

B.E. Computer Science & Engineering (Model Curriculum) Semester-VIII
BE201CS - Computer System Security

P. Pages : 2

Time : Three Hours



* 2 5 9 5 *

GUG/S/25/14339

Max. Marks : 80

- Notes :
1. All questions are compulsory.
 2. All questions carry equal marks.
 3. Due credit will be given to neatness and adequate dimensions.
 4. Assume suitable data wherever necessary.
 5. Illustrate your answers wherever necessary with the help of neat sketches.

- 1.** a) Discuss how the intruder generates an attack in TCP session. **8**
- b) Write notes on: **8**
- i) Man-in-middle attack
 - ii) TCP hijacking

OR

- 2.** a) Explain various types of security attacks. **8**
- b) Explain buffer overflow and format string vulnerabilities. **8**
- 3.** a) Explain in detail AES (Advanced Encryption Standard) Algorithm. **8**
- b) Explain Rail fence transposition technique? What would be the transformation of message “Computer System Security” using Rail-fence technique with rail value = 3. **8**

OR

- 4.** a) Explain in detail HMAC Algorithm. **8**
- b) Explain internet standard and RFC's. **8**
- 5.** a) Explain Certificate Authority (CA) of key management. **8**
- b) Explain location of Encryption device in detail. **8**

OR

- 6.** Write note on: **16**
- i) Public announcement
 - ii) Public Key Authority
 - iii) Public Key Directory
 - iv) Certificate Authority

7. a) Draw and Explain IP Security Architecture. **8**

b) Write short note on: **8**

i) Encapsulating Security Payload.

ii) S/MIME

OR

8. a) Discuss Pretty Good Privacy in detail. **8**

b) Write note on: **8**

i) SSL

ii) TLS

9. Explain the following: **16**

i) SNMP

ii) Trusted System

OR

10. a) Discuss Firewall Design Principles. **8**

b) Discuss Intruders, Viruses and Related Threats. **8**
