BUTAEEZ

Master of Computer Applications
MCAC 302: Information Security
Unique Paper Code:223401302 .
Semester III
December 2022
Year of admission: 2021

Time: Three Hours **Max. Marks: 70**

Instructions:

1. All questions are compulsory.
2. Attempt all the parts of a question together.

---

1. (a) Why needs security? How to maintain the security on message and entity. Justify your answer. (6)

   (b) What is the difference between threats and viruses (5)

2. (a) What is public key encryption? Explain the working of RSA public key encryption algorithm. (6)

   (b) Briefly define the following terms with example. (6)
   (i) Worms (ii) Trojan horse (iii) Trap door

3. (a) What is the difference between DES and AES algorithm? Explain with diagram. (6)

   (b) Encrypt and decrypt the message "Welcome to MCA course" using transposition cipher with encryption key=2413 and decryption key =1234. (6)

4. (a) What is Message Authentication Code (MAC)? Explain with diagram. (6)

   (b) Find the cipher text of the message "WE ARE DISCOVERED FILE AT ONCE" by Rail Fence cipher where number of Rail=3. (5)

5. (a) What is Digital Signature? Explain the role and working of Hash function in digital signature (6)

   (b) Using data given p=3, q=11, d=7 in RSA Algorithm find the cipher text of the given plain text "SUZANNE". [Hint: take S=19]. (6)

6. (a) What is NIST digital signature scheme? Explain its working with diagram (6)

   (b) How Diffie-Hellman key exchange algorithm work. Explain with diagram. (6)