

CERTIFICATION

This is to certify that this project, DEVELOPMENT OF A DATA ENCRYPTION APPLICATION FOR IMPROVED SECURITY ON WIRELESS NETWORKS was carried out by AKPIKIE, Oghenemairo with the matriculation number: SSE/011/10038 and supervised by Dr. A.O Akinwunmi

.....

Dr. A.O Akinwunmi

Supervisor's Signature

.....

Date

.....

Dr. O.O Adeosun

Head of Department's Signature

.....

Date

DEDICATION

I dedicate this project to God Almighty for his strength and protection during the period of the preparation of my project, my parent Mr. and Mrs. Akpikie and my friends who have been helpful in so many ways.

ACKNOWLEDGEMENT

I will like to acknowledge God almighty the creator of heaven and earth for his grace and favour upon my life, my parent Mr. & Mrs. Akpikie for their immense support in every way possible, my department HOD: Dr. O.O Adeosun, my supervisor: Dr. A.O Akinwunmi, my departmental lecturers: Dr. A.B.C Robert, Dr. O.G Lala, Mr. R.F Famutimi, Dr.Mrs. O.N Emuoyibofarhe, Mr. J.A Akinpelu, , Dr. M.O Oyetunji, Mrs. E.A Oladeji, Miss M.O Jayeola, Miss O.O Balogun, Mr. S. Adebayo, Mrs. R.F. Olorunfemi, Mr A.O. Ibitoye, Mr. H.O. Aworinde, Mr. O.B. Adeleke, Mr. A.A. Adetona, Mr. A.A. Alao, Engr. F.O Alamu, Mr. O.B Adeleke, Mrs. O.O Olaniran, Mr. A.A Adetona, Mr. Udo, Mr. Ayanniyi, Mr. E.K Olatunji, Miss. A.O Abiodun, , Dr. B.S Afolabi, Prof. E.O Omidiora, Prof. S.O Olabisi, Prof. Justice .O. Emuoyibofarhe, Prof. Sorinyan for their immense help, also to my friends: Ojo Oreoluwa, Kasali Oluwatobi, my roomates: Adamson Sodiq, Egunjobi Damola, Oladele Tolulope, Akano Olalekan, Adegboye Alex and all who have contributed to this point in the success of my academic pursuit. You all are deeply appreciated.

TABLE OF CONTENT

Abstract	i
Dedication	ii
Acknowledgement	iii
Table of content	iv
Table of Figures	viii
List of Tables	ix

CHAPTER ONE: INTRODUCTION

1.1 Background	1
1.2 Statement of Problems	1
1.3 Aim and Objectives	2
1.4 Methodology	2
1.5 Scope of Study	2
1.6 Significance of Study	3
1.7 Definition of Terms	3
1.8 Project Arrangement	4

CHAPTER TWO: LITERATURE REVIEW

2.1 Wireless Network security	6
-------------------------------	---

2.1.1 WLAN Security for 802.11	6
2.1.2 Benefits of Wireless LANs	7
2.1.3 WLAN Architecture	8
2.2 Applicability of Wireless Networks for Information Processing In a Corporate Environment	11
2.3 Best Practices in Corporate Deployment	13
2.4 Develop Incident Response Procedures	16
2.5 Virtual Private Network	16
2.5.1 Common Uses of VPNs	18
2.6 Ad-hoc Wireless Network	24
2.6.1 Architecture of the Multihop Ad-hoc Wireless Network	24
2.7 Data Encryption: Symmetric and Asymmetric Encryption	25
2.7.1 Symmetric Encryption	27
2.7.2 Asymmetric Encryption	29
2.8 Homomorphic Encryption	30
2.9 Wi-Fi Protected Access (WPA	31
2.10 Wi-Fi Protected Access 2 (WPA2	33

CHAPTER THREE: METHODOLOGY

3.1 Introduction	37
3.2 Analysis of Existing Systems	37
3.3 Approach	38
3.4 Data Encryption	38
3.5 Elliptic Curve Diffie-Hellman Encryption	39
3.6 Proposed System	40
3.7 Working principle of the Elliptic Curve Diffie-Hellman cryptography	40
3.8 System Design	42
3.9 Methodologies and Design	45
3.10 System Requirement Specification	42
 CHAPTER FOUR: RESULT AND DISCUSSION	
4.1 Overview	44
4.2 Implementation	44
4.3 Overview of Application	45
4.4 The “Browse For File” Button	47
4.5 The “Send To” drop-down box	49
4.6 The “Password File” checkbox	49
4.7 The “Send File” button	50

4.8 The “Browse For File” button (at the receiver’s end	50
4.9 Process train of how a file is encrypted, sent and decrypted from the sender and receiver’s end respectively	51
4.10 Testing	59
4.10.1 Unit testing	59
 CHAPTER FIVE: CONCLUSION AND RECOMMENDATION	
5.1 Summary	62
5.2 Contribution to Knowledge	62
5.3 Recommendation	63
5.4 Conclusion	63
5.5 Suggestion for Future Study	64
Reference	65
Appendix	67

TABLE OF FIGURES

2.1 A Virtual Private Network	18
2.2 VPN Connection to connect A Remote Client to A Private Intranet	20
2.3 Using a VPN Connection to connect two Remote Sites	22
2.4 Using a VPN connection to a secured or hidden network	24
2.5 Data Encryption and Decryption	27
2.6 Symmetric Encryption	29
2.7 Asymmetric Encryption	31
3.1 Activity Diagram	42
4.1 Overview Of The Encryption Software	49
4.2 File selection	52
4.3 Selecting recipient	53
4.4 Password setting to selected file	54
4.5 Browse for received encrypted file	55
4.6 Enter password for received encrypted file	56
4.7 Decrypted file	57
4.8 Back-end activities via command prompt	58

LIST OF TABLES

2.1 Differences between WEP and WPA	34
4.3 Unit testing table	60

ABSTRACT

Wireless networks today have many advantages, but it is also coupled with new security threats and alters the organization's overall information security risk profile. Although the usual solutions to these security risks lies in technological solutions, but wireless security is primarily a management issue. Effective management of the threat associated with wireless technology requires a sound and thorough assessment of risk given the environment and development of a plan to mitigate identified threats. Therefore communication serves as a livewire in all, the need for communication has brought up the issue on the use of computers for communication through networks around the world, but the issue on the safety of the communication, data transfer or the communication link. The study was designed, implemented and tested.

An encryption system was designed, implemented and tested. The encryption system was designed using C#. The system was implemented using Elliptic Curve Diffie-Hellman encryption and the application was tested on several computer systems to ascertain the functionality using windows 7 and windows 8.1 platforms.

The project provides security in sending and receiving of data in a wireless network. The encryption software sends and receives data/packages securely without interference of intruders.