

# COL215: Assignment 3(part2) - Implementation of AES decryption operation

**INSTRUCTOR NAME-PREETI RANJAN PANDA**

	NAME	ENTRY NO
MEMBER 1	AYUSH SINGH	2023CS10322
MEMBER 2	AAYUSH PRASAD	2023CS51132

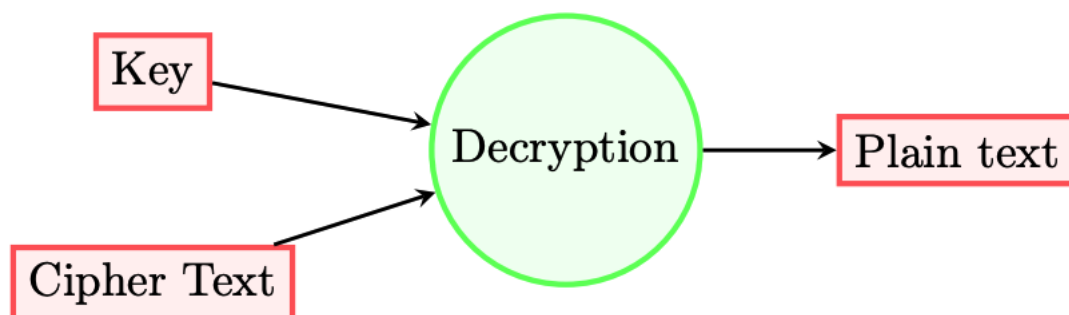
## Introduction

The objective of the assignment is: implementation of AES decryption operation. The components involved are memory elements (RAM, ROM and registers) and logical unit.

## Problem Description

Given a cipher text and a key, your task is to perform an AES decryption operation to display plain text on 7-seven display. An overview of the problem is shown in Figure 1.

Figure 1: Overview of task: Decryption



- Input cipher text is of the size in multiples of 128 bits and will be provided in the COE file (8 bit binary unsigned). The input file should be stored in 1-D array format in the block RAM, starting from address 0 (000016) in row major format.
- Key will be provided via the COE file. All the round keys will be provided in the COE file. You are allowed to use VHDL modules from previous hardware assignments.

In the Part I of the assignment, the objective will be to design and implement the following modules:

1. Memories (RAM/ROM)
2. Logical operations in AES decryption Primary focus will be on designing the individual components.

### **Basics of AES Encryption/Decryption**

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm that encrypts and decrypts data in blocks of 128 bits using keys of 128, 192, or 256 bits. The AES algorithm consists of several rounds, depending on the key size. Each round includes a series of transformations applied to the data. The decryption process mirrors the encryption process but with inverse operations. Below is a step-by-step explanation of both encryption and decryption operations

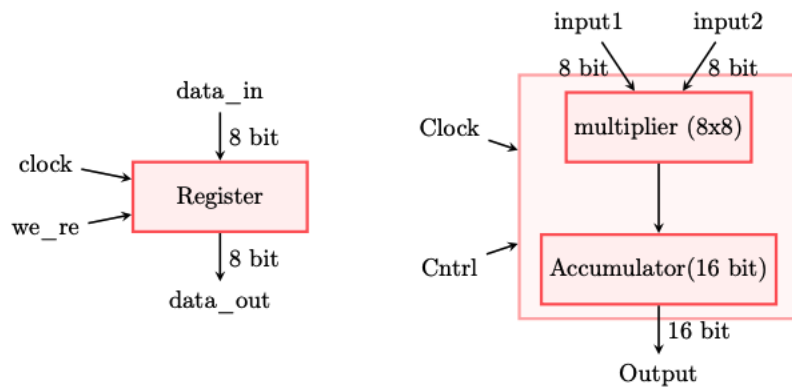


Figure 6: Register and MAC unit

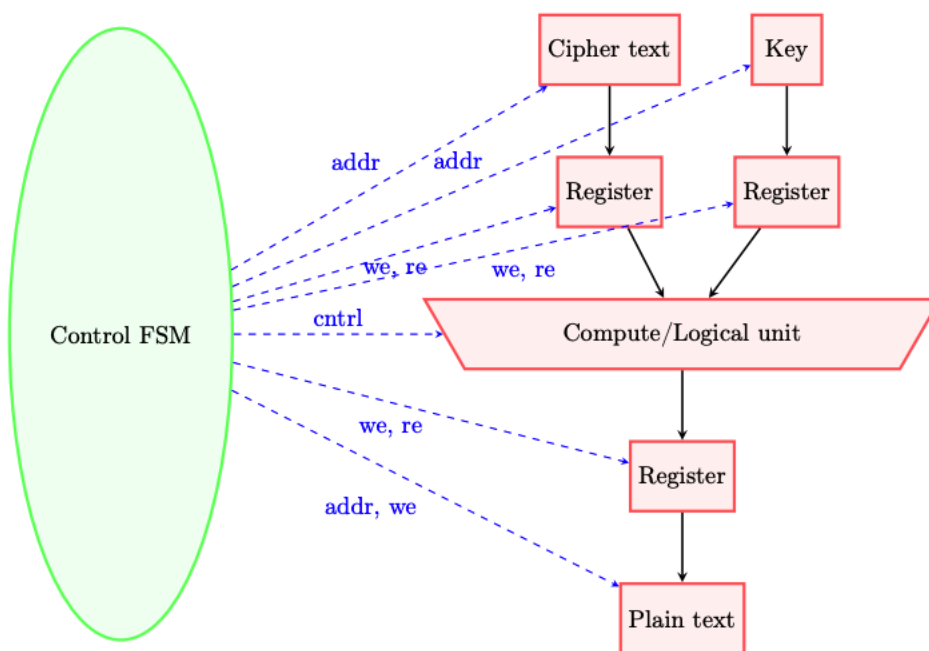


Figure 7: Overview of control path

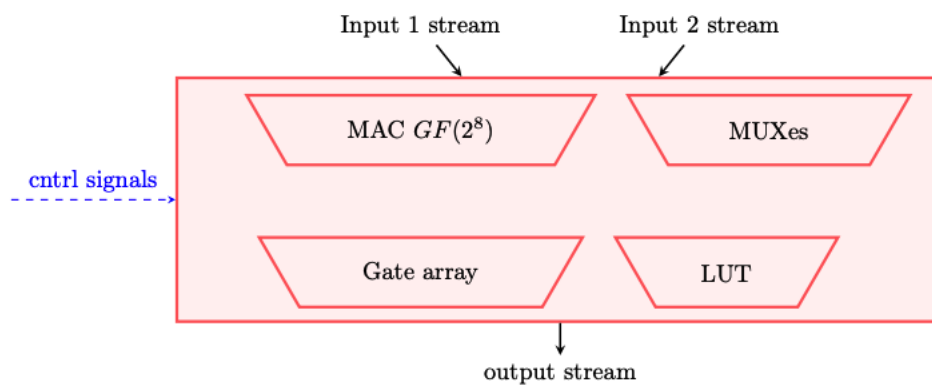


Figure 8: Details of Compute units

