IMPLEMENTATION OF A NEW OPTIMUM SBOX FOR AES ALGORITHM

N.PRIYA

PG STUDENT,ECE DEPARTMENT,

VELTECH DR.RR & DR.SR TECH UNIVERSITY,

CHENNAI.

priya050889@gmail.com.

JIBAN PRIYA DEVI

ASST PROFESSOR, ECE DEPARTMENT,

VELTECH DR.RR & DR.SR TECH UNIVERSITY,

CHENNAI.

mjivanpriya@gmail.com.

Abstract—

Cryptographic algorithms are the most essential elements in designing the system security. Though there are numerous encryption systems used in security systems by various organizations, for the wider use, a particular encryption method is used as a standard. The internationally accepted and acclaimed algorithm is Advanced Encryption Standard. Here in this paper we have implemented the Advanced Encryption Standard (AES) using hardware descriptive language (HDL) and constructed a new optimum S-box. The proposed S-box have been successfully synthesized and implemented using Xilinx ISE V13.2.