Manimuruk.

Avinashilingam Institute for Home Science and Higher Education for Women
Deemed to be University Estd.u/s 3 of UGC Act 1956, Category A by MHRD
Re-accredited with 'A++' Grade by NAAC. CGPA 3.65/4, Category I by UGC
Coimbatore-641 043, Tamil Nadu, India

Continuous Internal Assessment Test I – August 2024

Semester – III

Class: IIPG **Time: 2Hrs**

Major: Mathematics **Max. Marks: 60**

23MMAC16–Cryptography

Course Outcomes:

CO1: provide security of the data over the network.

CO2: implement confidentiality and modular arithmetic.

CO3: illustrate public and private key cryptography.

CO4: apply authentication algorithms.

CO5: use IP security in networking.

Part –A **6x1=6**

Choose the correct answer

1.What is the inclusion of a secret message in otherwise unencrypted text or images called. CO1K1

a.masquerade b.steganography c.spoof d. eye-in hand system

2. In the strength of DES, a key length of ____ bits, there are ____ possible keys. CO1K2

a. 54, 2^{54} b. 96, 2^{96} c. 56, 2^{56} d. 64, 2^{64}

3. Which of the following security attacks is a passive attack? CO2K2

a. traffic analysis b.modification of message

c. denial of service d. masquerade

4. The value of x satisfying $3x \equiv 2 \pmod 5$. CO2K2

a. 2 b. 1 c. 4 d. 3

5.Which of the following is the first step of RSA algorithm key generation? CO3K2

a. computation of n = pq b. gcd(e, $\lambda(n)$)

c. select large 2 prime numbers d. compute $\lambda(n)$

6. A _____ scheme is used to distribute the master keys. CO3K2

a. secret b. hybrid c. private key d. public ey

Part B **3 x 6 = 18**

Answer ALL questions

7. a. Explain the main objectives of security services. CO1K3

(or)

7. b. Explain cryptography and its types? CO1K2

8. a. Describe Groups, Rings and Fields. CO2K2

(or)

8. b. Explain the Euclidean Algorithm in cryptography? CO2K3

9. a. Write a short note on Public-Key Cryptosystems. CO3K2

(or)

9. b. Explain Diffle – Hellman key exchange algorithm. CO3K3

Part C **3 x 12 = 36**

Answer ALL questions

10. a. Explain briefly about the classical encryption techniques and their types. CO1K4

(or)

10. b.Explain block ciphers principals. CO1K3

11. a.What are the different types of key distribution techniques in cryptography? CO2K3

(or)

11. b. Explain Modular Arithmetic and their operation. CO2K4

12. a.State and prove Fermat's theorem and Euler's theorem. CO2K3

(or)

12. b. Explain RSA algorithm. CO3K3

No. of copies : ~~10~~ 30