Registration no: | | | | | | | | | | |

Total Number of Pages: 02

8th Semester Regular / Back Examination 2015-16
NETWORK SECURITY AND CRYPTOGRAPHY
BRANCH: AEIE, EIE, IEE
Time: 3 Hours
Max Marks: 70
Q.CODE: W131
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 is data integrity and confidentiality?
b) Distinguish between cryptography and steganography?
c) What is malicious program? Give examples of malicious errors.
d) Write relation between plain text and cipher text in Affine cipher?
e) Define "cyclic group " with a suitable example.
f) Find the multiplicative inverse of 7 in Z_{12}.
g) What is boot sector virus?
h) List different threats to email.
i) Write importance of firewall.
j) What is intrusion ? give an example of it.

Q2 a) What is Hill cipher? Using a key K=$\begin{matrix} 03 & 02 \\ 05 & 07 \end{matrix}$ encrypt the message "The north star".   **(5)**

b) In RSA cryptosystem, for n=12091 and e=13, encrypt the message "enemy of state".   **(5)**

Q3 a) What is a firewall? Mention different types of firewalls and explain their working principles.   **(5)**

b) Compose the advantage and disadvantage of stream and block encryption algorithm. Are AES and DES steam or block cipher.   **(5)**

Q4 a) What is a computer virus? List different types of viruses and how they affect the computer security.   **(5)**

b) Find the solution to the following linear equation   **(5)**
        5x+4y=6(mod 7)
        2x+5y=5(mod 7)

Q5 **a)** Find the inverse of $(x^3 + x + 1)$ in GF(2^4) using modulus $(x^4 + x^2 + 1)$. **(5)**

b) Solve the following congruence using quadratic residues **(5)**
$$x^2 \equiv 47 \bmod 77$$

Q6 **a)** Encrypt the message "cryptography and network security "using the Multiplicative cipher with key of 7. **(5)**

b) List different feature of Whirlpool hash function. **(5)**

Q7 **a)** Draw the block diagram for a Round key generator. Write the Necessity of parity bit drop during the generator. **(5)**

b) Explain Intrusion Detection System. **(5)**

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

a) Play fair cipher.

b) Affine cipher

c) cryptographic attacks

d) ElGamal Cryptosystem