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 II – October 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 **6 x 1 = 6**

Choose the Correct Answer

1. MAC is a CO3K1

a. one-to-one mapping b. many-to-one mapping

c. onto mapping d.key code

2. Which one of the following is not an application of hash functions? CO3K2

a. one-way password file b. key wrapping

c. virus detection d.intrusion detection

3. MD5 is a widely used hash function for producing hash value of CO4K2

a. 64 bits b. 128 bits c. 512 bits d.1024 bits

4. Digital signature cannot provide ___ for the message. CO4K1

a. Authentication b. Nonrepudiation

c. Confidentiality d.Integrity

5. In tunnel mode IPsec protects the CO5K1

a. Entire IP packet b. IP header

c. IP payload d. Session layer

6. Which one of the following is not a public key distribution means CO5K2

a. Public-Key Certificates b. Hashing Certificates

c. Publicly available directories d.Public-Key authority

Part B **3 x 6 = 18**

Answer ALL questions

7. a.Explain Hash function. CO3K3

(or)

7. b. Write a short note on Cryptanalysis. CO3K2

8. a. Describe an authentication protocols and their approaches. CO4K2

(or)

8. b. Explain the Digital signature standard approach and algorithm. CO4K3

9. a. Write an applications and benefits of IPsec. CO5K3

(or)

9. b. Explain an Encapsulating Security Payload. CO5K3

Part C **3 x 12 = 36**

Answer ALL questions

10. a. Explain an authentication functions. CO3K4

(or)

10. b. Explain briefly about the Message Authentication Code. CO3K3

11. a. Explain Digital Signature and their types. CO4K3

(or)

11. b.What is the difference between Kerberos version 4 and version 5. CO4K4

12. a. Explain briefly about an authentication header and their modes. CO5K4

(or)

12. b. Describe the types of Key Managementand their protocol. CO5K3

No. of copies :~~20~~ 28