MANAV RACHNA
vidyanatariksha

MANAV RACHNA
UNIVERSITY
(FORMERLY MANAV RACHNA COLLEGE OF ENGINEERING
NAAC ACCREDITED 'A' GRADE INSTITUTION)
Declared as State Private University under section 2f of the UGC act, 1956

DEPARTMENT OF MATHEMATICS

"T3 Examination , May 2017-18"

Semester: Fourth**Date of Exam**: 21/05/2018
Subject: Cryptography **Subject Code**: MAH630-T
Branch: Mathematics**Session**: I
Course Type: Elective**Course Nature:**Hard
Time: 3 Hours **Program: M.Sc.**
Max.Marks: 100 **Signature: HOD/Associate HOD:**

Note: All questions are compulsory from part A . Attempt any two questions from Part B (20 Marks each). Attempt any two Questions from Part -C (20 Marks each).

PART-A

Q.1 (a) Explain why we need fuzzy set theory. (3)

(b) State and prove second decomposition theorem. (7)

Q.2 Write a short note on:

(a) Differential crypt analysis

(b) Linear crypt analysis

(c) Differential Cryptanalysis of DES

(d) Linear cryptanalysis of DES

(e) The Boomeringattack (10)

PART- B

Q.2 (i)Find P+ Q if P, Q∈$E_{23}(1,1)$ and

(a) P = (3, 10) , Q = (9, 7)

(b) P = (6, 4), Q = (7, 12)(10)

(ii) Find additive inverse of P if $P \in E_{11}(1,1)$. (10)

Q.3 (a)Discuss the importance of Elliptic curve cryptosystem. How the key exchange in ECC is similar to that of very popular algorithm Diffe-Hellmen key exchange Cryptosystem. (10)

(b) Determine att the elements of the group $E_{11}(1,1)$which satisfy the elliptic curve $y^2 mod 11 = (x^3 + x + 1) mod 11.$ (10)

Q.4 If the cryptosystem parameters are $E_{23}(1,1), G = (3,10)$ and the private key of the user B is $n_B = 4$, then

(a) Find the public key of the user B.

(b) Find the cipher text $C_m$for the message P_m = (6,4).

(c) How can the user B recover the plain text P_m. (20)

****

PART-C

Q.5Discuss the following:

(a) Digital signature with appendix.

(b) Digital signature with message recovery.

(c) The RSA signature scheme.

(d) Feige-Fiat – Shamir signature scheme. (20)

Q.6 What is digital signature standard? Discuss digital signature algorithm and give proof. (20)

Q.7 What is mutual authentication? How can you achieve mutual authentication through?

(a) secrete shared key

(b) public key encryption.

(c) time stamp. (20)

****