International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 6 Issue 7, November-December 2022 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Secured and Encrypted Data Transmission over the Web Using Cryptography

Okpalla, C. L.*; Madumere, U.; Benson-Emenike M. E.; Onwuama T. U.; Onukwugha, C. G.

Department of Computer Science, Federal University of Technology, Owerri, Nigeria

ABSTRACT

Information security has emerged as one of the most pressing issues in data transmission, and it is now an inextricable aspect of the process. To solve this problem, cryptography can be used. This study presents a secure data transmission method and describes how data might be securely transmitted. Cryptography creates a secure and reliable transmission mechanism that can withstand attacks. The Vigenere cipher is employed in this work to encrypt the plain text content of the electronic mail that will be transmitted to the receiver, and a decryption key is required to convert the encrypted data to plain text. Confidentiality, honesty, usability, and efficacy are all important factors in our tests. The outcome of this study will serve as a guide to better methods for safeguarding and delivering data over the internet. The system was created with the Visual Basic Programming Language and the Microsoft Access Database, and it was successfully installed on the Windows Operating System. All electronic mail users, the military, and organizations that demand a high level of security in messages sent to and from their systems would benefit from our effort.

KEYWORDS: *Cryptography, Information security, Encryption, Decryption, Electronic mail*

How to cite this paper: Okpalla, C. L. | Madumere, U. | Benson-Emenike M. E. | Onwuama T. U. | Onukwugha, C. G. "Secured and Encrypted Data Transmission over the Web Using Cryptography" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-7, December 2022, pp.1013-1017, URL: www.ijtsrd.com/papers/ijtsrd52545.pdf

IJTSRD52545

1. INTRODUCTION

There have been numerous cases in recent years of secret data, such as customer personal records, being disclosed as a result of hacking into an organization's database or intercepting information transferred over the internet. Encrypting such data transported over the internet could have protected the hacked or modified data.

The process of converting data into a secret code is known as encryption. It is the most efficient method of ensuring data security. Data encryption converts data into a code that can only be read by persons who have a secret key (officially known as a decryption key) or password. Ciphertext refers to encrypted data, whereas plaintext refers to data that has not been encrypted. Encryption is currently one of the most common and effective data protection solutions in use by businesses. Asymmetric encryption, often known as public-key encryption, and symmetric encryption are the two basic methods of data encryption (Nate, 2019)

Encryption and cryptography are two approaches for ensuring the privacy of messages sent over the internet. Cryptography, on the other hand, is the practice and study of ways for secure communication in the presence of third parties known as adversaries; from Greek kryptós, meaning "hidden, secret," and graphein, meaning "writing," or -o -logia, "study," respectively (Rivest 1990). The fields of mathematics, computer science, and electrical engineering all cross in modern cryptography. ATM cards, computer passwords, and electronic commerce are all examples of cryptography applications. This work aims to give some level of control over messages sent via the internet in order to ensure some level of privacy (Menezes et. al, 2005).

2. Review of Related Literature

Ankit Fadia and Jaya Bhattacharjee (2007) explain how to encrypt data to keep it safe from prying eyes. It explains how encryption works and defines encryption and decryption in light of the growing necessity to protect one's privacy in communication and transactions. They covered cryptography, the most prominent encryption algorithms, how encryption works, digital signatures, and digital certificates, among other topics.

Information security is divided into four primary categories, according to Stamp (2011): Classic cryptosystems, symmetric key cryptography, public key cryptography, hash functions, random numbers, and information concealment are all covered in this section. Also, cryptanalytic techniques, including examples of attacks on cipher systems ; ii)Access Control: Covers authentication and authorization, password-based security, ACLs and capabilities, multilevel and multilateral security, covert channels and inference control, coverage of security models such as BLP and Biba's Model, discussion of firewalls and intrusion detection systems (IDS); iii)Protocols: Covers generic authentication protocols and real-world security; iv)Protocols: Covers generic authentication protocols and real-world security; v)Pro v)Software: Covers software flaws and malware, buffer overflows, viruses and worms, malware detection, software reverse engineering (SRE), digital rights management (DRM), secure software development, and operating system security functions, as well as Microsoft's "next generation secure computing base" (NGSCB).

Gattiker (2018) explains popular security and infrastructure protection terms in detail and in an understandable manner. In cryptography, computer security, information systems, role-based access management, and applicable fields that rely on those disciplines, special attention is paid to phrases that most commonly impede knowledgeable readers from comprehending journal articles or books. Computing forensics, malware attacks, privacy issues, system architecture, security auditing, and vulnerability testing are also covered. In one succinctly structured volume, this indispensable reference tool delivers cutting-edge information on the most recent words in usage. Language dictionaries, statistics dictionaries, epidemiology dictionaries, and other disciplines' dictionaries are similar.

Furnell and Dowland (2010) employ email clients to enhance security, maintain confidentiality, and safeguard the company's reputation. This guide provides a quick reference to the most important security challenges affecting individuals who install and utilize email to support their companies, concentrating on why adequate security policy and protections are critical in guaranteeing the viability of company operations. Because email is used by businesses and offices to communicate with official workers, partners, suppliers, and customers on a daily basis. While email is a crucial mode of communication, it also poses a risk to our data security. Email could be used by criminals to infect our computers with viruses or dangerous software, and fraudsters would try to gain sensitive information through phishing scams.

Bradley Dunsmore et al. (2001) look at firewall solutions from Cisco, Symantec, Microsoft, and Check Point to protect computer networks from assault across the Internet. It provides general guidance on how to put up a robust defense system (comprising a firewall, an intrusion detection system, authentication and cryptography schemes, and protocols like IPsec). It closes with details on how to configure a variety of items. A basic introduction to block cipher design and analysis is provided by Fauzan Mirza (2001). Block ciphers are explained in terms of their concepts and design principles, with a focus on the Feistel ciphers. The use of certain recent block cipher cryptanalysis methods to versions of a weak Feistel cipher dubbed Simplified TEA (STEA), which is based on the Tiny Encryption Algorithm, is presented (TEA). By carefully measuring the amount of time required to complete private key operations, attackers may be able to identify fixed Diffe-Hellman exponents, factor RSA keys, and break other cryptosystems, according to Kocher P.C. (2018). He also discussed RSA and Diffe-Hellman attack prevention strategies. Finally, he claimed that current cryptosystems must be changed to protect against the attack, and that future protocols and algorithms must include timing attack prevention mechanisms.

3. Research Problem

The difficulties involved with the transfer of information via the various communication technologies include:

- **Impersonation:** It is the act of impersonating another person for the aim of amusement or deception. It is possible for unwary users' internet communication medium account credentials to be compromised, allowing unauthorized users to impersonate them.
- **Lack of privacy:** privacy refers to the freedom from potentially detrimental publicity, public scrutiny, secret surveillance, or illegal revelation of one's personal data or information by a government, corporation, or individual. When a message is sent or received by email, it is stored on the machine of the email provider, who has access to its contents in order to monitor and guarantee that it complies with the email provider's terms of service. As a result, the messages' privacy is compromised**.**

- **Wrong recipient:** Because of the high likelihood of human error, delivering communications to the incorrect recipient has become a growing issue. For security-related businesses, the inability to prevent a previously sent message from reaching its intended recipient, potentially containing crucial information, has become a major issue.
- **Inability to cancel messages sent:** It is nearly hard to cancel a message that has been sent in error in recent times. It can never be canceled once it has been delivered, and it will always reach the intended recipient.
- **Unauthorized access:** Hackers can acquire unauthorized access to users' accounts and personal information, which could be disastrous.

4. Significance of the Research

The relevance of this research cannot be overstated.

- If the message is delivered to the wrong recipient, the recipient will not be able to view the contents since the key to decrypt the message will not be sent or received.
- It ensures that each message sent remains secret and only the intended recipient can view it.
- Impersonators won't be able to read intercepted communications since they won't have access to the decryption key, which will be supplied to the original email account owner's cell phone through SMS.

5. Methodology

Every system has a methodology that was used to create it. The Trustworthy Computing Security Creation Lifecycle Methodology was used in the development of this system due to the nature of its development.

Trustworthy Computing Security Development Lifecycle Methodology (TCSDLM)

The purpose of these process enhancements is to decrease the number and severity of security flaws in end-user software. Microsoft's Trustworthy Computing Security Development Lifecycle Methodology (TCSDLM) is a process for developing software that can withstand harmful attacks. A variety of security-focused activities and deliverables are added to each phase of Microsoft's software development process as part of this procedure.

6. Program Testing

Below are the images of various forms that make up the Secure and Encrypted Data Transmission Solution

Log in Form

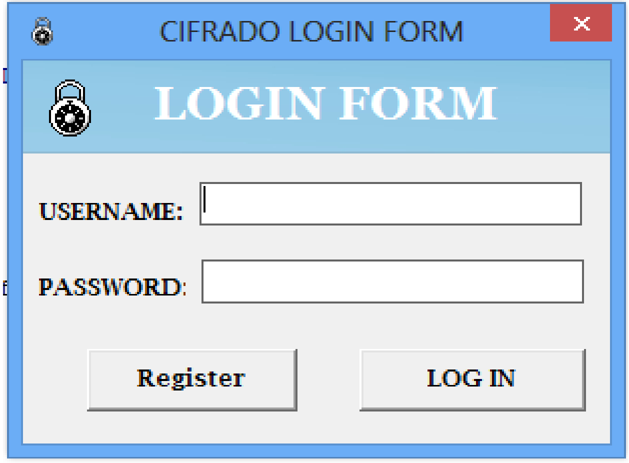


Figure 1: Log-in Form (This requires your log-in and password for access)

Registration Form

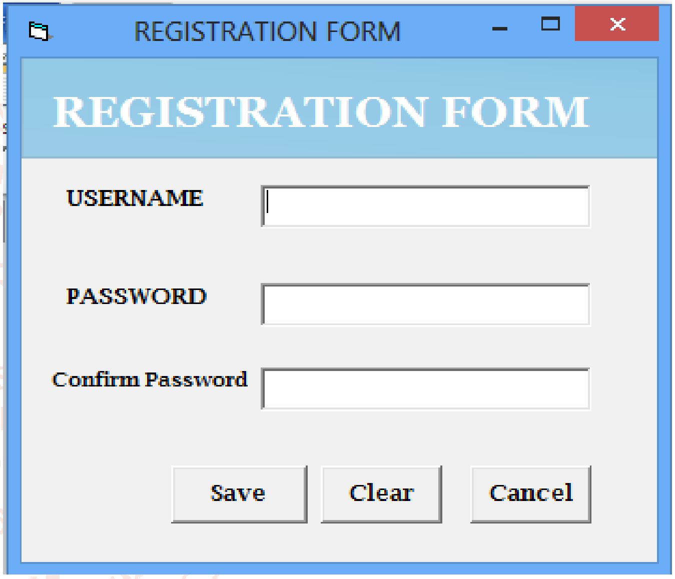


Figure 2: Registration Form (This requires your desired username and password)

MDI (Multiple-Document Interface)Form

Multiple-document interface (MDI) applications allow you to see multiple documents at once, each in its own window. Window menu items with submenus for switching between windows or documents are common in MDI applications.

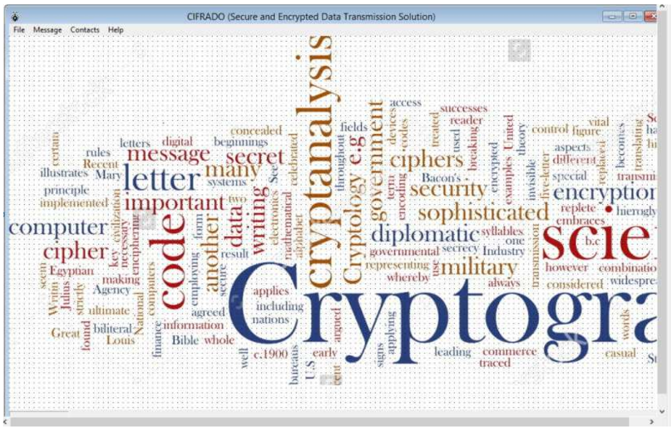
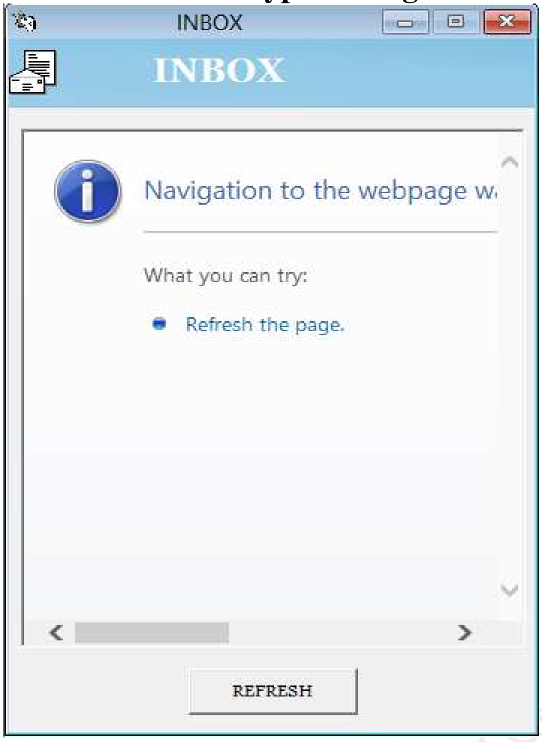


Figure 3: MDI Form

Email Inbox Form Decrypt Message Form

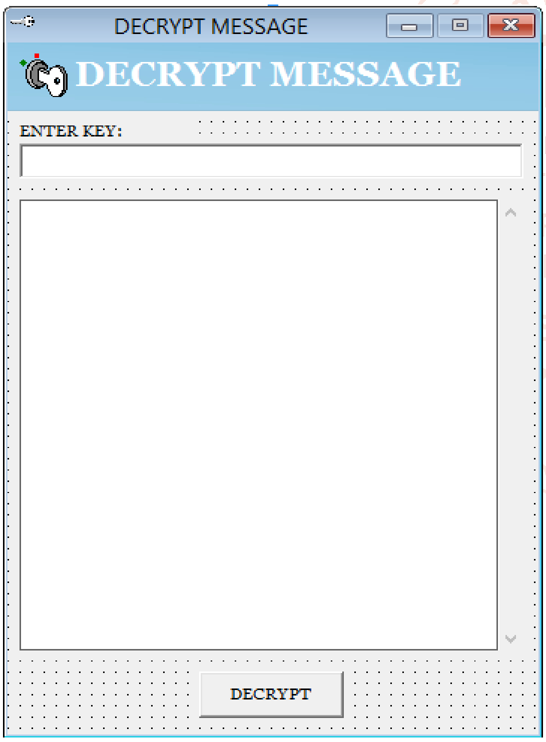


Navigation to the webpage w

What you can try:

- Refresh the page.

Figure 4: Email Inbox Form

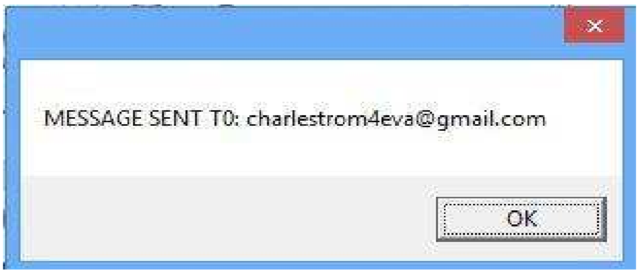


ENTER KEY:

Figure 5: Decrypt Message Form

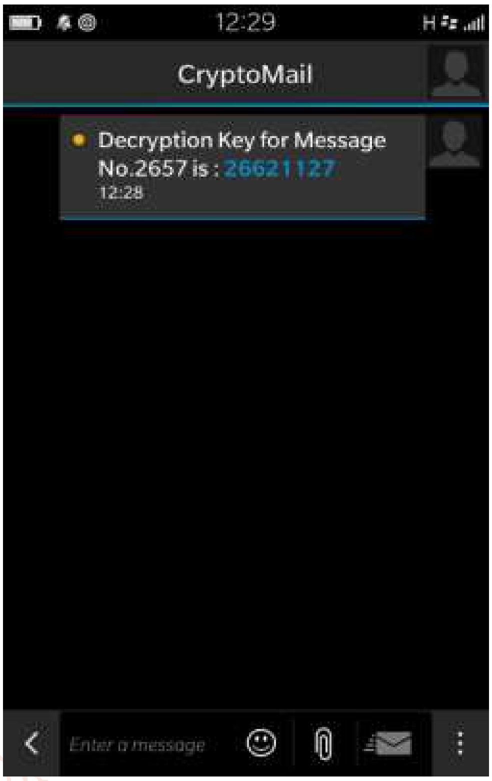
7. Results

The output of the various forms and codes above when compiled are as follows



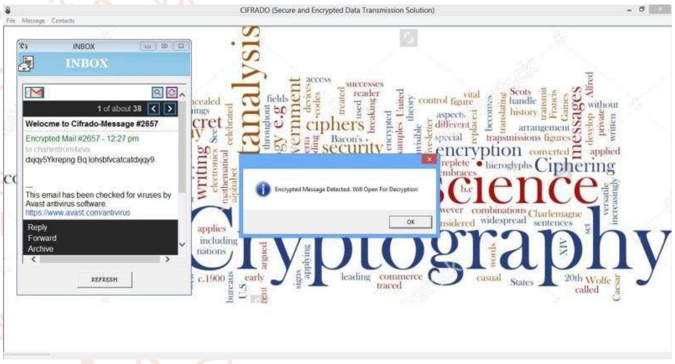
MESSAGE SENT TO: charlestrom4eva@gmail.com

Figure 6: Message to be sent being encrypted



Decryption Key for Message No.2657 is : 26621127
12:28

Figure 7: Encrypted Message Detection



CIFRADO (Secure and Encrypted Data Transmission Solution)

1 of about 38

Welocme to Cifrado-Message #2657

Encrypted Mail #2657 - 12:27 pm
to charlestrom4eva
dxjqy5Ykrepng Bq lohsbfvcatcatdxjqy9

This email has been checked for viruses by Avast antivirus software.
https://www.avast.com/antivirus

Encrypted Message Detected. Will Open For Decryption

Figure 8: Key sent to mobile successfully

8. Summary

The majority of the emails sent are not designated as sensitive. Yes, they can be personal, and you may wish to ensure that the content of a communication is kept private between the sender and the recipient on occasion. However, it is occasionally important to convey sensitive information, such as Social Security numbers, passport numbers, or credit card details, by email. It is required to send an encrypted email message at such times. Because standard email messages are sent in plain text, anyone can read them if they snoop on you. Encrypting mail, on the other hand, renders the communications illegible to anyone who does not have access to the decryption key. This has resulted in the development of a Secure and Encrypted Data Transmission Solution (Cifrado), which uses solid encryption to encrypt messages to be sent through the electronic mailing system and generates an encryption key that will be sent to the intended recipient via some other secure means of communication, who will use the key to decrypt and access the message's contents. The system was successfully implemented on Windows 7, 8, and 10 platforms, and it was created using the Visual Basic programming language, with some sample outputs attached.

9. Conclusion

This software was successfully implemented and provided a secure method of transmitting messages over the Internet via the electronic mailing system (E-mail). The findings of this study should be used to aid in the development of secure methods for exchanging information in additional Internet-based communication platforms.

10. Recommendation

The following suggestions should be considered based on this work:

- This research should be improved in the near future by adding new features;
- Findings from this research should be used in developing means of securing information exchange in other communication tools used over the Internet;
- The research is suitable for use by any organization that requires privacy in their mailing system, such as a bank or the military.

References

[1] Ankid Fadia, Jaya Bhattacharjee (2007), “Encryption, Protecting Your Data”, Vikash Publishing House Pvt Ltd, 2007, ISBN: 812592251-2

[2] Bradley Dunsmore, Jeffrey W. Brown, Michael Cross, “Mission Critical! Internet Security”, Syngress Publishing Inc., 2001, Isbn: 1-928994-20-2

[3] Fauzan Mirza (2001), "Block Ciphers And Cryptanalysis" PhD Thesis, Department of Mathematics, Royal Holloway University of London, 2001

[4] Furnell S., Dowland P. (2010), “E-Mail Security A Pocket Guide”, IT Governance Publishing, 2010, ISBN 978-1- 84928-097-6

[5] Gattiker Urs E., International School of New Media (2018), “The Information Security Dictionary”, Kluwer Academic Publishers, ISBN: 1-4020-7889-7. Retrieved on 20th October, 2018.

[6] Kocher Paul C. (2018), "Timing Attacks on Implementations of Diffe-Hellman, RSA, DSS, and Other Systems", Cryptography Research Inc., San Francisco, USA. Alongbar Daimary et al, / (IJCSIT) International Journal of Computer Science. Retrieved 20th October, 2018.

[7] Menezes, A. J.; van Oorschot, P. C.; Vanstone, S. A. (2005). Handbook of Applied Cryptography. ISBN 978-0849385230. Archived from the original on 7 March 2005.

[8] Nate Lord (2019). What is Data Encryption? Definition, Best Practices and More. https://digitalguardian.com/blog/what-data-encryption, Retrieved 12th January, 2019.

[9] Stamp Mark (2011) , “Information Security Principles and Practice”, Second Edition, a John Wiley & sons inc. Publication, 2011