

Reg. No: 

--	--	--	--	--	--	--	--	--	--

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

B.Tech IV Year I Semester Regular Examinations February-2022

CRYPTOGRAPHY &amp; NETWORK SECURITY

(Computer Science &amp; Information Technology)

Time: 3 hours

Max. Marks: 60

**PART-A**

(Answer all the Questions 5 x 2 = 10 Marks)

- |   |   |    |    |
|---|---|----|----|
| 1 | a Define cryptography.                                      | L1 | 2M |
|   | b What is the strength of DES?                              | L1 | 2M |
|   | c What are the applications of cryptographic hash function? | L1 | 2M |
|   | d What is wireless security?                                | L1 | 2M |
|   | e Define S/MIME.  | L1 | 2M |

**PART-B**

(Answer all Five Units 5 x 10 = 50 Marks)

**UNIT-I**

- |   |   |    |    |
|---|---|----|----|
| 2 | a Explain the substitution encryption techniques in detail. | L5 | 5M |
|   | b What are security services?                               | L1 | 5M |

OR

- |   |   |    |     |
|---|---|----|-----|
| 3 | Write a note on different types of Security Attacks and Services in Detail. | L6 | 10M |
|---|---|----|-----|

**UNIT-II**

- |   |  |    |     |
|---|--|----|-----|
| 4 | Briefly explain Diffie-Hellman Key Exchange. | L2 | 10M |
|---|--|----|-----|

OR

- |   |   |    |    |
|---|---|----|----|
| 5 | a Briefly explain design principles of block cipher   | L3 | 5M |
|   | b Perform decryption and encryption using RSA algorithm with $p=3$ $q=11$ $e=7$ and $N=5$ . | L3 | 5M |

**UNIT-III**

- |   |   |    |    |
|---|---|----|----|
| 6 | a Explain in detail about different ways of distribution of public keys | L2 | 5M |
|   | b Discuss about symmetric key distribution using symmetric encryption   | L6 | 5M |

OR

- |   |  |    |    |
|---|--|----|----|
| 7 | a Explain X.509 Authentication Services. | L2 | 5M |
|   | b Explain the public key infrastructure. | L5 | 5M |

**UNIT-IV**

- |   |  |    |     |
|---|--|----|-----|
| 8 | Elaborate different level of awareness of a connection in HTTPS. | L6 | 10M |
|---|--|----|-----|

OR

- |   |   |    |    |
|---|---|----|----|
| 9 | a What are the security areas are addressed by IEEE 802.11i?        | L1 | 5M |
|   | b How is the concept of an association related to that of mobility? | L1 | 5M |

**UNIT-V**

- |    |   |    |    |
|----|---|----|----|
| 10 | a Why is base64 conversion useful for an email application. | L1 | 5M |
|    | b Explain about internet key exchange.                      | L2 | 5M |

OR

- |    |   |    |     |
|----|---|----|-----|
| 11 | List and Identify the benefits of IPsec | L1 | 10M |
|----|---|----|-----|

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