

Code No: 126AQ

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

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

INFORMATION SECURITY

(Computer Science and Engineering)

Time: 3 hours

Max.Marks:75

Note: 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)

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

PART-B

(50 Marks)

- 2.a) Consider the following:
Plaintext: "PROTOCOL"
Secret key: "NETWORK"
What is the corresponding cipher text using play fair cipher method? [5+5]
 - b) What is the need for security? [5+5]
- OR**
- 3.a) Explain the model of network security. [5+5]
 - b) Write about steganography. [5+5]
4. Explain the AES algorithm. [10]
- OR**
5. Consider a Diffie-Hellman scheme with a common prime $q=11$, and a primitive root $a=2$.
a) If user 'A' has public key $Y_A=9$, what is A's private key X_A ? [5+5]
b) If user 'B' has public key $Y_B=3$, what is shared secret key K. [5+5]
6. Explain HMAC algorithm. [10]
- OR**
- 7.a) Explain the DSA algorithm. [5+5]
 - b) What is bio-metric authentication? [5+5]

R BR BR BR BR BR BR BI

- 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]

R BR BR BR BR BR BR BI

- 10. Explain secure electronic transaction. [10]

OR

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

R BR BR BR BR BR BR BI

---ooOoo---

R BR BR BR BR BR BR BI

R BR BR BR BR BR BR BI

R BR BR BR BR BR BR BI

R BR BR BR BR BR BR BI

R BR BR BR BR BR BR BI

R BR BR BR BR BR BR BI