1E-7906

Total Printed Pages : 3

Roll No. : _____

7906

M. Tech. Computer Science & Engg. (Sem. I)
Main/Back Examination,
January – 2008

Information System Security

Time : 3 Hours] [Totai Marks : 80
[Min. Passing Marks : 27

*Attempt any **five** questions.*
Marks of questions are indicated against each question.

Use of following supporting material is permitted during examination. (Mentioned in form No. 205)

1. Nil 2. Nil

1	(a)	What requirements must a public key cryptosystem fulfil to be a secure algorithm ?
	(b)	Which parameter and design choices determine the actual algorithm of a Fiestel cipher ?
	(c)	Explain and justify the steps used in DES algorithm which produce diffusion and confusion.
	(d)	Briefly state the encryption steps of AES algorithm, giving relevance of each step.
	(e)	Decrypt the following caeser cipher : IL YH HDVB SRLQWV.
	(f)	Is the one-time pad (a) secure and (b) practical?

2 (a) What is the assumption that makes one-time pads sufficient to provide perfect cryptographic security ?

(b) Broadly speaking, what are the system costs in using a one time pad ? Of RSA ? of DES ?

3 (a) With the ECB mode of DES, if there is an error in a block of the transmitted cipher text, only the corresponding plaintext block is affected. However in the CBC mode, this error propagates. For example, an error in the transmitted C1, corrupts P1 and P2. Are any blocks beyond P2 affected in case of CBC ? Justify.

(b) Describe two ways in which ICMP can be used for network attacks ? Why is TCP harder to spoof than UDP ? What kind of attacks can I frame exploiting the TCP protocol vulnerabilities if host machines are running without firewalls and OS is not properly patched ?

4 (a) Explain the network scenario which is prone to spoofing attack. Aid your explanation with an appropriate example How can you hijack a session between two commuters ?

(b) What are the characteristics of RSA algorithm. Explain with example.

5 (a) What brings the need of configuring DMZ in an organization ? Is it always a necessary requirement ?

(b) I need security at perimeter of my network. Once I protect it, I am safe from all the attacks and survive happily. Comment on the statement, giving appropriate justification to your answer.

6 When a combination of symmetric encryption and an error control code is used for message authentication, in what order must the two functions be used ?

7 Explain the three techniques of achieving confidentiality and authentication. Analyze the three different techniques. Also differentiate clearly between MAC and Hash.

8 Write short notes on :

(a) SHTTP

(b) Firewalls

(c) VPN.