Unit 1

Part A

1. What is OSI Security Architecture?
2. Compare / Differentiate active and Passive Attack Nov Dec 2016 / April May 2019
3. Categorize active and passive attack Nov Dec 2017
4. Categorize Security Services
5. Categorize Security Mechanisms
6. Distinguish between attack and threat Nov Dec 2018
7. List the Key concepts of Security or What is CIA Traid?
8. Specify the components of encryption algorithm or What are the ingredients of a Symmetric Cipher? April May 2019
9. How many keys are required for two people to communicate via a cipher?
10. What is the difference between a block cipher and a stream cipher?
11. What are the two general approaches to attacking a cipher?
12. What is the difference between an unconditionally secure cipher and a computationally secure cipher?
13. List the various Substitution Techniques
14. What are the two basic functions used in encryption algorithm?
15. Define Caesar Cipher
16. Define Monoalphabetic Cipher
17. Define Playfair cipher
18. What is the difference between a monoalphabetic cipher and a polyalphabetic cipher?
19. What are two problems with the one-time pad?
20. Calculate the cipher text for the following using one time pad cipher Nov Dec 2018
    a. Plain Text: ROCK & Keyword: BOTS
21. What is a transposition cipher?
22. What is steganography?
23. Compare and Contrast Steganography and Cryptography.
24. List the advantages and disadvantages of Steganography
25. List the various techniques used in Stegnanography
26. Define Group, Ring and Field
27. List the properties of Congruence
28. List the properties of Modular Arithmetic
29. Find gcd(1970,1066)using Euclid's algorithm. Nov Dec 2016
30. Determine the gcd(24140,16762)using Euclid's algorithm April May 2017
31. Determine the gcd(36939,15246)
32. Determine the gcd(5264,15472)
33. What is the difference between modular arithmetic and ordinary arithmetic?
34. List three classes of polynomial arithmetic.
35. State Fermat's theorem Nov Dec 2017 and April May 2017
36. State Euler's Theorem April May 2018
37. State Chinese Remainder Theorem

Part B

1. Explain OSI Security Architecture model with neat diagram. Nov Dec 2016
2. Describe the various Security Mechanisms. Nov Dec 2016
3. Encrypt the following using playfair cipher using the keyword MONARCHY. “SWARAJ IS MY BIRTH RIGHT”. Use X for blank spaces. Nov Dec 2017
4. Solve using playfair cipher method. Encrypt the word “Semester Result” with the Keyword “Examination”. Discuss the rules to be followed. April May 2019
5. What is monoalphabetic cipher? Examine how it differs from Caeser cipher? April May 2019
6. Describe Playfair cipher April May 2017
7. Describe Vignere Cipher April May 2017
8. Explain classical encryption techniques with symmetric cipher and Hill Cipher Model April May 2018
9. Perform Encryption and decryption using Hill Cipher for the following Message PEN and Key: ACTIVATED. Nov Dec 2018
10. Describe Railfence Cipher April May 2017
11. What is Steganogrpahy? Describe the various techniques used in Stegnanography? April May 2019
12. Discuss the properties that are to be satisfied by Groups, Rings and Fields Nov Dec 2017
13. Solve gcd(98,56)using Extended Euclidean algorithm. Write the algorithm also. Nov Dec 2018
14. State and prove Fermat’s theorem Nov Dec 2016
15. State and prove Euler’s theorem
16. State Chinese Remainder theorem and find X for the given set of congruent equation using CRT Nov Dec 2016
    X=2(mod 3) X=3(mod 5) X=2(mod 7)
17. State Chinese Remainder theorem and find X for the given set of congruent equation using CRT April May 2017
    X=1(mod 5) X=2(mod 7) X=3(mod 9) X=4(mod 11)

Unit 2

Part A

1. Give the five modes of operation of block cipher April / May 2017
2. Differentiate Stream and Block Cipher
3. Differentiate Diffusion and Confusion
4. Which parameters and design choices determine the actual algorithm of a Feistel cipher?
5. What is the purpose of the S-boxes in DES?
6. Explain the avalanche effect.
7. What is the difference between differential and linear cryptanalysis?
8. Compare the AES and DES. Nov / Dec 2018
9. List the parameters (block size, key size, and no. of rounds) for the three AES versions. April / May 2018
10. Brief the strengths of triple DES. Nov / Dec 2016
11. What is a meet-in-the-middle attack?
12. What are primitive operations used in RC5? April / May 2019
13. Give the application of the public key cryptosystem April / May 2019

14. State the difference between private key and public key. April / May 2017
15. What are the principal elements of a public-key cryptosystem?
16. Give the significance of hierarchical key control. Nov / Dec 2017
17. What is nounce?
18. What is an elliptic curve? Nov / Dec 2016
19. Why is trap door one way function used? Nov / Dec 2018

Part B

1. Explain about the Block Cipher modes of operation
2. Describe DES algorithm with neat diagram and explain the steps. **April / May 2017**
3. Describe in detail the key generation in AES algorithm and its expansion format(7) April / May 2019
4. What do you mean by AES ? Diagrammatically illustrate the structure of AES and describe the steps in AES encryption process with example. April / May 2018 (or)Explain AES algorithm with all its round functions in detail. Nov / Dec 2016
5. For each of the following elements of DES, indicate the comparable element in AES if available. Nov / Dec 2017

   XOR of subkey material with the input to function. , f function., Permutation p. ,Swapping of half of the blocks.
6. Describe triple DES and its application(6) April / May 2019
7. Explain Blowfish Algorithm
8. Explain RC5 Algorithm with Key Expansion
9. Explain public key cryptography and when it is preferred? (5) April / May 2019
10. Describe RSA algorithm(8) April / May 2019
11. Perform encryption and decryption using RSA algorithm for the following: p=7, q=11, e=7, M=9 (5) April / May 2019
12. Explain RSA algorithm, perform encryption and decryption to the system with p=7;q=11;e=17;M=8. Nov / Dec 2016 & April / May 2018
13. Perform encryption and decryption using RSA algorithm for p=17,q=11,e=7 and M=88 Nov / Dec 2018 & Nov / Dec 2017
14. Explain Diffie- Hellman key exchange algorithm in detail. April / May 2017
15. Find the secret key shared between user A and B using diffie hellman algorithm for the following.
16. q=353;α(primitive root)=3,X_A=45 and X_B=50 Nov / Dec 2018
17. Users Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q=83 and primitive root α=5. Nov / Dec 2017
    - **a.** If Alice has a private key Xa=6,what is Alice's public keyYA?
    - **b.** If Bob has a private key Xb=10, what is Bob's public key YB?
    - **c.** What is the shared secret key?
18. With a neat sketch explain the Elliptic curve cryptography with an example. April / May 2018

Part C

1. Explain briefly about Diffie Hellman key exchange algorithm with its merits and demerits (10) April / May 2019
2. Why is ECC is better than RSA? However why is is not widely used? Defend it. Nov / Dec 2018