

Application and Evaluation of Rivest Shamir Algorithm for Ensuring Mail Confidentiality within an Intranet

Alese B.K.*
Ogundele O.S.*
Iyare O.*
Ajayi M.O.**

Abstract

Electronic mailing system is a technology that has been adopted by most organization for communication and information storage. This is mainly due to its cheap cost and easy operation. This technology poses serious security problem as confidential messages may leak into an intruder's hand. Therefore, information to be passed within an organization's Intranet need to be protected from intruders. One way of dealing with this problem of security is through cryptography. The design adopted Rivest Shamir Algorithm for encryption/decryption to proffer simple solution to security of organization's mailing system.

The public key cryptosystem, RSA, was normalized and implemented using C++. Simulation runs of 15 mails were used to test the system and the performance was evaluated based on analysis of message length with encryption/decryption time. The results revealed that the more the message length, the higher the encryption and decryption time.

Keywords: Cryptography, Encryption, Decryption, Message length

1. Introduction

Security on the Internet and the Local Area Networks is now at the forefront of computer related issues. The technical jargon of the day is information warfare and network security, and there are valid reasons for their rise in importance. Throughout the evolution of networking and the Internet, the threats to information and networks have risen dramatically [3]. Many of these threats have become cleverly exercised attacks causing damage or committing theft. Consequently, the public has become more conscious of the need for network security and so too has the government. Protective tools and techniques exist to combat security threats; nevertheless, only with the proper implementation will they succeed.

Computer and information security covers many areas within an enterprise. Each area has security vulnerabilities and, hopefully, some corresponding countermeasures that raise the security level and provide better protection. Not understanding the different areas and security levels of network devices, operating systems, hardware, protocols, and applications can cause security vulnerabilities that can affect the environment as a whole.

Two fundamental concepts in computer and information security are the security model, which outlines how security is to be implemented and the architecture of a computer system [14].

Protection of information systems against unauthorized access to modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

Most definitions of information security tend to focus, sometimes exclusively on specific usages and, or, particular media; e.g., "protect electronic data from unauthorized use". In fact it is a common misconception, or misunderstanding, that information security is synonymous with computer security - in any of its guises: computer and network security, information technology (IT) security, information systems security, information and communications technology (ICT) security. Each of these has a different emphasis, but the common concern is the security of information in some form (electronic in these cases). Therefore all are subsets of information security.

As computer use becomes more widespread, so do the opportunities for misuse. Computer hackers (people who illegally gain access to computer systems) often violate privacy and can tamper with or destroy records. Programs called viruses or worms can replicate and spread from computer to computer, erasing information or causing malfunctions. Other individuals have used computers to electronically embezzle funds and alter credit histories [13].

While putting business systems on the Internet offers potentially unlimited Opportunities for increasing efficiency and reducing cost, it also offers potentially unlimited risk. The Intranets provides much greater access to data, and to more valuable data, not only to legitimate users, but also to hackers, disgruntled employees, criminals, and corporate spies [9].

Governments, military, corporate, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. [10] reported that hackers can utilize both active and passive method to overload networks and alter data. It has been demonstrated in [5] that network security applications such as Firewalls, password protection, and the inspection of networks can effectively protect network inputs. However, once data passes through firewalls it must be protected using different techniques. [15] also reported that attacks from within the organization are often difficult to defend since employee may have complete access to customer information.

In [6] their work states that if the data to be protected is within the organization, additional security layer is needed. This additional layer of security must be mission oriented and customizable in other to meet business requirement and allow data sharing within the network boundary.

Using various hacking techniques, intruder can gain access to an unsecured system from any location. The probability of identifying attacks is minimal (about 1 in 20,000) according to FBI

statistics [4]. The following are few alternatives of securing organization network as stated in [5]:

- **Password protection**
Passwords are utilized to control access to a system or networks. However, for a password to be effective it must be complicated and be design to be changed often so that it cannot be used extensively if discovered. Unfortunately users often fail to follow this simple guideline. According to [2], memorization of many passwords is difficult, if not impossible.
- **Protection of network Boundary and connections**
A firewall can protect a network from all external attack by examining all the packets of a message attempting to pass through the networks and rejecting the packet that do not meet the security restriction [11]. However it does not protect the data as it is transmitted from one network to the other.
- **Digital signature**
This is another alternative that may strengthen security. These signatures as reported in [8] can be sent via the public Key Infrastructure and combined with Smart cards and personal identification number (PIN).
- **Encryption and decryption**
Encryption means scrambling the text in a complex manner, so that its contents cannot be understood when reading it. Encryption translates the input text, commonly called plain text, into an unreadable sequence of characters, called cipher text. Only by applying the reverse function to the cipher text (i.e., decrypting) that the original text will be obtained.

The first encryption/decryption algorithms were based on the symmetric key encryption, which made it virtually impossible to decrypt an encrypted text into plaintext without the use of a secret key. Each participant possesses a secret, private key and a public key that is known to potential recipients. Both keys are used to encrypt, and matching keys are used to decrypt the message. The public key verifies that the sender is the one who transmitted it. The keys are modified periodically, further hampering unauthorized unscrambling and making the encrypted information more difficult to decipher. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption. The secret key must be known to both the sender and the receiver for encryption and decryption, and must use a private key. The same key must be used on the receiver end to decrypt the cipher text.

A more complex form of encryption uses two keys, called the public key and the private key, and a system of double encryption. Cryptography is used in information security to protect information from unauthorized or accidental disclosure [1] while the information is in transit (either electronically or physically) and while information is in storage [7].

To achieve a confidential exchange of information, cryptographic techniques are commonly used especially for confidentiality modeling. Another important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information

is equal and so not all information requires the same degree of protection [12].

2. Design Approach

Commercial off-the-shelf security software may not always provide the level of security anticipated. [16] examine product from 186 vendors and found out that only 11 were complaint with 75 percent of the study requirement and only 1 provided all the security features. The intention of this work is to illustrate that an additional layer of customized security can protect data within an organization's network. This work adopted the structure proposed in [5] as follows:

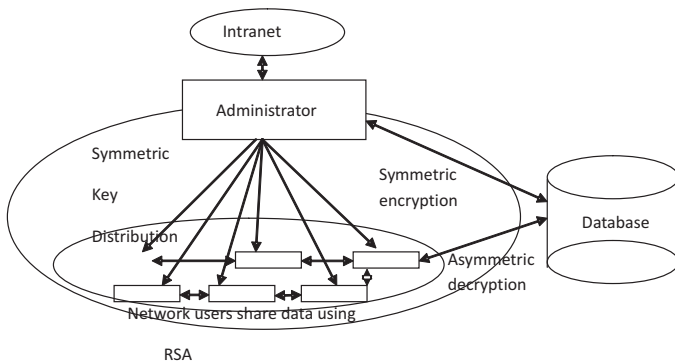


Fig. 1: Physical structure of Data Security for a Small Organization (Adapted from [5])

2.1 Functional Specification

Within the specified network, the Administrator agent and users' agent are the primary active component and their functions are described below.

2.1.1 Administrator Agent

The Administrator Agent provides restricted access to the database to the authorized User. This is accomplished by encrypting the mail prior to writing to the database. Each mail is encrypted using a different key, so that only the authorized workstation can gain access to the information. The Administrator Agent could exist in one of the following states.

Receiving State:

1. Accept new intake and mail to the database.
2. Determines which key to use for symmetric encryption.

Processing State:

1. Generates secret key for mail storage.
2. Create account for users based on privileges and rights

Sending State:

1. Distribute secret keys to users based on access right
2. Encrypts mail from each user using appropriate secret keys.
3. Stores the encrypted mail in the database.

2.1.2 Users Agent

Employees manage the mail account from their own workstation. The sharing of mail between Users Agent is protected by the RSA security layer. As with the Administrator each User can exist in one of three states.

Receiving State:

1. Receives encrypted mail.
2. Decrypts the cipher text using private key.
3. Displays decrypted files on the screen.

Processing State:

1. Performs day to day business activity.
2. Can also generate public key and private key using RSA algorithms.

Sending State:

1. Validates data to be delivered.
2. Encrypts data using the public key of the destination workstation.
3. Can also store the encrypted cipher text in the database.

To share data with other employee, the sender encrypts data using the receiver's public key and the receiver decrypts the data using associated private key. This additional layer of security protects data from internal users that do not have valid access.

The mail server was designed using Microsoft SQL Server 9.0.3042 which is the database where the users information and the mails were stored. SQL Server Management Studio Express, a graphical management tool based on SQL Server Management Studio makes it easy to manage and administer SQL Server Express databases. Reporting Services, an integrated report creation and design environment was used to create reports. Full-Text Search, a powerful search engine was also used for searching text-intensive data.

Column Name	Data Type	Allow Nulls
Sentby	char(150)	☐
Receiver	char(150)	☐
Subject	char(150)	☒
Body	varchar(MAX)	☒
Location	char(10)	☐
Owner	char(150)	☒
Status	tinyint	☒
DateSent	smalldatetime	☐
Ident	uniqueidentifier	☐
id	int	☐
Encrypted	tinyint	☒

Fig. 2: Mail Database

Column Name	Data Type	Allow Nulls
Surname	char(100)	☐
Contacts_name	char(100)	☐
Email	char(150)	☐
Password	varchar(MAX)	☒
Status	tinyint	☒
Owner	char(100)	☐
pubnod	varchar(MAX)	☒
pubexp	varchar(MAX)	☒
privnod	varchar(MAX)	☒
privexp	varchar(MAX)	☒

Fig. 3: Contact Database

3. Design Tools

The interface was designed with Borland C++ (version 6.0). C++ Builder is an Object-Oriented, Visual Programming environment for Rapid Application Development (RAD). Using C++ Builder, one can create highly efficient applications for Microsoft Windows XP, Microsoft Windows 2000 and Microsoft Windows 98 with a minimum of manual coding.

C++ Builder provides all the tools you need to develop, test, and deploy applications, including a large library of reusable components, a suite of design tools, application and form templates and programming.

The encryption and decryption is done by Turbo Power Lockbox, it is a cross-platform toolkit for data encryption. It contains routines & components for use with Borland Delphi, C++ Builder, & Kylix. It provides support for Blowfish, RSA, MD5, SHA-1, DES, triple-DES, Rijndael, & digital signing of messages. ZeosDBO is a database middleware components for Borland development tools, including Delphi, C++ Builder and Kylix. ZeosDBO supports direct connectivity to the following databases using the vendor provided, native interface: MySQL 3.20 - 4.1, PostgreSQL 6.5 - 7.3, Firebird 1.0 - 1.5, Interbase 5.0 - 7.5, Microsoft SQL Server 7, 2000 and Sybase ASE 12.0, 12.

4. System Simulation

The first interface is where the users will be identified as a valid user. The user's name and the password will be validated from the database. After the user has been authenticated the user can now view his mailbox. If the username or password is incorrect, then a small screen pops out to notify the user of the incorrect username or password.



Fig. 4: Mail Menu

The users can check mail from the menu mail which has been sorted into inbox, sent items, draft and deleted.

New mail can be sent by clicking on new button and the next screen pops out where the user can type the subject of the mail, the body of the mail and send it to other registered users whose details are found in the contact list. The contact screen is the drop down screen which shows the contact of all the users within the network.



Fig. 5: Contact List

The cancel will delete the mail and the encrypt button will encrypt the mail using RSA algorithm and the send button will send the mail.

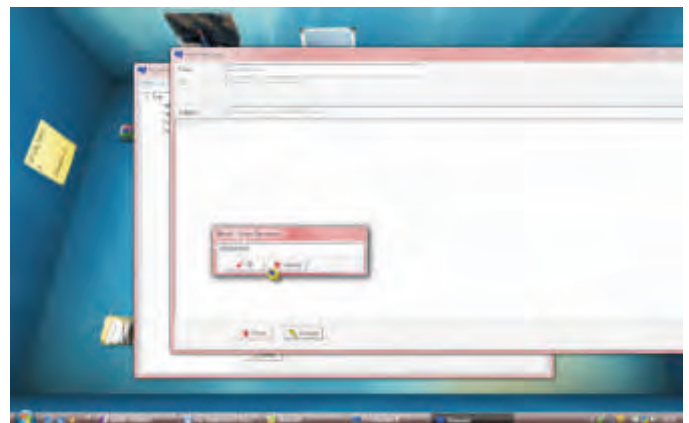


Fig. 6: Inbox

The mail in the inbox can be viewed by clicking the decrypt button, and then a small screen pops out and asks for the key which will be confirmed before a mail can be decrypted. This fastens integrity so that when a user's system is on and an authorized user wants to view the mail it will not respond until the password is confirmed and the authorized user can decrypt the mail. The close button will allow the user to go back to its mail box. The administrator alone has the right to maintain user by registering new user to the network.

The administrator can register new user to the network by new, and can also modify any user's data, for example Surname, First-name, Email and User name by clicking the change button.

The generate Encryption keys will generate key for the user and give that user the right to send mail and be able to encrypt and decrypt received mail, while the save button will save the data that was input by the administrator.

Performance evaluation of the system was determined using the following criteria;

Table 1: Encryption/Decryption Performance Analysis

SENTBY	RECIEVER	ID	ENCRYPTION TIME (MILLISEC)	MESSAGE LENGTH	FUNCTION	EFFICIENCY
Admin@mail.net	here@there.com	44	577	2217	Encrypt	0.26026161
Admin@mail.net	here@there.com	44	0	2217	Decrypt	0
Admin@mail.net	here@there.com	45	577	2217	Encrypt	0.26026161
Admin@mail.net	here@there.com	45	29469	2217	Decrypt	13.2922869
Admin@mail.net	walle@yahoo.com	46	390	1390	Encrypt	0.28057554
Admin@mail.net	walle@yahoo.com	46	0	1390	Decrypt	0
Admin@mail.net	walle@yahoo.com	47	390	1390	Encrypt	0.28057554
Admin@mail.net	walle@yahoo.com	47	19360	1390	Decrypt	13.9280576
Admin@mail.net	seunthetruth	49	312	1007	Encrypt	0.30983118
Admin@mail.net	seunthetruth	49	0	1007	Decrypt	0
Admin@mail.net	seunthetruth	50	312	1007	Encrypt	0.30983118
Admin@mail.net	seunthetruth	50	13244	1007	Decrypt	13.1519364
Admin@mail.net	O@mail.net	51	125	431	Encrypt	0.2900232
Admin@mail.net	O@mail.net	51	0	431	Decrypt	0
Admin@mail.net	O@mail.net	52	125	431	Encrypt	0.2900232
Admin@mail.net	O@mail.net	52	8439	431	Decrypt	19.5800464
seunthetruth	Admin@mail.net	53	156	314	Encrypt	0.49681529
seunthetruth	Admin@mail.net	53	0	314	Decrypt	0
seunthetruth	Admin@mail.net	54	156	314	Encrypt	0.49681529
seunthetruth	Admin@mail.net	54	5538	314	Decrypt	17.6369427
seunthetruth	O@mail.net	55	234	970	Encrypt	0.24123711
seunthetruth	O@mail.net	55	0	970	Decrypt	0
seunthetruth	O@mail.net	56	234	970	Encrypt	0.24123711
seunthetruth	O@mail.net	56	17597	970	Decrypt	18.1412371
seunthetruth	walle@yahoo.com	57	110	178	Encrypt	0.61797753
seunthetruth	walle@yahoo.com	57	0	178	Decrypt	0
seunthetruth	walle@yahoo.com	58	110	178	Encrypt	0.61797753
seunthetruth	walle@yahoo.com	58	1935	178	Decrypt	10.8707865
seunthetruth	here@there.com	59	63	260	Encrypt	0.24230769
seunthetruth	here@there.com	59	0	260	Decrypt	0
seunthetruth	here@there.com	60	63	260	Encrypt	0.24230769
seunthetruth	here@there.com	60	3775	260	Decrypt	14.5192308
walle@yahoo.com	Admin@mail.net	61	188	823	Encrypt	0.22843256
walle@yahoo.com	Admin@mail.net	61	0	823	Decrypt	0
walle@yahoo.com	Admin@mail.net	62	188	823	Encrypt	0.22843256
walle@yahoo.com	Admin@mail.net	62	6038	823	Decrypt	7.33657351
walle@yahoo.com	O@mail.net	63	171	625	Encrypt	0.2736
walle@yahoo.com	O@mail.net	63	0	625	Decrypt	0
walle@yahoo.com	O@mail.net	64	171	625	Encrypt	0.2736

walle@yahoo.com	O@mail.net	64	4680	625	Decrypt	7.488
walle@yahoo.com	here@there.com	65	219	797	Encrypt	0.27478043
walle@yahoo.com	here@there.com	65	0	797	Decrypt	0
walle@yahoo.com	here@there.com	66	219	797	Encrypt	0.27478043
walle@yahoo.com	here@there.com	66	5975	797	Decrypt	7.49686324
walle@yahoo.com	seunthetruth	67	78	217	Encrypt	0.359447
walle@yahoo.com	seunthetruth	67	0	217	Decrypt	0
walle@yahoo.com	seunthetruth	68	78	217	Encrypt	0.359447
walle@yahoo.com	seunthetruth	68	1935	217	Decrypt	8.91705069
O@mail.net	here@there.com	69	140	390	Encrypt	0.35897436
O@mail.net	here@there.com	69	0	390	Decrypt	0
O@mail.net	here@there.com	70	140	390	Encrypt	0.35897436
O@mail.net	here@there.com	70	5741	390	Decrypt	14.7205128
O@mail.net	walle@yahoo.com	71	156	302	Encrypt	0.51655629
O@mail.net	walle@yahoo.com	71	0	302	Decrypt	0
O@mail.net	walle@yahoo.com	72	156	302	Encrypt	0.51655629
O@mail.net	walle@yahoo.com	72	4337	302	Decrypt	14.3609272
here@there.com	O@mail.net	73	265	606	Encrypt	0.43729373
here@there.com	O@mail.net	73	0	606	Decrypt	0
here@there.com	O@mail.net	74	265	606	Encrypt	0.43729373
here@there.com	O@mail.net	74	8799	606	Decrypt	14.519802

- The encryption time which is the elapsed time for a mail that is about to be sent takes to encrypt, and is measured in Milliseconds.
- The decryption time which is the elapsed time for a mail that has been received to Decrypt for the user to read, and also measured in milliseconds.
- The message length which is the length of the message body.

Column Name	Data Type	Allow Nulls
Location	char(10)	☒
Owner	char(150)	☒
Status	tinyint	☒
DateSent	smalldatetime	☒
Ident	uniqueidentifier	☐
Id	int	☐
Encrypted	tinyint	☒
encime	float	☒
dectime	float	☒
messlength	float	☒

Fig. 7: Message Database

The simulation run was tested with 15 mails that were encrypted and sent from different users to other users within the Intranet. The receivers can only view the received message after decrypting them. The encrypted messages that were sent are of different length. This is in order to determine the relationship between message length and encryption/ decryption time.

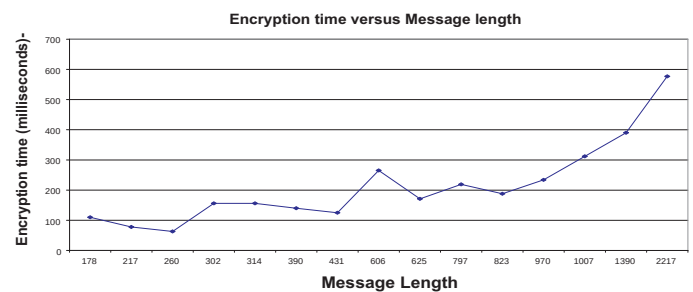


Fig. 8: Relationship between Encryption time and Message Length

It can be deduced from figure 8 that the lower the mail message length, the lower the encryption time. This statement is true for all the mails except few messages of certain length. For instance, mails of message length 2217 to 823 from the performance table follows relationship, while; the encryption time for mails of message length 794 and 606 was higher than the mails of message length 823. Mails with lower message length have lower encryption time compared to the mail of with higher message length.

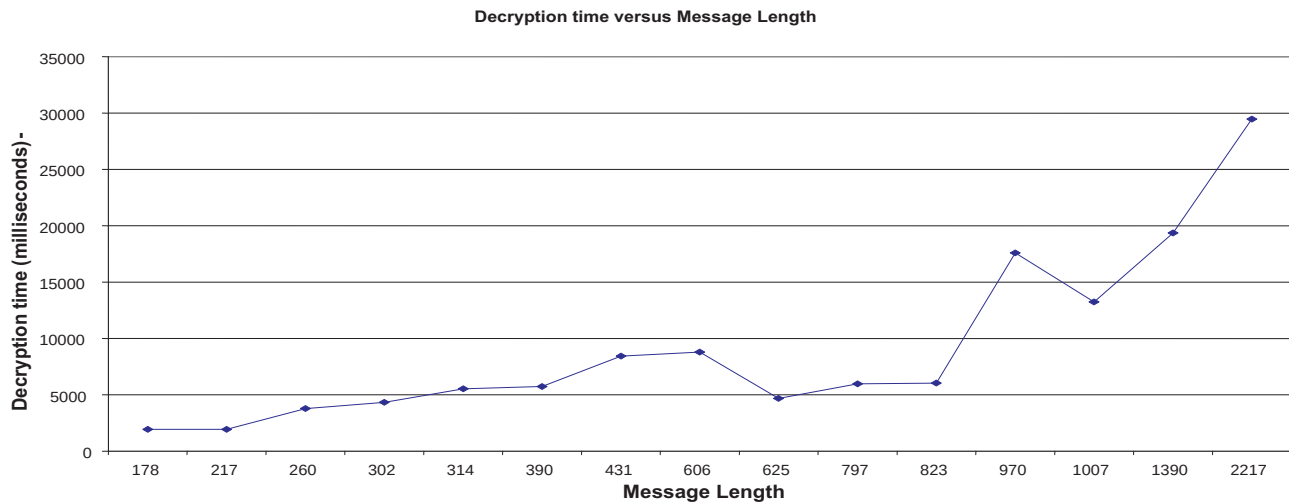


Fig. 9: Message length versus decryption time

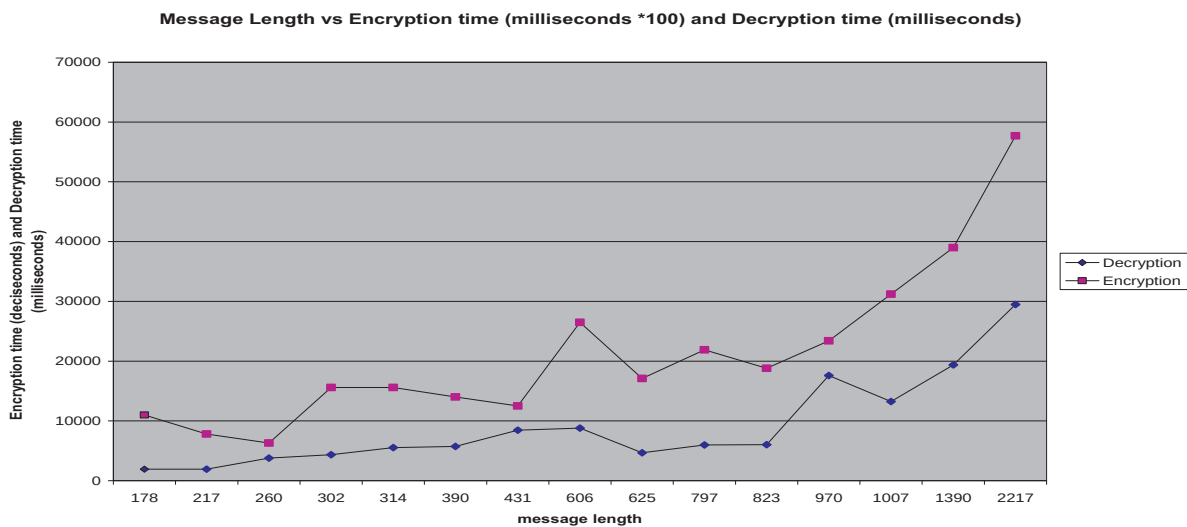


Fig. 10: Message lengths versus encryption time and decryption time

It can also be deduced from figure 9 that on the average the higher the mail message length, the higher the decryption time for all the mails except for very few mails.

Firstly the encryption time has a scale of 100:1 second due to the large difference in the value of encryption time and decryption time.

The graph almost followed the same trend as the encryption time and the decryption time fluctuate with the mail message length because they almost have the same rule of the higher the mail message length, the higher the encryption time, also the higher the mail message length the higher the decryption time.

5. Conclusion

Information Security issues have been major problems that individuals and organization face in everyday endeavours. Electronic mailing system is a common technology that has been adopted by most organization for exchanging messages and storing vital information. This is mainly due to its cheap cost and easy operation. This technology poses serious security problem

as confidential messages may sometime leak into an intruder's hand. Therefore, confidential information that is to be passed within an organization Intranet needs to be protected from intruders. One of way of dealing with this problem of security network is cryptography. The design of this work brings an understanding that the additional layer of security (encryption/decryption layers) included in the design provides great deal of simple solution to security of organization intranet mailing system.

In this research work, the public key cryptosystem, RSA, is evaluated in the context of carrying out in dept study of its features. The algorithm of the cryptosystem was normalized and implemented using C++ programming language.

The major contribution of this work is the introduction of an additional layer of security in securing message communication within an electronic mailing system and the performance analysis of message length with encryption/decryption time. The work is to further bring to bear some of the usefulness of these schemes especially in the area of network security design in industrial organizations, financial institution, research and academic development.

6. References

1. Alese, B.K (2004). "Design of Public Key Cryptosystem using elliptic curve," PhD Thesis, Federal University of Technology, Akure.
2. Armstrong, I (2003). "Password exposed, users are the weakest link". SC Magazine, Vol.14(6), 26-29.
3. Falaki, O.S (2002). "Information Technology in Nigeria, Now or Never", Inaugural Lecture series 29 Delivered at The Federal University of Technology, Akure.
4. Gabrys, E. (2002). "The international dimension of cyber-crime, Part 1". Information System Security, Vol. 11(4), pp21-32.
5. Ghasam S. Alijani, James E. Christy, Hugh Craft, Peter Mok, J. Steven Welsh (2004). Information Security Model for E-business". In the proceedings of ISECON, Rose Island II, Newport. Sat, Nov 6, 3:30 - 3:55,
6. Hammann, E., Henn, H., Schack, T., & Seliger, F. (2001). "Securing E-business Application using Smart Cards". IBM System Journal.
7. ISACA CISA (2006). "Information Systems Audit and Control Association". A review Manual.
8. Kuechler, W., & Grupe, F.H.(2003). Digital Signatures: A business view, Information Systems Management, Vol. 20(1), pp19-28.
9. Mary Ann Davidson. (2001). "Oracle9i Database Security for e-business," An Oracle White Paper.
10. Mirza, D.R., Dubrawsky, I, Flynn, H., Grand, J., Graham, R., Johnson, N.L.(2002). "Hack Proofing your network", second edition Rockland.
11. Moon, J., Cho, H., C, Jung, G, Younkwanga, J, & Choi, K. (2003). "Accelerating firewalls". In the proceeding of SAM '03 International conference.
12. Quist, Arvin S. (2002). "Security Classification of Information" (HTML). Volume 1
13. Snyder, Timothy Law (2007). "Computer." Microsoft® Student 2008 [DVD]. Redmond, W.A, Microsoft Corporation.
14. Stallings, W. (2000). Network Security Essentials. Upper Saddle River, NJ: Prentice Hall.
15. Tribunella, T. (2002). Twenty questions on E-commerce security. CPA Journal, Vol.72 (1), pp 60-63.
16. White, D., & Alijani, G. (2003). Identifying requirements for network security software. SAM '03 International Conference, 539-543.