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. Recognised by UGC Under Section 12 B
Coimbatore - 641 043, Tamil Nadu, India

**Master's Degree Examination – November 2024**
**III Semester**

**Class : II PG** **Time: 3 Hours**
**Major : Mathematics** **Max. Marks: 100**

## 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** **10 x 1 = 10**
**Choose the Correct Answer**

1. The _____ is the original message before transformation. CO1K1
a. cipher text b. plaintext c. secret-text d. none of the above

2. _____ is an example of a Monoal phabetic cryptosystem. CO1K1
a. shiftcipher b. substitutioncipher c. both a and b d. neither a and b

3. In the expression a=qn+r, r is referred to as _____ CO2K1
a. modulus b. residue c. prime modulo d. none of the above

4. gcd (a,b)= CO2K1
a. gcd(a, a mod b) b. gcd(b, a mod b) c. gcd(a, b mod a) d. gcd (b, b mod a)

5. _____ depend on running time of decryption algorithm. CO3K1
a. brute force b. birthday attacks c. timing attacks d. Mathematical attacks

6. Hash code is also referred as _____ CO3K1
a. message code b. message digest c. error code d. message decryption

7. SHA-512 logic algorithm takes as input a message with maximum length less than _____ CO4K1
a. $2^{120}$bits b. $2^{128}$ bits c. $3^{120}$ bits d. $2^{56}$ bits

8. In PGP a _____ Key is used to decrypt the message. CO4K1
a. key ID b. user key c. session key d. public key

9. _____ provides support for data integrity and authentication of IP packets. CO5K1
a. decryption file b. authentication header
c. public key d. security code

10. Oakley is a key exchange protocol based on _____ algorithm CO5K1
a. RST b.CRT c. Diffie Hellman d. Digital signature

## Part B 5 x 6 = 30

**Answer ALL questions**

**Each answer should not exceed 400 words or two pages**

11.a. Explain each of the following terms with an example CO1K3
i. Plain text ii. Cipher text iii. Key iv. Encryption algorithm.

(or)

11.b. Explain the construction of S box in the AES algorithm. CO1K2

12.a. Interpret chinese remainder theorem. CO2K2

(or)

12.b. Explain the term discrete algorithm. CO2K4

13.a. Explain the terms i) Public announcement of public key ii)Public available directory. CO3K4

(or)

13.b. Examine RSA algorithm. CO3K3

14.a. Discuss the various steps involved in MD5 message digest algorithm. CO4K2

(or)

14.b. Write down the digital signature algorithm. CO4K3

15.a. Explain the applications and benefits of IP security. CO5K4

(or)

15.b. Discuss the transport and tunnel mode supported by AH and ESP. CO5K2

## Part C 5 x 12 = 60

**Answer ALL questions**

**Each answer should not exceed 800 words or four pages**

16.a. Explain the term cryptography and several types of cryptography CO1K4

(or)

16.b. Summarize the several modes of operation of a block cipher. CO1K5

17.a. Explain Rabin Miller Algorithm for testing primality CO2K4

(or)

17.b. Write down the procedure for finding gcd of two positive integers using Euclidean algorithm, explain the Fermat's theorem and Eulers theorem. CO2K3

18.a. Classify the various types of authentication function. CO3K4

(or)

18.b. Summarize Diffie Hellman Key Exchange and its algorithm. CO3K5

19.a. Point out the environment limitations and technical deficiencies of kerberos version 4. CO4K4

(or)

19.b. Summarize security hash algorithm. CO4K5

20.a. Explain encapsulating security payload. CO5K4

(or)

20.b. Explain the key management Oakley key determination protocol CO5K3

******