

**M. SC. (COMPUTER SCIENCE) SEM – II (CHOICE BASED  
CREDIT & GRADE SYSTEM) : SUMMER - 2018  
SUBJECT : NETWORK SECURITY**

Day : **Friday**  
Date : **13/04/2018**

Time : **03.00 PM TO 06.00 PM**  
Max. Marks : **60**

**S-2018-0923**

**N.B.:**

- 1) All questions are **COMPULSORY**.
- 2) Figures to the right indicate **FULL** marks.

---

**Q.1** Explain RSA algorithm. Also explain how RSA can be used for authentication purpose. [15]

**OR**

What is encryption? Explain the various schemes for encrypting a large message.

**Q.2** A) Answer **ANY ONE** of the following: [08]  
i) Explain password-based and address based authentication system.  
ii) Explain basic structure of International Data Encryption Algorithm.

B) Answer **ANY ONE** of the following: [07]  
i) Explain e-mail system. How are distribution lists maintained?  
ii) Explain Euclid's algorithm with example.

**Q.3** Answer **ANY THREE** of the following: [15]  
a) Explain viruses, worms and Trojan horses.  
b) Explain the concept of pretty and good privacy.  
c) How to encrypt a large message? Explain.  
d) Explain how DSA is used for digital signatures.  
e) What is cryptography? Explain public key cryptography.

**Q.4** Write short notes on **ANY THREE** of the following: [15]  
a) Authentication of people  
b) Security services for electronic mail  
c) Firewall  
d) Generation of MAC  
e) TCP

\* \* \* \*