

Assignment No.6

6.1 Title:

Implementation of S-AES (Advanced Encryption Standard)

6.2 Problem Definition:

Implementation of S-AES

6.3 Prerequisite:

Basic of Python3, Concept of Advanced Encryption Standard

6.4 Hardware and Software Requirements:

- Fedora
- Python
- Anaconda
- Jupyter notebook
- Dell desktop

6.5 Hardware Requirement:

PIV, 2GB RAM, 500 GB HDD

6.6 Learning Objectives:

Learn How to Apply Advanced Encryption Standard Algorithm to encryption of given data.

6.7 Outcomes:

After completion of this assignment students are able Implement code for **Advanced Encryption Standard Algorithm** for given data and find the encrypted data of the given data.

6.8 Theory Concepts:

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six times faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows –

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C ,Java and Python

6.8.1 Operation of AES

AES is an iterative rather than Feistel cipher. It is based on the ‘substitution–permutation network’. It comprises a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix –

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration –

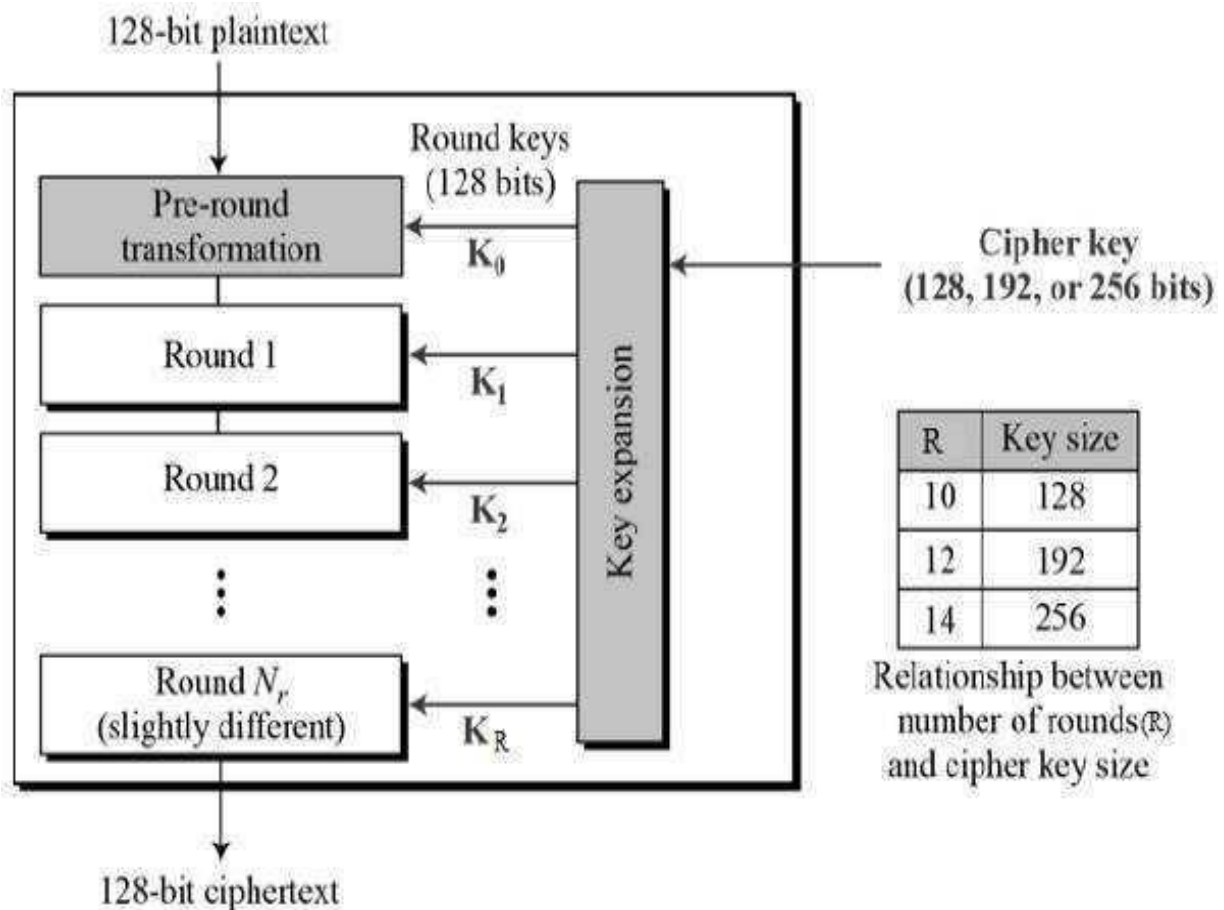


Figure 6.1 AES structure

6.8.2 Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprises four sub-processes. The first round process is depicted below –

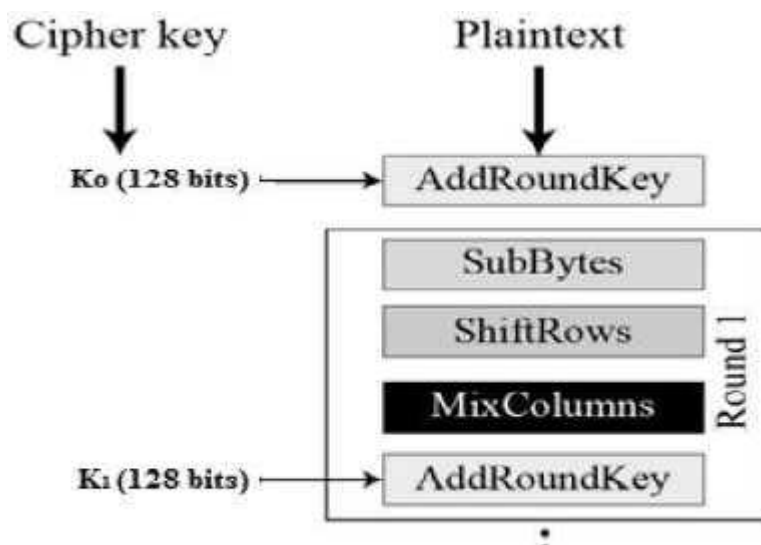


Figure 6.2 Encryption Process

Conclusion: Thus, we have successfully implemented the S-AES algorithm.