ASSIGNMENT B2

Title: Implementation of S-AES

Problem Statement: Implementation of S-AES

Objective: To understand how S-AES works and to implement it

Outcome: Students will be able to successfully implement S-AES

Requirements: python3, jupyter

Concept related theory

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

- A replacement for DES was needed because its key size was too small. With increasing computing power it was found to be vulnerable against exhaustive key search attacks. Triple DES was designed to overcome this drawback but was found to be too slow.

- Features of AES are as follows:

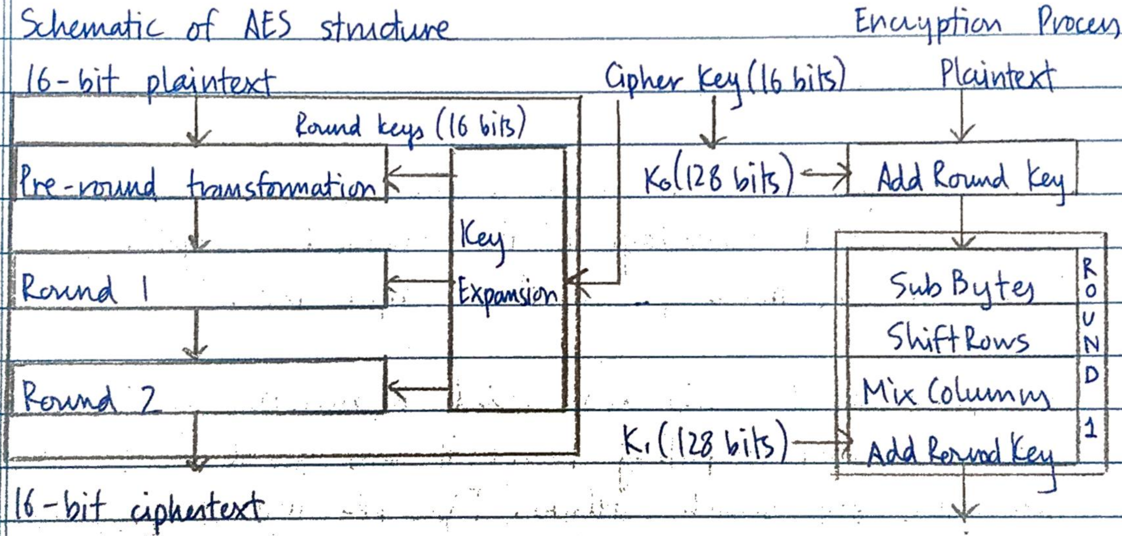
1. Symmetric key symmetric block cipher
2. 128-bit data, 128/192/256-bit keys
3. Stronger and faster than triple DES

AES is based on 'substitution-permutation' network. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and shuffling bits (permutations). AES performs all its computation on bytes rather than bits.

Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in 4 columns and 4 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.

Schematic of AES structure



Byte Substitution (SubBytes): The 16 i/p bytes are substituted by looking up a fixed table (S-box) given in design. The result is a matrix of 4 rows and columns.

Shift Rows

Each of the 4 rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of the row. Shift is carried as follows:

- First row is not shifted
- Second row is shifted one (byte) position to the left

- Third row is shifted two positions to the left
- Fourth row is shifted three positions to the left

Mix Columns

Each column is transformed using a special mathematical function. This function takes 4 bytes of one column as input and outputs 4 completely new bytes, which replace the original column. This step is not performed in the last step.

Add Round Key

The 16 bits of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round, the output is considered as cipher text. Otherwise, it is passed to the next round.

Decryption process

It is similar to the encryption process, but in the reverse order. Each round consists of the four processes conducted in the reverse order:

- AddRoundKey
- Mix Columns
- Shift Rows
- ByteSubstitution

Test Cases

Plaintext	Key	Expected CipherText	Actual CipherText
1101 0111 0010 1000	0100 1010 1111 0101	0010 0100 1110 1100	0010 0100 1110 1100
1101 0101 1010 1010	0100 1010 1111 0101	0001 0100 0110 0101	0001 0100 0110 0101

Conclusion

Successfully implemented and understood S-AES algorithm