THIS PIECE OF STUDY MATERIAL HAS BEEN BROUGHT TO YOU BY

MUSTUDENTS UNITED

CONTRIBUTED BY - ADMIN

CSS 1

1. Explain OSI Security Architecture.
2. Discuss various attacks on digital signatures.
3. Why are digital certificates and digital signatures required? What is the role of digital signature in digital certificates? Explain any one digital signature algorithm.
4. Explain AES. Describe its structure, rounds, and key expansion process.

CSS 2

1. DES uses 16 Feistel rounds. Every round takes Left 32 bits (L1-1) and Right 32-bits (R1-1) from the previous round to produce L_1 and R_1 which go to the next round. Each round uses two cipher elements: mixer and swapper. The swapper is invertible, the mixer is invertible because of XOR operation. — *Explain this.*
2. The Needham-Schroeder
3. Kerberos
4. What is a digital certificate? How does it help to validate the authenticity of a user? Explain X.509 certificate format.

CSS 3

1. Properties of hash function – Module 3
2. The message is divided into N blocks, each of b bits... (HMAC steps)
3. The message is divided into N blocks, each m bits long... (CMAC steps)

CSS 6

1. Difference between worms and viruses.
2. Types of worms and viruses.
3. Explain SQL Injection.
4. Give me all the questions in one place and remove any requests like “in simple Hindi” or anything—just give me the questions.