## Question Paper

# MANIPAL UNIVERSITY

**SCHOOL OF INFORMATION SCIENCES (SOIS)**
**SECOND SEMESTER MASTER OF ENGINEERING- ME( EMBEDDED AND WIRELESS TECHNOLOGY )**
**DEGREE EXAMINATION- May 2017**
**Thursday, 20, 2017**
**Time : 10:00 AM - 1:00 PM**

## Cryptography and Network Security [EWT 616]

**Marks: 100** **Duration: 180 mins.**

## Answer all the questions.

1) Discuss Network security model with a neat diagram (10)

2) a. Find the plaintext from the cipher text using Caesar cipher â€“ VSRQJHEREVTXDUHSDQWU. (10)

b. Is it secure to encrypt the message using Caesar cipher? Justify your response.

c. Explain why one time pad is perfect cipher

[2+ 3+ 5 = 10 Marks ]

3) Specify the design criteria of Blowfish block cipher with respect to (10)

a. Number of rounds
b. Design of the function F
c. Key scheduling

4) Explain Key Scheduling Algorithm(KSA) and Pseudo-Random Generation Algorithm(PRGA) algorithm with respect to RC4. (10)

5) List out the applications of Random Number Generator. Explain Bhum Bhum Shub generator with an example. (10)

6) Bob decides to use RSA with p = 11, q = 23, and e = 7. (10)

a. Find Bob public key.
b. Find Bobâ€™s private key d using the extended Euclidean algorithm.
c, Alice wants to send the message 44 to Bob. What is the encrypted message that Alice sends?

| | | |
|---|---|---|
| 7) | Define the term a. Confusion b. non-repudiation. c. One way function d.Stegnography | (10) |
| 8) | What is the difference between Link to Link and End to End encryption how to overcome network traffic in each method | (10) |
| 9) | What is MAC? List the importance of MAC. Explain Data Authentication Algorithm with neat diagram. | (10) |
| 10) | Explain the steps involved in SSL | (10) |