A Project Report on

**Advanced Encryption Standard Implemented on FPGA**

*Submitted in the Partial Fulfillment of the Requirements*

*For the Award of*

**Bachelor of Technology**

**in**

**Electronics & Communication Engineering**

*By*

**Himanshu Kumar**

**Kritika Kirthalaya**

**Rohit Prakash**

Under the guidance of

**Dr. Shweta Tripathi**

Assistant Professor



**Department of Electronics & Communication Engineering**

**Motilal Nehru National Institute of Technology, Allahabad**

**Allahabad – INDIA**

**Department of Electronics & Communication Engineering**

**Motilal Nehru National Institute of Technology Allahabad**

**Allahabad – INDIA**

**CERTIFICATE**

This is to certify that the work contained in the thesis titled **“Advanced Encryption Standard Implemented on FPGA”** submitted by **Himanshu Kumar(20105014),Kritika Kirthalaya(20105013)** and **Rohit Prakash(20105022)** in the partial fulfillment of the requirement for the award of Bachelor of Technology in Electronics and Communication Engineering to the Electronics and Communication Engineering Department, Motilal Nehru National Institute of Technology, Allahabad, is a bonafide work of the students carried out under my supervision.

Date:

Place:

Dr. Shewta Tripathi

Assistant Professor

ECE Department

MNNIT, Allahabad

**Acknowledgement**

It is a great privilege for us to express our deep sense of gratitude to our guide, Assistant Professor Dr. Shweta Tripathi of Electronics and Communication Engineering Department, MNNIT for her stimulating guidance and profound assistance .We shall always cherish our association with her for her constant encouragement and freedom to thought and action that she rendered to us throughout the project.

We also feel a great pleasure to thank all the staff members of the department for their cooperation which led to the successful completion of our project work.

Finally, we deem it a great pleasure to thank one and all whose valuable suggestion and in time cooperation helped us to carry out this project successfully.

We are also thankful to our friends and colleagues for their support.

**Abstract**

AES is the new encryption standard. In this project, we implement a very efficient pipelined hardware implementation of AES-128 cipher. It has a throughput of more than 500Mega bit per second. Besides, improving the encryption throughput, the pipeline can be taken advantage of if the number of rounds (currently 10) must increase for security reasons.

AES is based on a design principle known as a substitution-permutation network, 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.

**List of Figures**

1. Fig. 2.1 Circuit Diagram of Sensor…………………………………………5
2. Fig. 2.2 Electrical Equivalent of Sensor……………………………………6
3. Fig. 2.3 Shifted Rectangular Hyperbola…………………………………….7
4. Fig. 2.4 Block Diagram of Prototype……………………………………….8
5. Fig. 2.5 Circuit Diagram of Controller……………………………………...9
6. Fig. 2.6 Circuit Diagram of Interfacing Circuit……………………………..9
7. Fig. 2.7 Flowchart of the Prototype………………………………………...10
8. Fig. 3.1 Circuit Diagram of Sensor…………………………………………13
9. Fig. 3.2 Ideal Behaviour…………………………………………………….14
10. Fig. 3.3 Real Behaviour……………………………………………………..15
11. Fig. 3.4 Pin Configuration of ATmega 32………………………….………16
12. Fig. 3.5 Pin Diagram of TIP 31-A viewed with heat sink down…….…….17
13. Fig. 3.6 Block Diagram of TIP 31-A as connected in circuit…………..…..18
14. Fig. 3.7 IC 7805 in TO 220 case……………………………………………19
15. Fig. 3.8 Block Diagram of IC 7805 as used in the circuit…………………..20
16. Fig. 3.9 De-energized Simple Pole Double Throw Relay…………………..22
17. Fig. 3.10 Block Diagram of Electromechanical Relay ……………………...22
18. Fig. 3.11 Pin Configuration of 16 X 2 LCD…………………………………23
19. Fig. 3.12 Block Diagram of Water Pump……………………………………24

**List of Tables**

1. Table 3.1 Properties of Sensor………………………………………………13
2. Table 3.2 Pin Descriptions of LCD…………………………………………23
3. Table 3.3 Features of Water Pump………………………………………….24

**Table of Content**

Certificate i

Acknowledgement ii

Abstract iii

List of Figures iv

List of Tables iv

Chapter 1: Introduction

1.1: Motivation ……………………………………………………..2

1.2: User Manual……………………………………………………3

Chapter 2: Theory Behind

2.1: Soil Moisture Sensor…………………………………………..5

2.2: Circuit Analysis of Prototype…………………………………8

2.3: Working of Prototype…………………………………………10

2.4: Advantage of Prototype……………………………………….11

Chapter 3: Hardware Profile

3.1: Soil Moisture Sensor…………………………………………..13

3.2: Microcontroller ATmega 32…………………………………..16

3.3: TIP 31-A………………………………………………………17

3.4: IC 7805………………………………………………………..19

3.5: Electromechanical Relay………………………………………21

3.6: 16 X 2 LCD…………………………………………………..23

3.7: Water Pump…………………………………………………..24

Chapter 4: Conclusion

4.1: Conclusion……………………………………………………26

4.2: Scope For Future Improvements……………………………..26

Appendix 1: Microcontroller……………………………………..27

Appendix 2: Pseudo Code…………………………………………31

References………………………………………………………………..33