ASSIGNMENT NO	B2
TITLE	Implementation of S-AES
PROBLEM STATEMENT/ DEFINITION	Implementation of S-AES
OBJECTIVE	To understand how S-AES works
OUTCOME	Understanding and implementation of simplified AES algorithm
S/W PACKAGES AND HARDWARE APPARATUS USED	Core 2 DUO/i3/i5/i7 64-bit processor OS-LINUX 64 bit OS Editor-gedit/Eclipse S/W- C++/JAVA//Python
REFERENCES	1. Bernard Menezes, "Network Security and Cryptography", Cengage Learning India, 2014, ISBN No.: 8131513491 2. Nina Godbole, Sunit Belapure, "Cyber Security", Wiley India, 2014, ISBN No.: 978-81-345-2179-1 3. Atul Kahate, "Cryptography and Network Security", Mc Graw Hill Publication, 2nd Edition, 2008, ISBN: 978-0-07-064823- 4. William Stallings, "Cryptography and network security Principles and practices", Pearson, 6th Edition, ISBN: 978-93-325-1877-3 5. Forouzan, "Cryptography and Network Security (SIE)", Mc Graw Hill , ISBN 007070208X, 9780070702080
STEPS	1. 16-bit key and 16-bit plaintext 2. Key generation (K1 and K2 using K0) 3. **Encryption** • Add round 0 key • Round 1 1. Nibble substitution using S-boxes 2. Shift rows (swap 2nd and 4th nibble) 3. Mix column 4. Add round key 1 • Round 2 1. Nibble substitution using S-boxes 2. Shift rows (swap 2nd and 4th nibble) 3. Add round key 2 4. **Decryption** • Add Round 2 Key

	• Round 1
	  1. Inverse Shift Row
	  2. Inverse Nibble Sub
	  3. Add Round Key 1
	  4. Inverse Mix Columns
	• Round 2
	  1. Inverse Shift Row
	  2. Inverse Nibble Sub
	  3. Add Round Key 0

INSTRUCTIONS FOR WRITING JOURNAL	1. Date 2. Assignment No. 3. Problem Definition 4. Learning Objective 5. Learning Outcome 6. Concepts Related Theory 7. Algorithm 8. Test Cases 9. Conclusion/Analysis

Pr-requisites: Number theory, Discrete mathematics and any programming language C++/Java/Python.

Concepts Related Theory:

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 time 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 and Java

Operation of AES

AES is an iterative rather than Feistel cipher. It 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 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 −
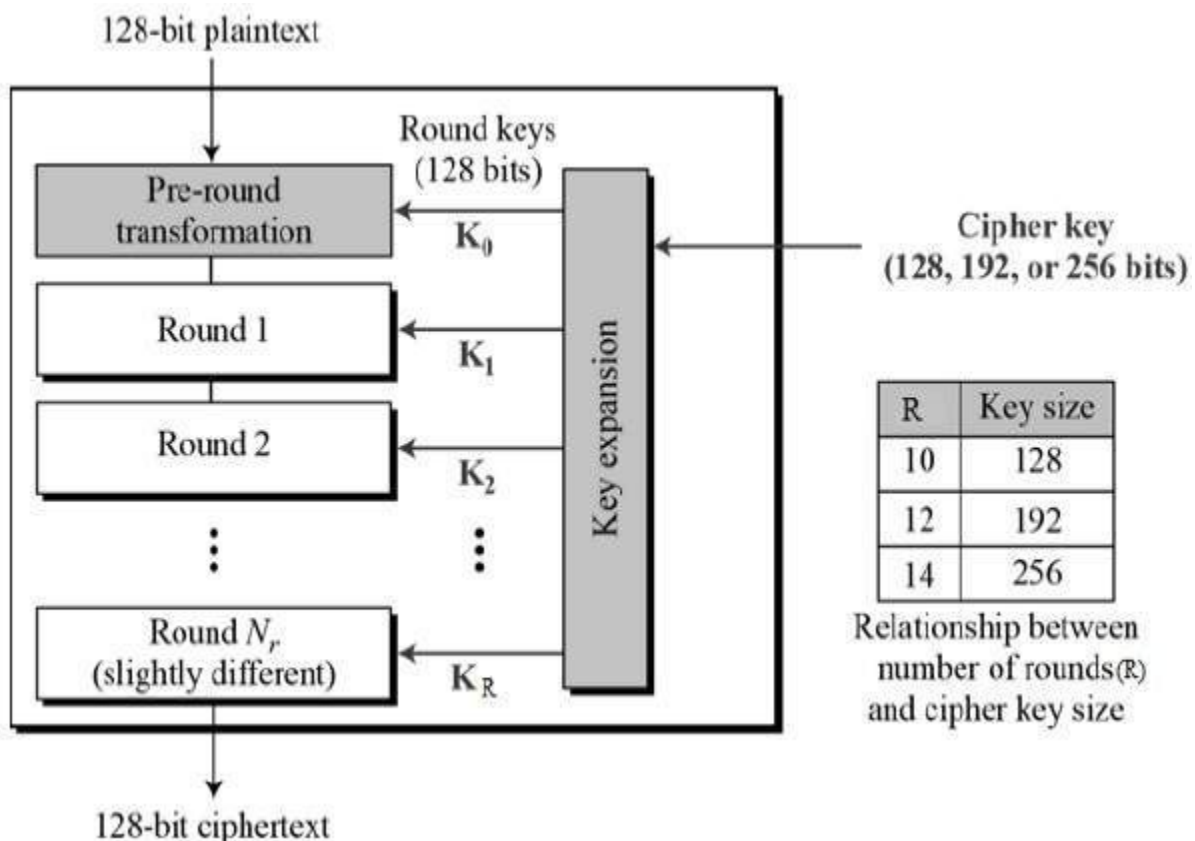
Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below −
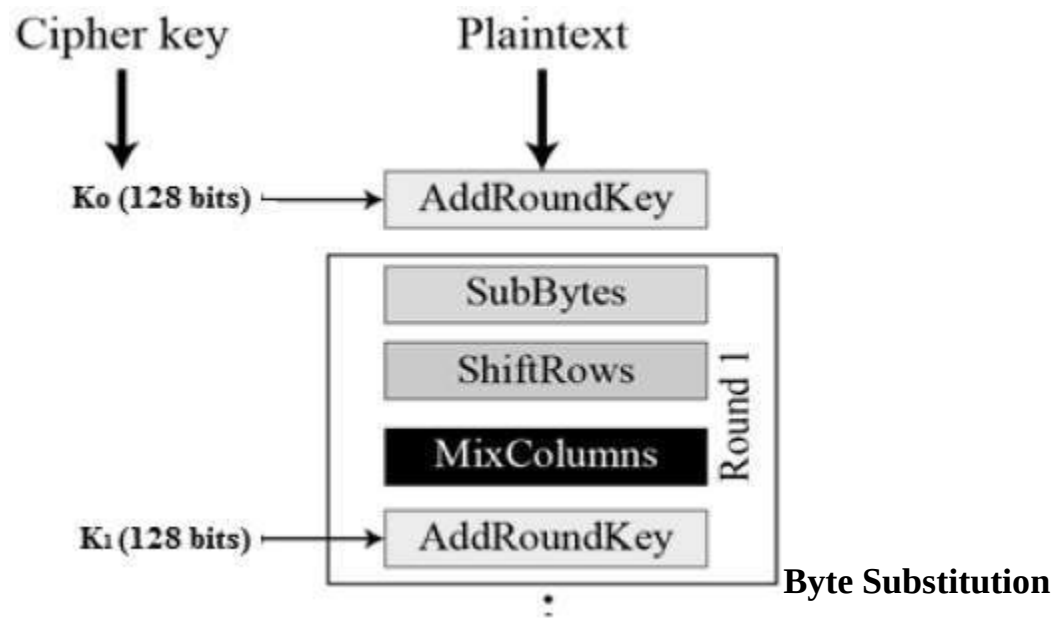
Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

Shiftrows

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out 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.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

MixColumns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Addroundkey

The 16 bytes 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 then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

- •Add round key
- •Mix columns
- •Shift rows
- •Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

AES Analysis

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches.

However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.