**SRI VENKATESWARA COLLEGE OF ENGINEERING**

**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING**

# Implementation of Reversible Substitution box using LFSR based dynamic key in Advanced Encryption Standard Algorithm

**UG Project work (EC18811) : 2022-2023**

| Students Name(s) | Reg. No | Batch No. | Review No. |
|---|---|---|---|
| Bhavan Kumar C | 190701013 | A1 | 2 |
| Deva S | 190701018 | | |
| Dhivyan K | 190701020 | | |

## ABSTRACT

Data security has been a major concern as that of the faster processing of data. As the capability of data processing is being evolved, the attacks on these devices for data extraction have also been increasing daily. It is well known that the AES algorithm has been registered as the standard encryption model since 2001. The purpose of this work is to optimise the security of current crypto coprocessors with the help of a Linear Feedback Shift Register (LFSR). This project work offers a simple and innovative method for building dynamic and key dependant S-boxes utilising Multiplicative Inverse and Affine transformation. Here AES with plain text (128-bit) given to the S-box, the 128 bits or 16 bytes is converted into four subcomponents each with 4 bytes. Each byte or 8-bit is given to the multiplicative inverse and affine transform, The output of this above process will be 128-bit cipher text. The 128-bit in the LFSR is xor with the output to become a dynamic s-box. The same will be continued for N rounds. Followed by this, reversible logic is applied. Reversible logic has numerous methods. Toffoli, one of the methods in reversible logic, is used to maximize speed and reduce energy consumption. The proposed model of generating dynamic and key depended on s-box is the alternative to the existing s-box. As a result, the efficiency of the s-box increases, and encryption becomes stronger.

| Name of Internal Guide | Designation-Dept. | Signature |
|---|---|---|
| Ms. B. Sarala | Professor | |