Question Paper

Exam Date & Time: 05-Jan-2018 (10:00 AM - 01:00 PM)

MANIPAL ACADEMY OF HIGHER EDUCATION

SCHOOL OF INFORMATION SCIENCES
FIRST SEMESTER MASTER OF SCIENCE - MSc (Information Science)
DEGREE EXAMINATION (MAKE - UP) - JANUARY 2018
DATE : FRIDAY, JANUARY 05, 2018
TIME : 10:00AM - 1:00PM

Computer and Information Security [MIS 607]

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

Answer all the questions.

1) For each asset, list whether you are concerned with its integrity, confidentiality, or availability (or a combination thereof) and explain why? (10)

a. Customer billing records
b. Customer contact information
c. Dating profiles

d. Web site
e. Intellectual property

[2+2+2+2+2]

2) a. Define Kerckhoff's Principle (10)

b. Encrypt the following "pilot's saying:" The nose is pointing down and the houses are getting bigger, using Columnar transposition and the keyword is "ANALYST"

c. How substation cipher differs from transposition cipher.

[3+ 4 + 3= 10 Marks]

3) Explain RC4 algorithm in detail. (10)

4) A Diffie-Hellman key exchange between Alice and Bob uses parameter p,g,x,y. (10)

a. What does Alice send to Bob?
b. What does Bob send to Alice
c. What is the session key that is computed by Alice and Bob?
d. What values may be public and what values must be secret?

[2+2+3+3 = 10 Marks]

5) Compare Symmetric key cryptography with asymmetric cryptography. (10)

6) What are the weakness of passwords, explain how to store the passwords and mitigate dictionary attacks. (10)

7) Briefly describe the security properties and the limitations of the Bell-LaPadula security model. (10)

8) List the design goals of Firewall. Briefly discuss the difference between packet filtering and stateful filtering Firewall with their pros and cons. (10)

9) Answer the following with respect to Fiat-Shamir protocol Alice selected N = 55 and her secret is S = 9. (10)

a. What is v?
b. Suppose Alice chooses r = 10. What does Alice send in the witness message?
c. What does Alice send in the response message, assuming Bob chooses e = 0?
d. What does Alice send in the third message, assuming Bob chooses e = 1?

[$2\frac{1}{2}$ x 4]

10) Explain IPSec in detail. (10)

-----End-----