B.E. sem 8 (Rev.) Comp. System Security 02/12/08

VT Oct. 08-193

Con. 5279–08. **(REVISED COURSE)** **RC–7658**

(3 Hours) **[Total Marks : 100**

N.B. : (1) Question No. **1** is **compulsory**.
(2) Attempt any **four** questions out of remaining **six** questions.
(3) **Figures** to the **right** indicate **full** marks.
(4) Answers to the questions should be **grouped** and written **together**.

1. (a) Compare secret key and public key encryption. **5**
(b) Explain how a Fence register is used for relocating a user's program. **5**
(c) Compare copyright, patent and trade secret protection. **5**
(d) Why segmentation recommended for network design ? **5**

2. The following questions are based on a scenario in which encrypted data are passed between Alice and Bon using the RSA algorithm. Alice's public key is {17, 321} and Bob's public key is {5, 321}. Assume that no one knows the private keys but the original owners. **20**
(a) Encrypt the message M = 7 using Bob's public key.
(b) What should Alice have to do to decrypt the message from part a ?
(c) What would Bob have to do to decrypt the message from part a ?
(d) What is Alice's private key ?
(e) What is Bob's private key ?

3. (a) What are the legal issues in computer security ? Is a Social Engineering attack more likely to succeed in person, over the telephone or through email ? Justify your answer. **10**
(b) What are the multilevel databases ? Discuss the designs of multilevel secure databases. **10**

4. (a) Compare copper wire, microwave, optical fiber, infrared and radio frequency wireless in their resistance to passive and active wiretapping. **10**
(b) Compare signature based and Heuristic based IDS. What are the limitations of IDS ? **10**

5. (a) (i) The distinction between a covert storage channel and a covert timing channel is not clearcut. Every timing channel can be transformed into an Equivalent storage channel. Explain how this transformation could be done. **5**
(ii) An Electronic mail system could be used to leak information. First, explain how the leakage could occur. Then, identify controls that could be applied to detect or prevent the leakage. **5**
(b) (i) The discussion of base/bounds registers implies that program code is execute-only and that data areas are read-write-only. Is this ever not the case ? Explain your answer. **5**
(ii) Can any no. of concurrent processes be protected from one another by just one pair of base/bounds registers ? Explain your answer. **5**

6. (a) A distributed denial-of-service attack requires zombies running on numerous machines to perform part of the attack simultaneously. If you were a system administrator looking for zombies on your network. What would you look for ? **10**

(b) Explain the different issues in security plan.(Explain at least seven issues). **10**

7. (a) Explain the basic steps of risk analysis. **10**

(b) Define the term Ethics. What is the difference between laws and Ethics ? What is IEEE Code for Ethics ? **10**

****