KUMARAGURU
college of technology
character is life

Register Number: ……..

B.TECH DEGREE EXAMINATIONS: APRIL/MAY 2016

(Regulation 2009)

Eighth Semester

ITY122: INFORMATION SECURITY

(Common to CSE/IT)

Time: Three Hours **Maximum Marks: 100**

Answer all the Questions:-

PART A (10 x 1 = 10 Marks)

1. Security should be considered as a balance between _____
   a) Protection and availability
   b) integrity and authentication
   c) Information and system
   d) Computer and protection
2. To ensure the principle of _____, the contents of a message must not be modified while in transit.
   a) Integrity
   b) Authentication
   c) Confidentiality
   d) Access control
3. What is the consequence of an integrity threat in web?
   a) Annoying
   b) Disruptive
   c) Loss of privacy
   d) Loss of information
4. An attack is the deliberate act that exploits _____
   a) Security
   b) Vulnerability
   c) Confidentiality
   d) Quality
5. What are the questions to assist in developing the criteria to be used for asset valuation?
   a) Which information asset is the most critical to the success of the organization?
   b) Which information asset generates the most revenue?
   c) Which information asset would be the most embarrassing or cause the greatest liability if revealed.?
   d) All the above
6. What is Asset Information for People?
   a) Position name
   b) Number
   c) ID
   d) All the Above

7. ISSP Stands for _____

a) Issue Security Specific Policy
b) Information Security Specific policy
c) Information Specific Security Policy
d) Issue Specific Security Policy

8. Transposition cipher involves _____

a) Replacement of blocks of text with other blocks
b) Replacement of characters of text with other characters
c) Strictly row to column replacement
d) Some permutations of input plain text to produce cipher text

9. In asymmetric key cryptography, _____keys are required per communicating party

a) 4
b) 3
c) 6
d) 2

10. Third Generation firewalls are _____

a) packet filtering firewalls
b) proxy server or application-level firewall
c) Stateful inspection firewalls
d) None of these

PART B (10 x 2 = 20 Marks)

11. State multiple levels of security required for a successful organisation.
12. Describe how a computer be a subject and an object of an attack respectively?
13. Reason out information security as a management problem. List the factors that the management can do, which the technology cannot do.
14. Distinguish between Denial of service and Distributed DoS.
15. Write the thumb rules applied in selecting the preferred risk mitigation strategy.
16. What are vulnerabilities? How do you identify them?
17. Give the resources available on the web, to assist an organization, in developing best practices as part of a security frame work?
18. State the inherent problems with ISO 17799.
19. Differentiate between digital signatures and digital certificates?
20. What are the credentials of information security potentials?

PART C (5 x 14 = 70 Marks)

21. a) (i) List and analyze the critical characteristics of information. Discuss their use in the study of computer security. (7)

(ii) Briefly explain the components of an Information system and their security. (7)

(OR)

	b)	(i)	Explain the various phases of security system development life cycle(SecSDLC) with necessary illustrations.	(7)
		(ii)	Describe the NSTISSC security model and the bottom-up approach to security implementation.	(7)
22.	a)	(i)	Discuss the ethical concepts in information security and the prevention of illegal and unethical behavior?	(7)
		(ii)	Describe the attack replication vectors and the major types of attacks.	(7)
			(OR)	
	b)	(i)	List any two information security professionals and elaborate on their roles and motivation?	(7)
		(ii)	How does a threat to information security differ from an attack? Explain any three groups of threats to information security.	(7)
23.	a)	(i)	Describe the process of risk identification in detail and state their significance.	(7)
		(ii)	What is benchmarking? Explain the metrics based measures used by the organizations to compare practices.	(7)
			(OR)	
	b)	(i)	Define constant benefit analysis (CBA) and its purpose. Explain how it is computed.	(7)
		(ii)	Discuss the risk assessment and documentation of its results.	(7)
24.	a)	(i)	State the issues specific security policy and describe its function in detail.	(7)
		(ii)	Explain the various components used in designing a security architecture and state their use.	(7)
			(OR)	
	b)	(i)	Discuss the VISA International Security Model	(7)
		(ii)	With illustration discuss the work breakdown structure and its significance in developing the project plan. State all the considerations of a project plan.	(7)
25.	a)	(i)	Explain the working of single round DES encryption algorithm with neat sketch.	(7)
		(ii)	Compare and contrast all factors and issues related to DES with 3DES.	(7)
			(OR)	
	b)	(i)	Explain the physical security plans required to detect and respond to fire hazards.	(7)

(ii) How does screened host architecture for firewall differs from screened subnet firewall architecture? (7)

****