Roll No. | | | | | | | | | | |

B.E (FT) END SEMESTER EXAMINATIONS – NOV / DEC 2024

Computer Science and Engineering
VII Semester
CS6007 – Information Security
(Regulation 2018 - RUSA)

Time: 3 Hours | Answer ALL Questions | Max. Marks 100

PART-A (10 x 2 = 20 Marks)

1. Give the critical characteristics of information.
2. Differentiate active and passive attacks.
3. What is rootkit?
4. How risk assessment is integrated in SDLC?
5. What are the properties of Bell – la –Padula model?
6. What requirements should a digital signature scheme satisfy?
7. What are the various substitution techniques used for encryption?
8. What are the types of attacks addressed by message authentication?
9. List out the requirements of Kerberos.
10. Write down the four SSL Protocols.

PART – B (8 x 8 = 64 marks)
(Answer any 8 questions)

11. Elaborate on security activities in SDLC. Draw and define each activity in detail.
12. What is a "man in the middle" attack? Cite a real life example of such an attack. Suggest a means by which sender and receiver can preclude a man-in-the-middle attack.
13. Describe and draw the components of Risk Identification.
14. Illustrate any two security models.
15. Describe digital signature algorithm and show how signing and verification is done using DSS. Provide example for the same.
16. What are the tools / techniques can be used to compare the features and components of each IDS?
17. Given the security levels TOP SECRET, SECRET, CONFIDENTIAL and UNCLASSIFED (ordered from highest to lowest) and the categories A, B and C, specify what type of access (read, write, both or neither) is allowed in each of the following situations. Assume that discretionary access controls allow anyone access unless otherwise specified. Additionally if the subject cannot read or write the object, then give one object classification that the subject can read or write (excluding the subject's own clearance).
(i) Paul cleared for (TOP SECRET,{A,C}) wants to access a document classified (SECRET,{B,C}).(2)

(ii) Anna cleared for (CONFIDENTIAL, {C}) wants to access a document classified (CONFIDENTIAL, {B}).(2)

(iii) Jesse cleared for (SECRET, {C}) wants to access a document classified (CONFIDENTIAL, {C}.(2)

(iv) Robin who has no clearances (and so works at the UNCLASSIFIED level) wants to access a document classified (CONFIDENTIAL, {B}).(2)

18. (i) Encrypt and decrypt the following using play fair cipher using (4)

Keyword : MONARCHY

Plaintext : SWATCH BHARATH

Provide the cipher text and decrypt the same.

(ii) Differentiate between Symmetric and Asymmetric Encryption / Decryption methods. (4)

19. Explain the conditions that need to be satisfied by an ideal biometric authentication system. How the created biometric authentication system is prone to errors? What security features Added would make it work without being error prone?

20. (i) Write in detail on what a digital certificate depicts? How is it issued and for what purpose? (4)

(ii) Some people think the certificate authorities for a PKI should be the government, But others think certificate authorities should be private entities, such as banks corporations or schools. What are the advantages and disadvantages of each approach? (4)

21. (i) Explain the Secure Socket Layer protocol with neat diagram. (4)

(ii) What attacks does this protocol prevents? (4)

22. Describe the SSL architecture in detail and explain how it helps in maintaining secure end to end communication.

PART – C (2 x 8 = 16marks)

23. Classify the following occurrence as an incident or disaster. If an occurrence is a disaster, Determine whether or not business continuity plans would be called into play.

(i) A hacker gets into the network and deletes files from a server.

24. Describe the various national laws that affect the practice of information security.