

# **CHAPTER ONE**

## **INTRODUCTION**

### **1.1 Background**

Wireless networking presents many advantages Productivity improves because of increased accessibility to information resources. Network configuration and reconfiguration is easier, faster, and less expensive. However, wireless technology also creates new threats and alters the existing information security risk profile. For example, because communications takes place "through the air" using radio frequencies, the risk of interception is greater than with wired networks. If the message is not encrypted, or encrypted with a weak algorithm, the attacker can read it, thereby compromising confidentiality. Although wireless networking alters the risks associated with various threats to security, the overall security objectives remain the same as with wired networks: preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems. The popularity of wireless Networks is a testament primarily to their convenience, cost efficiency, and ease of integration with other networks and network components. The majority of computers sold to consumers today come pre-equipped with all necessary wireless Networks technology. The benefits of wireless Networks include: Convenience, Mobility, Productivity, Deployment, Expandability and Cost.

### **1.2 Statement of problems**

The problem associated with wireless networks is in the area of data security. Most data/information shared on a wireless network are poorly protected or encrypted and this poses a huge problem in the privacy of information in an organization.

Hence, security or encryption of data shared in a network will provide data privacy and also limit the actions of intruders in a network.

### **1.3 Aim and objectives**

The aim of this project was to provide data encryption security on a wireless network.

The Objectives for embarking on this project are:

- i. to formulate a system for data encryption on a wireless network;
- ii. to design the system formulated above;
- iii. implement the system; and
- iv. test the system.

### **1.4 Methodology**

This study involved checking and reviewing relevant literatures and materials in the areas of wireless network security and data encryption. Elliptic Curve Diffie-Hellman encryption was used to design the system using Visual studio 2012. C# was used to implement the system. The application was tested on several computer systems to ascertain the functionality of the system; two operating systems were used for testing the system namely: Windows 7 and Windows 8.1.

### **1.5 Scope of study**

In recent times, the need for an efficient and reliable security of data shared in wireless networks of corporate organizations, schools, hospitals etc. has been on the rise.

The scope of this project covered the use of Elliptic Curve Diffie-Hellman encryption to secure data in a wireless network.

## **1.6 Significance of study**

This project is very necessary due to the fact that most corporations, industries, companies etc rely on wireless networks for files sharing, day to day transactions and most importantly internet connectivity. If there is a security breach in the wireless network of an institution, it is going to cause a lot of problem to that institution.

Therefore the need to encrypt data shared in a wireless network cannot be over emphasized as data security is the main concern of majority of corporations.

## **1.7 Definition of terms**

**Architecture:** The sum total of all of the specifications, protocols and implementations that define a particular networking system.

**Archive:** A storage of infrequently-used or historical data.

**Area:** Logical set of network segments (either CLNS-, DECnet-, OSPF-based) and their attached devices. Areas are usually connected to other areas via routers, making up a single autonomous system. See also autonomous system.

**ARM:** Asynchronous response mode, HDLC communication mode involving one primary station and at least one secondary station, where either the primary or one of the secondary stations can initiate transmissions. See also primary station and secondary station.

**ARP:** Address Resolution Protocol. The protocol for mapping IP addresses to physical addresses such as Ethernet or Token Ring.

**ARPA:** Advanced Research Projects Agency, Research and development organization that is part of DoD. ARPA is responsible for numerous technological advances in communications and networking. ARPA evolved in DARPA, and then back into ARPA again (in 1994).

**ARPANET:** Advanced Research Projects Agency Network. Landmark packet-switching network established in 1969. ARPANET was developed in the 1970s by BBN and funded by ARPA (and later DARPA). It eventually evolved into the Internet. The term ARPANET was officially retired in 1990.

**ARQ:** Automatic repeat request. Communication technique in which the receiving device detects errors and requests retransmission.

**ASCII:** Referring to a standard 7-bit character system that includes the alphanumeric characters and printer control codes.

**ASTA:** Advanced Software Technology and Algorithms. Component of the HPCC program intended to develop software and algorithms for implementation on high-performance computer and communications systems. See also HPCC.

**Bandwidth:** In analog communications, the difference between the highest and lowest frequencies available in the band. In digital communications, bandwidth is loosely used to refer to the information-carrying capacity of a network or component of a network.

**CIDR:** Classless Interdomain Routing. Technique supported by BGP4 and based on route aggregation. CIDR allows routers to group routes together in order to cut down on the quantity of routing information carried by the core routers. With CIDR, several IP networks appear to networks outside the group as a single, larger entity (WILD PACKETS INC, 2014).

## **1.8 Project arrangement**

This project is arranged into five chapters. The rest of the chapters are organized as follows:

Chapter Two – This chapter covers literature review. In this chapter, in-depth meaning of wireless network security. A number of journals were reviewed and different ideas were shared. This chapter also explains the different threats that affect wireless networks and also give reasons why data shared in a wireless network must be protected.

Chapter Three – This chapter covers analysis and design. It includes detailed methodology and about the processes involved in developing the encryption algorithm.

Chapter Four – This chapter covers the system implementation and documentation. It covers the implementation methods used in achieving the project.

Chapter Five – This chapter covers the summary of the project work, recommendations and conclusions arrived at this project work. The chapter also covers the limitations of the system, what should be for future research about the project work and the way(s) the project work has contributed to the security of wireless networks.

## **CHAPTER TWO**

### **LITERATURE REVIEW**

#### **2.1 Wireless network security**

Wireless and mobile networks are rapidly extending their capabilities. In addition to their increasing bandwidth and because of their flexibility and freedom they are becoming the communication infrastructure of choice (Boncella, 2002). As wireless communication and the internet are interoperable, users seek for more secure, efficient communication channel. The user expects three assurances:

- i. Authentication
- ii. Confidentiality
- iii. Integrity (Boncella, 2002)

##### **2.1.1 Wlan security for 802.11**

WLAN are best suited for networks with low security requirement. Unlike wired networks that require physical presence with the premises to have access to the network, wireless network can be accessed as long as the network is discoverable. The device that must connect to the access points must first of all be authenticated before access is enabled. The 802.11 standard provides the means to satisfy the security requirement, validation to allow access for devices (Boncella, 2002). The 802.11 standard represents a significant step in electronic-data infrastructure evolution, which in the last ten years has proceeded from coax, token ring, and 10/100 BaseT Ethernet cabling to wireless radio transmissions( Symantec Corporation,2002). The most widely used and best known variation of the 802.11 wireless LAN standard is the 802.11b (can also be

called WIFI). Under normal condition, the WIFI can receive and also transmit data at speeds between 1 and 5 Mbps. The WEP transmission encryption as regards 802.11b provides a level of privacy that is equivalent to wired LAN privacy, which is achieved via various physical security (Symantec Corporation, 2002).

### **2.1.2 Benefits of wireless LANs**

Wireless LANs generally are less expensive and less intrusive to implement and maintain than the wired network. The cost of implementing the wired network to a group of people is quite expensive and not cost effective. Some of the benefits of wireless local area network is as follows:

- i. **SIMPLIFIED IMPLEMENTATION AND MAINTENANCE:** Wireless APs can be installed in virtually anywhere in a room to accommodate endless network access or variety of office configurations. This is in contrast to wired network that consumes time and resources to run cables from a network closet to user's desktops and to other areas in the building (Symantec Corporation, 2002).
- ii. **EXTENDED REACH:** Wireless LANs enables users or employees in a company to access files on that network provided that the employee is within the AP's transmission range. This helps to improve the employee productivity (Symantec Corporation, 2002).
- iii. **INCREASED WORKER MOBILITY:** Wireless LANs provides users with the advantage of moving from one location to another under the connectivity of that network with their laptops or PDAs. Users can connect to public wireless LANs in coffee shops and airport lounges (Symantec Corporation, 2002).

- iv. **REDUCED TOTAL COST OF OWNERSHIP AND OPERATION:** The cumulative benefits of simplified implementation and maintenance, an extended LAN reach, and the freedom to roam minimize expenses and improve organizational and employee productivity. The result is reduced total cost of ownership and operation (Symantec Corporation, 2002).

### **2.1.3 Wlan architecture**

The WLAN is produced from stations and access points. The main structure of a WLAN is the BSS (basic service set). The Basic Service Set is divided into two types; Independent BSS and infrastructure BSS.

In the Independent BSS, the workstations communicate with each other without any third party device or system as long as they are in range of each other. They are sometimes referred to as ad hoc networks because they generally last for a short period of time. The use of Aps in a BSS infrastructure allows communications between stations (Boncella, 2002).

Some problems associated with WLAN are shown below:

- i. **INTECEPTION AND UNAUTHORIZATION MONITORING:** An unauthorized wireless client may join a BSS with the intention of eavesdropping on members of the BSS. This action provides the unauthorized client with access to carry out illegal packet analysis if the packets are not encrypted. Another form of insertion attack is to clone a legitimate access point in order to take over the BSS.
- ii. **DENIAL OF SERVICE (DOS):** The popular way of carrying out DOS is by signal jamming. This is possible due to their use of ISM band. Signals can be jammed using



baby monitors, a leaky microwave oven, cordless phones and any other ISM band frequency devices.

- iii. **CLIENT TO CLIENT ATTACKS:** Most DOS attacks carried out against WLAN is either by duplicating the MAC address or IP address. The usual TCP/IP service attacks can be carried out against wireless client providing these services (e.g., SNMP, SMTP, FTP).
- iv. **BRUTE FORCE ATTACKS AGAINST AP PASSWORDS:** Password scheme provides restricted access to an AP. This restriction can be compromised by the use of password dictionary attacks.
- v. **MISCONFIGURATIONS:** Most Aps use an unsecure configuration. If the engineer installing the AP use the default or factory settings, because the default setting is publicly known, it poses a security threat to that AP and BSS stations (Boncella, 2002).

Wireless network can be very vulnerable to attacks because the signals are broadcasted through the air over a radio signal. The typical indoor broadcast range of an access point is 150-300 feet. Outdoors broadcast may extend as far as 1,000 feet. Failure to secure your wireless network could potentially open your internet connection to a surprising number of users (US-CERT, 2008). The starting point to a secured wireless network is to disable identifier broadcasting in the access point. This makes the wireless network to be hidden from any other person than the owner of the network.

An unsecured wireless network spells disaster as files that are shared can be accessed by malicious users and those files can be viewed by the hacker. Another way in which wireless network can be secured is by changing or renaming the SSID (Service Set Identifier). Most of the default service set name are widely known by the public and this can provide easy access into the network. But with the introduction of another SSID, the network will not be easily guessed

by an unauthorized user (US-CERT, 2008). Nowadays, traffic passing through a wireless network can be monitored by unauthorized users, therefore there is a need to encrypt traffic passing through the wireless network. The security threats involved when using a public access point in a wireless-enabled laptop is as follows:

**a. Evil Twin Attacks**

In Evil Twin Attack, the attacker detects and gets information about a public access point in an environment. This attacker setup his own system with the aim of impersonating the original AP. The attacker then broadcast his signal to be stronger than that which is broadcasting from the original access point. When users connect with the impersonated signal, the attacker will have full access to the data being sent by the user. E.g. credit card numbers, username & password combinations etc.

**b. Wireless Sniffing**

Many wireless access points are poorly secured. As a result, malicious users can use sniffing tools to obtain important information on the network.

**c. Peer-to-Peer Connections**

Since laptops nowadays are equipped with a Wi-Fi wireless networking card, it is possible to create ad-hoc networks between systems at close range. The security threat with this connection is that if an attacker with a network card configured for ad-hoc mode with the same settings as the settings of any laptop in that network gains access into the network thereby exposing sensitive files to the attacker. This is popular in the 802.11 standard (US-CERT, 2008).

General solutions to wireless network security via access point is as follows:

- a. Encrypt your files
- b. Avoid using passwords and providing personal information to websites
- c. Use a virtual private network (VPN) if possible (US-CERT, 2008).

## **2.2 Applicability of wireless networks for information processing in a corporate environment**

In recent years, small and medium enterprises (SMEs) now turn towards wireless networks, part of the reasons is due to the low cost of wireless device and also convenience of using the network. Most large corporations now consider wide deployment of wireless networks. According to the Government of the Hong Kong Special Administrative Region (2010), the applicability of wireless network can be defined with respect to the transmission of various categories of information. Using the Hong Kong government as a case study, there are clear guidelines for the applicability of wireless network. Found below is the table:

Table 2.1: Guidelines for the applicability of wireless network

Category of Information	Applicability of Using Wireless Network for Transmission
TOP SECRET	Not allowed
SECRET	Not allowed
CONFIDENTIAL	<p>Allowed, provided that there are sufficient authentication and transmission encryption security controls that have attained the level of encryption required for CONFIDENTIAL information.</p> <p>Use of a VPN is recommended to provide a strong authentication and encryption tunnel over a WLAN connection. In addition, proper key management and configuration policies should also be established to complement the technical solution.</p>
RESTRICTED	<p>Allowed, provided that there are sufficient authentication and transmission encryption security controls that have attained the level of encryption required for RESTRICTED information.</p> <p>The same level of encryption required for CONFIDENTIAL information is recommended, using proper key management and configuration policies similar to those for CONFIDENTIAL information.</p>
Unclassified	Allowed. Following the principle that only

	<p>authorized parties are permitted to access the network where information is stored, wireless networks with sufficient authentication and transmission encryption measures where appropriate are considered suitable for use by Bureaux &amp; Departments.</p> <p>Similar to the specifications for CONFIDENTIAL and RESTRICTED information, proper key management and configuration policies should be established to complement the technical solution.</p>
--	---

**Source: (Government of the Hong Kong Special Administrative Region, 2010).**

## **2.3 Best practices in corporate deployment**

Organizations are getting more acquainted with wireless networks because of its cost effectiveness and convenience. The risks that come with this technology can be tackled but must first be considered throughout the entire deployment life cycle. A five-phase life cycle model for network deployment will be discussed to salvage security issues.

### **a. INITIALIZATION PHASE**

When designing a wireless network, the functional and business requirement of that network must be considered. These requirements may affect decisions on what kind of security measures should be deployed to protect the network. For example, if guest access is required, security best practices for guest access should be considered in the design stage.

### **b. DESIGN / PROCUREMENT PHASE**

Over the years, new enhancement has been made to strengthen data rates, signal range, and security of wireless networks especially the 802.11 standard. It is important to keep track of new development of new standards when planning on procuring or acquiring new wireless network services. In any new purchase, protection by one of the stronger wireless security protocols such as WPA/AES or WPA2/AES should be considered, but by no means should such wireless security protocols be solely relied upon to protect data confidentiality and integrity, as new weaknesses in protocols may be discovered in the future.

### **c. IMPLEMENTATION PHASE**

Implementing Strong Physical Security Controls: The loss of network equipment can pose a great risk to the wireless network as the configuration of that network can be

retrieved from the lost access point or wireless interface card. To secure and avoid this scenario from taking place, access points should be located in areas that are less accessible together with strong physical security controls. This will thereby limit the risk.

### Secure Access Points

The security of a wireless access point clearly has a major impact on the security of that network as a whole. Properly securing access points is the starting point of securing a wireless network. There are different steps involved in securing a wireless access point:

- i. Change the default configuration settings;
- ii. Change encryption keys regularly;
- iii. Ensure that all access points have strong, unique administrative passwords and change the passwords regularly;
- iv. Disable all insecure and unused management protocols on access points and configure the remaining management protocols for least privilege;
- v. Activate logging features and direct all log entries to a remote logging server;
- vi. Enable wireless threshold parameters, such as inactivity timeouts and maximum supported associations.

**Use Non-suggestive Service Set Identifier (SSID) Naming Conventions:** In a wireless network, an SSID serves as a network name for segmenting networks. A client station must be configured with the correct SSID in order to join a network. The SSID value is broadcast in beacons, probe requests and probe responses. To prevent a malicious attacker from collecting reconnaissance information on a wireless network by eavesdropping, SSIDs should not reflect internal information of the organization.

## Disable Direct Client-to-Client “Ad-Hoc Mode” Transmissions

In general, a wireless network can be operated using three different topologies; infrastructure mode, ad-hoc mode and bridging mode. When a wireless network operates in ad-hoc mode, client stations are connected directly and no access point is required. Using this mode, a potential attacker can gain access to a client station easily if the client station is improperly configured. Unless there is a specific business need, the ad-hoc mode should be disabled on wireless devices (Government of the Hong Kong Special Administrative Region, 2010).

### d. OPERATION AND MAINTENANCE PHASE

Educate Users about the Risks of Wireless Technology: Proper awareness should be made to users of this technology. It is also important to educate all users in following the policy. Best practices or security guidelines should be developed that end-users understand and adhere to.

#### Keep an Accurate Inventory of All Wireless Devices:

An accurate inventory of all authorized wireless devices helps identify rogue access points during security audits. This inventory will also be helpful for a variety of support tasks.

#### Publish a Coverage Map of the Wireless Network:

Network administrators should develop a coverage map of the wireless network, including locations of respective access points and SSID information. This map is a valuable asset for troubleshooting, or handling a security incident.

#### Develop Security Configuration Standards for Access Point:

To simplify daily operations and ensure all access points are protected with appropriate measures, it is recommended a baseline security configuration standard for access points be developed. It is not uncommon to see security settings restored to their default factory settings



after an access point is reset, which usually occurs when the access point experiences an operational failure. If a baseline security configuration standard is available, appropriate personnel can simply follow the standard settings to re-configure the access point.

#### **Review Audit Logs Regularly:**

Regular checking of log records must be performed, to ensure the completeness and integrity of all logs. Any irregularities spotted must be reported and a detailed investigation should be carried out if necessary.

### **2.4 Develop incident response procedures**

It is recommended that administrators develop a set of in-house procedures for incident response, and update these procedures from time to time to address new potential security threats.

### **2.5 Virtual private network**

According to Singh (2012), a Virtual Private Network (VPN) is a network technology that creates a secure network connection over a public network such as the Internet or a private network owned by a service provider. Most corporations use VPN technology to enable remote users to securely connect to a private network. A VPN can connect multiple sites over a large distance just like a Wide Area Network (WAN). VPNs are often used to extend intranets worldwide to disseminate information and news to a wide user base. Educational institutions use VPNs to connect campuses that can be distributed across the country or around the world. Figure 2.1 shows the illustration of a virtual private network.

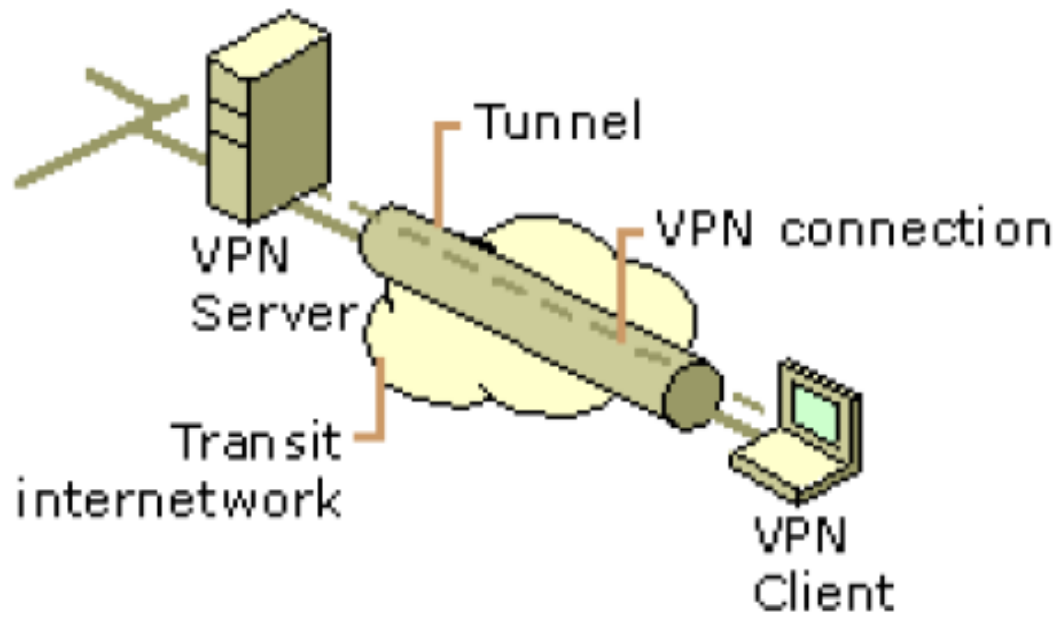


Figure 2.1: A Virtual Private Network (Source: Singh, 2012)

Singh (2012) discussed about the three levels of security that VPN technology provides:

- a) Authentication: Every user logged on to a wireless station as well as trying to connect to WLAN using VPN client must be authenticated. Therefore authentication is user based not machine based.
- b) Encryption: VPN provides another level of data confidentiality by encrypting the traffic passing through the network. Thus even if an intruder manages to get into the tunnel and intercepts the data, that intruder will have to go through a lot of effort and time decoding it (if he is able to decode it).
- c) Data authentication: This provides data integrity by ensuring that all traffic is from authenticated devices.

### **2.5.1 Common uses of VPNs**

The next few subsections describe the more common VPN configurations in more detail.

#### **i. Remote Access over the Internet**

VPNs provide remote access to corporate resources over the public Internet, while maintaining privacy of information. Figure 2.2 below shows how a remote user can connect to a corporate intranet using a VPN connection.

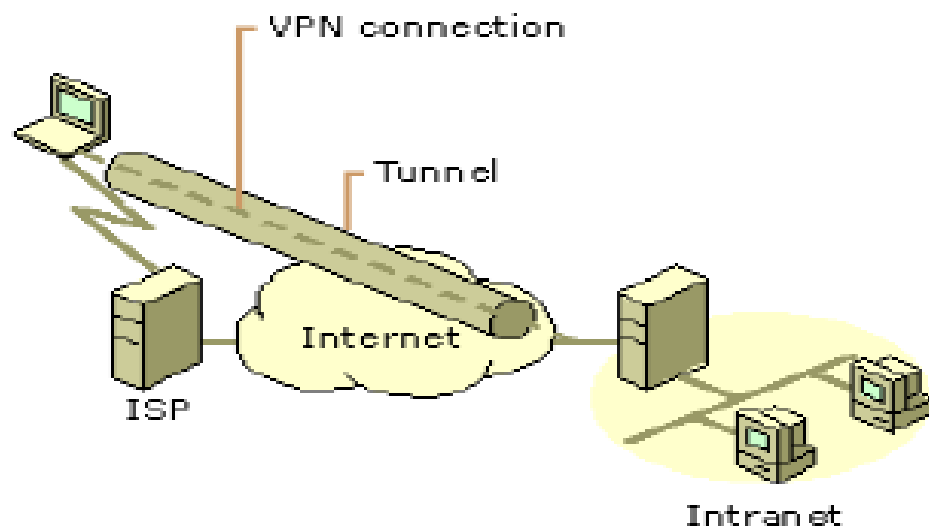


Figure 2.2: VPN connection to connect a remote client to a private intranet (Source: Singh, 2012)

Instead of making a long distance (or 1-800) call to a corporate, the user calls a local ISP. Using the connection to the local ISP, the VPN software creates a virtual private network between the dial-up user and the corporate VPN server across the Internet (Singh, 2012).

## **ii. Connecting Networks over the Internet**

There are two methods for using VPNs to connect local area networks at remote sites:

a) **Using dedicated lines to connect a branch office to a corporate LAN:** Rather than using an expensive long-haul dedicated circuit between the branch office and the corporate hub, both the branch office and the corporate hub routers can use a local dedicated circuit and local ISP to connect to the Internet. The VPN software uses the local ISP connections and the Internet to create a virtual private network between the branch office router and corporate hub router (Singh, 2012).

b) **Using a dial-up line to connect a branch office to a corporate LAN:** Rather than having a router at the branch office make a long distance (or 1-800) call to a corporate

Encryption: VPN provides a secure tunnel on top of inherently un-secure medium like the Internet. To provide another level of data confidentiality, the traffic passing through the tunnel is also encrypted. Thus even if an intruder manages to get into the tunnel and intercepts the data, that intruder will have to go through a lot of effort and time decoding it (if he is able to decode it).

Data authentication: It guarantees that all traffic is from authenticated devices thus implying data integrity or outsourced NAS, the router at the branch office can call the local ISP. The VPN software uses the connection to the local ISP to create a VPN between the branch office router and the corporate hub router across the Internet.

Figure 2.3 below shows an example of a VPN connection connecting two remote sites.

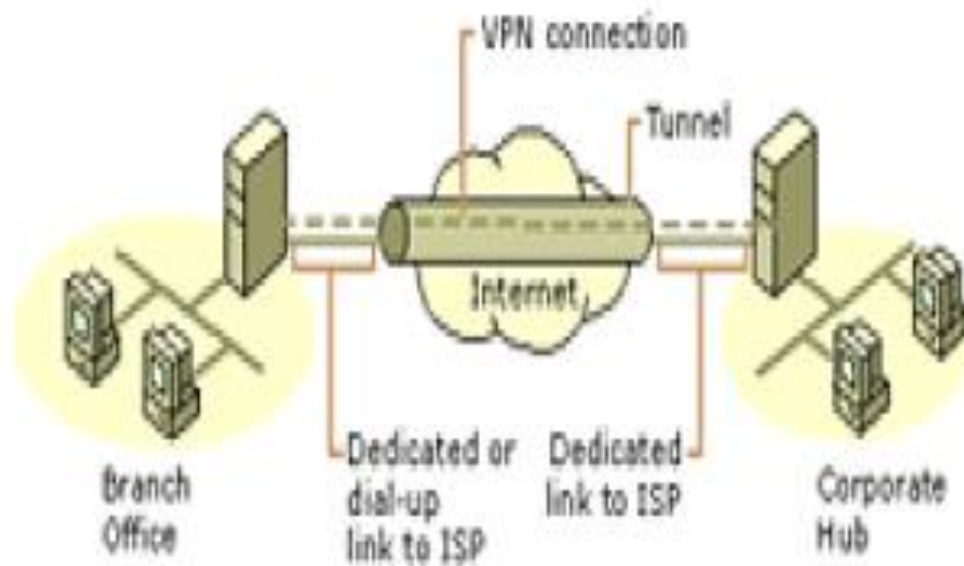


Figure 2.3: Using a VPN connection to connect two remote sites (Source: Singh, 2012)

The corporate hub router that acts as a VPN server must be connected to a local ISP with a dedicated line. This VPN server must be listening 24 hours a day for incoming VPN traffic (Singh, 2012).

### **iii. Connecting Computers over an Internet**

In most corporate internetworks, the data being sent on that network is so sensitive; therefore the department's LAN is physically disconnected from the rest of the corporate internetwork. This causes or creates information accessibility problems for those users not physically connected to the separate LAN.

Figure 2.4 below shows a VPN connection to a hidden network.

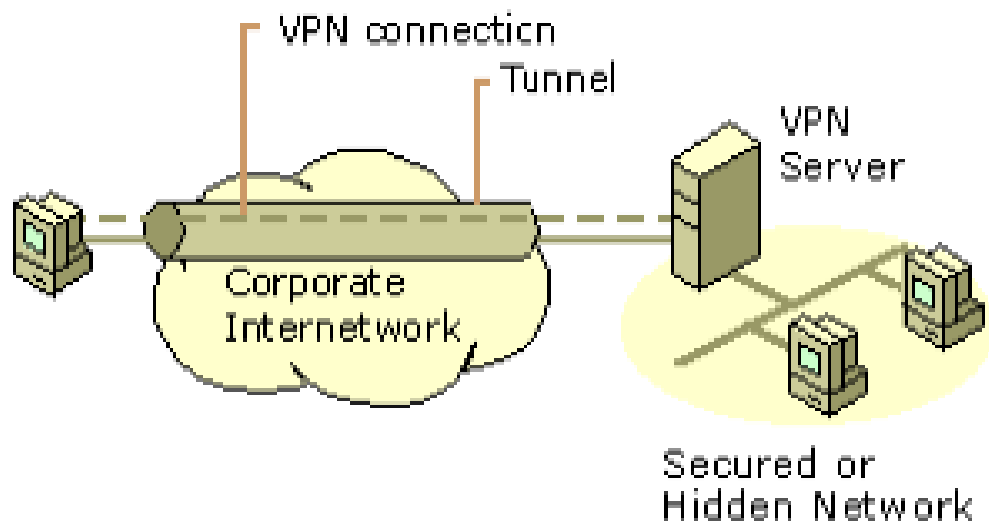


Figure 2.4: Using a VPN connection to a secured or hidden network (Source: Singh, 2012)



## **2.6 Ad-hoc wireless network**

According to Manikandan and Vijayaragavan (2010), Ad hoc wireless networks are an ideal technology to deploy an instant communication network for civilian and military applications. However, as the size of an ad hoc multi-hop network increases (as in battlefield applications), the available bandwidth to the mobile users decrease. Key causes of such degradation include the resulting excessive control traffic overhead required to maintain accurate routing tables in the presence of mobility, and the difficulty in guaranteeing any kind of bandwidth on a path with many wireless hops. There are many routing protocols for ad hoc wireless network. They can be classified into four different types:

- a) Global, precomputed routing
- b) On-demand routing
- c) Location based routing
- d) Flooding

These approaches all assume that the network is a homogeneous one. All nodes in homogeneous network have the same transmission capabilities and use the same frequency and channel access scheme. Among those four, on demand routing is the most recent one to enter into scalable wireless routing class. By relaxing the requirement of routes maintenance on all nodes, on demand routing avoids excessive routing overhead. The limitation is fundamentally due to the spatial concurrency constraints on nearby nodes sharing the same channel.

### **2.6.1 Architecture of the multihop ad-hoc wireless network**

The architecture of a 2-level heterogeneous ad-hoc wireless network with UAV was discussed below. The hierarchical infrastructure consists of the following two hierarchies:

**Level 1: Ground ad-hoc wireless network:**

Based on the hop distance of packet transfers, wireless networks can be divided into two types: singlehop and multihop. The multi-hop wireless network, also called “ad hoc” wireless network, allows all mobile hosts to move freely without any constraints by fixed communication infrastructure. Due to the ad hoc topology, maintaining efficient routes become very challenging. At this level, we have both regular ground mobile nodes and backbone nodes. Manikandan and Vijayaragavan proposed a variety of clustering algorithms for the dynamic creation of clusters and the election of clusters heads in ad hoc wireless networks (Manikandan and Vijayaragavan, 2010).

**Level 2: Ground embedded mobile backbone network:**

An embedded mobile backbone was introduced due to the poor performance of ad hoc wireless network where many hops are involved. In the tactical environment, special fighting units like trucks, tanks may carry a lot more equipment than individual soldiers. These mobile nodes, with the help of beam-forming antennas, can offer high-speed point-to-point direct wireless links. So if we select those mobile nodes as backbone nodes, we can establish a ground mobile backbone embedded within the ground ad hoc wireless network. In this level, we only have ground backbone nodes. Direct point-to-point wireless links are used for the communications (Manikandan and Vijayaragavan, 2010).

**2.7 Data encryption: Symmetric and Asymmetric encryption**

A security system’s strength is determined its ability to encrypt and decrypt the data sent on a particular network. The purpose of encrypting and decrypting data on a network is to avoid intruders from understanding the data. The figure 2.5 below shows the common use of encryption /decryption techniques.

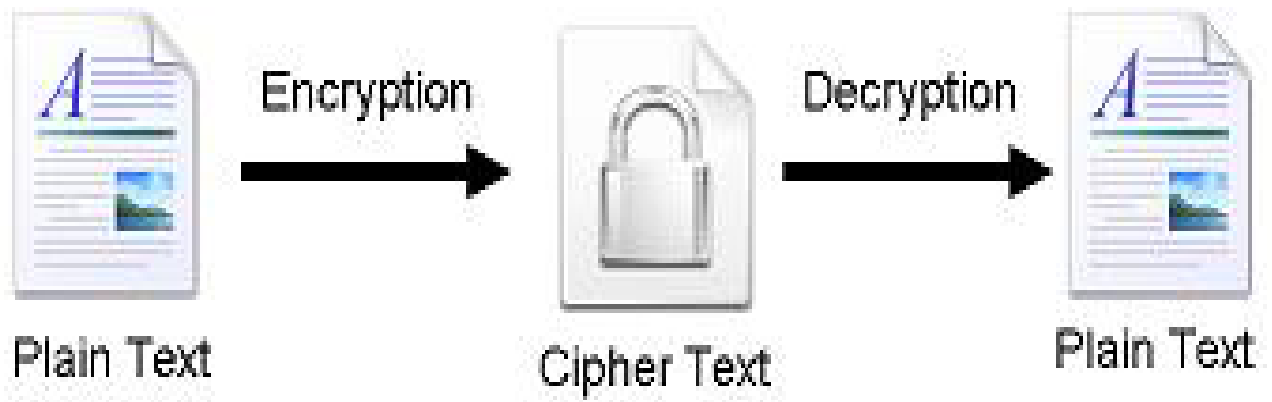


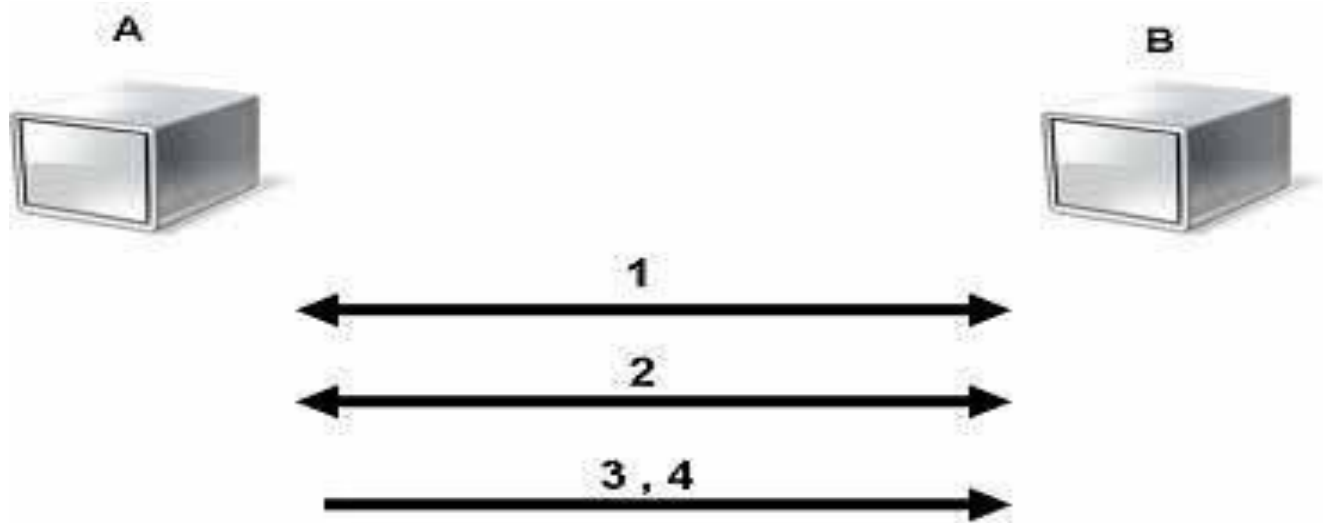
Figure 2.5: Data Encryption and Decryption Source: (Abdel-Karim and Tamimi, 2006)

Abdel-Karim and Tamimi discussed the two categories of data encryption which are Asymmetric and Symmetric techniques

### **2.7.1 Symmetric encryption**

In this type of encryption, the sender and the receiver both agree on a secret (shared) key. This key will be used to encrypt and decrypt their sent messages. The figure 2.6 below shows the process of symmetric cryptography. Node A and B is first on the encryption technique to be used in encryption and decryption of communicated data. Then they agree on the secret key that both of them will use in this connection. After the encryption setup finishes, node A starts sending its data encrypted with the shared key, on the other side node B uses the same key to decrypt the encrypted messages.

The major concern with symmetric encryption is how to share the secret key between the two peers. Once the key is known, the whole system collapses.



- 1- A and B agree on a cryptosystem.
- 2- A and B agree on the key to be used.
- 3- A encrypts messages using the shared key
- 4- B decrypts the ciphered messages using the shared key.

Figure 2.6: Symmetric encryption Source: (Abdel-Karim and Tamimi, 2006)

### **2.7.2 Asymmetric encryption**

In this type of encryption, two keys are used. What key1 can encrypt, key2 can decrypt, and vice versa. This kind of encryption is also known as Public Key Cryptography (PKC). This is because the user uses two keys, one which is known to the public and the other which is only known to the user. The figure 2.7 below shows a typical example of an Asymmetric Encryption.

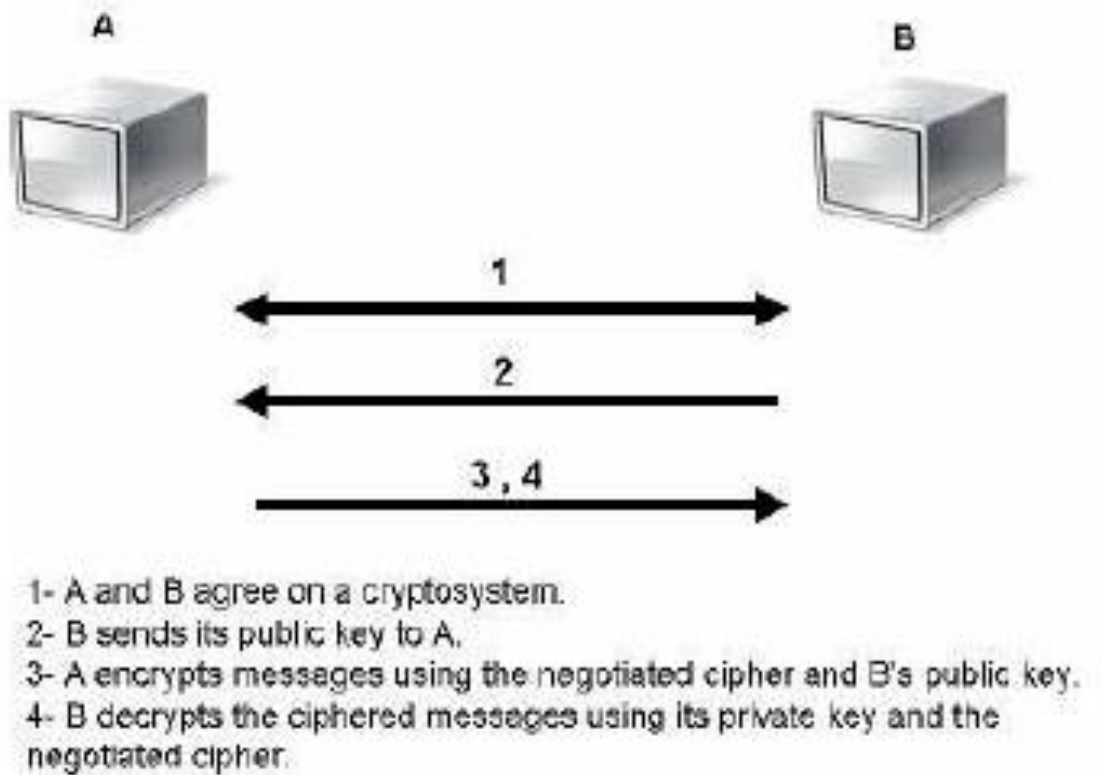


Figure 2.7: Asymmetric Encryption Source: (Abdel-Karim and Tamimi, 2006)

## 2.8 Homomorphic encryption

According to Smart and Vercauteren (2010), the fully homomorphic public key encryption scheme has been referred to as ‘holy grail’ for years. This problem was solved by Gentry by using properties of ideal lattices. Lattices are very vital to understand the workings of the scheme algorithms. The fundamental idea of the algorithm is “we are all perfectly colorblind relative to each other”. This idea was taken from a centuries old philosophical puzzle in which there is a man who has a very weird problem. Every time he looks at a color, it get swapped in his head with some other color. For example, if he looks at red, then as soon as red enters his retina, it becomes blue. When he looks at blue, it becomes green and green becomes red. The catch is that man “always” stays perfectly consistent with the labeling of the color. Labeling refers to the “name” of the color. When he is looking at “our red”, he would call it red but “actually” he is looking at blue, because our red becomes his blue and so on. Question is; is there a way we can detect that this person is “color-blind” as long as he stays perfectly consistent with the labeling? Answer is; NO, we can’t detect his color-blindness. Secret Key would be that morphism which swaps colors and public key would be those labels “red, blue, green etc.” We mathematically achieve this using p-adic ring homomorphism  $\psi$  from one p-adic ring extension  $X$  to another p-adic ring extension  $Y$ . These extensions are unramified. We call  $\psi$  “color-blinder”.  $\psi$  is that secret relation (morphism) between  $X$  and  $Y$  (Khan, 2012).

## 2.9 Wi-Fi Protected Access (WPA)

According to Wi-Fi Alliance (2003), WPA addresses the flaws in Wired Equivalent Privacy (WEP). The WEP has been the security mechanism for WLAN since the adoption of the Institute of Electrical and Electronic Engineers (IEEE) 802.11 standard in 1997.



The cryptography of WEP is very weak as compared to recent development in security of wireless network. WPA addresses flaws in WEP. WPA was invented to the fact that the weakness of WEP could hinder the adoption of Wi-Fi devices into the market. This is because WPA is a stronger, improved cryptography as compared to WEP. WPA provides a high level of security in which only authorized users can access that network. WPA was designed to minimize impact on network performance and to run as a software upgrade on the more than 650 Wi-Fi CERTIFIED products in today's market (Wi-Fi Alliance, 2003).

WPA presents a natural migration path for currently installed devices. Enterprises that are presently using 802.1 X/EAP authentications can upgrade to WPA without forfeiting their investment. For this to happen, IT managers are advised to ensure that the new devices that they are purchasing have WPA present in them. Most vendors offer a 'mixed mode' on access point to support WPA as well as WEP security, but this type security is not totally secure because it will constantly present open portholes through which intruders can access the wireless network.

WPA uses a greatly enhanced encryption scheme, Temporal Key Integrity Protocol (TKIP). Together with 802.1X/EAP authentication, TKIP employs a key hierarchy that greatly enhances protection. It also adds a Message Integrity Check (MIC, sometimes called "Michael") to protect against packet forgeries.

Table 2.1: Differences between WEP & WPA

	WEP	WPA
Encryption	Flawed, cracked by scientists and hackers	Fixes all WEP flaws
	40-bit keys	128-bit keys
	Static- same key used by everyone on the network	Dynamic session keys. Per user, Per session, per packet keys
	Manual distribution of keys – hand typed into each device	Automatic distribution keys
Authentication	Flawed, used WEP key itself for authentication	Strong user authentication, utilizing 802.1x and EAP

Source: (Wi-Fi Alliance, 2003)

## **2.10 Wi-Fi Protected Access 2 (WPA2)**

WPA2 provides a new, encryption scheme, the Advanced Encryption Standard (AES). AES has already been adopted as an official government standard by the U.S. Department of Commerce and the National Institute of Standards and Technology (NIST) (Wi-Fi Alliance, 2003). WPA was designed to secure all versions of 802.11 devices, some of which include 802.11b, 802.11a and 802.11g, multi-band and multi-mode

As a result of the various encryption advantages WPA2 brings, most corporations/enterprises now confidently move to this type of encryption because WPA2 is the next level of security for wireless network.

## **2.11 Elliptic Curve Diffie-Hellman cryptography**

Forecasters predict that in the year 2005, there will be a billion wireless users. This shows that there is a growing need for security. Applications in sectors like healthcare, financial services, government depend on a security platform to safeguard files and data (Lauter, 2004).

The three basic choices for public key systems are available for these applications:

- i. RSA
- ii. Diffie-Hellman (DH) or Digital Signature Algorithm (DSA) modulo a prime  $p$
- iii. Elliptic Curve Diffie-Hellman (ECDH) or Elliptic Curve Digital Signature Algorithm (ECDSA)

Elliptic Curves serves as the proposed basis for discrete logarithm-based cryptosystems over 20 years ago by Victor Miller of IBM and Neal Koblitz of the University of Washington (Lauter, 2004). For the purpose of cryptography, an elliptic curve can be thought of as being given by an affine equation of the form:  $y^2 = x^3 + ax + b$ , where  $a$  and  $b$  are element of a finite field with  $p^n$  elements, where  $p$  is a prime larger than 3.

To implement the Diffie-Hellman Key Exchange with an elliptic curve group, many iterations of the group operation must be performed. Therefore, it is important to optimize the implementation of the group operation. Many approaches have been explored, but choices about how to optimize the elliptic curve group operation often depend on the relative costs of operations such as multiplication and division of elements in the underlying field (Lauter, 2004).

## **CHAPTER THREE**

### **METHODOLOGY**

#### **3.1 Introduction**

The methodology provides the information by which the study's validity is ultimately judged; it also provides detailed explanation on the materials, procedures and methods used in carrying out the project.

System analysis is the study of a business process domain to recommend improvements and specify business requirements and priorities for the solution. It involves detailed study of the organization operation, analysis of the present system and functional requirement of the system.

This chapter analyzed systematically and theoretically the methods applied in carrying out the project, and typically encompass concepts such as paradigms, theoretical models, faces and qualitative techniques.

#### **3.2 Analysis of existing systems**

Quite a number of researches in Wireless network security has been checked before coming with the design. With the migration from wired network to wireless network, a lot of security issues have come up which prompted the need for security measures in this area. In past years, organizations have been making use of only password to secure the data being sent on their network. With the advent in technologies, the use of only password is not efficient in securing the network. Encryption of the wireless network prevents intruders and unauthorized access to the network. With the introduction of various encryption models like Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), Homomorphic encryption, Elliptic Curve Diffie-Hellman encryption etc. Wi-Fi Alliance (2003) explained the

working principles of WEP, the dangers and limitations which WEP exhibits and recommended better encryption for wireless networks which are WPA, WPA2, and Homomorphic encryption.

### **3.3 Approach**

This project was carried out by properly analyzing existing methods of encrypting data shared on a wireless network. Related works were reviewed on the proposed topic and this provided information on new findings in the area of wireless network security. Encryption of data was done using Elliptic Curve Diffie-Hellman encryption.

### **3.4 Data encryption**

Data encryption is the process of encoding data through a series of mathematical functions to prevent unauthorized parties from manipulating it. Its main role is to protect the confidentiality and integrity of the information, even when the encrypted data is in transit over unsecured media such as the Internet.

The main working principle of data encryption is done in such a way that only the recipient can decode the data using the decoding algorithm that is not necessarily secret and an encryption key that is secret. Therefore the use of encryption on data or the entire computer system can act as a protection from unauthorized people. A password has to be keyed in to gain access to the data or computer system and this is made up of characters, numbers, or in an alphanumeric form and the password is issued only to people authorized to use the system and this should be changed frequently to keep the data secure.

### 3.5 Elliptic Curve Diffie-Hellman encryption

It is an anonymous key agreement protocol that allows two parties, each having an elliptic curve public-private key pair, to be able to share secrets over an established insecure channel. This key can either be used as a key directly or can be used to derive another key which in turn can be used to encrypt subsequent communications using symmetric key cipher. This protocol enables parties involved to create a secure channel (<http://www.wikipedia.org>). There are two variants of ECDH, namely ephemeral-ephemeral and ephemeral-static. The ephemeral-ephemeral is anonymous and suffers Man in the Middle (MitM). The following will describe and explain how key establishment is made:

For instance, if Alice wants to establish a shared key with Bob, but the only channel that is available for them maybe eavesdropped by intruders. The domain parameters i.e  $(p, a, b, G, n, h)$  in the prime case or  $(m, f(x), a, b, G, n, h)$  in the binary case must be agreed upon. Each pair must have a key pair that is suitable for elliptic curve cryptography, consisting of a private key  $d$  (a randomly selected integer in the interval  $[1, n - 1]$ ) and a public key  $Q$  (where  $Q = dG$ , that is, the result of adding  $G$  together  $d$  times). Let Alice's key pair be  $(d_A, Q_A)$  and Bob's key pair be  $(d_B, Q_B)$ . Before the execution of the protocol, each party must know the other party's key prior to execution.

Alice computes  $(X_k, Y_k) = d_A Q_B$ . Bob computes  $(X_k, Y_k) = d_B Q_A$ . The shared secret is  $X_k$  (the X coordinate of the point). The shared secret calculated by both parties is equal, because  $d_A Q_B = d_A d_B G = d_B d_A G = d_B Q_A$ . The only information about her private key that Alice initially exposes is her public key. So, no party other than Alice can determine Alice's private key, unless that party can solve the elliptic curve discrete logarithm problem. Bob's private key is similarly

secure. No party other than Alice or Bob can compute the shared secret, unless that party can solve the elliptic Diffie-Hellman problem (Wikipedia, 2015). The Diffie-Hellman key exchange method enables two users that has no knowledge of each other to jointly establish a shared secret key over an insecure channel. This shared key can now be used to encrypt data or subsequent communications using a symmetric key cipher.

### **3.6 Proposed system**

Security with wireless network has become a major concern with corporations and businesses, thereby causing loss of data and also theft and snooping. In the view of this, the proposed system is going to provide high level encryption for the files/data shared on a wireless network. Users in a network trying to send data among themselves must first of all encrypt the data at the sender's side and decrypt the data at the receiver's side in order to view the original data.

### **3.7 Working principle of the Elliptic Curve Diffie-Hellman cryptography**

Alice and Bob aim to exchange information using a public key cryptosystem.

- a. They publicly choose a cyclic group  $G$  and a generator  $x$  of  $G$ .
- b. Alice and Bob choose private keys  $a$  and  $b$  respectively, where  $a$  and  $b$  are random integers.
- c. Alice computes  $x_a$ , Bob computes  $x_b$  and they exchange these values over an insecure network.
- d. On receiving the information from each other, both Alice and Bob compute the a value  $x_{ab}$  using their private keys and the fact that  $x_{ab} = (x_a)^b = (x_b)^a$ .



- ii. Now, both Alice and Bob share a secret, namely, the value  $x_{ab}$ . That is, Alice and Bob have exchanged a key,  $x_{ab}$ , that can now be used in a conventional cryptosystem to encrypt any messages between Alice and Bob.
- iii. If the message was intercepted, the eavesdropper, in order to decipher the message, has to obtain the value  $x_{ab}$  from  $x$ ,  $x_a$  and  $x_b$ . This problem is called the Diffie-Hellman problem. One way to tackle this problem is to try to compute  $a$  from  $x_a$ . This is known as the discrete logarithm problem.

Below are few facts about elliptic curves:

Given an elliptic curve  $E$  and a field  $F_q$ , we consider the rational points  $E(F_q)$  of the form  $(x,y)$  where both  $x$  and  $y$  belong to  $F_q$ . We choose the point at infinity to be  $\sigma$ .

- i. Define the operation “+” on the set of rational points of  $E$  as follows. If  $P$  and  $Q$  are two rational points on  $E$ , then  $P+Q$  is given by the following rule: Draw the line joining  $P$  and  $Q$ , take the third point of intersection of this line with the curve as  $R$ . Draw the line through  $\sigma$  and  $R$ , and take the third point of intersection of this line with  $E$ . This point is the point  $P+Q$ . Note the operation “+” is commutative. In particular we have,  $\sigma + \sigma = \sigma$  and  $P + (-P) = \sigma$ .
- ii. Define the operation “\*” as follows  $*$  :  $\mathbb{Z} \times E(F_q) \rightarrow E(F_q)$  and if  $P$  is some point in  $E(F_q)$ , then we define  $n*P$  as  $P+P+P+\dots+P$ ,  $n$  times. Note that for integers  $j$  and  $k$ ,  $j*(k*P) = (j*k)*P = k*(j*P)$ .
- iii. The set of rational points on  $E$  form an abelian group under the operation “+” with identity  $\sigma$ .

Definition: The elliptic curve discrete logarithm problem (ECDLP) is to determine the integer  $k$ , given rational points  $P$  and  $Q$  on  $E$ , and given that  $k \cdot P = Q$ .

### 3.8 Methodologies and design

There are five major development methodologies; the waterfall method, the parallel development method, the phased development method, system prototyping and design prototyping. The design model that would be preferred for this project is the waterfall model. This is primarily because this model prescribes a systematic approach to software development which starts with a well-defined, understood specification of requirements and moves through to deployment in a linear form. The waterfall model goes through the following process

- a. **Communication:** This basically involves requirement gathering which requires a great deal of interaction/communication and collaboration between the customers and the software developers.
- b. **Planning:** This is the area where the overall plan for the engineering work that follows is developed and established. This plan involves the technical tasks and tools or resources, the likely risks, and the work schedule for the software project
- c. **Modelling (Analysis and design):** This is both analysis and design which entails the creation of models for proper understanding of the requirements and how to best achieve the requirements.
- d. **Construction:** This is the development aspect which consists of coding and testing to uncover possible errors

- e. **Deployment:** The software is delivered as a complete product or in partial increment to the customer who evaluates and provides feedback based on the evaluation

The activity diagram is shown below in figure 3.1

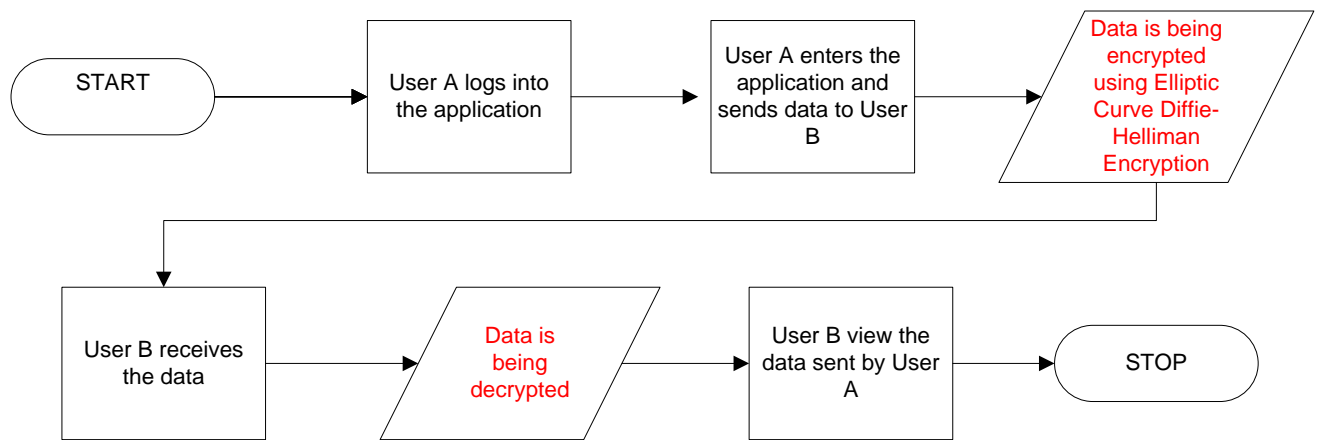


Figure 3.1: Activity diagram

### **3.9 System design**

After the requirements were gathered, the design of the system was created using UML (Unified Modelling Language). The UML was used to visualize the system under development.

C# dotnet Framework was used to build the interface to implement the project. C# is an elegant and type-safe object-oriented language that enables developers to build a variety of secure and robust applications that run on the .NET Framework. You can use C# to create Windows client applications, XML Web services, distributed components, client-server applications, database applications, and much, much more. Visual C# provides an advanced code editor, convenient user interface designers, integrated debugger, and many other tools to make it easier to develop applications based on the C# language and the .NET Framework.

C# makes it easy to develop software components through several innovative language constructs, including the following:

- i. Encapsulated method signatures called delegates, which enable type-safe event notifications.
- ii. Properties, which serve as accessors for private member variables.
- iii. Attributes, which provide declarative metadata about types at run time.
- iv. Inline XML documentation comments.
- v. Language-Integrated Query (LINQ) which provides built-in query capabilities across a variety of data sources.

### **3.10 System requirement specification**

#### **3.10.1 Software requirement**

In the development of this application, the following software requirements have been considered and specified.

##### **Development end:**

- a) Operating system: Windows 7 (32 or 64 bits), Windows 8
- b) Languages: c#.net
- c) Tools: Visual Studio 2013 (Dev. tool)
- d) Debugger: Visual Studio 2013 debugger

##### **Application end:**

Framework: Microsoft dotnet framework

#### **3.10.2 Hardware requirement**

- i. Processor: Pentium IV or higher
- ii. RAM: 256 MB or higher
- iii. Disk space: 250 MB or higher

## **CHAPTER FOUR**

### **RESULT AND DISCUSSION**

#### **4.1 Overview**

This chapter entails the phases and steps encountered during the execution of the project. Also the final software/output is compared with the intended project and the reasons for alterations are specified. The main objective of the Encryption application is to provide an easy to use interface for sending and receiving encrypted files via a wireless network.

As it is with every software development process, stages were involved in developing the application, stages which include: Problem Definition, Program Design, Coding, Debugging, Testing, and Documentation.

#### **4.2 Implementation**

The major processes involved are as follows

SENDER END:

- i. “Browse and load file/document”
- ii. “Select the destination system”
- iii. “Set password (optional)”
- iv. “Encrypt and Send”.

RECEIVER END:

- i. “Browse for encrypted file/document”
- ii. “Select encrypted file/document”
- iii. “Decrypt the Encrypted file/document
- iv. View the Decrypted file

### **4.3 Overview of application**

The figure 4.1 shows the pictorial overview of the application.





Figure 4.1: Overview of the encryption software

This application consists of two sides, namely: The Receiver End and The Sender End. This application enables the user to send and receive encrypted data over a wireless network and also decrypt encrypted files. This application allows for the specification of destination systems and enables data to contain password before being encrypted and sent over the network.

#### **4.4 The “Browse For File” button**

This button is used to locate files/documents that the user intends to encrypt and send. Any document that has been previously saved on the system can be located via the “Browse For File” button. The picture diagram is shown in figure 4.2 below.

#### **4.5 The “Send To” drop-down box**

This drop-down box contains the list of all computer systems or devices connected on the mutual network. The drop-down box also contains ‘localhost’ which makes it possible for the software to act as both a stand-alone application and also a multi-user application. The textbox below the drop-box allows the user to manually type in the preferred network ID he/she intends to send files/documents to.

#### **4.6 The “Password File” Checkbox**

This checkbox enables the user to password the encrypted file/document to be sent to a recipient. This gives an extra security to the file/document to be sent.

#### **4.7 The “Send File” button**

With the click of this button, it automatically encrypts the document/file using the elliptic Curve Diffie-Hellman Encryption and sends the encrypted file to the recipient. Without the click of this button, the recipient will not be able to receive the file.

#### **4.8 The “Browse For File” button (at the receiver’s end)**

This button enables the recipient to view the encrypted file being received. Before the click of this button, a voice notification is received indicating the arrival of a new encrypted file/document.

#### **4.9 Process train of how a file is encrypted, sent and decrypted from the sender and receiver’s end respectively**

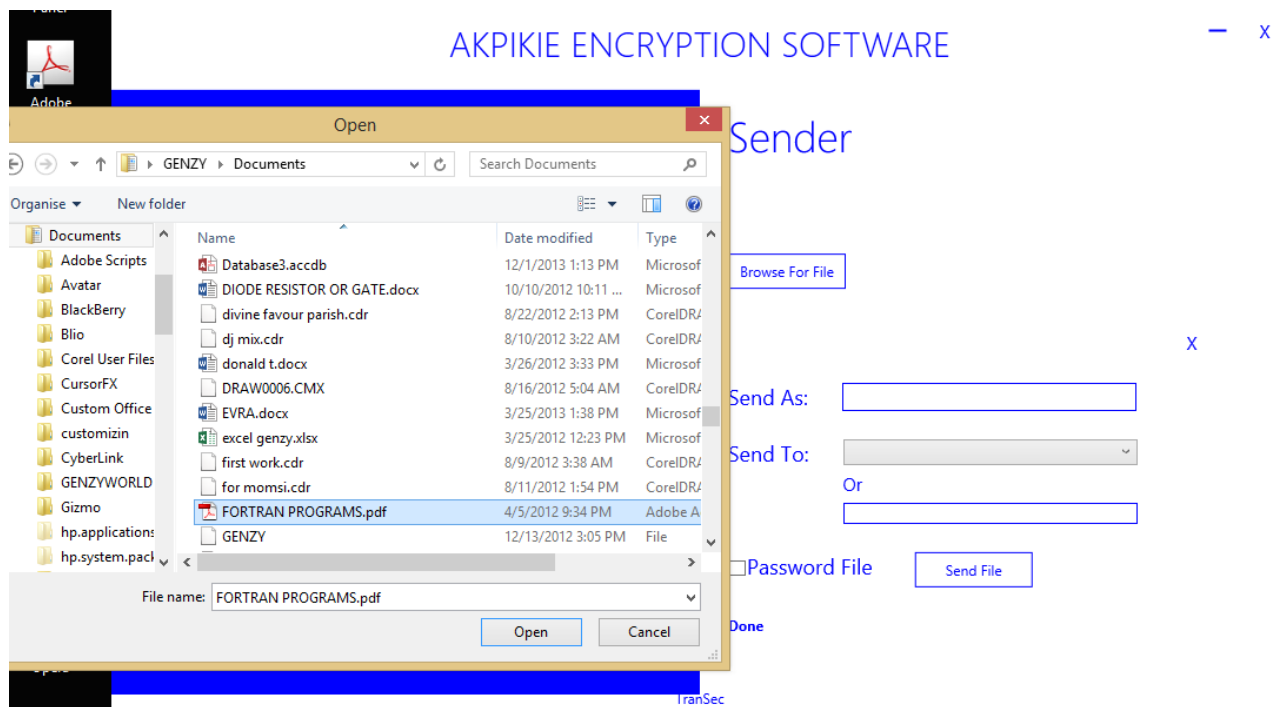


Figure 4.2: File selection

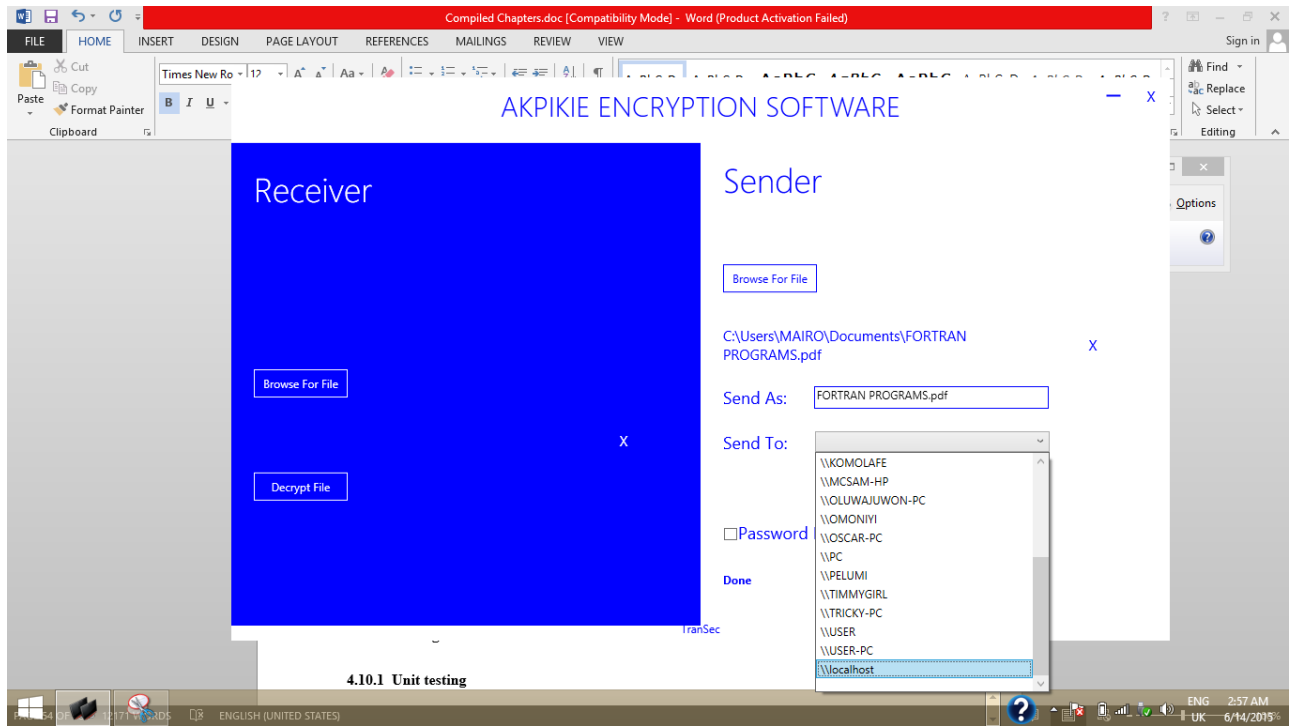


Figure 4.3: Selecting recipient

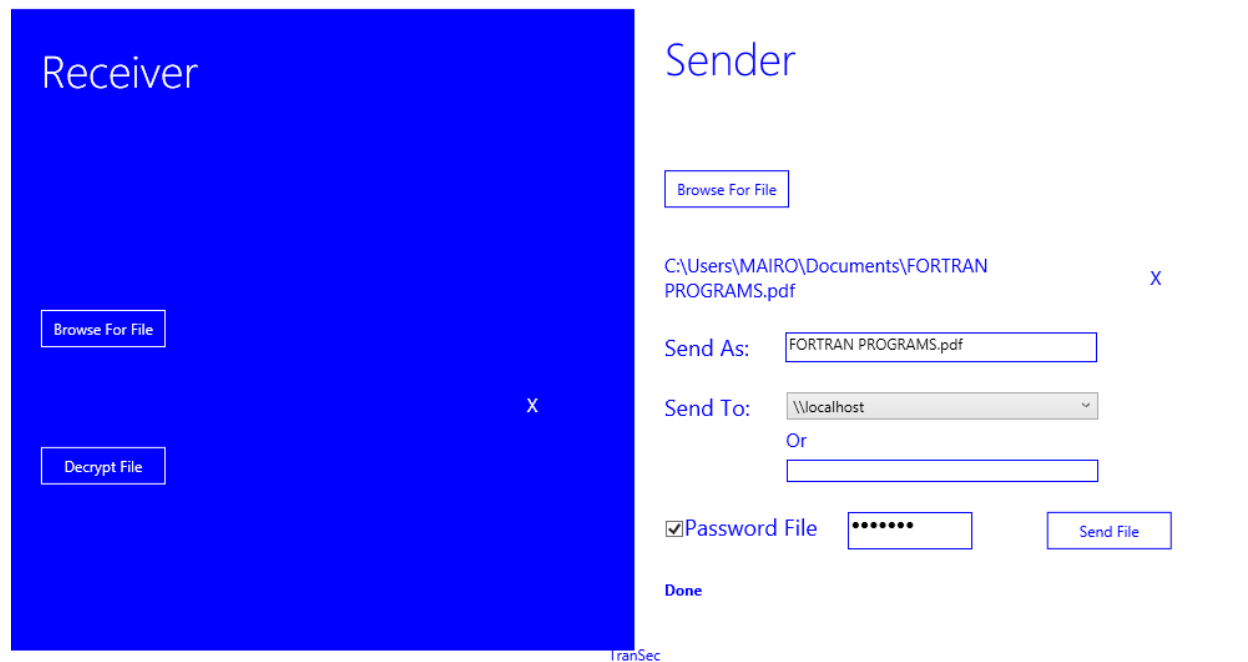


Figure 4.4: Password setting to selected file

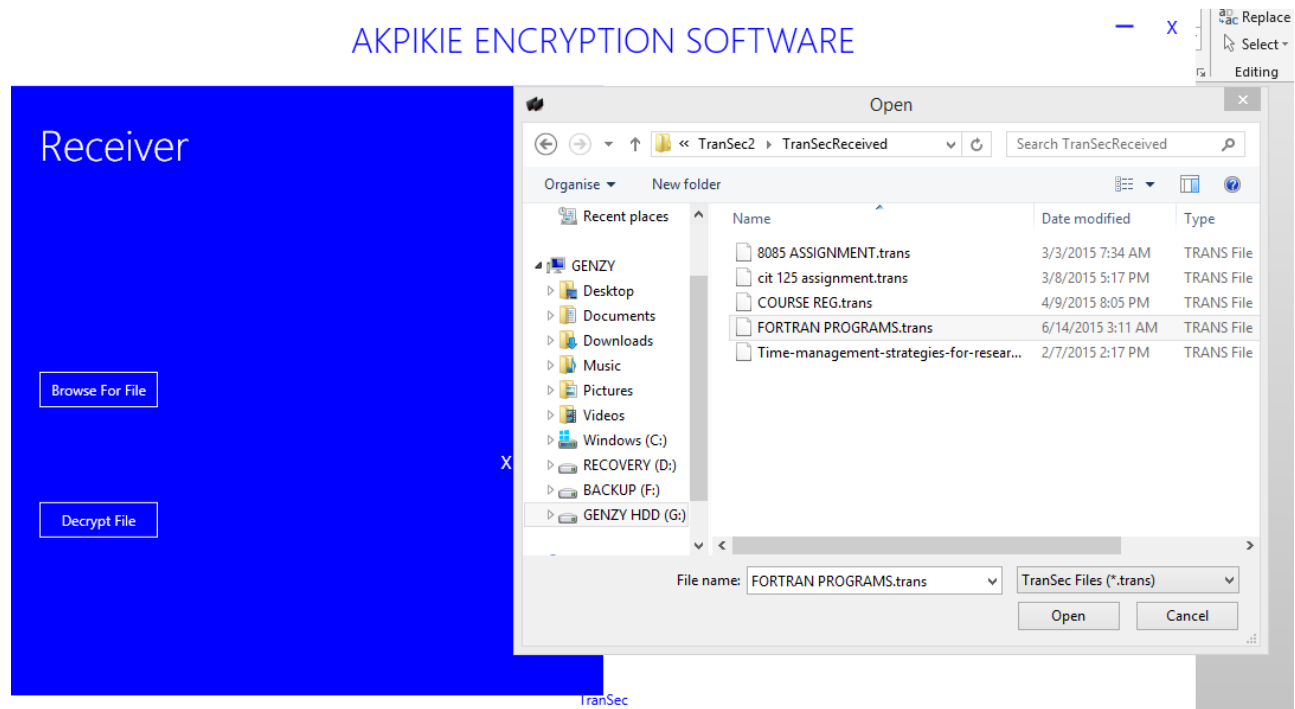


Figure 4.5: Browse for received encrypted file

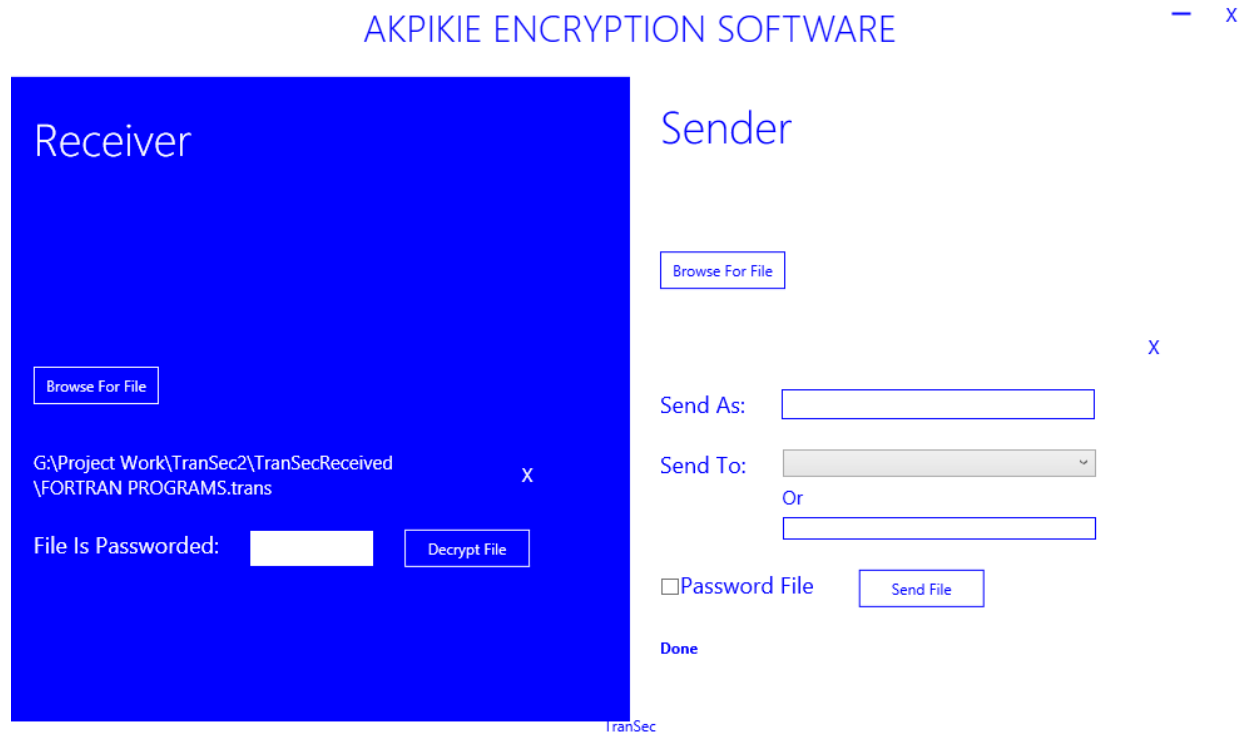


Figure 4.6: Enter password for received encrypted file

(This password must be shared by the sender and receiver ONLY. Without typing the correct password, the file cannot be decrypted. )



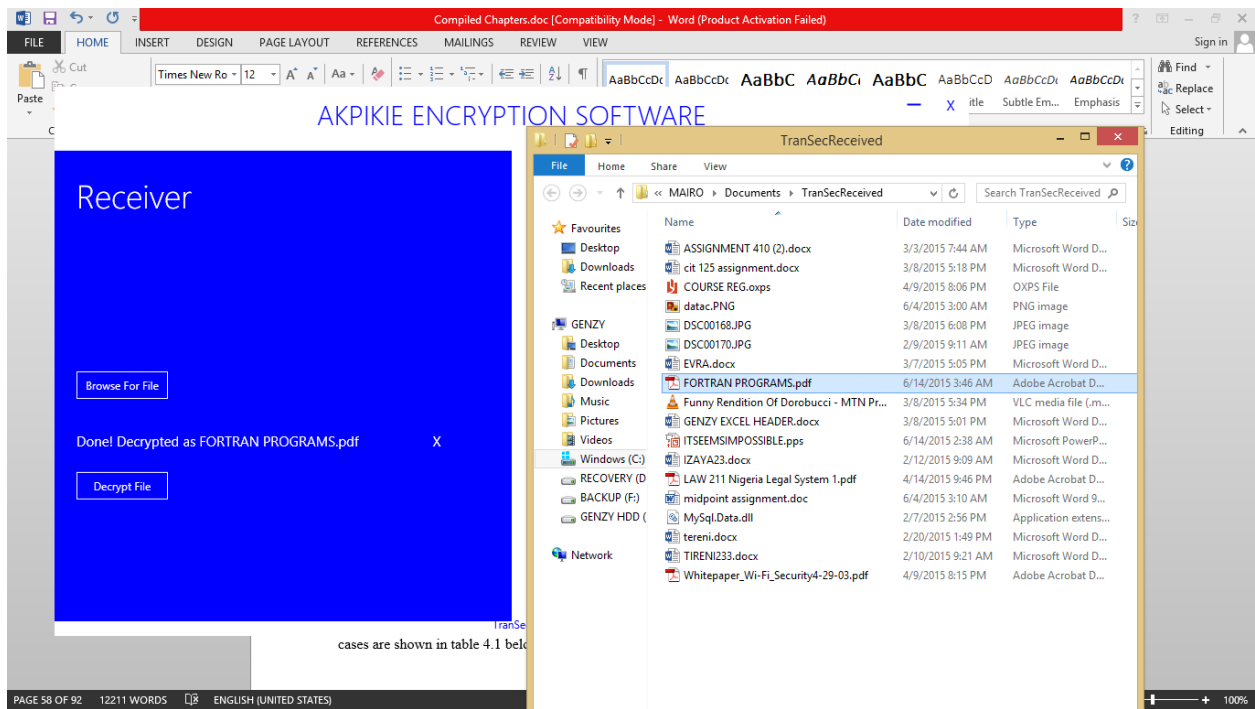
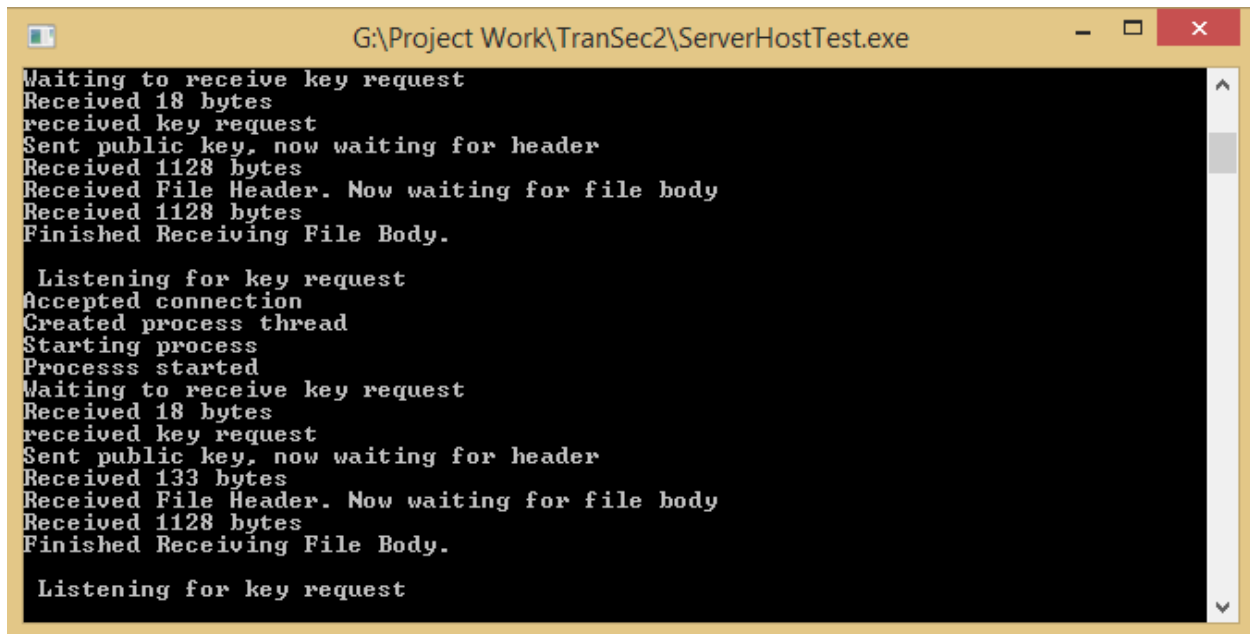


Figure 4.7: Decrypted file



```
G:\Project Work\TranSec2\ServerHostTest.exe
Waiting to receive key request
Received 18 bytes
received key request
Sent public key, now waiting for header
Received 1128 bytes
Received File Header. Now waiting for file body
Received 1128 bytes
Finished Receiving File Body.

Listening for key request
Accepted connection
Created process thread
Starting process
Processs started
Waiting to receive key request
Received 18 bytes
received key request
Sent public key, now waiting for header
Received 133 bytes
Received File Header. Now waiting for file body
Received 1128 bytes
Finished Receiving File Body.

Listening for key request
```

Figure 4.8: Back-end activities via command prompt

## **4.10 Testing**

### **4.10.1 Unit testing**

In Unit testing, each module of the application is tested separately and individually and the result is duly noted. Unit testing is done manually to find bugs and to test the functionality of the application. The manual unit testing was done using the windows 7 and 8.1 platforms. The test cases are shown in table 4.1 below:

Table 4.3: Unit testing table

S/NO	Sender's end	Test case	Expected result	Result
1	"Browse For File" button	Click the "Browse For File" button	Open document folder to allow for file selection	Pass
2	"Send To" Drop-down box	Click the drop-down box	Box displays a list of systems or devices connected to that network	Pass
3	"Send To" Text box	Manually enter the system's network ID	The application accepts the valid destination system's ID as an alternative to the "Send To" Drop-down box	Pass
4	"Password File" Checkbox	Select the checkbox	With the selection of the checkbox, it automatically shows a textbox which enables the user to enter a set of characters to secure the file that had been selected.	Pass
5	"Send File" button	Click the "Send File"	It sends the encrypted file/document to the	Pass

			recipient of the document	
<b>S/NO</b>	<b>Receiver's end</b>	<b>Test case</b>	<b>Expected result</b>	<b>Result</b>
1	"Browse For File" button	Click the button	The button opens the file in which the received encrypted documents are kept	Pass
2	"Decrypt File" button	Click the button	With the click of the button, the received encrypted document will be decrypted using the Elliptic Curve Diffie-Hellman decryption algorithm and automatically displays the decrypted document	Pass

This table shows that the application is running effectively and correctly. Each feature of the application has been tested and this result shows that each of those features are functioning effectively.

## **CHAPTER FIVE**

### **CONCLUSION AND RECOMMENDATION**

#### **5.1 Summary**

In this project, application for data encryption and decryption was developed from reviewing relevant literatures and because applications like this are not used by most companies and organizations worldwide.

Looking at the need for data/information security in our modern world, the need for an application that can encrypt relevant data and send to authorized recipient cannot be over emphasized. Therefore, the application was designed considering efficiency, satisfaction, simplicity and security.

This application was designed to work on multiple systems via a wireless network. It can also serve as a stand-alone application when testing is required on one system only.

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

#### **5.2 Contribution to knowledge**

This study will aid massive security improvement in the protection of data/information being sent in an organization, company, Government institution, military, etc.

Along with, evolving user/organizational/institutional etc. demands will fuel the ongoing development of data encryption system already involved, and encourage creative ideas about delivering services with a whole new scope and perspective.

This project identified opportunities for future development of a more robust encryption system for the transfer of data in an organization.

### **5.3 Recommendation**

The advancement in technology has increased the necessity for files and data to be kept safe and secured from unauthorized people. Most companies and organizations constantly search for a better and more secure way to send and receive data in their various organizations.

This application is highly for organizations of any type, especially Bowen University.

Sensitive files, documents etc. must be protected by multi-level password/encryption software in such a way that no unauthorized individual has access to the file/document being sent across the wireless network.

General laxity on the part of the user should be checked to ensure better security of computerized data.

This application will help to secure internal exchange of important information between staffs as well as staff and students.

### **5.4 Conclusion**

The availability of encryption software of this type, that can send and receive files over a wireless network, has reduced the vulnerability of sensitive files in an organization. In the nearest future, the percentage of wireless users would have raised, this implies that the need for a secure medium to send and receive data over a wireless network would increase. This project was aimed at providing a well secured application for individuals, organizations, schools etc.

## **5.5 Suggestions for future study**

This study covered developing an application that can encrypt and decrypt files using the Elliptic Curve Diffie-Hellman cryptography. However for future studies, users should not only be able to type in password to secure the encrypted file to be sent, it also should be able to accept other forms of added security such as optical recognition, facial recognition etc. The application of this sort should also be incorporated to a mobile application; this will aid a secure exchange of file between a mobile phone and a computer system via a wireless network.



## REFERENCE

- Abdel-Karim, R., Tamimi, AI. (2006). *Security in Wireless Data Networks: A Survey Paper*
- Boncella, R. J. (2002). *Wireless Security (9th ed.)*. Atlanta, NY:
- Corporation, S. (2002). *Wireless LAN Security*. USA: Author.
- Dorothy, E. Denning and Peter, J. Denning *Data Security* accessed June 2015
- Dr. Singh, G. (2012). *Security Issues in Wireless Local Area Network (WLAN)*
- Enge, A. (1999). *Elliptic Curve and their Application to Cryptography; an Introduction*
- Lauter, K. (2004). *The Advantages of Elliptic Curve Cryptography for Wireless Security*. UK: Microsoft Corporation
- Manikandan, J., Vijayaragavan, S. (2010). *Multihost ad-hoc Network with the clustered Security Networks*
- Neils, P. and Peter, H. (2003) “*Hide and Seek: An Introduction to Steganography*” IEEE Trans. Security and Privacy, MAY/JUNE 2003, 1540-7993
- Panduranga H.T., Naveen Kumar S.K (2010) / (IJCSSE) *International Journal on Computer Science and Engineering* Vol. 02, No. 02, 2010, 297-300
- Retrieved 13/04/15 [http://en.wikipedia.org/wiki/Elliptic\\_curve\\_Diffie-Hellman/](http://en.wikipedia.org/wiki/Elliptic_curve_Diffie-Hellman/)
- Wi-Fi Alliance. (2003). *Wi-Fi Protected Access: Strong, Standard-based, Interoperable Security for today's Wi-Fi Networks*
- Graham, E., Steinbart, P.J. (2006) *Wireless Security*

CSI. (2004). *CSI/FBI Computer Crime and Security Survey*.

Hopper, D. I.(2002). *Secret Service agents probe wireless networks in Washington*.

Kelley, D. (2003). *The X factor: 802.1x may be just what you need to stop intruders from accessing your network*. Information Security, 6(8), 60-69.

Kennedy, S. (2004). *Best practices for wireless network security*. Information Systems Control Journal (3).

McDougall, P. (2004, March 25). Laptop theft puts GMAC customers' data at risk. Information Week Security Pipeline.

Nokia. (2003). Man-in-the-middle attacks in tunneled authentication protocols.

Paladugu, V., Cherukuru, N., & Pandula, S. (2001). *Comparison of security protocols for wireless communications*.

Slashdot. (2002, August 18). Wardriving from 1500ft Up.

Stoneburner, G., Goguen, A., & Feringa, A. (2002, July). *Risk management guide for information technology systems*. NIST Special Publication 800-30.

Wailgum, T. (2004, September 15). *Living in wireless denial*. CIO Magazine.

## Appendix

// Server host test

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;

namespace ServerHostTest
{
    class Program
    {
        static void Main(string[] args)
        {
            Console.WriteLine("Starting up Server");
            TranSecServer.Listener listener = new TranSecServer.Listener();
            listener.Start();

            Console.Read();
            listener.StopListening();
        }
    }
}
```

// Listener

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Net;
using System.Net.Sockets;
using System.Threading;
using System.Threading.Tasks;
using System.IO;
using System.Diagnostics;
namespace TranSecServer
{
    public static class BinaryWriterExtension
    {
        public static void WriteString(this BinaryWriter writer, string data)
        {
            byte[] stringBuffer = Encoding.ASCII.GetBytes(data);

            writer.Write(stringBuffer.Length);
            writer.Write(stringBuffer);
        }
    }
    public static class BinaryReaderExtension
```

```

{
    public static string ReadByteString(this BinaryReader reader, int byteLength)
    {
        byte[] rawBytes = reader.ReadBytes(byteLength);
        return Encoding.ASCII.GetString(rawBytes);
    }
}

public class Listener
{
    TcpListener receiver;
    bool listening = true;
    Task listenerTask;

    /* public readonly string DATA_STORE_FOLDER =
        Environment.GetFolderPath(Environment.SpecialFolder.MyDocuments)+"\\"+
        "TranSecReceived";
    */

    public readonly string DATA_STORE_FOLDER =
        System.Reflection.Assembly.GetExecutingAssembly().Location.Substring(0,
            System.Reflection.Assembly.GetExecutingAssembly().Location.LastIndexOf('\\'))
        +"\\TranSecReceived";

    public void Start()
    {
        try
        {
            listenerTask = Task.Factory.StartNew(Listen,
                TaskCreationOptions.LongRunning);
        } catch (Exception ex)
        {
            LogException(ex);
        }
    }

    public void Listen()
    {
        try
        {
            SocketPermission permission = new
            SocketPermission(System.Security.Permissions.PermissionState.None);
            permission.AddPermission(NetworkAccess.Accept, TransportType.Tcp, "",
            25000);
            permission.AddPermission(NetworkAccess.Connect, TransportType.Tcp, "",
            25000);

            permission.Demand();
            permission.Assert();
        }
        catch (Exception ex)
        {
            LogException(ex);
        }
    }
}

```

```

    /* IPEndPoint endPoint = new IPEndPoint(localentry.AddressList.Where(addr =>
    addy.AddressFamily == AddressFamily.InterNetwork).First(), 25000);
    */
    receiver = new TcpListener(IPAddress.Any, 25000);

    receiver.Start(5);
    Console.WriteLine("Listening for any address on port 25000");
    // LogString("Listening for any address on port 25000");

    while(listening)
    {
        Socket receptor=receiver.AcceptSocket();
        LogString("Accepted connection");
        // System.Diagnostics.Debugger.Launch();
        Thread callback = new Thread(new
        ParameterizedThreadStart(AcceptCallback));
        LogString("Created process thread");
        callback.Start(receptor);
    }
}

void AcceptCallback(object parameter)
{
    try
    {
        LogString("Starting process");
        Socket receptor = (Socket)parameter;
        int receiveLoop = 0;
        string fileSinkPath = "";
        //continue from here
        ReceivingFlag recFlag = ReceivingFlag.DishOutPublicKey;
        LogString("Processs started");
        while (true)
        {
            byte[] buffer = new byte[1128];
            LogString("Waiting to receive key request");

            int noOfBytes = receptor.Receive(buffer);
            LogString("Received " + noOfBytes + " bytes");
            LogString("Key request received");
            if (recFlag == ReceivingFlag.DishOutPublicKey)
            {
                string forefront = Encoding.ASCII.GetString(buffer, 0,
noOfBytes);

                //LogString("On first reception: " + forefront);
                LogString("received key request");
                if (forefront != RequestType.KEY_REQUEST)
                {
                    receptor.Shutdown(SocketShutdown.Both);
                    receptor.Close();

                    break;
                }
            }
            KeyHandler.SendPublicKey(receptor);
        }
    }
}

```

```

        LogString("Sent public key");
        recFlag = ReceivingFlag.WaitingForHeader;
    }
    else if (recFlag == ReceivingFlag.WaitingForHeader)
    {
        byte[] header = new byte[noOfBytes];
        Array.Copy(buffer, header, noOfBytes);
        MemoryStream ms = new MemoryStream(header);
        ms.Seek(0, SeekOrigin.Begin);
        BinaryReader reader = new BinaryReader(ms);
        string forefront = reader.ReadByteString(reader.ReadInt32());
        if (forefront != RequestType.INCOMING_DATA_HEADER)
        {
            receptor.Shutdown(SocketShutdown.Both);
            receptor.Close();
            break;
        }
        // Thread.Sleep(2000);
        ReceiveDataHeader(receptor, ref receiveLoop, ref recFlag, buffer,
ref noOfBytes, ref header, ref ms, ref reader, ref fileSinkPath);
        LogString("Received File Header. Now waiting for file body");
    }
    else if (recFlag == ReceivingFlag.WaitingForData)
    {
        DownloadFile(receptor, receiveLoop, fileSinkPath, buffer,
noOfBytes);

        recFlag = ReceivingFlag.DishOutPublicKey;
        LogString("Finished Receiving File Body. \n\n Listening for key
request");

        break;
    }
}
}
}
catch (System.Net.Sockets.SocketException sock)
{
    Console.WriteLine(sock.Message + "\n\n" + sock.StackTrace);
    LogException(sock);
}
catch (System.Security.SecurityException sec)
{
    Console.WriteLine(sec.Message + "\n\n" + sec.StackTrace);
    LogException(sec);
}
catch (Exception ex)
{
    Console.WriteLine(ex.Message + "\n\n" + ex.StackTrace);
    LogException(ex);
}

}

private void LogException(Exception ex)
{
    LogString(ex.Message);
    string
errorLog=Environment.GetFolderPath(Environment.SpecialFolder.MyDocuments)
+"\TransSecListenerErrors";

```

```

        if(!Directory.Exists(errorLog))
        {
            Directory.CreateDirectory(errorLog);
            File.Create(errorLog + "\\error.log").Close();
        }
        StreamWriter writer = new StreamWriter(errorLog + "\\error.log");
        writer.BaseStream.Seek(0, SeekOrigin.End);

        writer.WriteLine();
        writer.WriteLine();
        writer.WriteLine( DateTime.Now.ToString() );
        writer.WriteLine();
        writer.WriteLine();
        writer.WriteLine("-----");
        writer.WriteLine();
        writer.WriteLine();
        writer.WriteLine(ex.Message);
        writer.WriteLine();
        writer.WriteLine();
        writer.WriteLine(ex.StackTrace);
        writer.Close();
    }

    private void LogString(string message)
    {
        // eventlog.WriteEntry(message);
        Console.WriteLine(message);

        File.AppendAllText(Environment.GetFolderPath(Environment.SpecialFolder.MyDocuments) +
            "\\TransSecListenerErrors" + "\\messages.txt",message);
    }

    private static void DownloadFile(Socket receptor, int receiveLoop, string
fileSinkPath, byte[] buffer, int noOfBytes)
    {
        FileStream trnFile = File.Open(fileSinkPath, FileMode.Open);
        trnFile.Seek(0, SeekOrigin.End);
        //do it once for sync purposes before looping
        trnFile.Write(buffer, 0, noOfBytes);
        for (int i = 0; i < (receiveLoop-1); i++)
        {
            noOfBytes = receptor.Receive(buffer);
            trnFile.Write(buffer, 0, noOfBytes);
        }
        trnFile.Flush();
        trnFile.Close();
        receptor.Shutdown(SocketShutdown.Both);
        receptor.Close();
    }

    private void ReceiveDataHeader(Socket receptor, ref int receiveLoop, ref
ReceivingFlag recFlag, byte[] buffer, ref int noOfBytes, ref byte[] header, ref
MemoryStream ms, ref BinaryReader reader,ref string fileSinkPath)
    {

```

```

        string fileName = reader.ReadByteString(reader.ReadInt32());
        //create file with custom extension
        if (!Directory.Exists(DATA_STORE_FOLDER))
        {
            Directory.CreateDirectory(DATA_STORE_FOLDER);
        }
        FileStream trnFile = File.Create(DATA_STORE_FOLDER + "\\ " +
RemoveFileExtension(fileName) + ".trans");
        fileSinkPath = DATA_STORE_FOLDER + "\\ " + RemoveFileExtension(fileName) +
".trans";
        int pwdLength = reader.ReadInt32();
        BinaryWriter headerWriter = new BinaryWriter(trnFile);
        headerWriter.WriteString(fileName);
        string pwd = reader.ReadByteString(pwdLength);
        headerWriter.WriteString(pwd);
        byte[] senderPubKeyRaw = reader.ReadBytes(reader.ReadInt32());
        headerWriter.Write(senderPubKeyRaw.Length);
        headerWriter.Write(senderPubKeyRaw);

        receiveLoop = reader.ReadInt32();

        reader.Close();
        headerWriter.Close();
        ms.Close();

        recFlag = ReceivingFlag.WaitingForData;
    }

    string RemoveFileExtension(string fileName)
    {
        return fileName.Substring(0, fileName.LastIndexOf('.'));
    }

    public void StopListening()
    {
        listening = false;
        receiver.Stop();
    }
}

```