Registration No: □□□□□□□□□□

Total Number of Pages: 01

M.TECH
P2CTCC09

2^{nd} Semester Regular Examination 2016-17

CRYPTOGRAPHY

BRANCH: COMPUTER ENGG, COMPUTER SCIENCE, COMPUTER SCIENCE AND ENGG, COMPUTER SCIENCE AND TECH., Information Tech Eng, INFORMATION TECH.

Time: 3 Hours

Max Marks: 100

Q.CODE: Z806

Answer Question No.1 which is compulsory and any FOUR from the rest.
The figures in the right hand margin indicate marks.

Q1 Answer the following questions: ***Short answer type*** **(2 x 10)**

a) What is dictionary attack?

b) What is the difference between Symmetric Key and Asymmetric Key Encryption?

c) What are the properties of Hash function?

d) What is the condition that a predicate is hardcore for a function?

e) What is the difference between chosen plaintext attack and chosen cipher text attack?

f) Define Homomorphic encryption.

g) Define Trap-door permutation.

h) Why PRNG’s required in cryptography?

i) Give asymptotic definition of One way function.

j) What are the three properties of Zero Knowledge protocols?

Q2 a) Explain Goldwasser and Micali encryption scheme. **(10)**

b) Describe DES scheme in symmetric key cryptosystem. **(10)**

Q3 a) Prove that if (Enc,Dec) is perfectly secure, then k≥m, where ‘k’ is length of the key and ‘m’ is message length. **(10)**

b) Explain How one way function helps in generating Pseudo random number. **(10)**

Q4 a) If B is (t,ε)-hardcore then G BM is a (t−mTIME(f),εm)-PRNG. , Prove the Theorem. **(10)**

b) Explain IND-CPA algorithm for chosen plain text attack. **(10)**

Q5 a) Explain RSA cryptosystem. **(10)**

b) What is Random Oracle.? Explain its application in Cryptography and its limitation. **(10)**

Q6 a) Describe the process of MAC and its limitations? **(10)**

b) Describe the model of Digital signature with diagram and its importance? **(10)**

Q7 a) What is Zero knowledge proof? Explain its application in protocol design and identification scheme. **(10)**

b) What is fiat-Shamir protocol? How it works? **(10)**