) CTR, ECB 1 b) CTR, CFB 1 c) CFB, OFB 1 12. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The Cipher text is 1 a) 42 9 1 b) 93 1 1 c) 74 1 1 d) 12 1 1 a. entity authentication 1 1 b. message authentication 1 1 c. message confidentiality | d) Shift Rows | |
| *LUCKY" we get cipher text a) nlazeiibljii b) nlazeiibljii c) olaaeiibljki d) mlaaeiibljki l0. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes the two numbers n and r to be 20 and 7 respectively. Encrypt the binary message "1101". Display the cipher text in decimal. a. 16 b. 18 c. 28 d. 20 11. Which of the following modes does not implement chaining or "dependency on previous stage computations"? a) CTR, ECB b) CTR, CFB c) CFB, OFB d) ECB, OFB 12. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The Cipher text is a) 42 b) 93 c) 74 d) 12 13. In, a claimant proves her identity to the verifier. a entity authentication b. message authentication c. message confidentiality d. message integrity | 9. On Encrypting "cryptography" using Vignere Cipher System using the keyword | 1 |
| a) nlazeiibljii i b) nlazeiibljii i c) olaaciibljki i d) mlaaeiibljki i 10. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes 1 the two numbers n and r to be 20 and 7 respectively. Encrypt the binary message 1 "1101". Display the cipher text in decimal. a. 16 b. 18 c. 28 i c. 28 i i d. 20 i 1 11. Which of the following modes does not implement chaining or "dependency on previous stage computations"? 1 a) CTR, ECB i 1 b) CTR, CFB i 1 c) CFB, OFB i 1 12. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The l 1 Cipher text is a) 42 1 b) 93 i 1 c) 74 i 1 d) 12 i 1 13. In, a claimant proves her identity to the verifier. 1 a. entity authentication i 1 b. message authentication i 1 c. | "LUCKY" we get cipher text | |
| b) nlazeiibljii c) olaaeiibljki d) mlaaeiibljki 10. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes the two numbers n and r to be 20 and 7 respectively. Encrypt the binary message "1101". Display the cipher text in decimal. a. 16 b. 18 c. 28 d. 20 11. Which of the following modes does not implement chaining or "dependency on previous stage computations"? a) CTR, ECB b) CTR, CFB c) CFB, OFB d) ECB, OFB 12. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The Cipher text is a) 42 b) 93 c) 74 d) 12 13. In, a claimant proves her identity to the verifier. a. entity authentication b. message authentication c. message confidentiality d. message integrity 14. Myna tries to exchange some confidential information with Sabrina in a meeting, 1 | a) nlazeiibljji | |
| c) olaaeiibljki1d) mlaaeiibljki110. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes the two numbers n and r to be 20 and 7 respectively. Encrypt the binary message "1101". Display the cipher text in decimal. a. 16 b. 18 c. 28 d. 20111. Which of the following modes does not implement chaining or "dependency on previous stage computations"? a) CTR, ECB b) CTR, CFB c) CFB, OFB112. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The c) PB112. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The d) 12113. In, a claimant proves her identity to the verifier. a. entity authentication b. message authentication114. Mura tries to exchange some confidential information with Sabrina in a meeting 11 | b) nlazeiibljii | |
| d) mlaaeiibljki 1 10. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes 1 the two numbers n and r to be 20 and 7 respectively. Encrypt the binary message 1 "1101". Display the cipher text in decimal. 1 a. 16 1 b. 18 1 c. 28 1 d. 20 1 11. Which of the following modes does not implement chaining or "dependency on previous stage computations"? 1 a) CTR, ECB 1 b) CTR, CFB 1 c) CFB, OFB 1 12. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The Cipher text is 1 a) 42 1 b) 93 1 c) 74 1 d) 12 1 13. In, a claimant proves her identity to the verifier. 1 a entity authentication 1 b. message authentication 1 c. message confidentiality 1 d. message integrity 1 | c) olaaeiibljki | |
| 10. Bob sets up a Knapsack Cryptosystem with private key b =[1,3,5,10] and initializes 1 the two numbers n and r to be 20 and 7 respectively. Encrypt the binary message "1101". Display the cipher text in decimal. a. 16 b. 18 | d) mlaaeiibljki | |
| the two numbers n and r to be 20 and 7 respectively. Encrypt the binary message "1101". Display the cipher text in decimal. a. 16 b. 18 c. 28 d. 20 11. Which of the following modes does not implement chaining or "dependency on previous stage computations"? a) CTR, ECB b) CTR, CFB c) CFB, OFB d) ECB, OFB 12. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The Cipher text is a) 42 b) 93 c) 74 d) 12 13. In, a claimant proves her identity to the verifier. 1 b . message authentication c. message confidentiality d. message integrity | 10. Bob sets up a Knapsack Cryptosystem with private key $b = [1,3,5,10]$ and initializes | 1 |
| "1101". Display the cipher text in decimal. Image: Complexity of the cipher text in decimal. a. 16 Image: Complexity of the cipher text in decimal. b. 18 C. 28 c. 20 Image: Complexity of the cipher text in decimal. 11. Which of the following modes does not implement chaining or "dependency on previous stage computations"? Image: Complexity of the cipher text is and CTR, ECB b) CTR, CFB CFB, OFB c) CFB, OFB Image: Complexity of the cipher text. The cipher text is and 42 b) 93 C) 74 c) 74 Image: Complexity of the cipher text is and the cipher tex | the two numbers n and r to be 20 and 7 respectively. Encrypt the binary message | |
| a. 16 1 b. 18 | "1101". Display the cipher text in decimal. | |
| b. 18Image: 10 transformed and transf | a. 16 | |
| c. 281d. 20111. Which of the following modes does not implement chaining or "dependency on previous stage computations"?1a) CTR, ECB1b) CTR, CFB1c) CFB, OFB1d) ECB, OFB112. Using Rabin cryptosystem with p=23 and q=7,encrypt P=24 to find ciphertext. The Cipher text is a) 421b) 931c) 741d) 12113. In, a claimant proves her identity to the verifier.1a. entity authentication1b. message authentication1c. message confidentiality1d. message integrity1 | b. 18 | |
| d. 2011. Which of the following modes does not implement chaining or "dependency on previous stage computations"?1a) CTR, ECB1b) CTR, CFB1c) CFB, OFB1d) ECB, OFB112. Using Rabin cryptosystem with p=23 and q=7,encrypt P=24 to find ciphertext. The Cipher text is a) 421b) 931c) 741d) 12113. In, a claimant proves her identity to the verifier.1a. entity authentication c. message authentication c. message confidentiality d. message integrity1 | c. 28 | |
| 11. Which of the following modes does not implement chaining or "dependency on previous stage computations"? 1 a) CTR, ECB b) CTR, CFB b) CTR, CFB c) CFB, OFB d) ECB, OFB 1 12. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The Cipher text is 1 a) 42 b) 93 c) 74 b) 93 c) 74 1 d) 12 13. In, a claimant proves her identity to the verifier. 1 a. entity authentication nessage confidentiality 1 b. message integrity 1 1 | d. 20 | |
| previous stage computations"? Image: computations in a meeting a) CTR, ECB image: computations in a meeting b) CTR, CFB image: computations in a meeting c) CFB, OFB image: computations in a meeting d) ECB, OFB image: computations in a meeting 12. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The 1 Cipher text is a) 42 b) 93 c) 74 c) 74 image: computation in a meeting d) 12 image: confidential information with Sabrina in a meeting | 11. Which of the following modes does not implement chaining or "dependency on | 1 |
| a) CTR, ECB b) CTR, CFB b) CTR, CFB c) CFB, OFB d) ECB, OFB c) CFB, OFB 12. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The Cipher text is a) 42 b) 93 c) 74 c) 74 d) 12 13. In, a claimant proves her identity to the verifier. 1 a. entity authentication 1 b. message authentication 1 c. message confidentiality 1 d. message integrity 1 | evious stage computations"? | |
| b) CTR, CFBc) CFB, OFBd) ECB, OFB12. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The1 Cipher text isa) 42 b) 93 c) 74d) 1213. In, a claimant proves her identity to the verifier.1 a. entity authentication b. message authenticationc. message confidentialityd. message integrity | a) CTR, ECB | |
| c) CFB, OFBId) ECB, OFB12. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The Cipher text is a) 421b) 93c) 741c) 7401213. In, a claimant proves her identity to the verifier.1a. entity authentication b. message authentication c. message confidentiality d. message integrity1 | b) CTR, CFB | |
| d) ECB, OFB12. Using Rabin cryptosystem with p=23 and q=7,encrypt P=24 to find ciphertext. The Cipher text is a) 421b) 93 c) 74 d) 12613. In, a claimant proves her identity to the verifier.1a. entity authentication b. message authentication c. message confidentiality d. message integrity114. Myna tries to exchange some confidential information with Sabrina in a meeting1 | c) CFB, OFB | |
| 12. Using Rabin cryptosystem with p=23 and q=7, encrypt P=24 to find ciphertext. The Cipher text is a) 42 b) 93 c) 74 d) 12113. In, a claimant proves her identity to the verifier. a. entity authentication b. message authentication c. message confidentiality d. message integrity1 | d) ECB, OFB | |
| Cipher text is a) 42 b) 93 c) 74 d) 12 13. In, a claimant proves her identity to the verifier. a. entity authentication b. message authentication c. message confidentiality d. message integrity 14. Myna tries to exchange some confidential information with Sabrina in a meeting 1 | 12. Using Rabin cryptosystem with $p=23$ and $q=7$, encrypt $P=24$ to find ciphertext. The | 1 |
| a) 42 b) 93 c) 74 d) 12 13. In, a claimant proves her identity to the verifier. a. entity authentication b. message authentication c. message confidentiality d. message integrity 14. Myna tries to exchange some confidential information with Sabrina in a meeting 1 | Cipher text is | |
| b) 93c) 74d) 1213. In, a claimant proves her identity to the verifier.1a. entity authenticationb. message authenticationc. message confidentialityd. message integrity14. Myna tries to exchange some confidential information with Sabrina in a meeting1 | a) 42 | |
| c) 74d) 1213. In, a claimant proves her identity to the verifier.1a. entity authenticationb. message authenticationc. message confidentialityd. message integrity14. Myna tries to exchange some confidential information with Sabrina in a meeting1 | b) 93 | |
| d) 1213. In, a claimant proves her identity to the verifier.a. entity authenticationb. message authenticationc. message confidentialityd. message integrity14. Myna tries to exchange some confidential information with Sabrina in a meeting1 | c) 74 | |
| 13. In, a claimant proves her identity to the verifier. 1 a. entity authentication 1 b. message authentication 1 c. message confidentiality 1 d. message integrity 1 14 Myna tries to exchange some confidential information with Sabrina in a meeting 1 | d) 12 | |
| a. entity authentication b. message authentication c. message confidentiality d. message integrity 14 Myna tries to exchange some confidential information with Sabrina in a meeting | 13. In, a claimant proves her identity to the verifier. | 1 |
| b. message authentication c. message confidentiality d. message integrity 14 Myna tries to exchange some confidential information with Sabrina in a meeting 1 | a. entity authentication | |
| c. message confidentiality d. message integrity 14 Myna tries to exchange some confidential information with Sabrina in a meeting 1 | b. message authentication | |
| d. message integrity 14 Myna tries to exchange some confidential information with Sabrina in a meeting 1 | c. message confidentiality | |
| 14 Myna tries to exchange some confidential information with Sabrina in a meeting 1 | d. message integrity | |
| 14. Myna thos to exchange some confidential mormation with Sabima in a moeting 1 | lyna tries to exchange some confidential information with Sabrina in a meeting | |
| having 20 members. Before actual data exchange, Myna authenticates herself to | having 20 members. Before actual data exchange, Myna authenticates herself to | |
| Sabrina without sending any secret. To do so she answered Sabrina's question :"Add | Sabrina without sending any secret. To do so she answered Sabrina's question :"Add | |
| 20 to your favorite number". The scheme used in this scenario is | 20 to your favorite number". The scheme used in this scenario is | |

| a. Zero knowledge scheme | |
|--|---|
| b. Challenge response scheme | |
| c. Encryption Scheme | |
| d. Hashing scheme | |
| e. None of the options. | |
| 15. A MDC is amessage digest. | 1 |
| a. Kevless | _ |
| b. Keved | |
| c. Both the options | |
| d. Neither of the options | |
| 16 criteria of a hash function ensures that no two | 1 |
| messages hash to the same digest | • |
| a. Strong-collision resistance | |
| h One-wayness | |
| c. Pre-image resistance | |
| d All of the options | |
| 17 Digital Signature cannot provide | 1 |
| a Integrity | 1 |
| h. Confidentiality | |
| c Non-Repudiation | |
| d Authentication | |
| 18 The Certification Authority (CA) signs the digital certificate to prevent forgery | 1 |
| using | 1 |
| a user's public key | |
| a. user's private key | |
| o, its own public key | |
| d its own private key | |
| 10. In Konkanan increase the tight to the year requesting a complex | 1 |
| 19. In Kerberos issues the licket to the user requesting a service. | 1 |
| h. Ticket Creating Server | |
| | |
| | |
| u. CA | 1 |
| 20. A user has created a new program and wants to distribute it to everyone in the | 1 |
| company. The user wants to ensure that when the program is downloaded that the | |
| is not changed when downloaded? | |
| is not changed when downloaded? | |
| a) Use Firewalls | |
| b) Encrypt the program and require a password after it is downloaded. | |
| c) Encrypt the session | |
| d) Create a hash of the program file that can be used to verify the integrity of | |
| the file after it is downloaded. | |
| e) Provide IP security | 1 |
| 21. Alice and Bob use the same password to login into the company network. This | 1 |
| means both would have the exact same hash for their passwords. What could be | |
| implemented to prevent both password hashes from being the same? | |
| a) RSA | |

| b) peppering | |
|---|---|
| c) salting | |
| d) pseudo-random generator | |
| 22. What term is used to describe concealing data in another file such as a graphic, | 1 |
| audio, or other text file? | |
| a) Masking and scrambling | |
| b) steganography | |
| c) obfuscation | |
| d) cryptology | |
| 23. A company is concerned with traffic that flows through the network. There is a | 1 |
| concern that there may be malicious traffic that exists that is not being blocked or | |
| eradicated by antivirus. What technology can be put in place to detect potential | |
| malware traffic on the network in real time? | |
| a) IDS | |
| b) firewall | |
| c) IPS | |
| d) Session Hijacking | |
| 24. Compute the RSA digital signature for the following scenario. | 1 |
| "Sign the message m=35. The private key used is (29,91) with the public key being | |
| (5,91)." | |
| a. 35 | |
| b. 42 | |
| c. 41 | |
| d. 38 | |
| 25. In an Elgammal Cryptosystem, Sender chooses $p = 107$, $e1 = 2$, $d = 67$, and the | 1 |
| random integer is r=45. Find the plaintext to be transmitted if the ciphertext is (28,9). | |
| a) 45 | |
| b) 76 | |
| c) 66 | |
| d) 13 | |
| 26.HMAC is slower than CMAC and is similar to cipher block chaining mode. The | 1 |
| given statement is | |
| a. True | |
| b. False | |
| | |
| 27. The responsibility of a certification authority for digital signature is to | 1 |
| authenticate the | |
| a) hash function used | |
| b) private keys of subscribers | |
| c) public keys of subscribers | |
| d) tickets generated | |
| 28. Data origin authentication cannot be provided using | 1 |
| a. Digital signature | |
| b. MAC | |
| c. symmetric encryption | |
| d.None of the answers. | |
| | |

| a. Authentication | |
|---|---|
| b. Key Generation | |
| c. Certificate verification | |
| d. None of the answers | |
| 30. If an attacker stole a password file that contained one way encrypted passwords, what type of an attack would he/she perform to find the encrypted password?(a)Man-in-the middle attack (b)Birthday attack (c)Denial of service attack | 1 |
| (d)Dictionary attack | |