Code No. 3172

FACULTY OF INFORMATICS

B. E. 4/4 (IT) I – Semester (Suppl.) Examination, June / July 2011

Subject: Information Security (Elective – III)

Time: 3 Hours **Max. Marks: 75**

Note: Answer all questions from Part A. Answer any FIVE questions from Part B.

PART – A (25 Marks)

1.	Differentiate between a virus and a worm.	2
2.	Define the 'man-in-the middle' attack.	3
3.	Differentiate between a policy and law as applicable to procedures of organizational functioning.	2
4.	Define risk and how it can be identified?	3
5.	What is a 'demilitarized zone' (DMZ) as applicable to information security?	3
6.	Differentiate between 'foot printing' and finger printing as relevant to tools for implementing information security.	3
7.	How can public key cryptography be used to implement authentication?	3
8.	What is the basic difference between the implementation of the DES & AES data security algorithm?	2
9.	What is the main real would application domain of SET?	2
10.	Describe the basic functionality of the MD-5 algorithm.	3

PART – B (50 Marks)

11.(a)	Explain the various stages in the Sec S DLC.	6
(b)	What are the main components of an information system?	4
12.(a)	Briefly explain the ethical issues involved in the formulation of information security procedures in an organization.	5
(b)	How can we control the risks that result from incapabilities in information security?	5
13.(a)	Outline the key components of an information program architecture.	6
(b)	Briefly explain the operation of an intrusion detection system (IDS).	4
14.(a)	Enumerate the criteria for the evolution of the Advanced Encryption Standard (AES) with an real time application.	5
(b)	Briefly describe the RSA algorithm.	5
15.(a)	Explain the principle of operation of digital signatures.	5
(b)	Describe the protocols by which SSL provides a secure end-to-end service.	5
16.(a)	Discuss the various types of malicious codes that affect information system software.	5
(b)	Explain the key components of a risk management strategy.	5
17.(a)	Explain the criteria for selecting a firewall for a network.	6
(b)	How are content fitters used to protect an organizations system from	