Registration No : | | | | | | | | | | |

Total Number of Pages : 02 **MCA**
MCA505A

5th Semester Regular / Back Examination 2019-20
CRYPTOGRAPHY AND CYBER LAW
BRANCH : MCA
Max Marks : 100
Time : 3 Hours
Q.CODE : HRB325

Answer Question No.1 (Part-1) which is compulsory, any EIGHT from Part-II and any TWO from Part-III.

The figures in the right hand margin indicate marks.

Part- I

Q1 Only Short Answer Type Questions (Answer All-10) (2 x 10)

a) What are two different uses of public key cryptography related to key distribution?
b) What is the avalanche effect?
c) What is encipherment?
d) Prove that 3 is a primitive root of 7.
e) What is weak collision resistance? What is the use of it?
f) What is meant by one-way property in hash function?
g) Define Masquerade.
h) How Digital signature differs from authentication protocols?
i) What Is Software Piracy? Name Two Organizations That Investigate Allegations Of Software Abuse.
j) Define Cyber-Crime. What are the differences between Computer Crime and Computer-related crime?

Part- II

Q2 Only Focused-Short Answer Type Questions- (Answer Any Eight out of Twelve) (6 x 8)

a) Explain Cyber Crime and Criminal Justice in the Indian IT Act 2000.
b) Explain the Copyright issue in India. Also explain the Copyright in WWW.
c) Explain the difference between Cipher Feedback(CFB) Mode and Output Feedback(OFB) Mode
d) Explain about MD5 in details.
e) What are the various types of intrusion detection systems? Explain.
f) Discuss authentication header and ESP in detail with their packet format.
g) Differentiate between linear cryptanalysis and differential cryptanalysis with an example from each.
h) State Chinese remainder theorem and find X for the given set of congruent equations using CRT.
i) Explain various web security mechanisms with an example.
j) Explain the steps for creating a Digital Certificate.
k) Explain the working of SSL protocol. Why is it required?
l) State and explain Chinese Remainder theorem. Explain how to solve $x^2\equiv1(\text{mod}35)$ using Chinese remainder theorem.

Part-III

Only Long Answer Type Questions (Answer Any Two out of Four)

Q3 Differentiate between transposition cipher and substitution cipher. Apply two stage transpositions Cipher on the “treat diagrams as single units” using the keyword “sequence”. **(16)**

Q4 Evaluate using Diffie-Hellman key exchange technique. Users A and B use a common prime q=11 and a primitive root alpha=7. **(16)**

a) If user A has private key X_A=3.Whatis A’s public key Y_A?

b) If user B has private key X_B=6.Whatis B’s public key Y_B?

c) What is the shared secret key?

Q5 Explain how digital certificates are revoked. Why the certificates needs to be revoked? **(16)**

Q6 Explain the differences between Cyber cheating and Cyber Frauds. Describe the strategies to tackle cyber crime and trends. **(16)**