A.I.S.S.M.S
INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near R.T.O., Pune - 411 001.

* Laboratory Practice II (Information Security) - Experiment Number - 4.

Name :- Kaustubh Shrikant Kabra.
Class :- Third Year Engineering.
Div :- A
ERP Number :- 38
Department :- Computer Department.
College :- AISSMS's IOIT.

Title :-

AES Algorithm

Aim :-

Write a Java/C/C++/Python program to implement AES Algorithm.

Objective :-

1. To understand and learn AES algorithm.
2. To implement AES algorithm.

Theory :-

AES Encryption :-

The AES is likely to be commercial grade symmetric algorithm of choice for years, if not decades. Let us look at it more closely.

AES is based on a design principle known as substitution-permutation network, combination of both substitution and permutation and is fast in both software and hardware. Unlike

its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192 or 256 bits. By contrast the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

AES operates on a 4×4 column-major order matrix of bytes, termed the number of repitions of transformation rounds that convert the input called the plaintext into the final output, called the cipher text. The number of cycles of repition are as follows:

- 10 year of repetition for 128-bit Keys.
- 12 cycles of repetitions for 192-bit Keys.
- 14 cycles of repetitions for 256-bits Keys.

Algorithm Description:

1. Key Expansions-

Round Keys are derived from the cipher key using Rijndael's Key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2. Initial Round-

i) Add Round Key - each byte of the state is combined with a block of the round key using bitwise XOR.

3. Rounds -
   i) Subbytes - A non-linear substitution step where each byte is replaced with another according to a lookup table.
   ii) Shift Rows - A transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
   iii) Mix Columns - A mixing operation which operates on the columns of the state, combining the four bytes in each column.
   iv) Add Round Key

4. Final Round (no mix column):-
   i) Sub Bytes
   ii) Shift Rows
   iii) Add Round Keys.

Optimization of the Cipher:-

On systems with 32-bit or larger words, it is possible to speed up execution of this Mix Column step by transforming them into a sequence of table lookups. This requires four 256-entry 32 bit tables, and utilizes a total of four Kilobytes of memory - 1 kb for each table. A round can then be done with 16 table lookups and 12 32-bit exclusive-or operations, followed by four 32-bit exclusive-or operations in the Add Round Key steps.

A.I.S.S.M.S
INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near R.T.O., Pune - 411 001.

Conclusion :-

Thus we used the AES algorithm technique to implement a program using the mentioned steps and procedure.