

**BINDURA UNIVERSITY OF SCIENCE EDUCATION**

**FACULTY OF SCIENCE AND ENGINEERING**

**DEPARTMENT OF COMPUTER SCIENCE**



**POINT-TO-POINT MULTI-LAYERED  
CRYPTOGRAPHY SYSTEM BASED ON RSA & CHAOS  
SYNCHRONISATION**

**By VINCENT KAPIKINYU**

**SUPERVISOR: MR MATOMBO**

*A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF  
THE REQUIREMENTS FOR THE BACHELOR OF SCIENCE HONOURS  
DEGREE IN INFORMATION TECHNOLOGY-NETWORK ENGINEERING*

**2022**

## Approval Form

The undersigned certify that they have supervised the student **VINCENT KAPIKINYU** in the research dissertation entitled, “**Point-To-Point Multi-Layered Cryptography System Based On RSA & Chaos Synchronization**” submitted in partial fulfilment of the requirements for a Bachelor of Science Honors Degree in Information Technology at Bindura University of Science Education.

**STUDENT:**

**DATE:**

.....

.....

**SUPERVISOR:**

**DATE:**

.....

.....

**CHAIRPERSON:**

**DATE:**

.....

.....

**EXTERNAL EXAMINER:**

**DATE:**

.....

.....

## **Abstract**

The communication between communication links/branches of different organizations are prone to hacks and loss of sensitive information since the issues of confidentiality, authentication and privacy for in transit network traffic are not being adhered to as they should be (Fernando, 2021). The confidential data that is being transferred between branches is exposed to hacks and other security threats. The first objective was to analyze different techniques used to encrypt data and distribute keys efficiently for data in transit. The second objective was to design and implement a model which encrypts data in transit between two links using RSA algorithm, P2PE and chaos synchronization. The last objective was to benchmark test and evaluate the effectiveness and efficiency of RSA algorithm, P2PE and chaos synchronization in encryption. As seen from chapter 4 ,the author managed to develop the multi-layered encryption system using chaos synchronization for key distribution in a simulated environment using C# and try to intercept the connection using Wireshark. The system was evaluated in terms of encryption strength, key length and speed of delivery. Therefore, all the three objectives were achieved. The author evaluated the simulation solution and achieved satisfactory results. The system was tested using white and black box and also the encryption key length was used as a measure of performance. The proposed solution can create long key up to 256 bits depending on the data which needs to be transferred. The author tested the traffic of the tunnel using Wireshark and modelled how data is transferred between two links.

## **Acknowledgements**

I would like to extend my gratitude and sincere thanks to my supervisor Mr Chikwiro for his constant motivation and support during the course of my work. I truly appreciate and value his esteemed guidance and encouragement from the beginning. I also want to thank Mr Matombo, Mr. Chaka for their co-supervision, I really appreciate all the time and efforts they put with the bid of helping me to come up with a quality research. Furthermore, I would like to mention my father, who made this all possible and also played a supporting role which contributed positively to my welfare.

## Contents

<b>Abstract</b> .....	3
<b>Acknowledgements</b> .....	4
<b>CHAPTER 1: PROBLEM IDENTIFICATION</b> .....	7
<b>1.1 Introduction</b> .....	7
<b>1.2 Background</b> .....	7
<b>1.3 Problem Statement</b> .....	9
<b>1.4 Research Aim</b> .....	9
<b>1.5 Objectives</b> .....	9
<b>1.6 Research Questions</b> .....	9
<b>1.7 Significance Of The Study</b> .....	9
<b>1.8 Scope Of The Study</b> .....	10
<b>1.9 Limitations</b> .....	10
<b>1.10 Definition Of Terms</b> .....	10
<b>CHAPTER 2: LITERATURE REVIEW</b> .....	11
<b>2.1 Introduction</b> .....	11
<b>2.2 Cyber Crime</b> .....	11
<b>2.3 Data Breaches</b> .....	11
<b>2.4 Causes of Data Breach</b> .....	12
<b>2.5 Effects of Data Breaches</b> .....	13
<b>2.6 The RSA algorithm</b> .....	15
<b>2.7 Encryption Key Distribution Via Chaos Synchronization</b> .....	16
<b>2.7 Review Of Related Literature</b> .....	16
<b>2.9 Chapter Summary</b> .....	18
<b>CHAPTER 3: METHODOLOGY</b> .....	19
<b>3.0 Introduction</b> .....	19
<b>3.1 Research Design</b> .....	19
<b>3.2 Requirements Analysis</b> .....	19
<b>3.2.1 Functional Requirements</b> .....	20
<b>3.2.2 Non-Functional Requirements</b> .....	20
<b>3.2.3 Hardware Requirements</b> .....	20
<b>3.2.4 Software Requirements</b> .....	20
<b>3.3 System Development</b> .....	21

3.3.1 System Development tools .....	21
3.3.2 Prototyping .....	21
3.4 Summary of how the system works .....	21
3.5 System Design.....	21
3.5.1 System Dataflow diagrams (DFDs).....	21
3.5.2 Proposed System flow chart .....	22
.....	23
3.6 Data collection methods.....	23
3.7 Implementation .....	23
3.8 Conclusion .....	25
<b>CHAPTER 4: DATA ANALYSIS AND INTERPRETATIONS .....</b>	<b>25</b>
4.0 Introduction.....	25
4.1 Testing.....	26
4.1.2 Black box Testing.....	26
4.1.2 White box testing.....	28
4.2 Evaluation Measures and Results.....	29
4.2.1 Encryption Key Length .....	29
4.6 Summary of Research Findings.....	31
4.7 Conclusion .....	31
<b>CHAPTER 5: CONCLUSION AND RECOMMENDATIONS .....</b>	<b>32</b>
5.1 Introduction.....	32
5.2 Aims & Objectives Realization .....	32
5.3 Major Conclusions Drawn .....	32
5.3 Recommendations & Future Work.....	33
References.....	33

# **CHAPTER 1: PROBLEM IDENTIFICATION**

## **1.1 Introduction**

As our daily activities become more and more reliant upon data networks, the importance of an understanding of such security issues .The spectacular growth of the internet has caused an increase in the awareness and interest in security issues. will only increase. Point-to-point encryption (P2PE) is a process of securely encrypting a signal or transacted data through a designated "tunnel." According to Muhamed and Bujar (2020), Point-to-Point Encryption provide organizations with a secure method for transmitting sensitive data. This technology renders information unreadable during transit, with the data only legible once safely decrypted at its destination. This process removes the valuable target of in-the-clear data, giving no incentive for unauthorized individuals to tap into your lines of communication. With applications for all industries that need to securely receive, transmit, and process data, P2PE provides the versatility to integrate directly into your existing system with an additional layer of security for your sensitive data. The coupling of P2PE and RSA algorithm encrypts data by using a tunnel between two end points. In this way, it is possible to browse and transfer data safely, and securely over a public network.

Most organizations make use of the internet in their day-to-day activities. The goal of this research project is to design and implement a secure site to site links using P2PE and Chaos Synchronization so that the data can be transported back and forth securely over a non-secure public network infrastructure that is the internet.

## **1.2 Background**

According to Al-Maadeed et al., (2012), the basic principle of encryption with chaos is based on the ability of some dynamic systems to produce sequence of numbers that are random in nature. This sequence is used to encrypt messages. For decryption, the sequence of random numbers is highly dependent on the initial condition used for generating this sequence. A very minute deviation in the initial condition will result in a totally different sequence. This sensitivity to initial condition makes chaotic systems ideal for encryption. The development of new strategies to protect sensitive information from interception and eavesdropping has been receiving significant attention, especially in our present-day worldwide communication networks (Keuninckx et al, 2017). The development and implementation of a novel random key

distribution system based on the concept of generalized synchronization between distant elements in large networks is a major step in cloud security. Such a random key synchronization system successfully realized in photonics would have significant impact in the field of physical layer based encryption techniques, offering not only high confidentiality but also potential high-speed real-time encryption and decryption. Implemented in photonic systems, it would be fully compatible with present and future telecommunication networks (Keuninckx et al, 2017).

Key Public Cryptography(KPC) works on the concept of dual keys. While the recipients' public key is used to encrypt the message, the private key is used for decryption, so there is no need to share a secret key as required in secret key (symmetric) cryptography (Anderson, 2017). PKC is largely used for authentication, non-repudiation, and key exchange (Nisha & Farik, 2020). The most widely used PKC algorithm in the world today, Rivest, Shamir, and Adleman algorithm (RSA) is considered superlative in comparison with algorithms such as the symmetric key Advanced Encryption Standard (AES) and the asymmetric Goldwasser and Micali (GM) algorithms (Nisha & Farik, 2020). Officially launched in 1977 and named with the surname initials of inventors Ron Rivest, Adi Shamir, and Leonard Adleman, RSA is actually a set of two algorithms; key generation, the most complex part used to produce the public and private keys, and RSA function evaluation which looks at encrypting and decrypting.

The IPv4 implementations are strongly recommended to support P2PE and IPv6 implementations are required to do so. P2PE gives the base protection capabilities for the network. P2PE is a security scheme for intercommunicating with two authorized networks from different locations and is built for secret communication and is reliable over the IP network by using authentic and cryptographic security services. It uses a framework to secure information, so that the data sent through the IPsec have data integrity and data confidentiality (Miller, 2017). P2PE ensures peer-to-peer data security by using encryption. It is the most popular technology for securing an enterprise, personal, or government network.

Against this background, it becomes instruct to model a point-to-point multi-layered cryptography system using RSA,P2PE and Chaos Synchronization for key distribution.



### **1.3 Problem Statement**

The communication between communication links/branches of different organizations are prone to hacks and loss of sensitive information since the issues of confidentiality, authentication and privacy for in transit network traffic are not being adhered to as they should be (Fernando, 2021). The confidential data that is being transferred between branches is exposed to hacks and other security threats.

### **1.4 Research Aim**

The main aim of the research is to provide in transit security on the network traffic data transferred between company branches or any sensitive communication links.

### **1.5 Objectives**

- To analyze different techniques used to encrypt data and distribute keys efficiently for data in transit.
- To design and implement a model which encrypts data in transit between two links using RSA algorithm, P2PE and chaos synchronization.
- To benchmark test and evaluate the effectiveness and efficiency of RSA algorithm, P2PE and chaos synchronization in encryption.

### **1.6 Research Questions**

- What are the different techniques used to encrypt data and distribute keys efficiently for data in transit?
- How to design and implement a model which encrypts data in transit between two links using RSA algorithm, P2PE and chaos synchronization?
- Is the use of RSA algorithm, P2PE and chaos synchronization in encryption effective and efficient?

### **1.7 Significance Of The Study**

Many organizations have moved away from traditional methods of sharing data over unsecure public networks that mostly caused data loss. By implementing P2PE, an organization will be protecting its sensitive data such as financial transactions, medical records, business communications and other data.

## **1.8 Scope Of The Study**

The research is based on designing and implementing a system for securing data in transit and determine the effectiveness. The researcher will demonstrate the application of P2PE and Chaos Synchronization in organizational networks using a simulated environment.

## **1.9 Limitations**

- The amount of time required to complete the research is limited.

## **1.10 Definition Of Terms**

- **Cryptography-** cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher.
- **Point-to Point Encryption-** is a technology standard created to secure electronic financial transactions.
- **Chaos Synchronization-**

## **CHAPTER 2: LITERATURE REVIEW**

### **2.1 Introduction**

Literature review entails the methodical gathering, organization, and analysis of papers containing information about the study subject under consideration. Its goal is to provide in-depth understanding of the subject being researched. It aids the researcher in discovering what other researchers have done in relation to the subject under investigation. It assists a researcher in avoiding unnecessary and unintended duplication, as well as providing a framework for interpreting study findings (Mugenda and Mugenda, 2013). Functionalities, benefits of implementation, key steps for successful implementation, challenges of implementation, successes and opportunities for success, objectives of implementing a P2P cryptography system are all covered in the reviewed literature.

### **2.2 Cyber Crime**

Cybercrime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cyber-crime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cybercrimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cyber-crime may be defined as crime committed using a computer and the internet to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. As day by day technology is playing in major role in a person's life the cyber-crimes also will increase along with the technological advances.

### **2.3 Data Breaches**

The release of confidential data, commonly known as personally identifiable information, from a secured location in a computer or an electronic device to an unsecured site is a data breach. US Department of Health and Human Services (DHHS) for their purposes defines a breach as "generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information (US Department of Health and Human Services, 2009). Hence, DHHS considers not only the disclosure of protected

information but also the impermissible use as a breach. California's data breach notification law defines a data breach as "breach of the security of the system" as "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business" (State of California, 1988). Similarly, US National Initiative for Cybersecurity Careers and Studies (NICCS) (2018) in their glossary define data breach as "the unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information." After the farming of Facebook data by Cambridge Analytica, there has been a growing demand to extend the definition of a data breach to include manipulation of data through social engineering (Kilovaty, 2018).

Similarly, there are federal and state laws that require the breached company to notify affected individuals and government officials (Callahan, 2017). At the same time, the individuals whose confidential information has been compromised are adversely impacted and will have to take several measures to mitigate the release of their confidential information and subsequently possible identity thefts. Such individuals usually look upon the breached company to make reasonable the actual and any anticipated losses, they might suffer.

## **2.4 Causes of Data Breach**

Generally, a data breach occurs because of a lack of security, elimination of security, and a breach of security. Lack of security may be as a result of unwillingness on the part of the organization to consider itself to be prone to data breaches or is considered too cost-prohibitive to secure the information. Elimination of security may be as a result of slackness on the part of the organization to beef-up the data security, and either insiders or outsiders purposefully eliminate the security protocols to make the data vulnerable. Such elimination may also be because of accidental loss of privileges and equipment or some state-sponsored actors purposefully removing the security to create vulnerability - for e.g., Desjardins Group data breach exposing 2.9 million members was caused by an employee (Smith, 2019). Breach of security is intentional on the part of actors to steal the data using malware, hacking, virus, social engineering, cyber espionage, and sabotage. It could be accidental when sensitive information is leaked inadvertently by accidentally publication, configuration errors, improper encryption, lost computer, and privilege abuse (Cheng, Liu, & Yao, 2017). A survey by

Clearswift (2013) in the UK showed 42% of data breaches were targeted from outsiders, 58% were from insiders - extended enterprise (33% employees, 7% Ex-employees, and 18% third parties) -majority of internal security threats were as a result of inadvertent human error, lack of awareness, and malware via personal devices.

McAfee (2017) reported a 43% -57% split between internal and external actors for data loss. The internal actors included employees, contractors, and third-party suppliers - half of the data loss was attributable as accidental. Wikina (2014) reported that data breaches involved computer systems and networks, desktop, laptops, paper records, emails, electronic health records, and portable devices. The researcher also reported that theft (47%) and loss (27%) - not hacking (7%) was the major type of data breaches reported. Table 1 shows the method data for the last five years: The data in Table 1 shows that hacking came down from 17.2% to 9.2% in 2017 as compared to 2016, which may have been because of intervention strategies but it has slowly but surely climbed to 2016 level in the year 2019. It may have been very well that the hackers have found new ways, or the precautions taken by entities have slackened off over the years. Since hacking is one of the highest contributing methods with 69.5% instances followed by poor security of about 23%, a combination of laws, investment in precautionary measures, and training the cybersecurity personnel may be a better strategy (Ayyagari, 2012). Lost devices are some of the most interesting as many devices these days have a hard drive; a protocol for their disposal is a must. For e.g., a stolen digital camera belonging to the University of Arkansas for Medical Sciences (UAMS) in Little Rock contained photographs of new-borns and their information which was responsible for the data breach (Stolen Camera Creates Privacy Breach for Arkansas Hospital, 2011). The same is possible from copy machines, fax machines, and biomedical equipment.

## **2.5 Effects of Data Breaches**

Gatzlaff and McCullough (2010) examined the stock market's reaction to data breaches in publicly listed companies and concluded that data breaches negatively affected shareholder wealth, especially for those firms with higher market-to-book ratios. Garg, Curtis, and Halper (2003) reported a 0.5% -1.0% loss of revenue on an annual basis. They also said that the insurance-sector reacted favorably in anticipation of increased cyber-insurance sales and the higher premiums resulting from a heightened awareness of cyber-insurance. Supriya (2018)

asserted that depending upon the organization and information breached, the affected organization may lose its financial sustainability in one extreme to not being an issue at all in another extreme of the spectrum. For organizations, like Health and Education, a data breach will lead to privacy concerns relating to the Health Insurance Portability and Accountability Act (HIPAA) and the Family Education Rights and Privacy Act (FERPA) violations. They may not face financial consequences unless the data is tampered with impacting the integrity of the information but will suffer punitive and compensatory damages when the breached data becomes available on the darknet.

The impact is judged on confidentiality, integrity, and availability of the data breached. For example, a data breach at Facebook created its stock price to lose value but it was a minor issue for them in terms of confidentiality as no credit card information was stolen. Therefore, the effect could be explicit or implicit, and both. The outcome will be felt differently by the organization, and those impacted individuals whose personally identifiable information has been breached. The risk factor is more for companies that store, process, and transmit sensitive information like a credit card, social security numbers, medical records, educational records, financial records, and other personally identifiable information.

Toe (2013) considered the three areas: organizational reputation, customer resentment, and possible lawsuits apart from immediate operating expenses for customer notification, upgrades in security infrastructure, and credit monitoring service costs and regulatory or industry-specific fines. All these have explicit and implicit financial implications (Confente, Siciliano, Gaudenzi, & Eickhoff, 2019). Some could result in the bankruptcy of the victim organizations like the American Medical Collection Agency (AMCA) whose data breach compromised 20 million records (Stone, 2019) and filed for bankruptcy immediately following the breach. On the other hand, Plachkinova and Maurer (2018) opined that despite one of the most significant data breaches in history, Target is still a successful business. The initial estimate of the costs to Target was reported \$ 3.6 billion. The resiliency to come out of such an event could be a business continuity plan which kicks in, and the crisis is managed.

Solove and Citron (2018b) laid out the concept of data breach harm as a result of risk and anxiety for those whose information has been compromised by the data breach. E.g., Marriott breach resulted in loss of hundreds of millions of customer details, including credit card and passport numbers which has ensued the risk of those information being misused by bad actors (Fruhlinger, 2019a) leading to possible class lawsuits citing three injuries: “(1) the cost of fraudulent transactions, (2) the increased risk of future identity theft resulting from the breach, and (3) the burden of closing affected accounts and opening new ones” (Richie, 2015). Berezina, Cobanoglu, Miller, and Kwansa (2012) concluded that data breaches in a hotel led to a decrease in customers' perceptions of reliability and assurance of quality services. Lending, Minnick, and Schorno (2018) found that banks with data breaches had significant declines in deposits and nonbanks had substantial decreases in sales in the long run. Furthermore, they reported companies were more likely to replace their chief executive officer and chief technology officer and invest more to improve in their corporate governance and social responsibilities. Fruhlinger (2019b) reported that Equifax had spent \$1.4 billion on clean-up costs, including the cost for the transformation of technology to improve the application, network, and data security. On the other hand, there still is a lot of anxiety for almost 40% of Americans whose data was exfiltrated in the Equifax hack Fruhlinger (2019b).

## **2.6 The RSA algorithm**

RSA (Rivest-Shamir-Adleman) is an asymmetric cryptographic algorithm used to encrypt and decrypt messages by modern computers (Asjad,2019).. Asymmetric states that there are two different keys used in the encryption and decryption process, which also is called public-key cryptography. This is simply because one of the two keys can be given to anyone without exploiting the security of the algorithm. The RSA algorithm involves both private and public keys. The public key can be known and published to anyone, as it is used to encrypt the messages from plaintext to ciphertext. The messages that are encrypted with this specific public key can however only be decrypted with the corresponding private key. The key generation process of the RSA algorithm is what makes it so secure and reliable today, as it contains a high level of complexity compared to other cryptographic algorithms (Asjad,2019).

## **2.7 Encryption Key Distribution Via Chaos Synchronization**

Chaos cryptography is a recent encryption technique (the idea was proposed in the early 90s), and it will take some time for its security analysis to mature. Some rules have been suggested to achieve a reasonable degree of security (Alvarez & Li, 2006). Methods to quantify the cryptanalysis of chaotic encryption schemes have been also proposed (Tenny & Tsimring, 2004). However, more research needs to be done to develop a systematic cryptographic approach for the analysis of the security of different chaotic communication systems. Many chaos-based encryption schemes have been proposed, and many of those schemes have been broken later on. Some chaotic encryption systems were broken even without reconstructing the transmitter's chaotic dynamics, that is, without searching for the secret key that was used to encrypt the message. This kind of attack is usually applicable if the statistical properties of the ciphertext change as a result of changing the transmitted plaintext. Return maps (Perez & Cerdeira, 1995) and spectral analysis (Yang et al., 1998a) of the transmitted ciphertext have been used to decode the message eliminating the need to reconstruct the secret dynamics. Chaos synchronization is based on synchronized random bit generation (Banerjee, 2010). It relies on the synchronization between a transmitter and a distant receiver through an uncorrelated chaotic driver signal. From the synchronized chaotic signals, a random key can be distilled that would be extremely difficult to be reconstructed from the information shared in the public channel.

## **2.7 Review Of Related Literature**

A lot has been done pertaining this theory with completely diverse methods at different times and places. The evolution of wireless technologies has offered so many opportunities to the scholars and researchers at large to go further into exploring different methodologies. This section will mainly focus on analyzing how other scholars and researchers have addressed the concept of point-to-point encryption system for data in transit.

Sharma, (2021) proposed a Remote Access IPSEC based VPN offering encryption using the chaos synchronization which gives the solution of remote access to e-library resources, networks resources and so on very safely through a public network. The network establishes a safe and stable tunnel which encrypts the data passing through it with robust secured algorithms. A virtual private network established in Internet, so that the two long-distance network users can transmit



data to each other in a dedicated network channel therefore multi-network campus can communicate securely in the unreliable public internet.

Dhall et al., (2012) proposed a working principle implementation of P2PE in various network devices (hosts and routers). Their research was focused on allowing peer-to-peer communication between branches of an organization without the risk of data breaches. When comparing the time difference with AH implemented and without AH implemented data packet for variable number of nodes, compared to a lower number of total nodes versus higher number of nodes, time difference when delivering the packets differs considerably; but for the extra time, all users in the network can get authentication service for all data packets in ad-hoc network. When comparing the time difference with P2PE implemented and without chaos synchronization implemented data packets, the time difference varies slightly. Their findings showed point to point encryption has more timing overhead and the time difference between ESP implemented packets is higher than AH implemented packets (Dhall et al., 2012).

Campbell et al. (2013) investigated the stock market reaction of information security breaches on public firms. The authors concluded that the economic consequence of a security breach depends on the nature of the breach. They found a highly significant negative market reaction when breaches are related to unauthorized access to confidential data. However, the authors did not find any significant market reaction for other types of security breaches.

Garg et al., (2013) estimated that security incidents can cost breached companies 0.5 to 1 percent of annual sales on average. The authors also tested for the spillover effects on security vendors and insurance carriers and found that security vendors experienced a share price increase between 1 to 3 percent and insurance carriers experienced 1 to 2 percent increase in a share price as a result of security breach.

Similar to the study by Garg et al.(2013), Cavusoglu et al.(2004) found that the security breach announcements affect the value of breached firms and also of Internet security developers. On average, the breached firms lost 2.1 percent of their market value within two days following the public announcement. On the other hand, the security developers realized an average abnormal return of 1.36 percent during this period.

## **2.9 Chapter Summary**

The researcher has managed to gather information which is relevant for this project. Some of the concepts from research journals, internet, textbooks and unpublished material reveals the depth and gap to be filled. The information gathered is to be used in the chapters to follow to meet the set objectives.

# **CHAPTER 3: METHODOLOGY**

## **3.0 Introduction**

Research is a fact-finding activity that includes scientific research or an in-depth analysis of a particular issue of interest. Depending on whether the research is exploratory, descriptive, or diagnostic, quantitative or qualitative methodologies are used. When it comes to making economic decisions, research has shown to be a significant tool for government institutions and policymakers. Mackey and Gass (2013). Methodology is defined as the systematic, theoretical analysis of the methods or procedures applied to a particular field of study. The author will define approaches used to attain the proposed research and system objectives in this chapter. The author will create the necessary procedures to build a solution and be able to choose among competing strategies to achieve the research's desired results using the information obtained in the previous chapter. To make the study procedure easier, secondary data was used for analysis. The information for this study was gathered through official sources, the internet, and journals.

## **3.1 Research Design**

Research design is a study's architectural backbone (Moule & Goodman, 2013). According to Polit and Hungler (2014), research design refers to the strategy for answering research questions and managing problems throughout the study process. A researcher can employ one of four research models: observational, experimental, simulation, or derived. Because the application must be constructed and regularly tested to verify whether it is generating the desired effect, the researcher chose to use both experimental approaches.

## **3.2 Requirements Analysis**

Requirements analysis is crucial to a project's success or failure, and the created requirements must be practical, documented, tested, executable, traceable, and measurable, as well as related to identified business needs and precise enough to make system design easier (Abram Moore, Bourque, & Dupuis 2004). As a result, it's critical to document all of the required system's functional and non-functional specifications at this point. To create uniform and unambiguous requirements, the acquired requirements are reviewed, revised, and scrutinized.

### **3.2.1 Functional Requirements**

These can be characterized as a system's or component's function. A function is made up of three parts: inputs, behavior, and outputs. "Functional requirements are those acts that a system must be able to accomplish, without regard for physical limits," Bittner explained. Computations, specialized subtle elements, data control and preparation, and other specific functionalities that define what a system should achieve are examples. Use cases depict the behavioral conditions that apply to the great majority of instances in which the system applies the functional requirements.

The proposed system must be able to meet the following requirements:

- i. to encrypt the data transferred between two links
- ii. to establish a secure tunnel for data transfer
- iii. to avoid unauthorized data access

### **3.2.2 Non-Functional Requirements**

They are often referred to as quality requirements and used to judge the performance of a system rather than its intended behavior. The proposed system must be able to meet the following:

- i. Performance requirements
- ii. Flexibility requirements
- iii. Quick response time

### **3.2.3 Hardware Requirements**

- Core i5 processor or better

### **3.2.4 Software Requirements**

- Windows 10 Operating system
- Visual Studio Professional 2019
- Microsoft Visual C#
- .Net Framework 4.5.2
- Wireshark
- Tomcat server

### **3.3 System Development**

This system describes the overview of the system and how it was developed so as to produce the results. It specifies all the software tools and models used in the development of the system.

#### **3.3.1 System Development tools**

#### **3.3.2 Prototyping**

### **3.4 Summary of how the system works**

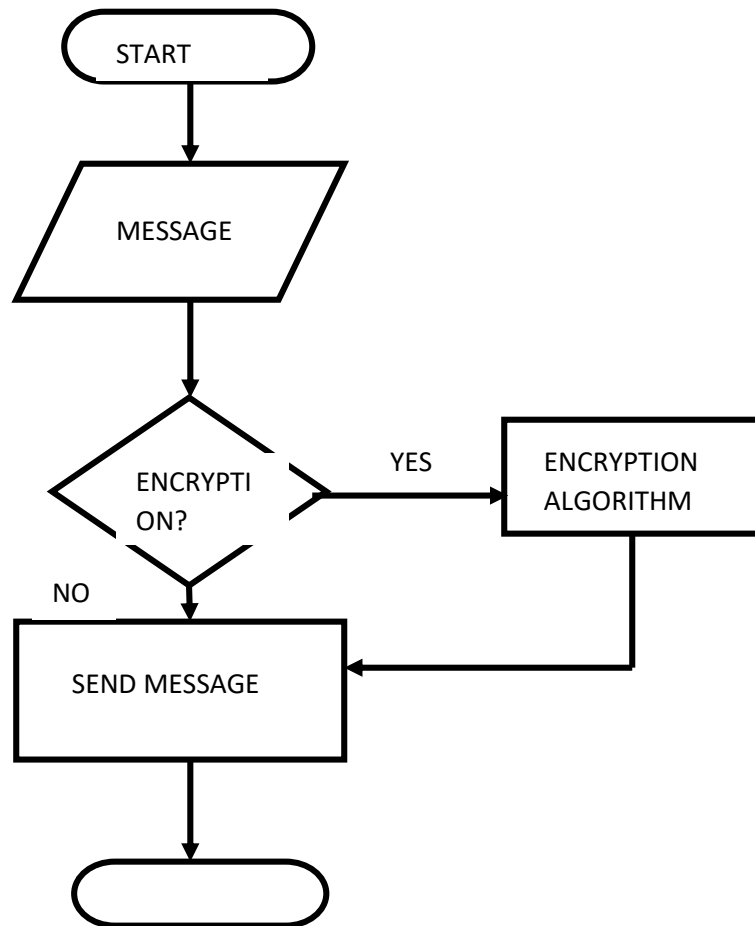
The simulated implementation of the system solution shows a L2L or the Site-to-Site type of a network is to link branch offices or remote, distant offices together. The simulated environment shows that the first step is to paste any data/information on a CMD prompt. Firstly, the data is encrypted before transferring. The data is sent over the internet to the destination IP address. Wireshark is used to test the strength of the data encryption. The user tries to spoof the data using Wireshark and visualize how the data is transmitted between two IP addresses. The final result shows that the data has been transferred successfully and not been tampered with. It makes it possible for two different sites that may be distant from each other to stay connected by secure means. It was achieved by encrypting the link between the two different site-to-site connections with an IPsec tunnel. This type of site-to-site security provides not only a secure connectivity between two organization segments, but also a secure link within the organization itself.

### **3.5 System Design**

#### **3.5.1 System Dataflow diagrams (DFDs)**

### 3.5.2 Proposed System flow chart

A flowchart is a graphical depiction of a sequence of activities in a process. This diagram helps in defining the system flow of data and all process found within the proposed solution



STOP

### 3.6 Data collection methods

### 3.7 Implementation

This section implicates setting the system into action thus coordination and directing the resources elaborated in the previous chapter to meet the objectives of the research plan. Thus, all the

documentation from all previous chapters are being finalized to align it in order to deliver the system.

```
Enter text that needs to be transmited ...
As I'm writing this, my heart is ladened with awe. It is ladened because when I retrace my steps to a few years back, I
could not have dreamt of being where I am today. Since you became part of the Long john family, I've seen impossibility
become possibl
??j?>P?|?@z4?7?1'\$?+?▼?.2u??{3X+?uZNI?+???S??T??EIN"??>?▼?5??c??dQ*!??f-#3n?E%??/?4(?z4?2v?a◀Q! ?vOU????\qFs?c10~R=?0?
?n??0+E?Yh_??G??R?r???? qe▲??*Q^??B4▼U?hI?Z??E?)??F??ntB?A=?? .1*???:?02??x??I??5?4?(?0?8?? Key: -"rA0obTñIyñeM?L]C]Z"~f
i?'Tlx-46
Transmiting data to Server => 172.16.2.30
Request posted.
```

Figure 1:Transferring data

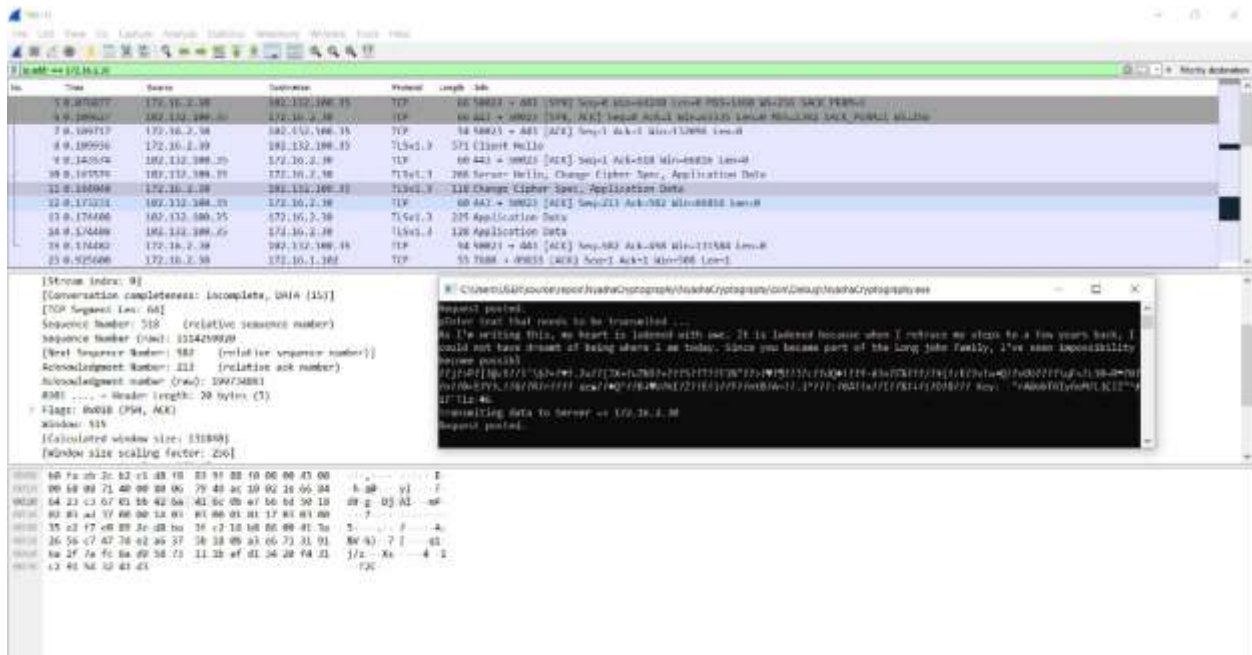


Figure 2: Monitoring Data transfer Using Wireshark

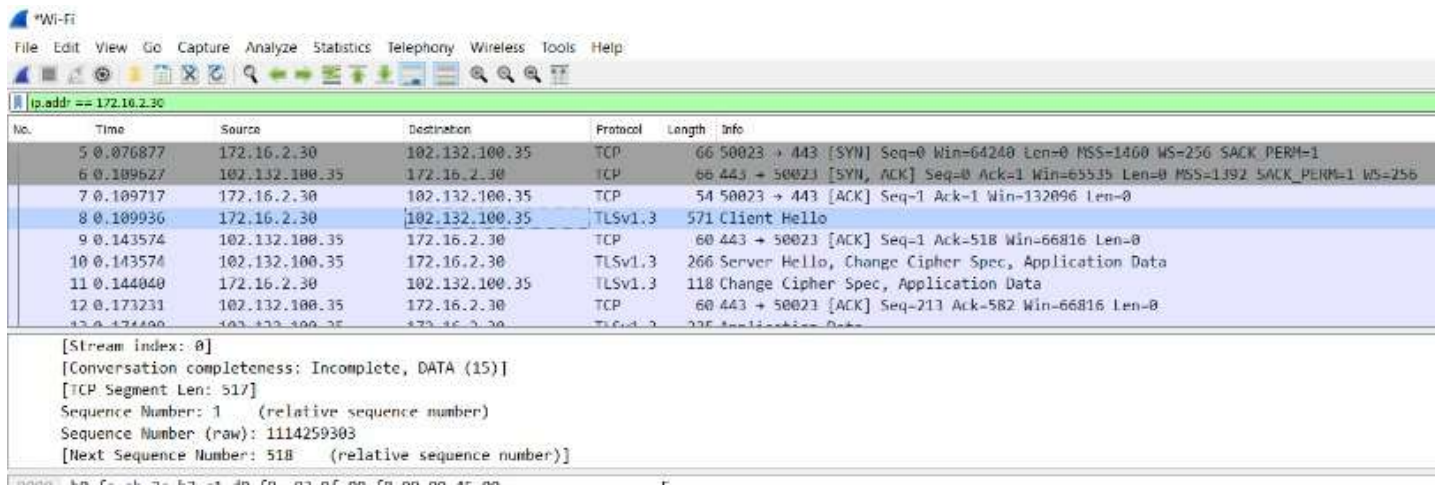


Figure 3: Showing source and destination IPs



### **3.8 Conclusion**

The chapter mainly focused on the methods and tool that were used to develop the model. Thus, different techniques and methods were used in developing the model solution up to the end, as mentioned above, the model was developed using C#.

## **CHAPTER 4: DATA ANALYSIS AND INTERPRETATIONS**

### **4.0 Introduction**

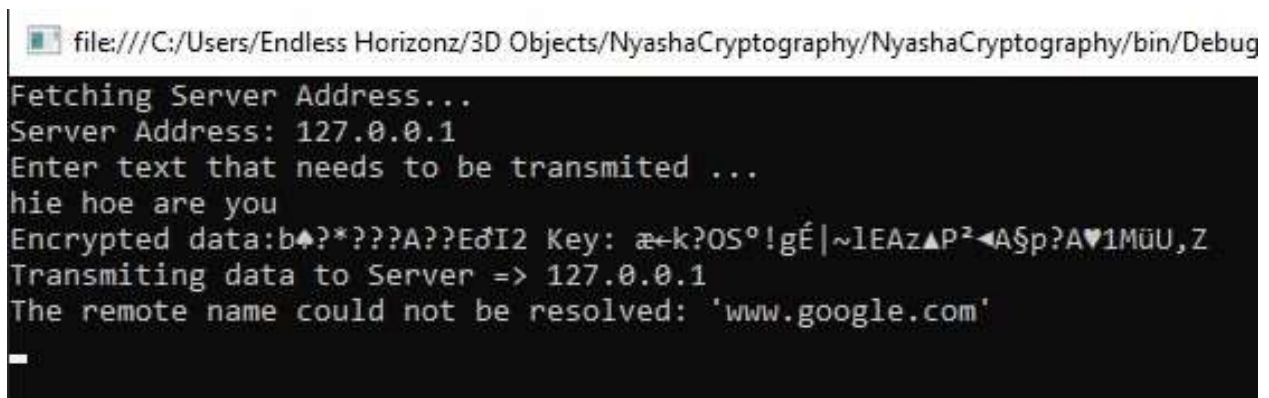
Following the completion of the system, it is necessary to assess the efficiency of the provided solution. The matrices utilized to determine the efficiency and efficacy of the produced solution were accuracy, performance, and response time. The information gathered in the previous chapter was evaluated to come up with useful results. The behavior of the constructed system was also studied under various conditions. As a key part of research work, this chapter focuses primarily on presenting research findings, analyses, interpretations, and discussions.

## 4.1 Testing

System testing is defined as testing of a complete and fully integrated software product. It is a level of testing that validates the complete and fully integrated software product. The purpose of a system test is to evaluate the end-to-end system specifications. Usually, the software is only one element of a larger computer-based system. Ultimately, the software is interfaced with other software/hardware systems. System Testing is actually a series of different tests whose sole purpose is to exercise the full computer-based system.

### 4.1.2 Black box Testing

Black box testing is a technique of software testing which examines the functionality of software without peering into its internal structure or coding. The primary source of black box testing is a specification of requirements that is stated by the customer. In this method, tester selects a function and gives input value to examine its functionality, and checks whether the function is giving expected output or not. If the function produces correct output, then it is passed in testing, otherwise failed. The test team reports the result to the development team and then tests the next function. After completing testing of all functions if there are severe problems, then it is given back to the development team for correction.



```
file:///C:/Users/Endless Horizonz/3D Objects/NyashaCryptography/NyashaCryptography/bin/Debug
Fetching Server Address...
Server Address: 127.0.0.1
Enter text that needs to be transmited ...
hie hoe are you
Encrypted data:b... Key: æ+k?OS°!gÉ|~lEAz▲P²◀AŞp?A♥1MÜU,Z
Transmiting data to Server => 127.0.0.1
The remote name could not be resolved: 'www.google.com'
```

*Figure 4:Running the simulation with no internet*



## 4.1.2 White box testing

White box testing is software testing technique in which internal structure, design and coding of software are tested to verify flow of input-output and to improve design, usability and security. In white box testing, code is visible to testers so it is also called clear box testing, open box testing, transparent box testing, code-based testing and glass box testing.

```
Console.WriteLine("Transmitting data to Server => "+ip);

//Http Client

//var httpWebRequest = (HttpWebRequest)WebRequest.Create("http://"+ip+":8080/nyasha/index.php");
string json = "{\data\:" + System.Text.Encoding.UTF8.GetString(encrypted) + "::::;" + key + "\", " +
    "\dvqww\:" + vxsasaxx123131$#**(@*$)jjkjsha\"}";
var httpWebRequest = (HttpWebRequest)WebRequest.Create("https://www.google.com/search?q="+ json);
httpWebRequest.ContentType = "application/json";
httpWebRequest.Method = "GET";
//httpWebRequest.Headers.Add("sadza",key);

/*using (var streamWriter = new StreamWriter(httpWebRequest.GetRequestStream()))
```

*Performing a web HTTP request*

```
// Create encryptor
ICryptoTransform encryptor = aes.CreateEncryptor(Key, IV);
// Create MemoryStream
using (MemoryStream ms = new MemoryStream())
{
    // Create crypto stream using the CryptoStream class. This class is the key to encryption
    // and encrypts and decrypts data from any given stream. In this case, we will pass a memory stream
    // to encrypt
    using (CryptoStream cs = new CryptoStream(ms, encryptor, CryptoStreamMode.Write))
    {
        // Create StreamWriter and write data to a stream
        using (StreamWriter sw = new StreamWriter(cs))
            sw.Write(plainText);
        encrypted = ms.ToArray();
    }
}
```

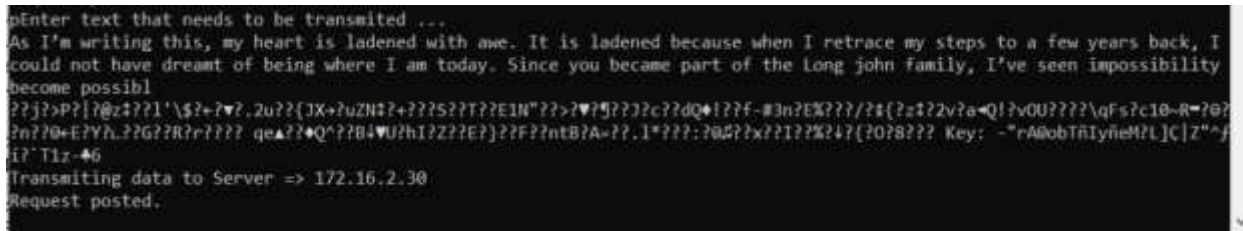
*Initiating the encryption function*

## 4.2 Evaluation Measures and Results

An evaluation metric measures the performance of a model (Hossin & Sulaiman, 2015). Moreover, according to Hossin & Sulaiman (2015), model evaluation metrics can be grouped into three types namely threshold, probability and ranking.

### 4.2.1 Encryption Key Length

In cryptography, key size, key length, or key space refer to the number of bits in a key used by a cryptographic algorithm (such as a cipher). Key length defines the upper-bound on an algorithm's security (i.e. a logarithmic measure of the fastest known attack against an algorithm), since the security of all algorithms can be violated by brute-force attacks. Ideally, the lower-bound on an algorithm's security is by design equal to the key length (that is, the security is determined entirely by the key length, or in other words, the algorithm's design does not detract from the degree of security inherent in the key length). Most symmetric-key algorithms are designed to have security equal to their key length. However, after design, a new attack might be discovered. If a key is  $n$  bits long, then there are two to the  $n$ th power ( $2^n$ ) possible keys. For example, if the key is one bit long, and that one bit can either be a zero or a one, there are only two possible keys, 0 or 1. However, if the key length is 40 bits long, then there are  $2^{40}$  possible keys.



*Figure 5: Key length In The Encryption Process*

Wireshark interface showing a packet capture with a list of packets and a detailed view of a TCP segment.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
2	0.000000	192.132.199.35	172.16.2.38	TCP	60	8082 → 60443 [ACK] Seq=1 Win=0 Len=0
3	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
4	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
5	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
6	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
7	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
8	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
9	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
10	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
11	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
12	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
13	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
14	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
15	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
16	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
17	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
18	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
19	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
20	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0

Packet 11 details:

```

[Stream index: 0]
[Conversation completeness: Incomplete, DATA (15)]
[TCP segment Len: 60]
Sequence Number: 518 (relative sequence number)
Sequence Number (raw): 122429500
[Next Sequence Number: 582 (relative sequence number)]
Acknowledgment Number: 213 (relative ack number)
Acknowledgment Number (raw): 199734811
RST: ... = RST (length: 20 bytes (3))
Window: 0
[Calculated window size: 13280]
[Window size scaling factor: 26]
  
```

Packet 11 hex dump:

```

0000  60 7a 2b 2c 62 c1 43 10 83 91 00 10 00 00 43 00  ...
0004  00 60 00 71 40 00 00 00 79 40 00 10 00 20 00 00  ...
0008  64 23 c3 07 01 82 06 41 8c 00 0f 5d 5d 90 18 00  ...
000c  02 81 ad 07 00 00 1a 00 01 00 01 01 17 01 01 00  ...
0010  35 c3 f7 00 00 2d 00 38 c3 10 00 00 00 41 20 5...
0014  26 56 c7 47 7d 02 85 37 38 18 00 01 05 73 31 01  ...
0018  8a 2f 7a 7c 0a 09 5d 73 11 25 0f 01 24 20 74 23  ...
001c  c2 43 5d 12 43 43 720
  
```

Wireshark interface showing a packet capture with a list of packets and a detailed view of a TCP segment.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
2	0.000000	192.132.199.35	172.16.2.38	TCP	60	8082 → 60443 [ACK] Seq=1 Win=0 Len=0
3	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
4	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
5	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
6	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
7	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
8	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
9	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
10	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
11	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
12	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
13	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
14	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
15	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
16	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
17	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
18	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
19	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0
20	0.000000	172.16.2.38	192.132.199.35	TCP	60	60443 → 8082 [ACK] Seq=1 Win=0 Len=0

Packet 11 details:

```

[Stream index: 0]
[Conversation completeness: Incomplete, DATA (15)]
[TCP segment Len: 60]
Sequence Number: 518 (relative sequence number)
Sequence Number (raw): 122429500
[Next Sequence Number: 582 (relative sequence number)]
  
```

Packet 11 hex dump:

```

0000  60 7a 2b 2c 62 c1 43 10 83 91 00 10 00 00 43 00  ...
0004  00 60 00 71 40 00 00 00 79 40 00 10 00 20 00 00  ...
0008  64 23 c3 07 01 82 06 41 8c 00 0f 5d 5d 90 18 00  ...
000c  02 81 ad 07 00 00 1a 00 01 00 01 01 17 01 01 00  ...
0010  35 c3 f7 00 00 2d 00 38 c3 10 00 00 00 41 20 5...
0014  26 56 c7 47 7d 02 85 37 38 18 00 01 05 73 31 01  ...
0018  8a 2f 7a 7c 0a 09 5d 73 11 25 0f 01 24 20 74 23  ...
001c  c2 43 5d 12 43 43 720
  
```



### 4.6 Summary of Research Findings

The author evaluated the simulation solution and achieved satisfactory results. The system was tested using white and black box and also the encryption key length was used as a measure of performance. The proposed solution can create long key up to 256 bits depending on the data which needs to be transferred. The author tested the traffic of the tunnel using Wireshark and modelled how data is transferred between two links.

### 4.7 Conclusion

This chapter focused on presenting the results of the simulation of the system. The results were satisfactory despite issues such as poor network in the testing environment.

# **CHAPTER 5: CONCLUSION AND RECOMMENDATIONS**

## **5.1 Introduction**

In this chapter a conclusion of our research is presented. The chapter represents the summary of findings, conclusion drawn from the research and recommendations for further studies. In this chapter a conclusion of our research is presented. Also, suggestions for further research and our contribution to the subject are mentioned. The purpose of this study was to develop a simulated environment to show the implementation of a point-to-point multi-layered encryption system using chaos synchronization for key distribution.

## **5.2 Aims & Objectives Realization**

The first objective of this study was to analyze different techniques used to encrypt data and distribute keys efficiently for data in transit. The second objective was design and implement a model which encrypts data in transit between two links using RSA algorithm, P2PE and chaos synchronization. The third objective was to benchmark test and evaluate the effectiveness and efficiency of RSA algorithm, P2PE and chaos synchronization in encryption. In chapter 2, the researcher managed to review literature from multiple scholars and acquired insight on methods used to implement a multi-layered encryption system. As seen from chapter 4 ,the author managed to develop the multi-layered encryption system using chaos synchronization for key distribution in a simulated environment using C# and try to intercept the connection using Wireshark. The system was evaluated in terms of encryption strength, key length and speed of delivery. Therefore, all the three objectives were achieved.

## **5.3 Major Conclusions Drawn**

The author concludes that the use of chaos synchronisation to develop a multi-layered point-to-point encryption system is effective and organisations should encrypt their data in transit by adopting this more secure and reliable method.



### **5.3 Recommendations & Future Work**

The author recommends the use of multiple nodes in demonstrating and testing the system. This comes as an advantage since it will be implemented and used by many company branches at the same time.

### **References**

1. Dhall, Batra, Rani, a. Implementation of ipsec protocol. 2012 Second International Conference on Advanced Computing & Communication Technologies, 2012: 176-181.

2. Mugenda, A. and O. Mugenda, 2013. Research methods: Quantitative and qualitative approaches. Nairobi: ACTS Press.
3. Qu, W., Srinivas, S. IPsec-based secure wireless virtual private network. MILCOM 2012. Proceedings, 2012, 2, 1107-1112.
4. Sun, S. H. The Advantages and the Implementation of SSL VPN. 2011 IEEE 2nd International Conference on Software Engineering and Service Science. Beijing: IEEE, 2011: 548- 551.
5. Lee, H., Nah, J., Jung, K. The Remote Access to IPsec- VPN Gateway over. The 7th International Conference on Advanced Communication Technology, 2015: 567- 569. Taejeon: IEEE.
6. Kim, B.-J., Srinivasan, S. Simple Mobility Support for IPsec Tunnel Mode. 2013, 3: 1999-2013.
7. Lakbabi, A., Orhanou, G., Hajji, S. E. VPN IPSEC & SSL Technology. 2012 Next Generation Networks and Services NGNS. Agdal: IEEE, 2012: 202-208.
8. Halaye & Jebur, WS. EA (2014). Implementing Virtual Private Network using Ipv6 Framework. International Journal of Engineering Research & Technology. Vol. 3 Issue 8. pp 1710-1711.
9. Campbell, K., Gordon, L., Loeb, M. and Zhou, L. "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," Journal of Computer Security, Vol. 11, Number 2003, pp. 431-448.
10. Cavusoglu, H., Mishra, B. and Raghunathan, S. "The effect of Internet security breach announcements on market value: capital market reactions for breached firms and Internet security developers," International Journal of Electronic Commerce, Vol. 9, Number 1, 2004, pp. 69-104.
11. Dasgupta, S., Laplante, B. and Mamingi, N. "Capital market responses to environmental performance in developing countries", Development Research Group, [http://www.worldbank.org/nipr/work\\_paper/market /MARKETS-htmp2.htm](http://www.worldbank.org/nipr/work_paper/market /MARKETS-htmp2.htm), .
12. Egan, M. and Mathen, T., The executive guide to information security threats, challenges, and solutions, Addison-Wesley, Indianapolis, 2005.
13. Garg, A., Curtis, J. and Halper, H. "The financial impact of IT security breaches: what do investors think?," Information Systems Security, Vol. 12, Number 1, 2003, pp. 22-33.

14. Garg, A., Curtis, J. and Halper, H. "Quantifying the financial impact of IT security breaches," *Information Management & Computer Security*, Vol. 11, Number 2/3, 2003, pp. 74-83.
15. Gordon, L., Loeb, M. P., Lucyshyn, W. and Richardson, R. "CSI/FBI Computer crime and security survey," CSI/FBI, Computer Security Institute, 2004.
- 16.