No. of Printed Pages : 2

**RCSE-022**

# Ph.D. PROGRAMME IN COMPUTER SCIENCE

00054

## Term-End Examination

## December, 2014

## RCSE-022 : SECURITY AND CRYPTOGRAPHY

*Time : 3 hours* *Maximum Marks : 100*

***Note :*** *Attempt any **five** questions. All questions carry equal marks.*

**1.** Write an algorithm to generate the encryption and decryption keys in RSA. Also, give an example to show the process of encryption and decryption keys generations. *20*

**2.** What is Digital Signature ? Explain two important approaches of generating digital signatures. *20*

**3.** "Password policies have conflicting requirements." Justify this statement using suitable examples. *20*

**4.** What is the size of IPSec header ? Draw the IPSec header. Also, explain the significance of each header field in IPSec. *20*

**5.** Explain the various types of security firewalls used in corporates. Also, discuss the intelligent Intrusion Detection Systems (IDS) used in firewalls. *20*

**6.** What is Kerberos ? Draw and explain how it provides authentication services. *20*

**7.** Differentiate between the following pairs : *20*

(a) Stream Cipher and Block Cipher

(b) DES and RSA

(c) Quantum Cryptography and Visual Cryptography

(d) Confidentiality and Integrity