Printed Pages - 3 **NMCAE21**

(Following Paper ID and Roll No. to be filled in your Answer Books)

Paper ID : 2012314 **Roll No.** | | | | | | | | | | |

MCA

Regular Theory Examination (Odd Sem-V), 2016-17

NETWORK SECURITY & CRYPTOGRAPHY

Time : 3 Hours ***Max. Marks : 100***

Section - A

1. Attempt all parts. All parts carry equal marks. Write answer of each part in short. (10×2=20)

a) For each of the following ciphers, say whether it is stream cipher or block cipher. Defend your answers.

i) Playfair

ii) Hill cipher

iii) Vignere cipher

b) Encrypt the message "health" using additive cipher with key value 20. Also show how it will be decrypted to get the original plaintext.

c) Draw the Block diagram of one round of DES cipher

d) State the block size, key size and number of rounds for three AES versions.

e) 'State Euler's theorem.

f) What is Shanon's theory of confusion and diffusion.

g) What are requirements of digital signature.

h) Contrast the key management in PGP and S/MIME

i) Distinguish between the two modes of IPSec.

j) What is logic bomb

Section - B

Attempt any 5 questions from this section.

(5×10=50)

2. What is a x.509 digital certificate? How is PKI maintained? Describe.

3. Describe at least three modes of operation block ciphers for encipherment.

4. Draw the structure of one round in AES and describe in brief

5. Write RSA cryptographic algorithm and explain the principle behind various choices in the algorithm.

6. Write and explain digital signature algorithm (DSA) of digital signature standard.

7. Explain how the diffie hellman key exchange algorithm is vulnerable to man in the middle attack.

8. Describe the responsibilities of various servers and write the sequence of message exchanges in kerberos-version4

9. Write short note on the firewall

Section - C

Attempt any 2 questions from this section.(2×15=30)

10. a) Compute 77^{-1} mod 411 using extended eudidean algorithm

    b) Write the message format of a typical PGD message.

11. Write notes on secure electronic transaction (SET)

12. a) With the help of suitable example , explain the birthday attack on a Hash Function

    b) Prove that a group in which all elements are their own inverses is an abelian group.
