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 – June 2021
VI Semester

Class : III UG **Time : 3 Hours**
Major : Information Technology **Max. Marks: 100**

18BITC28 Cryptography and Network Security

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

1. The keys used in cryptography are CO1 K1
   a. secret key b. private key
   c. public key d. All the above

2. Encryption Strength is based on CO1 K2
   a. strength of algorithm b. secrecy of key
   c. length of key d. all the above

3. The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not CO2 K1
   a. Authenticated b. Joined
   c. Submit d. Separate

4. In Elgamal cryptosystem, given the prime p=31, Encrypt the message "HELLO"; use 00 to 25 for encoding. The value of C2 for character 'O' is CO2 K2
   a. 9 b. 7 c. 23 d. 27

5. SHA-l has a message digest of CO3 K2
   a. 160 bits b. 512 bits
   c. 628 bits d. 820 bits

6. To check integrity of a message, or document, receiver creates the CO3 K1
   a. Hash-Table b. Hash Tag
   c. Hyper Text d. Finger Print

7. PGP offers___ block ciphers for message encryption? CO4 K2
   a. Triple-DES b. CAST
   c. IDEA d. All the above

8. Which of the following is not a strong security protocol? CO4 K1
   a. HTTPS b. SSL
   c. SMTP d. SFTP

9. Which of them is not an ideal way of spreading the virus? CO5 K1
   a. infected website b. E-mails
   c. Official Antivirus CDs d. USBs

10. A computer ____ is a malicious code which self-replicates by copying itself to other programs. CO5 K2
   a. program b. virus
   c. application d. Worm

Part B **5 x 6 = 30**

Answer ALL questions

Each answer should not exceed 400 words or two pages

11.a. Explain in detail different passive and active attacks.	CO1 K2
(or)	
11.b. Differentiate the cipher properties of confusion and diffusion.	CO1 K2
12.a. What is the importance Chinese Remainder Theorem in cryptography? Explain.	CO2 K2
(or)	
12.b. Using CRT, solve for x for the following $x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 5$; $x \equiv 2 \pmod 7$	CO2 K3
13.a. Explain the process involved in message digest generation and processing of single block in SHA-512.	CO3 K2
(or)	
13.b. Illustrate Birthday Attack on Digital Signatures? Can it be performed by an 'Outsider'?	CO3 K3
14.a. Write Radix 64 format? What is its use in PGP?	CO4 K3
(or)	
14.b. Explain how authentication is performed in Kerberos.	CO4 K2
15.a. Define a worm? Name some known worms	CO5 K1
(or)	
15.b. List the types of Computer Crime and Give a brief on it	CO5 K1

Part C **5 x 12 = 60**

Answer ALL questions

Each answer should not exceed 800 words or four pages

16.a. Explain AES encryption and Decryption in detail.	CO1 K2
(or)	
16.b. Compare the substitution method in DES and AES. Why do we need only one substitution table in AES, but several in DES?	CO1 K2
17.a. State and prove Chinese remainder theorem	CO2 K1
(or)	
17.b. Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7 and N=5	CO2 K3
18.a. Describe the steps in message digest generation in Secure Hash Algorithm in detail.	CO3 K2
(or)	
18.b. What is message authentication? List the authentication requirements.	CO3 K1
19.a. What is Public Key certificate? Explain its usage with X.509 certificates.	CO4 K4
(or)	
19.b. Explain the architecture of IP Security	CO4 K3
20.a. List four techniques used by firewalls to control access and enforce a security policy and also explain the types of firewall	CO5 K1
(or)	
20.b. Define three types of intellectual property. What are the basic conditions that might be fulfilled to claim a copyright.	CO5 K1

*****