35095

MSc. DEGREE EXAMINATION – OCTOBER 2015
THIRD SEMESTER
Computer Science
Paper V –CRYPTOGRAPHY AND NETWORK SECURITY

Time : 3 Hours Max.Marks : 75

PART – A (5 X 3 = 15 Marks)
Answer any FIVE questions.
Each Question carries Three (3) marks.
Each Answer should not exceed One (1) page.

1. What is Steganography?
2. What is Avalanche effect?
3. What is Clogging attack?
4. Define Birthday attack?
5. What are the problems with one time pad?
6. What is Security Parameter Index?
7. Differentiate modular arithmetic and ordinary arithmetic.
8. Differentiate between weak and strong collision resistance.

PART – B (4 X15 = 60 Marks)
Answer ALL questions.
Each Question carries Fifteen (15) marks.
Each Answer should not exceed Six (6) pages.

9. What is OSI Security architecture? Explain in detail about the various types of attacks the internet work is vulnerable to and respective security services.

(OR)

10. a. Discuss the conventional encryption model with a neat diagram.
    b. Explain about any two Block Cipher modes of operation.
11. a. Discuss in detail about Blowfish.
    b. What requirements must a public key Cryptosystem fulfill to be a secure system?

(OR)

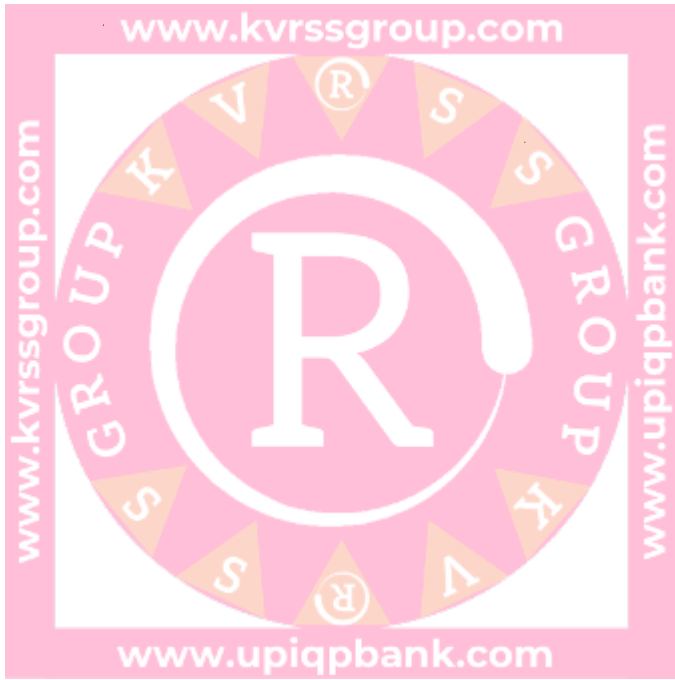
12. Explain about RSA algorithm with an example. Discuss its strength.
13. Describe the hash function in detail with neat diagram.

(OR)

14. Define digital signature. What is DSS? Explain in detail.
15. a. What problems were Kerberos designed to address?
    b. What are the services provided by the S/MIME in Email security?

(OR)

16. Explain about the different types of viruses and worms.


www.kvrssgroup.com
www.kvrssgroup.com
www.upiqpbank.com
www.upiqpbank.com