

**B.E./B.TECH DEGREE EXAMINATIONS MAY/JUNE 2013**

Eighth Semester

**ITY122: INFORMATION SECURITY**

(Common to CSE & IT)

**Time : Three Hours**

**Maximum Marks :100**

**Answer ALL Questions**

**PART A (10 x 1 = 10 Marks)**

1. The unauthorized interception of information.  
a) Snooping      b) Masquerading      c) Spoofing      d) Modification
2. A false denial that an entity sent something, is a form of deception known as \_\_\_\_  
a) Delay      b) Repudiation of origin      c) Delegation      d) Repudiation of receipt
3. It is a statement of what is, and what is not, allowed.  
a) Security architecture      b) Security mechanism  
c) Security policy      d) Goal of security.
4. It is a tool that can describe the current protection state.  
a) Protection state      b) Access control matrix  
c) security policy      d) Security mechanism
5. Risk management is \_\_\_\_\_  
a) avoiding risk      b) identifying risk  
c) controlling risk      d) all the above
6. A----- security policy is developed primarily to provide integrity.  
a) Commercial      b) Military      c) Transaction-oriented      d) Social
7. ----- is the breaking of codes.  
a) Cryptography      b) Cryptology      c) Cryptanalysis      d) Encryption
8. ----- has the key value 3.  
a) Play fair cipher      b) Caesar cipher      c) Hill cipher      d) Poly alphabetic cipher.
9. A ----- changes characters in the plaintext to produce the cipher text.  
a) Substitution cipher      b) Transposition cipher  
c) Rail fence cipher      d) Block cipher
10. ----- encipher and decipher multiple bits at once.  
a) Stream cipher      b) Block cipher      c) Hill cipher      d) Play fair cipher

**PART B (10 x 2 = 20 Marks)**

11. What is information security?
12. Define confidentiality.
13. Differentiate threat and attack.
14. What is masquerading?
15. What are the types of risk?
16. Give two examples of security standards.
17. Write short notes on blueprint for security.
18. What is IDS?
19. Define protection state.
20. What are the substitution ciphers?

**PART C (5 x 14 = 70 Marks)**

21. a) What are the components of an information system? Explain.

**(OR)**

- b) Explain the security SDLC.

22. a) What are the types of attacks? Explain in detail.

**(OR)**

- b) Discuss the ethical and professional issues involved in security investigation in detail.

23. a) Explain how to identify and assess risk?

**(OR)**

- b) Explain how to control risk?

24. a) Explain security policies in detail.

**(OR)**

- b) Describe the design of security architecture.

25. a) Discuss the types of access control in detail.

**(OR)**

- b) Explain classical cryptosystems with example.

\*\*\*\*\*