Registration no:

Total Number of Pages: 02 **B.TECH**
FECE6404

8^{th} Semester Regular / Back Examination 2016-17
NETWORK SECURITY AND CRYPTOGRAPHY
BRANCH(S): ECE, ETC
Time: 3 Hours
Max marks: 70
Q.CODE: Z161

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

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

a) What are the differences between Symmetric and Asymmetric Encryption system?
b) Distinguish between diffusion and confusion.
c) Why does DES function need an expansion permutation?
d) What is a key distribution center?
e) Use the additive cipher with key=20 to encrypt the message “HELLO”.
f) What is the difference between Worm and Viruses?
g) What is an Intrusion Detection System (IDS)?
h) Define Digital signature and explain its advantages.
i) Distinguish between Message Integrity and message Authentication.
j) What are the requirements and protections for a secure e-mail?

Q2 **a)** Discuss the tradeoff between Conventional and Public key Cryptosystems. **(5)**

b) Draw the block diagram of DES cryptosystem. Explain the key generation process for different rounds. **(5)**

Q3 **a)** Explain Diffie-Hellman key Exchange algorithm. **(5)**

b) Give general format of a PGP message. Explain why PGP generates a signature before applying compression. In what form the private key is kept in Private Key Ring? **(5)**

Q4 **a)** What is firewall? Discuss different types of firewall in brief. **(5)**

b) What is computer virus? List different type of computer viruses and how they affect computer security. **(5)**

Q5 **a)** What do you mean by sensitive data? Discuss various factors that make data sensitive. **(5)**

b) State Euclidean algorithm. Using this algorithm find gcd(32,10). **(5)**

Q6 **a)** What is multilevel database? How we provide security to it? **(5)**

b) State Chinese Remainder Theorem. Use it to solve the following congruence: X=4 mod 7, X=4 mod 13, X=0 mod 12. **(5)**

Q7 **a)** What is Kerberos? What requirements were found for Kerberos? Describe the sequence of message exchanges of Kerberos Version 4. **(5)**

b) Explain the various Ethical Issues in Computer Security. **(5)**

Q8 **Write short notes on any two:** **(5 x 2)**

a) RSA algorithm
b) Playfair Cipher
c) Random Oracle Model
d) VPN