le No: 126AQ

R13

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

B. Tech III Year II Semester Examinations, May-2016

INFORMATION SECURITY

(Computer Science and Engineering)

e: 3hours **Max.Marks:75**

e: This question paper contains two parts A and B.
Part A is compulsory which carries 25 marks. Answer all questions in Part A. Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 10 marks and may have a, b, c as sub questions.

PART- A

(25 Marks)

What are the types of security attacks? [2]
Compare substitution ciphers with transposition ciphers. [3]
Compare block ciphers with stream ciphers. [2]
Write about strength of DES algorithm. [3]
What is a digital signature? [2]
What properties must a hash function have to be useful for message authentication?[3]
What are the various PGP services? [2]
What parameters identify an SA and what parameters characterize the nature of a particular SA? [3]
What is cross site scripting vulnerability? [2]
What are the limitations of firewalls? [3]

PART-B

(50 Marks)

Consider the following:
Plaintext: "PROTOCOL"
Secret key: "NETWORK"
What is the corresponding cipher text using play fair cipher method?
) What is the need for security? [5+5]

OR

). Explain the model of network security.
). Write about steganography. [5+5]

Explain the AES algorithm. [10]

OR

Consider a Diffie-Hellman scheme with a common prime q=11, and a primitive root α=2.
a) If user 'A' has public key Y_A=9, what is A's private key X_A.
b) If user 'B' has public key Y_B=3, what is shared secret key K. [5+5]

Explain HMAC algorithm. [10]

OR

) Explain the DSA algorithm.
) What is bio-metric authentication? [5+5]

8.a) Explain PGP trust model.
b) What are the key components of internet mail architecture? [5+5]

OR

9.a) Explain MIME context types.
b) What are the five principal services provided by PGP? [5+5]

10. Explain secure electronic transaction. [10]

OR

11.a) Explain password management.
b) What are the types of firewalls? [5+5]

---ooOoo—