K23U 2302

Reg. No. : .....

Name : .....

V Semester B.C.A. Degree (C.B.C.S.S. – O.B.E. – Regular/ Supplementary/ Improvement) Examination, November 2023
(2019-2021 Admissions)
Core Course
5B16BCA-E01 : INFORMATION SECURITY

Time : 3 Hours Max. Marks : 40

PART – A

Short Answer

Answer **all** questions. **(6×1=6)**

1. What is an affine cipher ?
2. What do you mean by DES ?
3. List the four possible approaches to attack RSA algorithm.
4. What is Avalanche effect ?
5. What are the security services provided by a digital signature ?
6. What is a CCA ?

PART – B

Short Essay

Answer **any 6** questions. **(6×2=12)**

7. Distinguish between passive attacks and active attacks.
8. What is the difference between asymmetric and symmetric cryptography ?
9. Explain why all block ciphers are polyalphabetic.

P.T.O.

10. Write a note on Kirchhoff's principle.

11. What is double DES ?

12. What is blinding ?

13. Distinguish between key only attack and known message attack on digital signature.

14. What is the difference between existential and selective forgery ?

PART – C
Essay

Answer **any 4** questions. **(4×3=12)**

15. Briefly explain the basic information security principle.

16. Explain cryptanalysis and its common types.

17. Briefly explain the RSA digital signature scheme.

18. Write down the applications and requirement for public key cryptosystem.

19. What is a digital signature ? Explain the difference between conventional and digital signature.

20. Describe the cipher and reverse cipher generation in DES.

PART – D
Long Essay

Answer **any 2** questions. **(2×5=10)**

21. Explain various types of information security attacks.

22. What is a substitution cipher ? Explain various monoalphabetic and polyalphabetic ciphers.

23. Briefly explain the structure of DES.

24. With an example explain the RSA algorithm.

K22U 2254

Reg. No. : .....

Name : .....

V Semester B.C.A. Degree (CBCSS-OBE-Regular/Supplementary/ Improvement) Examination, November 2022
(2019 Admission Onwards)
Core Course
5B16BCA – E01 INFORMATION SECURITY

Time : 3 Hours Max. Marks : 40

PART – A
Short Answer

Answer **all** questions : **(6×1=6)**

1. What do you mean by confidentiality ?
2. What do you mean by substitution cipher ?
3. What do you mean by cryptanalysis ?
4. List out any two private key algorithms.
5. What are the principles of a public key cryptographic algorithm ?
6. What do you mean by message authentication ?

PART – B
Short Essay

Answer **any 6** questions : **(6×2=12)**

7. List out the needs for information security.
8. What is a symmetric key ?
9. List out some weaknesses of DES algorithm.
10. What are the criteria that a cryptographic hash function must satisfy ?

P.T.O.

11. What do you mean by cryptanalysis system ?

12. What are the benefits of RSA digital signature ?

13. What is steganography ?

14. What are the features of Trogan horse ?

PART – C
Essay

Answer **any 4** questions : **(4×3=12)**

15. Briefly explain various principles of security.

16. What are various categories of traditional ciphers ?

17. Explain brute force attack.

18. Differentiate public key and private key cryptographic systems.

19. What do you mean by message digest ?

20. Explain Kirchoff's principle of cryptography.

PART – D
Long Essay

Answer **any 2** questions : **(2×5=10)**

21. Describe various types of security attacks.

22. Explain DES algorithm in detail.

23. Describe RSA algorithm.

24. Compare various digital signature schemes.

K21U 4675

Reg. No. : .....

Name : .....

V Semester B.C.A. Degree CBCSS (OBE) Regular Examination, November 2021
(2019 Admn. Only)
Core Course
5B16BCA-E01 – INFORMATION SECURITY

Time : 3 Hours Max. Marks : 40

PART – A
Short Answer

Answer **all** questions : **(6×1=6)**

1. List the goals of Information security.
2. Define Cryptography.
3. A cryptanalyst may use _____ attack to break the cipher.
4. DES is a block cipher. State True or False.
5. Expand RSA.
6. Name any two attacks on RSA signature.

PART – B
Short Essay

Answer **any 6** questions : **(6×2=12)**

7. Differentiate Active and Passive attacks.
8. Explain about Known plain text attack with neat sketch.
9. Write short note on encryption and decryption with DES.
10. Mention some weaknesses found in the cipher design of DES.

P.T.O.

11. What is the principle of public key cryptosystems ?

12. What are the applications of key cryptosystems ?

13. Explain about adding confidentiality to a digital signature.

14. Define forgery. Explain its types.

PART – C

Essay

Answer **any four** questions : **(4×3=12)**

15. Write short note on Principles of Security.

16. Explain about polyalphabetic ciphers with example.

17. Explain about the key generation in DES with diagram.

18. Write and explain the RSA algorithm.

19. Explain the differences between the conventional signature and digital signature.

20. Write note on public key cryptosystems.

PART – D

Long Essay

Answer **any 2** questions : **(2×5=10)**

21. Explain in detail about the attacks threatening confidentiality, integrity and availability.

22. Explain in detail about the classifications of transposition ciphers with example.

23. Explain about Multiple Data Encryption Standard (Multiple DES).

24. Explain in detail about RSA digital signature scheme.