Question Paper

Exam Date & Time: 20-Nov-2018 (02:00 PM - 05:00 PM)

MANIPAL ACADEMY OF HIGHER EDUCATION

SCHOOL OF INFORMATION SCIENCES

THIRD SEMESTER M.Sc INFORMATION SCIENCE

Computer and Information Security [MIS 607]

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

END SEMESTER DEGREE EXAMINATION NOVEMBER 2018

Answer all the questions.

1) Explain CIA. List out, which of the fundamental challenges in information security are CIA. Give an example where confidentiality is required but not integrity. Give an example where integrity is required, but not confidentiality. (10)

[10 Marks]

2) a. Find the plaintext from the cipher text using Caesar cipher - 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) Alice and Bob will use Diffie-Hellman to compute a shared secret. They select p=5 and g=2. Alice picks a k_{Alice} of 11 and Bob picks k_{bob} of 7. (10)

a. Show the computations performed by Alice and Bob to calculate a shared secret.

b. What values are hidden?

c. What values can be sent over an insecure channel. [5 + 1 + 4 = 10 Marks]

4) Alice needs to pick a public and private RSA key to communicate with Bob. (10)

a. Alice Selects p=7 and q=13. What is 'n' and 'm' ?

b. Alice select e=29 and d=5. Show that these are valid RSA encrypting and decrypting values.

c. What would Alice publish as public key.

d. Now Bob wants to send the message "test' so it only can be read by Alice. Computer the cipher text he should sent to Alice. Assume a=0.

[2+ 4+ 2+2=10 Marks]

5) Define the term authentication. Explain 2- Factor Authentication [2 + 8 = 10 Marks] (10)

6) Alice can read and write to the file x, can read the file y, and can execute the file z. Bob can read x, can read and write to y, and cannot access z. (10)
a) Write a set of access control lists for this situation. Which list is associated with which file?
b) Write a set of capability lists for this situation. What is each list associated with?

[2 X 5 = 10 Marks]

7) What is confused deputy, how it occurs and how you can avoid. Explain with suitable example. (10)

[1 X 10 = 10 Marks]

8) Define the term Malware, Explain any two different methods to detect it. (10)
[1 X 10 = 10 Marks]

9) Write short notes on the properties of Zero knowledge proof and its application. [1X10 = 10 Marks] (10)

10) What is Intrusion Detection System? List the importance of it. Compare Signature based and Anomaly based Intrusion Detection system. (10)

[1 X 10 = 10 Marks]

-----End-----