Question Paper

MANIPAL ACADEMY OF HIGHER EDUCATION

SIXTH SEMESTER B.TECH MAKEUP EXAMINATIONS, JULY 2022

CYBER SECURITY [ICT 4306]

Marks: 50   **Duration: 180 mins.**

DESCRIPTIVE

Answer all the questions.

Instructions to Candidates: Answer ALL questions Missing data may be suitably assumed

1)

A)   Describe with relevant diagrams any 2 types of Single Sign-On Configurations.   (5)

B)   What is Software Piracy? Briefly describe any 4 types of software piracy.   (3)

C)   How does asymmetric key cryptography provide the confidentiality of a message and authenticity of the message originator?   (2)

2)

A)   For the data p=7, q=17, and e=5. Perform the following operations using the RSA algorithm: (5)

    a. Compute the decryption key d.

    b. Show the steps involved in decrypting the ciphertext C=40.

B)   Differentiate between the following: (3)

    a. First versus third party tracking

    b. Generation and Mutation Fuzzing Approach

    c. Monoalphabetic and Polyalphabetic Ciphers

C)   What is a digital certificate? List the data it contains.   (2)

3)

A)   With appropriate examples, explain the various categories of Active and Passive Attacks.   (5)

B)   Define Computer Forensics. Compare and contrast Imaging and Carving forensic techniques.   (3)

C)   Differentiate between the following: (2)

    a. Side-Channel Attacks and Replay Attacks

    b. Cryptanalytic attack and Brute force attack.

4)

A)   Encrypt the word "Education is worth more than gold" using the following symmetric cipher techniques.   (5)

    a. Additive Cipher with key =4.

b. Multiplicative Cipher with key =11.

c. Autokey Cipher with key =20.

d. Vignere Cipher with key =" Einstein".

e. Rail Fence Cipher with key =3.

B)   What are the various categorizations in digital forensics? Exemplify what each of them does.   (3)

C)   Differentiate between the following: (2)

a. Strict and Lax Same Site Cookie Attribute

b. Session Cookies and Permanent Cookies.

5)   How is a Web Application Firewall different from Network Firewall? Compare and contrast the   (5)
filtering approaches used in Web Application Firewall. Mention its benefits.

A)

B)   What are the main categories of modification check values? Differentiate between them.   (3)

C)   How to establish Client-Server Trust Boundaries? Explain in brief.   (2)

-----End-----