

Total No. of Questions : 10] [Total No. of Printed Pages : 3

Roll No.

IT-801(N)

B. E. (Eighth Semester) EXAMINATION, June, 2011

(Information Technology Engg. Branch)

INFORMATION SECURITY

[IT-801(N)]

Time : Three Hours

Maximum Marks : 100

Minimum Pass Marks : 35

Note : Attempt any *one* question from each Unit.

Unit-I

1. (a) What are *three* basic operations in cryptography ? 10
- (b) What is hash function and what can it be used for ? 10

Or

2. (a) How can a security framework assist in the design and implementation of a security infrastructure ? 10
- (b) Explain the following : 10
 - (i) Confidentiality
 - (ii) Integrity
 - (iii) Availability

Unit-II

3. (a) What are *six* components of public key infrastructure (PKI) ? 10

P. T. O.

- (b) What drawbacks to symmetric and asymmetric encryption are resolved by using a hybrid method like Diffie-Hellman ? 10

Or

4. (a) What is the difference between digital signatures and digital certificates ? 10
(b) What is the fundamental difference between symmetric and asymmetric encryption ? 10

Unit – III

5. (a) IP sec can be used in two modes. What are they ? 10
(b) Using a modern pentium 4 computer, how long would it take to crack a cryptosystem that is based on a 32-bit key, 56-bit key, 64-bit key ? 10

Or

6. (a) Explain what is authentication and its types. 10
(b) What do you mean by transport layer security (TLS) ? Explain. 10

Unit – IV

7. (a) What security protocols are predominantly used in web-based electronic commerce ? 10
(b) Explain the terms Phishing attacks, SQL injection attacks and format string attacks. 10

Or

8. (a) What security protocols are used to protect e-mail ? 10
(b) What is the most popular symmetric encryption system used over the web ? 10
-

Unit - V

9. (a) What are web security problems ? Explain. 10
(b) Explain intrusion detection system (IDS). 10

Or

10. (a) What is the role of application level gateway ? 10
(b) Explain the functionality of firewalls. 10