

B.E./B.TECH. Degree Examination, December 2020

Seventh Semester

**IT16702-INFORMATION SECURITY**

(Regulation 2016 )

Time: Three hours

Maximum : 80 Marks

Answer **ALL** questions**PART A - (8 X 2 = 16 marks)**

1. \_\_\_\_\_ is a generic name for the collection of tools designed to protect data and to thwart hackers.
  - a. Computer Security
  - b. Network Security
  - c. Internet Security
  - d. Operations Security
2. The Key size in DES & Triple DES is \_\_\_\_\_ & \_\_\_\_\_ respectively.
  - a) 64,172
  - b) 56,168
  - c) 64,192
  - d) 56,192
3. Hash function is used to produce
  - (a) Finger print of a file
  - (b) Useful for message authentication
  - (c) Both a and b
  - (d) None of the above
4. The first phase of hacking an IT System is compromise of which foundation of security?
  - (a) Availability
  - (b) Confidentiality
  - (c) Integrity
  - (d) Authentication
5. Distinguish between ethical and unethical behavior.
6. Decode by Ceasar Cipher using frequency analysis with shift +5 "KGYEZUHXXKGQ"
7. How will you evaluate the effectiveness of biometrics?
8. Differentiate Private Law and Public Law.

**PART B - (4 X16 = 64 marks)**

9. (a) (i) Assume that a security model is needed for the protection of information in your class. Using the CNSS model, examine each of the cells and write a brief statement on how you would address the three components of each cell (8)
- (ii) Analyze which are the main types of attacks to be focused by any organization to protect their secured data from the set of available common attacks? State the reason. (8)

**(OR)**

- (b) (i) Consider that an individual threat agent, like a hacker, can be a factor in more than one threat category. If a hacker breaks into a network, copies a few files, defaces a Web page, and steals credit card numbers, how many different threat categories does the attack fall into? (8)
- (ii) Compare and contrast SDLC and SecSDLC (8)
10. (a) Using the key matrix as  $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$  (16)
- (i) Encrypt "CASER" using Hill Cipher
- (ii) Decrypt "OEIM" using Hill Cipher
- Illustrate both Incryption and Decryption process.

**(OR)**

- (b) (i) Apply RSA Algorithm to compute the cipher text for the given plain text "CODE". Assume the prime numbers  $p=7$  &  $q=19$ . Public key  $e=11$ . (8)
- (note: consider the value of the alphabets from 0 to 25).
- (ii) Encrypt a message "Behaviour is a mirror in which everyone displays his own image" using the keyword "monarchy" using Playfair technique. (8)

11. (a) Illustrate with a neat sketch different types of firewall Architectures (16)

**(OR)**

- (b) Distinguish between different types of IDPS Control strategies. Also demonstrate how Organizations measure the effectiveness of IDPSs. (16)
12. (a) Once the project team for information security development has created The ranked vulnerability worksheet, the team must choose one of four basic strategies to control the risks that result from these vulnerabilities. what are the four strategies? (16)

**(OR)**

- (b) (i) Suppose XYZ Software Company has a new application development ( 8 ) project with projected revenues of \$1.2 million. Using the following table, calculate the ARO and ALE for each threat category the company faces for this project.

Threat Category	Cost per incident(SLE)	Frequency of occurrence
Programmer mistakes	\$5000	1 per month
Software piracy	\$500	1 per week
Loss of Intellectual property	\$70000	1 per year
Theft of information	\$3000	1 per quarter
Denial of Service Attacks	\$3500	1 per 6 months

- (ii) Demonstrate with a neat sketch, the technical implementation aspects of secured project management. ( 8 )