

Question Paper

Exam Date & Time: 07-Jan-2019 (10:00 AM - 01:00 PM)



MANIPAL ACADEMY OF HIGHER EDUCATION

SCHOOL OF INFORMATION SCIENCES

THIRD SEMESTER MASTER OF SCIENCE - M.Sc. (INFORMATION SCIENCE) DEGREE EXAMINATION (MAKE-UP) - JANUARY 2019

Computer and Information Security [MIS 607]

Marks: 100

Duration: 180 mins.

MAKEUP JAN 2019

Answer all the questions.

- 1) a. Encrypt the message "Computer and information security is my favorite subject" using double transposition with the key1 "sois" and key2 "manipal" (10)
b. Decrypt using ceaser cipher "lolnhpdqldso" [7+ 3 =10 Marks]
- 2) Explain the classification of Cryptanalysis with respect to Amount of Information Available to Attacker[1X10 =10 Marks] (10)
- 3) a. What are Vulnerability and Attack? Give an example. (10)
b. Define Kerckhoffs' Principle in the context of cryptography. Give a real-world example where Kerckhoffs' Principle has been violated. Did this cause any security problems?
[2X5 = 10 Marks]
- 4) Given Super increasing knapsack {2,3,6,13,27,52}, with $n=31$ and $m=105$ (10)
a. Find the general knapsack.
b. Encrypt the message: 110101
c. Decrypt the above result [3 + 2 + 5 = 10 Marks]
- 5) a. Explain the applications of key-hash and non-key hash (10)
b. Explain Key generation in detail with respect DES
[2X5 = 10 Marks]
- 6) Find a private key corresponding to the following RSA public key { $e=3$, $p=11$, $q=3$ } (10)
Encrypt the message "HI"
[1X10 =10 Marks]
- 7) Explain the steps involved in Tiger Hash (10)
[1X10 =10 Marks]
- 8) What is Covert Channel? Explain its types and properties (10)
[1X10 =10 Marks]
- 9) Define the term Ingress filter. Explain Packet based Firewall in detail. List out the possible attacks on it. (10)

[2+6+2 = 10 Marks]

10)

Define the term

(10)

- a. Virus
- b. Worm
- c. Logic Bomb
- d. Race Condition

Marks]

[4X2.5 =10

-----End-----