**IMPLEMENTATION OF QUANTUM KEY DISTRIBUTION USING BB84 PROTOCOL**

Major Project report submitted in partial fulfillment of the Requirements for the Award of the Degree of

**BACHELOR OF ENGINEERING**

In

**ELECTRONICS AND COMMUNICATION ENGINEERING**

By

**PALADUGULA KALYAN KUMAR (BE/10496/14)**

**ARAVIND REDDY (BE/10262/14)**

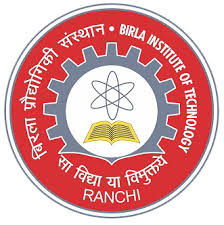
**GOWTHAM NALLA (BE/10377/14)**

|  |  |
| --- | --- |
|  |  |

Supervised By

**Dr. SWAPAN KUMAR GHORAI**  
Professor

Department Of Electronics and Communication

****

**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING, BIRLA INSTITUTE OF TECHNOLOGY, MESRA, RANCHI – 835215**

**MAY 2018**

**DECLARATION CERTIFICATE**

This is to certify that the work presented in this project entitled “**Implementation of Quantum Key Distribution using BB84 Protocol**”, in partial fulfillment of the requirement for the award of degree of **Bachelors of Engineering in Electronics and Communication Engineering**, submitted to the Department of Electronics and Communication Engineering Birla Institute of Technology, Mesra, Ranchi, Jharkhand is a bonafide work carried out by **Paladugula Kalyan Kumar, Aravind Reddy, Gowtham Nalla** under my supervision and guidance.

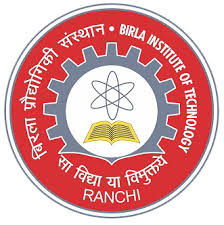
To the best of my knowledge, the content of this project, either partially or fully, has not been submitted to any other institution for the award of any other degree.

Dr, Swapan Kumar Ghorai

Date: Department of ECE

Birla Institute of Technology

Mesra, Ranchi.



**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING, BIRLA INSTITUTE OF TECHNOLOGY, MESRA, RANCHI – 835215**

**CERTIFICATE OF APPROVAL**

This is to certify that the project entitled “**Implementation of Quantum Key Distribution using BB84 Protocol**” is hereby approved as a suitable design of an engineering subject, carried out and presented in satisfactory manner to warrant its acceptance as prerequisite to the degree for which it has been submitted,

It is understood that by this approval, the undersigned do not necessarily endorse any conclusion drawn or opinion expressed there, approve the project for which it is submitted.

Internal Examiner External Examiner

Date: Date:

Dr. Srikanta Pal

Professor and Head of Department

Department of Electronics and Communication Engineering

Birla Institute of Technology

Mesra, Ranchi

**ACKNOWLEDGEMENT**

We owe our deepest gratitude to our advisor **Dr. Swapan Kumar Ghorai**, for his constant support and motivation, despite his extremely busy schedule. Our interactions with him always resulted in new ideas and proved beneficial towards our work. Without his constant presence and supervision our work would not have been successful.

We are very grateful to **Dr. Srikanta Pal, Professor and Head of Department of Electronics and Communication Engineering, Birla Institute of Technology, Mesra** for extending all the facilities at all times for pursuing this course.

And lastly our batch mates who have always been there with valuable suggestions and support in our endeavors.

PALADUGULA KALYAN KUMAR

ARAVIND REDDY

GOWTHAM NALLA

**ABSTRACT**

Nowadays, every information is in digital Form which is vulnerable to hackers and there are many hacking incidents reported also. If Quantum Computers come into existence, they will break the Ciphers very easily even the stronger ones like AES ciphers etc. So, there is a need of strong cryptography techniques to ensure data security. Then, a promising family of quantum solutions comes into picture. Most modern cryptographic studies design cryptosystems and algorithms using mathematical concepts. In designing and analyzing cryptosystems and protocols, mathematical concepts are critical in supporting the claim that the intended cryptosystem is secure. Most early cryptographic algorithms are based either on factorization or on discrete logarithm problem. Such systems generally adopt rather simple mathematics, and, therefore, need extensive secondary index computation. This article gives an insight into the Cryptography and its types. Then, it explains a Symmetric Block Cryptography technique called Advanced Encryption Standard (AES), its Structure and its stages. Then, it explains about Quantum Cryptography, its Security and different Quantum key Distribution Protocols. Then, it describes a technique of quantum key distribution called BB84 and gives insight to quantum physics governing the proper operation of any system in quantum cryptography and then presents the detailed analysis of BB48 system and its steps. Then, it presents the implementations of BB84 and AES using key from BB84 and their results. Ultimately, we conclude with practical implementations of quantum cryptography.

**CONTENTS**

|  |  |  |
| --- | --- | --- |
| 1. | List of Tables | 1 |
| 2. | List of Figures | 2 |
| 3. | **CRYPTOGRAPHY**  1. Introduction  2. Historical Background  3. Security Services offered by Cryptography  4. Cryptography Primitives  5. Structure of a Cryptosystem  6. Types of Cryptography  6.1 Symmetric Cryptography  6.2 Asymmetric Cryptography  7. Advanced Encryption Standard (AES)  7.1 Prerequisite Information  7.2 AES Key Expansion Algorithm  7.3 Stages in Each Round  a) Substitute Bytes  b) Shift Rows  c) Mix Columns  d) Add Round Key | 3  3  4  4  6  6  6  7  7  8  10  10  12  13  15  16  16 |
| 4. | **QUANTUM CRYPTOGRAPHY**  1**.** Introduction  2. Historical Background  3. Why Quantum Cryptography is Secured?  4. Structure of a Quantum Cryptosystem  5. Basic Idea  5. List of Quantum Key Distribution Protocols  6. BB84 Protocol  6.1 Overview of BB84 Protocol  6.2 Steps Of BB84 Protocol  6.3 Pictorial Presentation of BB84 protocol  6.4 BB84 With Evesdropper | 18  18  19  19  20  21  21  22  22  24  25  28 |
| 5 | **WHY PYTHON IS USED FOR QKD?** | 30 |
| 6 | **IMPLEMENTATIONS**  1. Implementation of Quantum Key Distribution using Python  2. Implementation of AES using Python and Tkinter | 30  30  34 |
| 7 | Practical Implementations of QKD | 35 |
| 8 | Conclusion | 36 |
| 8 | References | 38 |