Avinashilingam Institute for Home Science and Higher Education for Women

(Deemed to be University under Category 'A' by MHRD, Estd. u/s 3 of UGC Act 1956)
Re-accredited with 'A+' Grade by NAAC. Recognised by UGC Under Section 12B
Coimbatore - 641 043, Tamil Nadu, India

Bachelor's Degree Examination – August 2020
VI Semester

Class : III UG **Time : 2 Hours**
Major : Information Technology **Max. Marks : 50**

15BITC28 Cryptography and Network Security

Part - A **10 x 1 = 10**
Choose the Correct Answer

1. A Mechanism that is designed to detect, prevent or recover from a security attack is called
   a. security mechanism b. security service
   c. access control d. data confidentiality

2. Triple Data Encryption Standard algorithm is a symmetric-key _____, which applies the DES cipher algorithm three times to each data block.
   a. block chain b. authentication
   c. block cipher d. hash function

3. Diffie-Hellman is used to secure a variety of _____ services.
   a. ethernet b. internet
   c. intranet d. layer security

4. Public key cryptography is a _____ technique that uses a paired public and privae key algorithm for secure data communication.
   a. encryption b. decryption
   c. symmetric d. asymmetric

5. _____ algorithm is a symmetric key cryptographic technique to provide message authentication.
   a. Public key b. Private Key
   c. MAC d. Secret Key

6. Digital Signatures are the public-key primitives of _____ authentication.
   a. key b. data
   c. signal d. message

7. Kerberos is a network protocol that uses _____ cryptography to authenticate client/server applications.
   a. transport key b. secret key
   c. authorization key d. private key

8. Security is _____ to web services.
   a. easy b. difficult
   c. critical d. transparent

9. Password managers store the passwords in a_____ format.
   a. symmetric b. asymmetric
   c. decrypted d. encrypted

10. A _____ is a system designed to prevent unauthorized access to or from a private network.
    a. firewall b. packet filters
    c. stateful inspection d. proxy server

Part B **3 x 6 = 18**

Answer any **Three** questions

Each answer should not exceed 400 words or two pages

11. Outline the Block Cipher principles in detail.
12. Elaborate the Triple DES algorithm.
13. Give a summary of Diffie-Hellman key exchange algorithm.
14. Explain the Confidentiality using symmetric encryption.
15. List out the Authentication functions in detail.
16. Write a short note on Digital Signature Standard.
17. What is the use of Digital Certificates? Explain.
18. Discuss the Web security with suitable example.
19. Explain the Intrusion detection techniques in detail.
20. What is mean by Trusted Systems? Explain.

Part C **2 x 11 = 22**

Answer any **Two** questions

Each answer should not exceed 800 words or four pages

21. Illustrate the OSI Security Architecture in detail.
22. Explain the evaluation criteria for AES algorithm.
23. Detail discussion about the Elliptic Curve Cryptography algorithm.
24. Describe RSA public key cryptography algorithm in detail.
25. Explain the MD5 message digest algorithm in detail.
26. Describe the HMAC Digital Signatures in detail.
27. Explain the X.509 Authentication services in detail.
28. Discuss about the Electronic Mail Security.
29. List out the various Viruses and related Threats.
30. Elucidate the Firewall design principles.

****