

**SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY:: PUTTUR**  
(AUTONOMOUS)

**B.Tech. III Year II Semester Regular & Supplementary Examinations June-2025**

**CRYPTOGRAPHY & DATA SECURITY**  
(CSE with Specialization in Cloud Computing)

**Time: 3 Hours**

**Max. Marks: 60**

(Answer all Five Units 5 x 12 = 60 Marks)

**UNIT-I**

- |   |   |  |     |    |    |
|---|---|--|-----|----|----|
| 1 | a | What is meant by security services? Explain various security services listed in X.800? | CO1 | L1 | 6M |
|   | b | Differentiate Substitution and Transposition techniques.                               | CO1 | L3 | 6M |

**OR**

- |   |   |  |     |    |    |
|---|---|--|-----|----|----|
| 2 | a | Simplify various non-cryptographic vulnerabilities.                          | CO1 | L1 | 6M |
|   | b | What is security approaches? Explain various methods of security approaches? | CO1 | L2 | 6M |

**UNIT-II**

- |   |   |  |     |    |    |
|---|---|--|-----|----|----|
| 3 | a | Illustrate Conventional encryption model.                    | CO2 | L2 | 6M |
|   | b | State and explain the principles of public key cryptography? | CO2 | L5 | 6M |

**OR**

- |   |   |   |     |    |    |
|---|---|---|-----|----|----|
| 4 | a | Explain Railfence Technique and Row Columnar techniques.                  | CO2 | L5 | 6M |
|   | b | Categorize any two Substitution Techniques in symmetric key cryptography. | CO2 | L4 | 6M |

**UNIT-III**

- |   |   |   |     |    |    |
|---|---|---|-----|----|----|
| 5 | a | Explain the RSA algorithm. Compute cipher text for M=88, p=17, q=11, e=7. | CO3 | L2 | 6M |
|   | b | Generalize the structure of DSA and its algorithms.                       | CO3 | L3 | 6M |

**OR**

- |   |   |  |     |    |    |
|---|---|--|-----|----|----|
| 6 | a | Examine the structure of X448 key exchange and its algorithms. | CO3 | L6 | 6M |
|   | b | Explain the concepts of Random Bit Generation.                 | CO3 | L5 | 6M |

**UNIT-IV**

- |   |   |   |     |    |    |
|---|---|---|-----|----|----|
| 7 | a | Explain Vulnerability and its types?      | CO4 | L2 | 6M |
|   | b | Enumerate security goals and its methods. | CO4 | L3 | 6M |

**OR**

- |   |   |  |     |    |    |
|---|---|--|-----|----|----|
| 8 | a | Define Non-malicious Program errors and identify Buffer overflow in Nonmalicious Program errors. | CO4 | L3 | 6M |
|   | b | Evaluate the types and characteristics of Data Integrity.  | CO4 | L4 | 6M |

**UNIT-V**

- |   |   |   |     |    |    |
|---|---|---|-----|----|----|
| 9 | a | Discuss Model of Digital Signature and Encryption with Digital Signature. | CO5 | L6 | 6M |
|   | b | Differentiate between SHA1 and SHA2.                                      | CO5 | L3 | 6M |

**OR**

- |    |   |   |     |    |    |
|----|---|---|-----|----|----|
| 10 | a | Illustrate the steps involved in DSA Algorithm.   | CO1 | L2 | 6M |
|    | b | Examine the Proof of Digital signature algorithm. | CO1 | L6 | 6M |

\*\*\* END \*\*\*