B.E Comp VII (Rev) System Security

Con. 3121–11. **(REVISED COURSE)** **RK–3360**

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

N.B. : (1) Question No. **1** is **compulsory.**
(2) Attempt any **four** questions out of remaining **six** questions.
(3) Make **suitable** assumption wherever **necessary** and clearly **justify** them.

1. a) What are the different types of threats? 05

b) What is the difference between symmetric and asymmetric key cryptography? 05

c) Give the differences between stream and block cipher. 05

d) Explain diffusion and confusion. 05

2. a) Explain the information security goals. 10

b) Explain A5/1 stream cipher. 10

3. a) Explain control of access to general objects in operating system. 10

b) What are the properties of cryptographic hash function? Explain the birthday problem. 10

4. a) Explain the Diffie – Hellman key exchange algorithm. 10

b) Write a detailed note on Biometric techniques. 10

5. a) What is the use of Tiger Hash? Explain it in detail. 10

b) What is a firewall ? Explain different types of firewalls. 10

6. a) Explain the different software flaws with examples. 10

b) What is Spoofing? Explain ARP spoofing. 10

7. Write short notes on the following:– 20
a) Session Hijacking
b) SYN Flood
c) CAPTCHA
d) Covert Channel .