

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

**B.Tech II Year II Semester Regular & Supplementary Examinations August-2023**  
**CRYPTOGRAPHY & 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 What is security approaches? Explain various methods of security approaches? CO1 L1 6M  
b Explain in detail possible types of attacks in cryptography? CO1 L2 6M

OR

- 2 a Explain substitution techniques. Explain the different types of substitution techniques? CO1 L2 6M  
b Write short note on linear and differential cryptanalysis? CO1 L1 6M

**UNIT-II**

- 3 a Write short note on block cipher principles. CO2 L1 6M  
b Explain single round DES with neat sketch. CO2 L2 6M

OR

- 4 a Explain the block cipher modes of operation. CO2 L2 6M  
b Explain Double & Triple DES with keys. CO2 L2 6M

**UNIT-III**

- 5 a What is Elgamal Cryptography? Explain in detail. CO3 L2 6M  
b Illustrate the structure of X448 key exchange. Explain with algorithms and advantages/disadvantages. CO3 L3 6M

OR

- 6 a Give the structure of AES. Explain with algorithms. CO4 L2 6M  
b Explain Random Bit Generation. CO4 L2 6M

**UNIT-IV**

- 7 a Explain in detail about various types of attacks. CO5 L2 6M  
b Explain in detail Hash Functions. CO5 L2 6M

OR

- 8 a Explain in detail Time-of-check to Time-of-use Errors. CO5 L2 6M  
b Explain in detail man in middle attack. CO5 L2 6M

**UNIT-V**

- 9 a Explain in detail Digital Signature Standard approach and its algorithm. CO6 L2 6M  
b Describe the steps in message digest generation in Secure Hash Algorithm in detail. CO5 L1 6M

OR

- 10 a Write and explain TLS functions and alert codes of Transport Layer Security. CO5 L1 6M  
b Discuss clearly Secure Hash Algorithm(SHA). CO5 L1 6M

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

