

Walchand College of Engineering, Sangli (Government Aided Autonomous Institute)	
AY 2025-26	
Course Information	
Programme	B.Tech. (Computer Science and Engineering)
Class, Semester	Final Year B. Tech., Sem VII
Course Code	6CS451
Course Name	Cryptography and Network Security Lab

Experiment No. 06

Title - Apply AES algorithm for practical applications

Objectives:

- Study the structure of AES, including key sizes (128, 192, 256 bits), encryption rounds, and the internal processes (Sub Bytes, Shift Rows, Mix Columns, Add Round Key).
-

Problem Statement:

In an era where digital communication and data storage have become integral to everyday life, ensuring the security and privacy of sensitive information is a critical challenge. With the increasing frequency of cyberattacks, data breaches, and unauthorized access, traditional methods of data protection are no longer sufficient. Individuals, businesses, and governments alike require robust encryption techniques to safeguard confidential data.

The **Advanced Encryption Standard (AES)** is a symmetric key encryption algorithm that has been widely accepted as a secure and efficient standard for encrypting digital data. Despite its proven security, many real-world systems either lack proper encryption or use outdated or weak encryption mechanisms. Moreover, improper implementation of AES can lead to vulnerabilities that compromise the overall security of the system.

This project addresses the need to **apply the AES algorithm effectively in practical applications**, such as secure file storage, encrypted messaging, and protected communication in IoT systems. By integrating AES into these applications, the goal is to enhance data confidentiality and security without significantly impacting system performance or usability.

Equipment/Tools:

Theory:

Procedure:

Steps:

Observations and Conclusion: