Roll No : 41163

Page No.
Date: / /

Assignment B2

Execution Date : 08/03/2021

Submission Date : 19/05/2021

Title: S-AES algorithm

Problem Statement:

To implement a simplified - advanced encryption standard algorithm.

Objective:

Understand basic concepts of S-AES algorithm

Learn general structure of S-AES

Outcome:

On completing this assignment student will be able to implement the S-AES algorithm.

Software Requirements:

- Jupyter Notebook
- Python 3.8.5
- 64 bit operating system

Hardware Requirements:

- Computer with 64 bit processor

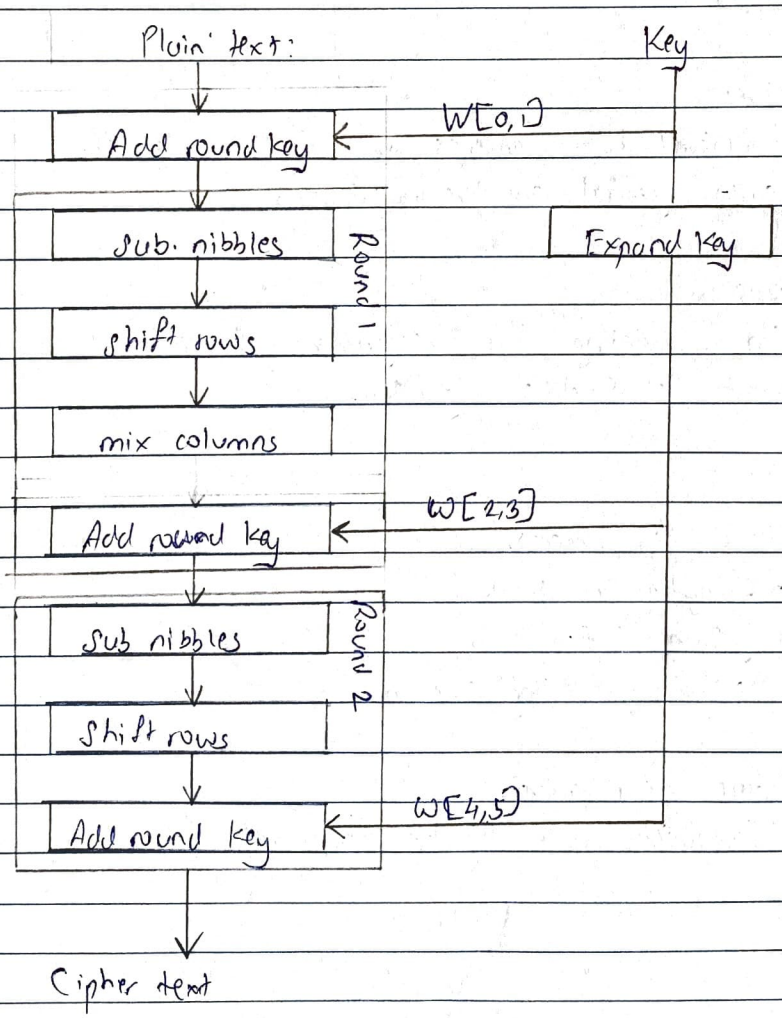
Page No.
Date: / /

Theory:

S-AES is to AES as S-DES is to DES. In fact, the structure of S-AES is exactly same as AES

The difference between S-AES and AES is in key size (16 bit), block size (16 bit) and number of rounds (2).

Overview:



Page No.
Date: / /

~~Add round key:~~

Substitute Nibbles:

Instead of dividing the block into a four by four array of bytes, S-AES divides it into a two by two array of nibbles, which are four bits long. They are substituted by looking up a fixed table (S-box) given in design).

Shift rows:

The first row is not shifted but the second row is shifted.

$S_{0,0}$	$S_{0,1}$
$S_{1,0}$	$S_{1,1}$

⟹

$S_{0,0}$	$S_{0,1}$
$S_{1,1}$	$S_{1,0}$

Mix columns:

After shifting rows, each column is multiplied with the matrix: $\begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}$

$$\begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \times \begin{bmatrix} S_{00} & S_{01} \\ S_{10} & S_{11} \end{bmatrix} = \begin{bmatrix} S_{00} & S_{001} \\ S_{10} & S_{11} \end{bmatrix}$$

Here 1 corresponds to polynomial 1 and 4 corresponds to polynomial x^2.

Page No.
Date: / /

Add round Key:

The last stage of each round of encryption is to add round key.

Before the first round, the first two words (W_0, W_1) of the expanded key are added. In the first round, W2 and W3 are added. In the last round, W4 and W5 are added.

Test Cases:

	Description	Expected O/P	Actual O/P
1)	I/P = AB Key = 0100101010010101	Cipher text of 16 bits	Successful
2)	Decrypt given 16 bit cypher text	AB (initial given input)	Successful

Conclusion:

Therefore, successfully completed implementation and understood S-AES algorithm.