Assignment B2

Title: Implementation of S-AES.

Problem Statement:

Implement the Simplified - Advanced Encryption Standard (S-AES) algorithm.

Objectives:

- To learn the basic concept of S-AES.
- To learn the general structure of S-AES.

Outcomes:

Students will be able to:

- learn the basic concept of S-AES.
- learn the general structure of S-AES.

Software and Hardware Requirements:

Laptop / Desktop system with 13 processor, 4 GB RAM, 500 GB HDD.

OS: Fedora 20, Jupyter Notebook Eclipse IDE.

Theory

Introduction

S-AES is to AES AS S-DES is to DES. Infact, the structure of S-AES is exactly same as AES. The difference is in (if bits), the black size (16 bits) and the number of rounds key size(2 rounds).

Figure1

Substitute nibbles:

Instead of dividing the black into a 4-by- 4 array of byles, S-AES divides it into a 2-by-2 array are 4 bits long. This is called the state array.

Diagram1

In the first stage of each encryption round on S-box in used to translate each nibble into a new nibble. First we associate a nibble bobibabs with the polynomial boxs + bixe + hox + ho. This polynomial is then Inverted as an element of GF (16) with the prime polynomial used being X1 + X+1. Then we multiply by a matrix and add vector as in AES.

Diagram2

Remember that the addition and multiplication in the equation are being done module 2 with XOR but not in GIF (16).

Shift rows.

The next stage is to shift rows. The first row is left alone and second is shifted.

Diagram3

Mix columns:

After shift rows, each column is multiplied by the matrix Have 1 corresponds to polynomial and 4 corresponds to polynomial 2^2

Figure2

Add round key

The last stage of each round of encryption, is to add round key. Before the first round, the first two words (w0, W1) of the expanded key are added. In the last round Wa and Ws are added. All additions are done modulo 2. which is XOR

Key expansion:

The four nibbles in the key are grouped into two 8 bit words, which are expanded into 6 words.

Conclusion:

We have successfully learnt and implemented the S-AES algarithm

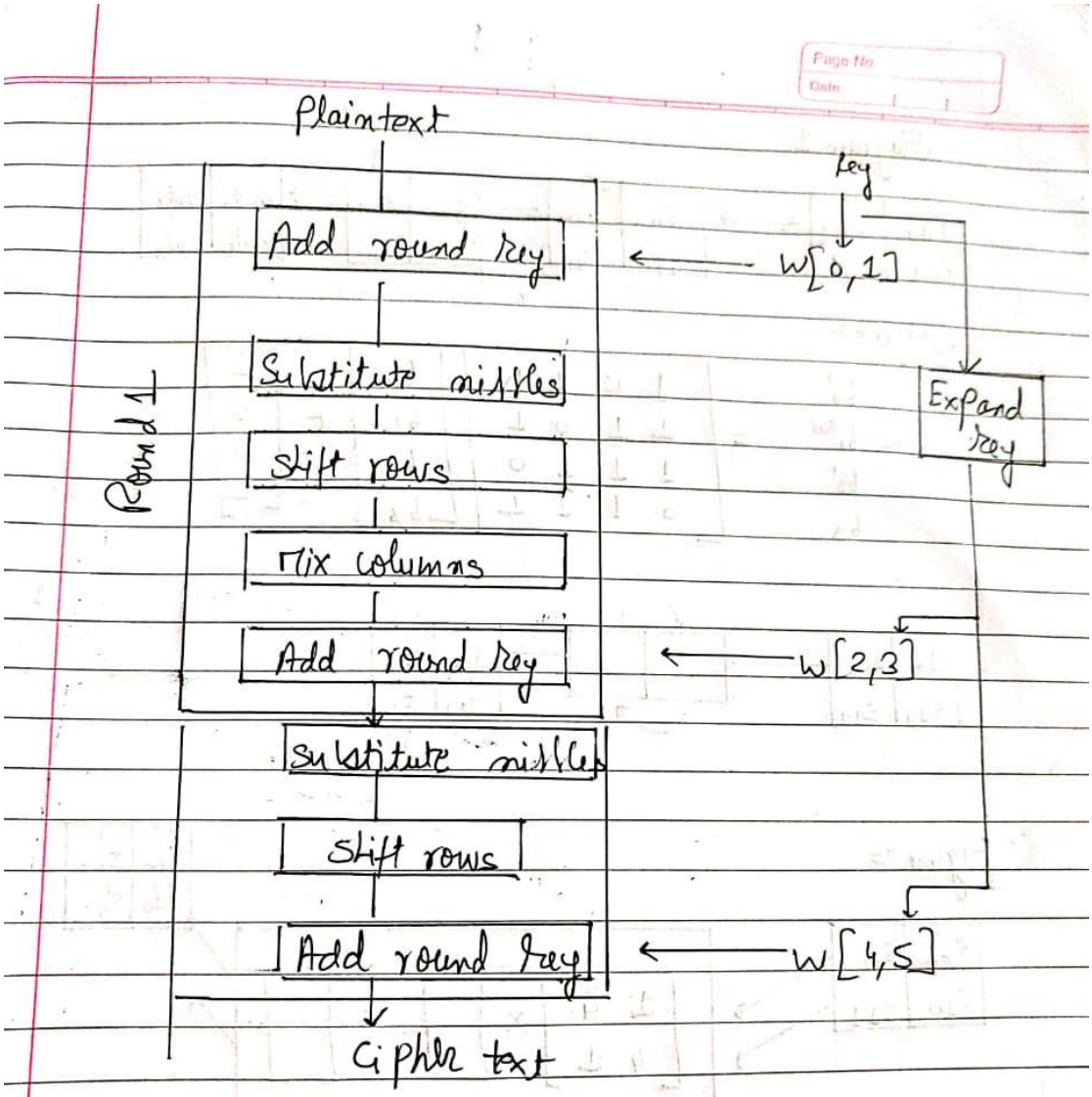


Figure-1 S-AES

Page No.
Date

Diagram 1

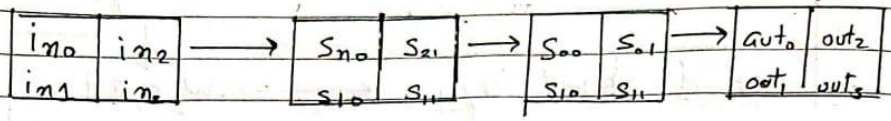


Diagram 2

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

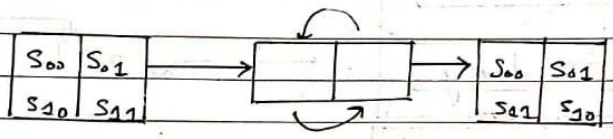
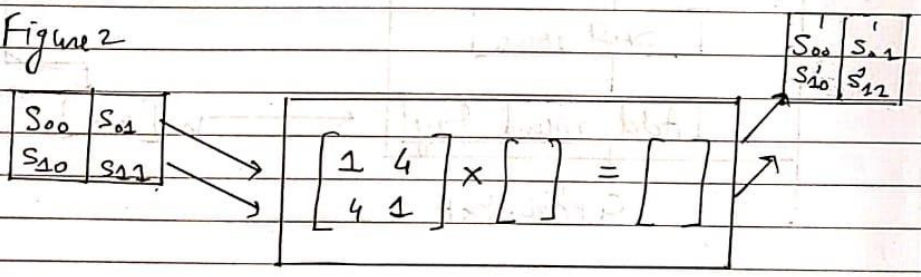


Figure 2



AES mix column transformation