Avinashilingam Institute for Home Science and Higher Education for Women

Coimbatore -641043

Master's Degree Examination – November 2017

Semester III

Class: II P.G **Max. Marks: 60**

Major: Mathematics **Time : 3 Hours**

12MMAC16 Cryptography

Part - A **10 x ½ = 5**

Choose the correct Answer:

1.Two integers a and b are said to be relatively prime if ----------

a) gcd(a,b) = 1 b) gcd(a,b) > 1 c) gcd(a,b) < 1 d) gcd(a,b) ≠ 1

2.r = $(a \pm b) mod n$ means ----------

a) (a modn $\pm bmodn) modn$ b) (a modn $\pm bmodn$)

c) (a modn $+bmodn) modn$ d) (a modn $- bmodn) modn$

3.Hash algorithm are based on ---------- function

a) one-way b) one-to-one c)onto d) none of these

4)Every polynomial in GF(2^n) can be represented by ---------- number

a) one bit b) two bit c)three d) n bit

5.Substitution and ---------- are two basic building blocks of all conventional encryption techniques.

a) transposition b)addition c)multiplication d) transformation

6)In polyalphabetic Cipher ----------is one of the best known Cipher.

a)Ceaser b)Vigenere c) Hill d) Affine

7 The simplified version of DES stands for ----------

a) . S-DES b) DES c) SDE d) SED

8.Shannon's Theory of ----------

a)Confusion b)Diffusion c) Both (a) & (b) d) neither (a) nor (b)

9._____ of stored computer data provides protection against the disclosure of stolen data.

a) Encryption b)Decryption c) Encryption and decryption d) None of these

10.A ---------- is a correspondence between code words and data elements.

a) code b) data c) encryption d)None of these

Part B **5X4=20**

Answer All Questions

11.a. Explain Euclidean Algorithm

(Or)

11.b.State and prove Euler theorem

12.a.Find all primitive roots of 15

(Or)

12.b.Explain Hash algorithm

13.a.Explain Hill Cipher with suitable example

(Or)

13.b.Give some examples of steganography

14.a. Explain the simplified version of DES

(Or)

14.b.Explain Shanon's theory of Confusion

15.a.Write short note on "Spoofing"

(Or)

15.b.Explain Key Management in DES

Part C **5X7=35**

Answer All Questions

16.a. State and prove Fermat's Little Theorem

(Or)

16.b.State and prove Chinese remainder Theorem

17.a.Let $p(x)= x^6 + x^4 + x^2 + x + 1$, $f(x) = x^7 + x + 1$ and $m(x) = x^8 + x^4 + x^3 + x + 1$, by XOR operation show that $p(x)f(x) \bmod m(x) = x^7 + x^6 + 1$

(Or)

17.b.What are the drawbacks of classical cryptography ?How does the public key algorithm overcome theses drawbacks

18a. Encrypt the message READY FOR WAR with N=27, a=3,b=4 and using digraph and affine Transformation

(Or)

18.b. Explain some important Substitution Ciphers with suitable examples

19.a. Discuss Block Cipher Principles

(Or)

19.b. Encrypt plain text block (10010011) with k = (1110011001) using S-DES

20.a. Explain the uses of data encryption

(Or)

20.b.Discuss the concept of encoding and enciphering

****