

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

**B.Tech II Year II Semester Regular & Supplementary Examinations June-2024**  
**CRYPTOGRAPHY AND DATA SECURITY**

CSE (Internet of Things and Cyber security including Block Chain Technology)

**Time: 3 Hours**

**Max. Marks: 60**

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

**UNIT-I**

- |   |   |     |    |    |
|---|---|-----|----|----|
| 1 | a Examine the properties of Security Mechanisms.      | CO1 | L3 | 6M |
|   | b Classify possible types of attacks in cryptography. | CO1 | L2 | 6M |

**OR**

- |   |  |     |    |    |
|---|--|-----|----|----|
| 2 | a Simplify various non-cryptographic vulnerabilities.                              | CO1 | L4 | 6M |
|   | b Discuss in detail about Denial of services (DOS), Spoofing and Phishing attacks. | CO1 | L2 | 6M |

**UNIT-II**

- |   |  |     |    |     |
|---|--|-----|----|-----|
| 3 | Describe Hill cipher and Monoalphabetic ciphers in detail. | CO2 | L2 | 12M |
|---|--|-----|----|-----|

**OR**

- |   |   |     |    |    |
|---|---|-----|----|----|
| 4 | a Categorize any two Substitution Techniques in symmetric key cryptography. | CO2 | L4 | 6M |
|   | b Compare conventional key with public key encryption.                      | CO2 | L5 | 6M |

**UNIT-III**

- |   |   |     |    |    |
|---|---|-----|----|----|
| 5 | a Explain the RSA algorithm. Compute cipher text for M=88, p=17, q=11, e=7. | CO3 | L2 | 8M |
|   | b Write about the strength of RSA.  | CO3 | L1 | 4M |

**OR**

- |   |   |     |    |     |
|---|---|-----|----|-----|
| 6 | Discuss any one Asymmetric Key cipher algorithms with example. List out the advantages and disadvantages. | CO4 | L3 | 12M |
|---|---|-----|----|-----|

**UNIT-IV**

- |   |   |     |    |    |
|---|---|-----|----|----|
| 7 | a Define Non-malicious Program errors and identify Buffer overflow in Non-malicious Program errors. | CO5 | L2 | 6M |
|   | b Evaluate the types and characteristics of Data Integrity.   | CO5 | L5 | 6M |

**OR**

- |   |  |     |    |    |
|---|--|-----|----|----|
| 8 | a Infer in detail about Time-of-check to Time-of-use Errors. | CO5 | L2 | 6M |
|   | b Examine the need for firewalls and role of firewalls.      | CO5 | L4 | 6M |

**UNIT-V**

- |   |   |     |    |     |
|---|---|-----|----|-----|
| 9 | Explain various types of Authentication Protocols and its advantages and disadvantages. | CO6 | L2 | 12M |
|---|---|-----|----|-----|

**OR**

- |    |  |     |    |     |
|----|--|-----|----|-----|
| 10 | Generalize Authentication header and its modes of operation in detail. | CO6 | L6 | 12M |
|----|--|-----|----|-----|

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

54