ADVANCED ENCRYPTION STANDARD(AES) ALGORITHM TO ENCRYPT AND DECRYPT THE DATA

A Project report submitted in partial fulfilment of the requirements for the award of degree of

BACHELOR OF TECHNOLOGY

IN

ELECTRONICS AND COMMUNICATION ENGINEERING

SUBMITTED BY

G.TRIVENI
18811A0413
G.SATYA HEMALATHA
19815A0411

A.SUMITH GOLDIE YUVRAJ
18811A0402
G.LAVANYA
18811A0411

Under the guidance of

T.PATTALU NAIDU M.Tech.,(Ph.D)
ASSISTANT PROFESSOR

AVANTHI INSTITUTE OF ENGINEERING & TECHNOLOGY

DEPARTMENT OF

ELECTRONICS AND COMMUNICATION ENGINEERING

NAAC Accredited, Approved by A.I.C.T.E,

Permanently Affiliated to J.N.T.U. KAKINADA

TAMARAM (P.O), MAKAVARAPALEM (M.O), NARSIPATNAM (R.D)

VISAKHAPATNAM DISTRICT-531113

2018-2022

AVANTHI INSTITUTE OF ENGINEERING & TECHNOLOGY

(NAAC Accredited, Approved by A.I.C.T.E, Permanently Affiliated to J.N.T.U. KAKINADA)

TAMARAM (P.O), MAKAVARAPALEM (M.O), NARSIPATNAM (R.D)
VISAKHAPATNAM DISTRICT-531113

DEPARTMENT OF

ELECTRONICS AND COMMUNICATION ENGINEERING

CERTIFICATE

This is to certify that project entitled "ADVANCED ENCRYPTION STANDARD(AES) ALGORITHM TO ENCRYPT AND DECRYPT THE DATA" in partial fulfilment for the degree of bachelor of technology in ELECTRONICS AND COMMUNICATION ENGINEERING at AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY, MAKAVARAPALEM, VISAKHAPATNAM is a bonafied work carried out by G.TRIVENI(18811A0413), A.SUMITH GOLDIEE YUVRAJ(18811A0402), G.SATYA HEMALATHA(19815A0411), G.LAVANYA(18811A0411) under the guidance and supervision during 2018-2022.

T.P. Naidu

PROJECT GUIDE	**HEAD OF THE DEPARTMENT**
T. PATTALU NAIDU M.Tech ,(Ph. D)	**Dr. E.GOVINDA, M. Tech., Ph. D**
Assistant professor	Associate Professor

EXTERNAL EXAMINER

ABSTRACT

Security is major concern in communication, data handling, message transmission on public network. Cryptography is the encryption process of transmission of data to make secure and difficult to attack. Advanced Encryption Standard (AES) algorithm is one of the most commonly used symmetric block cipher algorithm and is proved to be highly secure, faster, and strong encryption process. 128bit AES encryption and Decryption by using AES algorithm is been made into a synthesizable using Verilog code which can be easily implemented on to FPGA. The algorithm is composed of three main parts: cipher, inverse cipher and Key Expansion. Cipher converts data to an unintelligible form called plaintext. Key Expansion generates a key schedule that is used in cipher and inverse cipher procedure. Cipher and inverse cipher are composed of special number of rounds. For the AES algorithm, the number of rounds to be performed during the execution is depends on block size and is composed of four different byte-oriented transformations: Sub Bytes, Shift Rows, Mix Columns and Add Round Key.

Advanced Encryption Standard (AES) algorithm is one on the most common and widely symmetric block cipher algorithm used in worldwide. This algorithm has an own particular structure to encrypt and decrypt sensitive data and is applied in hardware and software all over the world. It is extremely difficult to hackers to get the real data when encrypting by AES algorithm. Till date is not any evidence to crake this algorithm. AES has the ability to deal with three different key sizes such as AES 128, 192 and 256 bit and each of this ciphers has 128 bit block size. This paper will provide an overview of AES algorithm and explain several crucial features of this algorithm in details and demonstration some previous researches that have done on it with comparing to other algorithms such as DES, 3DES, Blowfish etc,.