International Journal of Information Processing and Communication
Vol. 4 No. 1&2

2016

EMAIL DATA SECURITY USING CRYPTOGRAPHY

***A. O. Bajeh, A. O. Ayeni, A. O. Balogun and M. A. Mabayoje**
Department of Computer Science,
Faculty of Communication and Information Sciences,
University of Ilorin, Ilorin.
*Corresponding Author: bajehamos@unilorin.edu.ng

Abstract

Email has become one of the prominent medium of message transmission between web users. Thus, email security measures need to evolve from time to time in order to mitigate security threats which are also evolving and becoming sophisticated. This paper presents a study that proposed, implemented and evaluated the performance of an email security approach that utilizes the Rivest Shamir Adleman algorithm as an additional layer of security. The approach involves an application that converts messages into cipher text as a separate platform. The cipher text is transmitted as the original message on the email platform. Also, the cryptograph keys are transmitted between communicating users via another media such as mobile phone. The proposed approach is evaluated by measuring the accuracy of the message transmitted between users. It showed an average accuracy of 98% over all the scenarios examined.

Keywords: e-mail, security, Rivest Shamir Adleman (RSA) algorithm, cryptography, confidentiality.

Introduction

Security of vital information has been a major challenge facing man even before the advent of information technology. Controlling and safe guarding information and communication in this technology age is as important as controlling water in the desert (Ēlî Biham, 2007). Encryption is the transformation of message (d ata/information) into form unreadable without the secret decryption key. The purpose is to enforce the security of vital information from unauthorized access. It can be used to make data private; it helps in making an unsecured transmission channel serve as a secured means of communication.

Until the advent of computer, one of the main constraints of cryptography had been the ability of the code clerk to perform necessary computation often on the battle field - as the early use of encryption was in military- with little equipment. However, the fear of code clerk being captured by the enemy has made it essential to change encryption method and computer has greatly helped in this change.

Encryption can be defined as the process of converting plain text into cipher text that is incomprehensible but can be converted to its original comprehensible form by using a secret key. Encryption is one of the prominent ways to ensure electronic mails (email) and other important files on a network gets to their intended recipient without a third part getting to know the message content of the email or file. It would be insensitive to underrate the part encryption technology plays in protecting our public and private networks. It is important because it safeguards not just e-mails but also medical records, confidential and corporate information, data on personal buying habits, legal documents, credit histories and transactions. Safeguarding data is essential to peace of mind in communicating business and personal information (Encryption and Its Importance to Networking Device, 2017).

As data sharing or distribution and data security becomes more important and integrity of data is becoming a nightmare, companies, individuals and organizations sought various ways to protect their information (Berry, 2008) . The increase in the sophistication and complexity of the modus operandi of cybercrime and security bridging has necessitated the frequent evolution and innovation of security measures to combat the theft of information and compromise of the integrity of data. This paper proposes email security architecture that adds a security layer on the conventional emailing system so that the message from a sender is originally a cypher text generated using Rivest Shamir Adleman (RSA) cryptography algorithm.

The remaining parts of this paper are organized as follows: section 2 presents a background to the study and a review of related works in the area of email security. The proposed architecture is presented in section 3. The results of the application of the proposed system and a discussion of the results and the performance of the proposed approach are presented in section 4. Section 5 concludes the paper and presents some future area worth studying further.

Background and Related Works

Security Threat

Email should normally include simple tasks of sending and receiving information without any security measure, but several threats have made the need for data security in emailing system very necessary. Data security refers to protective digital measures applied to prevent unauthorized access to computer databases and websites. The focus behind data security is to ensure privacy while protecting private or corporate data. (Alex Biryukov, 2004). There are many different threats to computer systems in general and the data stored on them in particular. These threats increased considerably when computer networking started and with the internet, they have become one of the most important considerations in managing a computer system (Threats to Data Security, 2017). These threats include the following:

Hackers: Unless they are protected, computer system and its content are vulnerable to anyone who wants to edit, copy or delete file without the owner’s permission, such individuals are usually called hackers. A study formulated by researchers at the Ponemon Institute, which measures data collection and information security in the public and private sectors also determined that the number of hacked accounts belonging to individuals numbered at or near 432 million (Jessica, 2015).

Malware: Malware, short for **mal**icious soft**ware**, is designed to gain access to computer system without the owner's consent. The expression is also a general term used to describe a variety of hostile, intrusive, or annoying software. These software are sometimes incorrectly referred to as computer viruses. Malware is not the same as defective software that has a legitimate purpose but contains harmful bugs. The AV- TEST Institute registers over 390,000 new malicious programs every day. These are examined using the analysis tools: Sunshine and VTEST, and are classified according to their characteristics. An updatable visualization program represents the results of the current malware statistics in the form of visual diagrams. Figure 1 depicts the trend of increase in malware infection for over the last thirty years.

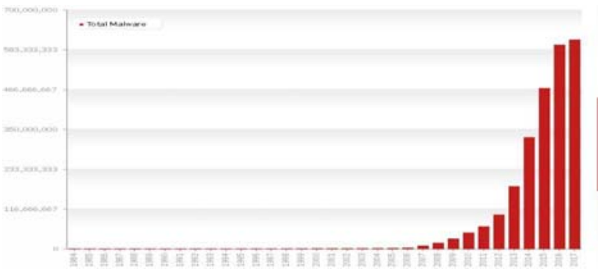


Figure 1: Malware spread (Malware Statistics and Trends Report , 2017)

Crime ware: This is a class of malware designed to specifically automate cybercrime. Its purpose is to carryout identity theft. It is most targeted at financial services companies such as banks and online retailers for the purpose of taking funds from those accounts or making unauthorized transactions to benefit the perpetrator controlling the Crime ware (Markus Jakobsson, 2008).

Spyware: spyware is a type of malware that is installed on computer and collects bits of information at a time about users on the network without their knowledge. It can be very difficult for a user to tell if spyware is on the computer. As many as 90% of U.S. home computers have been infected with spyware at some time and a majority of PC owners do not know how to solve the problem (Leath, 2004).

Virus: A computer virus is a piece of software designed to disrupt or stop the normal working of a computer. They are called viruses because like a biological virus, they are passed on from one infected machine to another and can self-replicate on the machine. Downloading software from the Internet, attachments to emails or using USB memory sticks are the most common ways of a virus spreading or infecting computers. It accounts for 57% of the threats affecting data security (Brain, 2016).

***Worms*:** A worm is a computer program, which can self-replicate and propagate over the network, with or without human intervention, and has malicious intent. It uses a computer network to send copies of itself to computers on the network and it may do so without any user intervention. It is able to do this because of security weaknesses on the target computer (Syed, 2009). Unlike a virus, it does not need to attach itself to an existing program. Worms usually cause at least some harm to the network, if only by consuming bandwidth whereas viruses corrupt or modifies files on a targeted computer.

***Trojan Horses*:** Trojan horses are designed to allow a hacker remote access to a target computer system. Once a Trojan horse has been installed on a target computer system, it is possible for a hacker to access it remotely and perform various operations. The operations that a hacker can perform are limited by user privileges on the target computer system and the design of the Trojan horse, it is estimated that Trojan horses account for 83% of the worlds' malware infections (Radware, 2017).

***Phishing*:** Phishing is an e-mail fraud method in which the criminal sends out legitimate- looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well-known and trustworthy Web sites. Web sites that are frequently spoofed by phishers include financial and commercial sites such as PayPal, eBay, MSN and Yahoo. A phishing expedition, like the fishing expedition it is named after, is a speculative venture in which the phisher puts the bait (fraudulent email message) hoping to fool at least a few of the prey that encounter it and take the bait. The criminal could then use the information to take money from the person’s account for example. Cyber attackers are playing the long game against large companies, but all businesses of all sizes are vulnerable to targeted attacks. In fact, the number of spear- phishing campaigns targeting employees increased to 55% in 2015 (Internet Security Threat Report, 2016) . The number of phishing website observed by APWG for example, increased 250% from the last quarter of 2015 through the first quarter of 2016 (APWG, 2016).

Cryptography

Cryptography is utilized in various applications and environments. The specific utilization of cryptography and its implementation will be based on many factors particularly to the computer system and its associated components. In general, cryptography is used to protect information while it is being communicated between two points or while it is stored in a medium vulnerable to theft (Coppersmith, 1994) . In communication, cryptograph provides protection to data by enciphering it at the transmitting point and deciphering it at the receiving point. In file security, protection of data is by enciphering it when it is recorded on storage medium and deciphering it when it is read back from the storage medium. In the first case, the key must be available at the transmitter and receiver ends simultaneously during communication. In the second case, the key must be maintained and accessible for the duration of the storage period (Hansche, 2005).

One of the most popular cryptography algorithms is the Rivest Shamir Adleman (RSA) (Wolf, 2008). RSA is a public key cryptosystem for both encryption and authentication that was invented in 1977 by Ron Rivest Adi Shamir and Leonard Adelman. It is the most widely used public-key cryptosystem today and has often been called the de facto standard (Frösen, n.d.). The operation of RSA is as follows:

> *Take a large primes, p and q and find their product in a PQ. Choose a number, less than n and relatively prime to (p-l)(q-I) and find its inverse d, mod (p-I)(q-I), which means that 6d= I mod (p-l)(q-l); 6 and d are called the public and private exponents respectively. The public key is the pair (7, 6) and the private key is d.*
> *The factors p and q must be kept secret or destroyed. It is difficult to obtain the private key d from the private key (n, e) if one could factor n into p and q. However, one could obtain the private key d. Thus, the entire security of RSA is predicted on the assumption that factoring is difficult (Howe, 2004).*

RSA operations are all based on series of multiplications. In practical applications, it is common to choose a small public exponent for the public key. Entire groups of users can use the same public exponent. Algorithmically, this encryption is faster than decryption and verification is faster than signing in: public key operations take 0(k/\2) steps, private key operations take 0(k/\3) steps and key generation takes 0(k/\4) steps, where k is the number of bits in the modules (Junod, 2001).

The security of RSA depends on the difficulty of factorization. There are several methods to try factoring, but as long as the keys are long enough there's small risk of having the RSA encoded messages broken. 384 bits can be broken relatively easily, 512 bits is probably unsecured and breakable by government personnel, 768 bits probably is relatively safe, 1024 bits should be secured for decades according to today’s information, and 2048 bits will probably remain safe for a long time.

Email transmission

An email usually sent through an address in the form of mails are composed and sent on a client computer to an outgoing mail server through the Simple Mail Transfer Protocol (SMTP) server, which is like the local post office that checks postage, address and figures out where the mail should be sent. The SMTP server then contacts a Domain Name System (DNS) server for the interpretation of the domain. The DNS server translates domain names to IP address. It also checks if the domain name has mail exchange servers on it, which is required to know where the mail is supposed to go and if the receiver has facilities to receive it. With the proper information at the disposal of the SMTP, the message is dispatched from the SMTP to the desired domain exchange server called Mail Transfer Agent (MTA) which resolves the best place to put the mail. The mails are fetched using a client that operates through Post Office Protocol (POP) invented in 1984 used for downloading emails from a remote server or Internet Message Access Protocol (IMAP) invented in 1986, designed to allow remote access to emails stored on remote server (Sieber, 2012).

Emails are liable to information exposure. With access to certain tools, a third party can easily gain access to its contents (Toorani, 2008). Thus, in order to ensure privacy email encryption methods are adopted (Lee, 2013) using protocols such as Bitmessage, OpenPGP, Secure/Multipurpose Internet Extensions (S/MIME) and Transport Layer Security (TLS).

Most email clients offer support for the encryption protocols mentioned above, add- ons are also available to support specific type of protocol e.g. PGP Desktop email provides backbone for OpenPGP encryption (Geier, 2012; Henry, 2013). While these protocols and add-ons can protect messages, they also have their shortcomings:

i. They can be very tough to use the intended way. Whitten (1999) showed that most users of PGP for example could not sign in and encrypt messages. In another study published by the same institution in 2005 when a newer version of PGP was available, showed that decrypting with the new version was easier, however, users still toiled with encrypting messages, verifying public encryption keys and revealing their own keys (Cranor, 2005).

ii. With the difficulty that comes with encryption, most companies and individuals have automated the encryption process by using third party appliances and services. This takes the entire process out of the users' hands leaving it to configured gateway appliances to guarantee strict conformity with stated rules and security policies. The brunt of the whole process is however borne by the recipient who must use the same encryption gateway appliance which may not be readily available. Not being behind the same encryption gateway means the recipient has to procure the public key each time a message is sent or log into a designated portal to gain access (Rivera, 2016).

iii. Inconsistent implementation: Yahoo's automatic encryption connection between users and its mail service for example came into existence in 2014 with full support for HTTPS—SSL/TLS encryption over HTTP. Its implementation however seems inconsistent across servers and technically insecure in some cases (Geier, 2012).

The proposed system will provide a simple, friendly interface and environment for users to quickly sign in and encrypt/decrypt messages using easily verifiable keys between the sender and receiver of the message. The system will also be cheaper to use than most third party appliances and services with configured gateway because there will be no extra charge for keys each time a message is to be encrypted/decrypted. Its implementation is server independent thus making it consistent across different servers.

The pivotal article of (Babrahem, et al 2015) examined several solutions and standards that have been fashioned according to recent security requirements in order to enhance email security. They noted that some of the existing enhancements focused on keeping the exchange of data via email in confident and integral way while the others focus on authenticating the sender and prove that they will not repudiate from his message. The paper surveyed various email security solutions and introduced different models and techniques used to solve and enhance the security of email systems and evaluate each one from the viewpoint of security. Table 1 presents these studies and their strength and shortcomings.

S/N	Email security model	Author(s)	Strength	Weakness
1.	Developing a Model to Enhance E-Mail Authentication against E-Mail Address Spoofing Using Application.	(Zadgaonkar, S., Pandey, V.C. and Pradhan, P.S., 2013)	Authenticate the identity of the e-mail sender by checking the header field of the message	It requires the distribution of public keys and biding them to their owners which is time consuming.
2.	Identity Based Email Sender Authentication for Spam Mitigation.	(Hameed, S., Kloht, T. and Fu, X.M., 2013)	Authenticate identity by providing signature to provide easy and reliable approach to combine the legitimate sender identity unambiguously to his e-mails	iSAT has low computational footprints and overhead is imposed.
3.	An SSL-Based Client-Oriented Anti-Spoofing Email	(Mooloo, D. and Fowdur, T.P. , 2013)	Provide authentication by using cryptographic self-	To receive a confirmation

	Application.		signed certificates for a secure exchange	message, the client computers have to be authenticated alongside the e-mail turned on and the application must be running to avoid spoofing.
4.	Secure and Privacy-Enhanced E-Mail System Based on the Concept of Proxies.	(Kounelis, I., Muftic, S. and Loschner, J., 2014)	Protection of e-mails, including privacy of locations from which the e-mail system is accessed.	The proxy server represents a single point of failure, when it is fails, we need authentication of legitimate users. Implementation issue is complicated.
5.	CryptoNET: Design and Implementation of the Secure Email System.	(Ghafoor, A., Muftic, S. and Schmölzer, G., 2009)	Enhance e-mail system using certificates, smart Cards and crypto objects with high degree of Security for professional users.	The proxy server represents a single point of failure, when it fails we need a backup.
6.	Trusted Email Protocol: Dealing with Privacy Concerns from Malicious Email Intermediaries.	(Jang, J., Nepal, S. and Zic, J., 2008)	Parties involved can be trusted according to their TPM message.	Requires a paid key which can be expensive.
7.	Biometric-Based Security System for Plaintext e-Mail Messages	(Al-taee, M.A. et al 2009)	Ensures the confidentiality of email message plaintext using improved encryption authentication between the email sender and receiver using biometric features.	Exponential Relationship between the time used for the encryption/decryption and decryption algorithm ensures a certain plaintext size
8.	Stallings, W.	(Stallings, 2014)	Provides e-mails with confidentiality by using Symmetric block ciphering algorithm. The integrity is provided	The system can be initiated before inserting the E-Token

			using the SHA-1 and RSA. It uses three authentication techniques: password, Biometric authentication and E-Token to validate the e-mail account and the user. Non-Repudiation achieved using the bi-directional digital signature.	

The models however could not effectively:

i. protect emails transfer from sender to receiver via secure channel.
ii. apply client-side security system to provide more of restrictions and to make effective and secure transactions.
iii. consider other environments that use the e- mail systems. That is, they are not platform independent.

The main enhancements they founded are in two directions, which are the authentication of the email user identity and the confidentiality and privacy of the email transforming. They showed that these enhancements have improved the performance of the proposed systems and they reached a required level of security.

Hosnieh (2013) classified security approaches used in email system according to the protection mechanism provided by the email components. The latest developments in email security using cryptography were considered in details. They also described the use of these approached in the new generation of Internet Protocols IPV6 in comparison to the old Internet Protocol, IPV4.

Proposed System Architecture

The proposed email security architecture is depicted in Figure 2. It shows the conventional email system in which email messages are transferred between a sender client and a recipient client through email servers on the internet. In addition to this, is a computer program that initially transforms the original email message into a cipher text at the sender end and also transform the cipher text back to the original message at the receiver end.

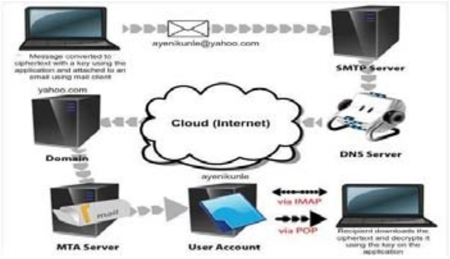

ayenikunle@yahoo.com
Message converted to ciphertext with a key using the application and attached to an email using mail client
SMTP Server
yahoo.com
Cloud (Internet)
Domain
DNS Server
ayenikunle
mail
via IMAP
via POP
MTA Server
User Account
Recipient downloads the ciphertext and decrypts it using the key on the application

Figure 2: Proposed email system architecture

Figure 3 depicts the how the architecture is used to secure email messages.

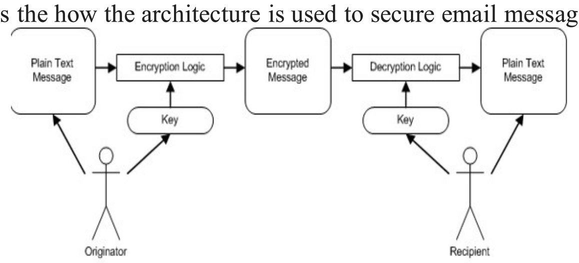


Figure 3: Encryption and Decryption of email messages

In this architecture, email messages are encrypted on the sender's computer using the RSA algorithm. The generated cipher text can be pasted as the email content or as an attached message and sent to the recipient. At the receiver's end, the recipient copies the email content or download the attached message and load it on the computer program for decryption purpose. The procedure for the use of the proposed email architecture is as follows:

Start
Step 1: The sender composes the message to be sent with the application
Step 2: The application encrypts it with a key using the application to create a cipher text.
Step 3: The sender logs into a mail client.
Step 4: The sender attach the cipher text to the mail composed with the mail client.
Step 5: The mail along with the attachment is sent to the recipient.
Step 6: An alternative means e.g. mobile phone is used to send the encryption key to the recipient.
Step 7: The recipient logs into a mail client.
Step 8: The recipient downloads the cipher text.

Step 9: The recipient decrypts the cipher text using the same application and the key generated by the sender.

End

A practical scenario of the use of the proposed system is:
Suppose an encrypted Message, Msg. is to be sent to Kenny from Tai. Kenny will use Tai's public key (*z,e*) to calculate Msg.** *e* (modulus *z*) = *r*, where *r* is the cipher text. Kenny sends r to Tai. Tai then calculates r**w (modulus *z*) = Msg. The value *w* is only known to Tai which means he alone can calculate r**w (modulus z) = Msg to recover the message.

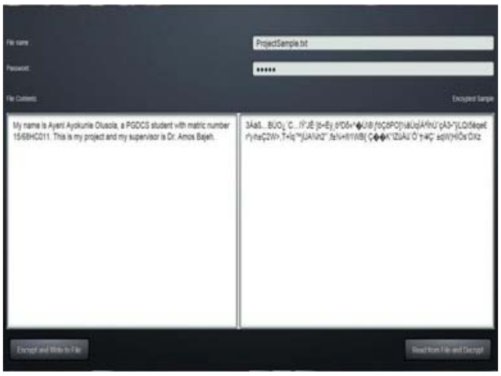
Results and Discussion

This section presents the observed results in the application of the proposed e-mail security approach (presented in section 3) in sending emails. The performance of the approach is also evaluated and discussed.

Results

Several messages were prepared and sent using the approach proposed in the system architecture. Figures 4 (a) to (e) presents the prepared message and its corresponding cipher text at the sender's end.

(a)



File name: ProjectSample.txt

Password: •••••

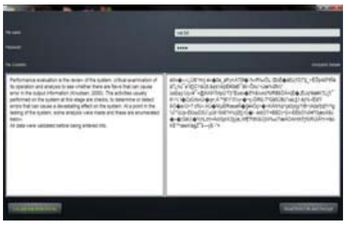
File Contents

My name is Ayeni Ayokunle Olusola, a PGDCS student with matric number 15/68HC011. This is my project and my supervisor is Dr. Amos Bajeh.

Encrypted Sample

[illegible]

(b)



File name: [illegible]

Password: ••••

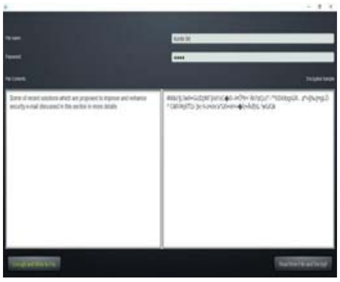
File Contents

Performance evaluation is the review of the system, critical examination of its operation and analyses to see whether there are flaws that can cause error in the output information (Knudsen, 2000). The activities usually performed on the system at this stage are checks, to determine or detect errors that can cause a devastating effect on the system. At a point in the testing of the system, some analysis were made and these are enumerated below:-
All data were validated before being entered into.

Encrypted Sample

[illegible]

(c)



File name: kunle.txt

Password: ••••

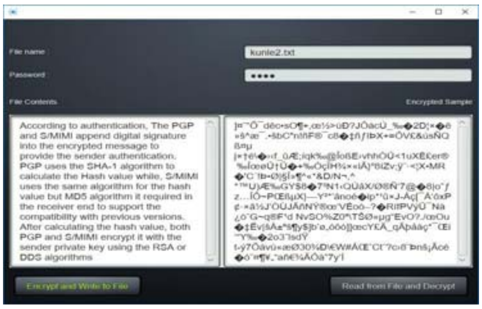
File Contents

Some of recent solutions which are proposed to improve and enhance security e-mail discussed in this section in more details

Encrypted Sample

[illegible]

(d)



File name: kunle2.txt

Password: ••••

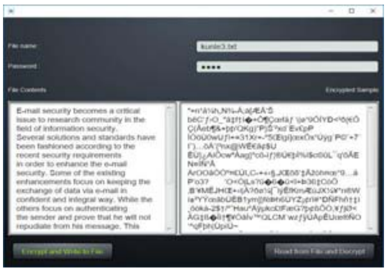
File Contents

According to authentication, The PGP and S/MIMI append digital signature into the encrypted message to provide the sender authentication. PGP uses the SHA-1 algorithm to calculate the Hash value while, S/MIMI uses the same algorithm for the hash value but MD5 algorithm it required in the receiver end to support the compatibility with previous versions. After calculating the hash value, both PGP and S/MIMI encrypt it with the sender private key using the RSA or DDS algorithms

Encrypted Sample

```
]¤¯Õ¯déo•sO¶•,œ½>ûĐ?JÔácÙ_‰�2D¦×�ê
»š^æ¯.·šbC"nñF®¯cß�‡ñƒÎÞX+=ÖV£&ûsÑQ
ß¤µ
|×†ê\�›f_ûÆ;íqk‰@ÎoßE›vhhÖÜ<1uXÊ£er®
‰ÎœøÛ†Ü�+‰ÖçÎH¼××ÍÅ)*ßíZv;ÿ¨·<¦X•MR
�'C¨Ib÷Ø)§Î»¶^«*&D/N¬.^
*™Ú)Æ‰GY$ß�7'N1‹QÙàX/ØßÑ'7@�ß|o"ƒ
z…ÌÖ~PŒfiµX]—Ÿ²*änoé�ìp*'ü×J-Âç[¯Ä'ôxP
¢·×ä½J'ÖÙJÄñNŸ®œ'VÈoô–?�RifPVÿÛ¯Nä
¿ó¨G~q®F'd NvSO%Z0*\TŜØ»µg"EvO?./œOu
�‡Êv|šÅ±*š¶y$]b'ø,óôö‖œcYÊÅ_qÅþäâç*¯Œi
¯Ÿ‰�2o3¯lsdŸ
t-ÿ7Öåvû«æØ30%Ð\€W#ÅŒ'Ct¨7c›ß¯Þnš¡Åoé
�ó¨#¶¥,˜añ€¾ÅÖä"7y'l
```

(e)



File name: kunle3.txt

Password: ••••

E-mail security becomes a critical issue to research community in the field of information security.
Several solutions and standards have been fashioned according to the recent security requirements in order to enhance the e-mail security. Some of the existing enhancements focus on keeping the exchange of data via e-mail in confident and integral way. While the others focus on authenticating the sender and prove that he will not repudiate from his message. This

```
"•n'Ä¼,N¼-Ä,a¢ÆÄ'Š
bßC'ƒ›O_"ä‡†!◆+Ô¶Çœtä ƒ \œ"9ÔÏYÐ<'ð¡€Ö
Ç(Äœb¶&+þþ/QKg)"P)Š"xd EvÇpP
ÌÖöÙ0wÚƒl••31X÷-"5ŒgÌ)œxÔx'Ùyg P0'+7
Î")…ôÄ'(¹nx@WÊ€Ä¢$U
ÊÜ¡¿AìÒcw"Äag)"cô-Ìƒ)8Ù€þ¾$c0ôL¨q'óÄE
NèÏÑ'Ä
ArOOäÖÖ"¤EÜLC-•+¡§,JŒ5ô'‡Ä2òhœ"9…ä
P'o3?     'O<Ö¦Ls?G◆G◆G<9•Þ36‡OôÖ
.B'¥MÊJHŒ•÷¡Ä?ôa½[¯}yÊfKmÆüJX¼¥"nßW
ia"YYœàbÜÊB1ym@ÑôHGÜYZ¿ën¥"DÑFhñ†‡!
_ôókâ-2$†/"Hau"ÄÿµAcDFæG7þ¢ßÔÖ,¥ƒþ<
ÄG‡B◆li†¶¥Oälv"™QLCM wzƒÿÜApÊUœtÑÖ
^qFþ¾(ÛpÙ~
```

Figures 4 (a)-(e): messages and their corresponding cipher text in the proposed architecture

Discussion

Unlike the email security systems reviewed by Afnan (2015), the proposed architecture added another layer of security using a computer program that uses the RSA algorithm for the encryption and decryption of email messages. The message that will be sent over the network will be cipher text that will be near impossible to be deciphered by a third party who may get hold of the message. The RSA algorithm, known for its robustness, ensures the confidentiality of the message sent over computer network.

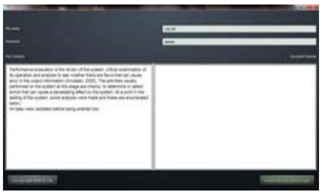
The performance of the system is measured using the accuracy of the received text transmitted over the network compared to the original text from the sender. Accuracy is measured using the following formal expression:

$$Accuracy = \frac{No. of\ words\ coorectly\ decrypted}{No. of\ words\ encrypted} X\ 100$$

This measure gives the number of words correctly encrypted, transmitted and decrypted at the receiver end. Thus, it measures the performance of the proposed system in delivering email messages successfully.

Figure 5 (a) and (c) gives instances measured during the evaluation of the proposed architecture. An average accuracy of 97% was recorded in the evaluation of the proposed approach over 20 examined scenarios.

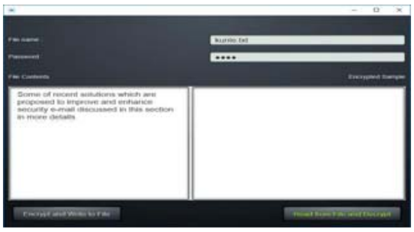
(a)



Performance evaluation is the review of the system, critical examination of its operation and analysis to see whether there are flaws that can cause error in the output information ([illegible], 2005). The activities usually performed on the system at this stage are checks, to determine or detect errors that can cause a devastating effect on the system. At a point in the testing of the system, some analysis were made and these are enumerated below.
All data were validated before being entered into.

Number of words correctly decrypted = 82
Number of words encrypted = 83
Thus, a**ccuracy** = 82/83 X 100 = 98.8%.

(b)

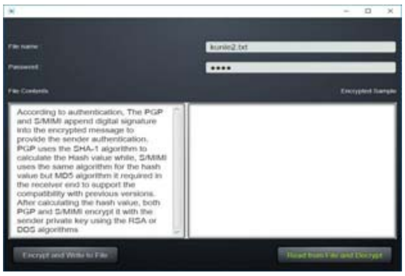


File name: kunle.txt
Password: ****

Some of recent solutions which are proposed to improve and enhance security e-mail discussed in this section in more details.

Number of words correctly decrypted = 19
Number of words encrypted = 20
Thus, a**ccuracy** = 82/83 X 100 = 95%.

(c)



File name: kunle2.txt
Password: ****

According to authentication, The PGP and S/MIMI append digital signature into the encrypted message to provide the sender authentication. PGP uses the SHA-1 algorithm to calculate the Hash value while, S/MIMI uses the same algorithm for the hash value but MD5 algorithm it required in the receiver end to support the compatibility with previous versions. After calculating the hash value, both PGP and S/MIMI encrypt it with the sender private key using the RSA or DDS algorithms.

Number of words correctly decrypted = 76
Number of words encrypted = 75
Thus, a**ccuracy** = 82/83 X 100 = 98.7%.

Figures 5 (a)-(c): Performance evaluation result

With the observed level of accuracy, the proposed approach shows a promising method for email security. Unlike in the reviewed approaches in the literature, the original message in this proposed approach is cipher text which can only be deciphered by the message recipients using a key that is transmitted via another medium such as mobile phone.

Conclusion

The issue of encryption should be stressed to eliminate eavesdroppers and hackers. The importance of encryption in information and communication transfer cannot be over emphasized as it has greatly prevented the theft of valuable information, protected the privacy of individuals and the organization at large. It is becoming more refined increasingly and highly secured (Biham, 2007). The use of cryptography in email messaging provides an enabling and secure environment for users to interact freely with friends, clients, families and associates without the fear of data/information leakage. It also helps in achieving the fundamental aims of computer networking. Without data protection, networking will be rendered porous and useless. However, one thing is certain, a good encryption system must have a very large factor, (i.e. the amount of time required by determined hacker to break it) such as 50 million years or more so that the time factor required breaking it becomes a discouraging factor.

This paper presents an architecture which provides an additional layer of security to the conventional system of email messaging. RSA algorithm is implemented as a computer program that will be used to encrypt and decrypt email messages by users. The application serves as an additional means of making messages sent over mail clients more secured and shows that cryptography is an excellent way of hiding contents of a message in a network environment. The encrypted message (cipher text) serves as the original message to be sent by the sender and received by the recipient who can decrypt the text into the comprehensible form of the message. The proposed system was empirically tested and proved to be reliable. The performance of the process was measured by computing the accuracy of the message delivered to the recipient compared to the originally message prepared by the sender. On the average, a performance of 98% accuracy was observed showing that the proposed architecture is reliable for message transmission between email clients.

Further study will focus on a wider performance evaluation of the proposed system using more users and over a wider area such as across states and regions. Also, the use of steganography to ensure confidentiality of the transmission of information via email will be carried out.

References

Alex Biryukov, C. D. (2004). On Multiple Linear Approximations. *Annual International Cryptology Conference* (pp. 1-22). Berlin: Springer.

Alma Whitten, J. D. (1999). Why Johnny Can't Encrypt:. *8th USENIX Security Symposium*, (pp. 169-183). Washington D.C.

Al-taee, M.A., Al-Hassani, H.N., Bamajbour, B.S. and Al-Jumeily, D. (2009). Biometric-Based Security System for Plaintext e-Mail Messages. *Second International Conference on Developments in eSystems Engineering (DESE)*, (pp. 202-206). Abu Dhabi.

APWG. (2016, May 23). *Phishing Activity Trends Report, 1st quarter, 2016.* Retrieved from APWG: https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf

Babrahem, A.S., Alharbi, E.T., Alshiky, A.M., Alqurashi, S.S. and Kar, J. (2015). Study of the Security Enhancements in E-mail Systems. *Journal of Information Security*, 6, 1-11.

Berry, H. (2008). *Every company needs to have a security program*. Retrieved from Appliedtrust: https://www.appliedtrust.com/resources/security/every-company-needs-to-have-a-security-program

Brain, S. (2016). *Computer Virus Statistics*. Retrieved from Statistic Brain Research Institute: http://www.statisticbrain.com/computer-virus-statistics/

Coppersmith, D. (1994). The data encryption standard (DES) and its strength against attacks. *IBM Journal of Research and Development, 38(3)*, 243–250.

Ēlî Biham, A. S. (2007). Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, 3–72.

Encryption and Its Importance to Networking Device. (2017). Retrieved from Lantronix: https://www.lantronix.com/wp-content/uploads/pdf/Encryption-and-Device-Networking_WP.pdf

Frösen, J. (n.d.). *Practical Cryptosystems and their Strength*. Retrieved from tml: http://www.tml.tkk.fi/Opinnot/Tik-110.501/1995/practical-crypto.html#SCH94

Geier, E. (2012, April 5). *How to Encrypt Your Email*. Retrieved from PCWorld: http://www.pcworld.com/article/254338/how_to_encrypt_your_email.html

Ghafoor, A., Muftic, S. and Schmölzer, G. (2009). CryptoNET: Design and Implementation of the Secure Email System. *Proceedings of the 1st International Workshop on Security and Communication Networks (IWSCN)*, (pp. 402-407). Trondheim.

Hameed, S., Kloht, T. and Fu, X.M. (2013). Identity Based Email Sender Authentication for Spam Mitigation. *International Conference on Digital Information Management (ICDIM)*, (pp. 14-19). Islamabad.

Hansche, S. (2005). *Official (ISC)2® Guide to the CISSP®-ISSEP® CBK®*. Boca Raton, Florida: CRC Press, 2005.

Henry, A. (2013, August 14). *How to Encrypt Your Email and Keep Your Conversations Private*. Retrieved from Lifehacker: http://lifehacker.com/how-to-encrypt-your-email-and-keep-your-conversations-p-1133495744

Hosnieh Rafiee, M. v. (2013). Cryptography in Electronic Mail. In A. e. Elçi, *Theory and Practice of Cryptography Solutions for Secure Information Systems* (pp. 406-427). Pennsylvania (USA): IGI Global.

Howe, D. (2004, Juy 14). *RSA Encryption*. Retrieved from Dictionary of Computing: http://www.dictionary.com/browse/rsa-encryption

Internet Security Threat Report. (2016). Retrieved from Symantec: https://www.symantec.com/security-center/threat-report/

Jang, J., Nepal, S. and Zic, J. (2008). Trusted Email Protocol: Dealing with Privacy Concerns from Malicious Email Intermediaries. *8th IEEE International Conference on Computer and Information Technology*, (pp. 402-407). Sydney.

Jessica, C. (2015, January 14). *How Much Privacy is Good Privacy?* Retrieved from Prezi: https://prezi.com/oq4lp2ihmy15/how-much-privacy-is-good-privacy/

Junod, P. (2001). On the complexity of Matsui's attack. *Selected Areas in Cryptography (SAC'01)* (pp. 199-211). Toronto: Springer.

Kounelis, I., Muftic, S. and Loschner, J. (2014). Secure and Privacy-Enhanced E-Mail System Based on the Concept of Proxies. *37th International Convention on Information and Communication Technology, Electronics and Microelectronics*, (pp. 1405-1410). Opatija.

L. Cranor, G. S. (2005). Security and Usability: Designing Secure Systems that People Can Use. In G. S. L. Cranor, *Security and Usability* (pp. 679-702). Sebastopol, California: O'Reilly.

Leath, P. (2004, November 2). *A Discussion of Spyware.* Retrieved from SANS Institute: https://www.sans.org/reading-room/whitepapers/awareness/discussion-spyware-1546

Lee, M. (2013). *Encryption Works: How to Protect Your Privacy In The Age of NSA Surveillance.* San Francisco, CA 94102: FREEDOM OF THE PRESS FOUNDATION.

Malware Statistics and Trends Report . (2017, February 22). Retrieved from AV-TEST: https://www.av-test.org/en/statistics/malware/

Markus Jakobsson, Z. R. (2008). *Crimeware: Understanding New Attacks and Defenses.* Boston: Addison-Wesley Professional.

Mooloo, D. and Fowdur, T.P. . (2013). An SSL-Based Client-Oriented Anti-Spoofing Email Application. *AFRICON, Pointe-Aux-Piments*, 1-5.

Radware. (2017). *DDoS Attack Definitions - DDoSPedia*. Retrieved from radware: https://security.radware.com/ddos-knowledge-center/ddospedia/trojan-horse/

Rivera, L. (2016). *Protecting customer privacy through email encryption*. Retrieved from scmagazine: https://www.scmagazine.com/protecting-customer-privacy-through-email-encryption/article/538445/

Sieber, T. (2012, August 15). *What Is POP & IMAP and Which One Should You Use for Your Email?* Retrieved from makeuseof: http://www.makeuseof.com/tag/pop-vs-imap/

Stallings, W. (2014). *Electronic Mail Security, in Cryptography and Network Security Principles and Practice. 6th Edition.* Upper Saddle River : Pearson Education.

Syed, F. (2009, April). *Understanding Worms, Their Behaviour and Containing Them.* Retrieved from CSE: https://www.cse.wustl.edu/~jain/cse571-09/ftp/worms/

Threats to Data Security. (2017). Retrieved from ict4u: http://www.ict4u.net/security/threats.php

Toorani, M. (2008). SMEmail - A New Protocol for the Secure E-mail in Mobile Environments. *Australian Telecommunications Networks and Applications Conference* , (pp. 39-44). Adelaide.

Wolf, M. (2008). *Security Engineering for Vehicular IT Systems: Improving the Trustworthiness and Dependability of Automotive IT Applications.* Mörlenbach, Germany : STRAUSS GMBH.

Zadgaonkar, S., Pandey, V.C. and Pradhan, P.S. (2013). Developing a Model to Enhance E-Mail Authentication against. *International Journal of Science and Modern Engineering (IJISME)*, 13-17.