Third Semester Regular/ Back Examination – 2015-16
INFORMATION SECURITY AND CYBER LAW
BRANCH: MBA
Time: 3 Hours
Max marks: 70
Q.code:T699
Answer Question No.1 & 2which are compulsory and any five from the rest.
The figures in the right hand margin indicate marks.

Q1   Answer the following questions: (2x10)

a) Define cryptography and cryptanalysis.

b) Differentiate between Authentication and Authorization.

c) What is DoS attack?

d) Encrypt the message "HELLO" by using Caesar Cipher.

e) What is passive attack? Give an example.

f) What is OTP? Write its advantages?

g) What do you understand by digital signature?

h) What are the guidelines to construct a strong password?

i) What is a computer virus? How do you know that your system is virus affected?

j) What is Salami attack? Give an example.

Q2   Case Analysis: (10)

Worksource Private Limited is a business process outsourcing (BPO) outfit handling business process outsourcing for various clients in North America and Europe. The employees of Worksource become privy to confidential customer information during the course of their work. The nature of this information ranges from medical records of individuals to financial data of companies

The unprocessed data is transmitted from the client's location to Worksource offices in Gurgaon, Pune and Bhubaneswar through the Internet using VPN (Virtual Private Network) connections on broadband. Worksource allows clients to transfer information via dedicated FTP servers on the Internet, which can

then be accessed and processed by its employees.

Worksource, through its website, worksource.com allows its clients to log in and view billing and other information specific to them. Access to this information is restricted through the usual user name - password combination found on most websites.

Looking at the above scenario,
  a) Discuss the threats Workforce faces to its information and suggest controls which it may put in place to secure its information from such threats.
  b) Discuss the legal issues relating to securing such information.

Q3 a) What is information security? List and explain different types of security services.   (5)
    b) Discuss how cyber criminals commit crime.   (5)

Q4 a) List and briefly define different techniques used to avoid guessable passwords.   (5)
    b) What is biometrics? How can a biometrics be used for access control? Discuss the criteria for selection of biometrics

Q5 a) Write RSA algorithm? List its advantages.   (5)
    b) What is intrusion detection ?Describe the approaches used for intrusion detection in a system   (5)

Q6 Explain various legal issues and applicable laws in information security .   (10)

Q7 a) Briefly explain risk management process to protect information system.   (5)
    b) What is security planning? Discuss various issues that are addressed by a security plan.   (5)

Q8 Writes short notes (any two)   (5x2)
    a) Digital Rights Management
    b) ISO standards for information security
    c) Malicious software
    d) Firewalls