Printed Pages : 1 **Roll No.** | | | | | | | | | | | **ECS029**

B.TECH.
THEORY EXAMINATION (SEM–VI) 2016-17
CRYPTOGRAPHY & NETWORK SECURITY

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

Note : *Be precise in your answer. In case of numerical problem assume data wherever not provided.*

SECTION-A

1 Explain the following : **(10×2=20)**

a) Explain Weakness of DES.

b) What do you mean by cryptanalysis?

c) Difference between RSA and Diffie-Hellman key exchange cryptographic algo?

d) Explain Euler's Totient Function.

e) State benefits provided by MAC.

f) Explain Firewall.

g) (g)What is the requirement of security?

h) (h)Explain Shannon theory of confusion and diffusion.

i) (i)What is monoalphabetic Cipher?

j) (j)Explain Euclidean theorem.

SECTION-B

2 Attempt any five of the following: **(10×5=50)**

a) What are the principal differences between version 4 and version 5 of Kerberos?

b) What is mono-alphabetic cipher? How it is different from Caesar Cipher.

c) What is transposition cipher? Illustrate with an example.

d) What do you mean by Hill Cipher technique? By using Hill Cipher technique encrypt the message "AT" with the help of key K= [5 3] 3 4

e) What is IP security Architecture? Explain in detail.

f) Explain Euclidean Algorithm. Find the value of GCD (1970, 1066).

g) State and prove Fermat's theorem, determine the value of 3^{201} mod 11.

h) What are the requirements of Message Authentication Code (MAC)? List and explain them.

SECTION-C

Attempt any two of the following: **(15×2=30)**

3 Write short note on any two of the following:

(i)Secure Electronic Transaction (SET)

(ii) Firewalls.

(iii)Intrusion Detection

4 Write the steps of RSA Key generation

5 Draw a block level diagram to depict the structure of AES with strength and weakness of AES.