Covenant Journal of Informatics and Communication Technology (CJICT) Vol. 2, No. 2, December, 2014.

Implementation of Secured Message Transmission using DES and RSA Cryptosystem

Jelili Oyelade[1,*], Itunuoluwa Isewon[1], Olufunke Oladipupo [1] & Abolaji Famuyiwa [2]

[1]Department of Computer and Information Sciences
Covenant University
PMB 1023, Ota, Nigeria.

[2]Department of Computer Science and Technology
Bells University of Technology
P.M.B. 1015, Ota, Nigeria.

* Corresponding Author; ola.oyelade@covenantuniversity.edu.ng.

Abstract: In the past, Cryptography was used in keeping military information, diplomatic correspondence secure and in protection of national security. Nowadays, the range of cryptography applications have been expanded a lot in the modern area after the development of communication means; cryptography is essentially required to ensure that data are protected against penetrations. This is used to ensure that the contents of a message are confidentially transmitted and would not be altered. In this paper, we have implemented a cryptosystem (encrypting/decryption) for text data using both Data Encryption Standard (DES) and Rivest-Shamir-Adleman (RSA) cryptosystem. The asymmetric algorithm was used for the key encryption and decryption process because it provides a means to deliver keys on a secure channel, while the data to be sent will be encrypted and decrypted using the symmetric algorithm. This system was designed to accomplish a number of security features such as authentication, confidentiality, integrity, and non-repudiation. Also the combination of the speed and strength of the symmetric algorithm with the robustness and key management capability of the asymmetric algorithm, thereby producing an enhanced encryption algorithm and we employed text data as our experimental data.

Key words: Cryptography, encrypion, decryption, cryptosystem

1.0 Introduction

The evolution of the Internet has rendered cryptography more essential and crucial subject in electronic application systems. Except the system is capable of offering some mechanisms to ascertain security services, the system will have difficulties to be acknowledged. More reliable cryptosystems is needed to be recommended and cryptography

being a critical part of today's information systems. Cryptography can be defined as the science of using employing mathematics to encrypt data. It allows us to retain or transfer delicate information across unsafe networks such as the Internet. So that it is made impossible to be interpreted by anyone asides the intended recipient (Schneier and John, 1996). Cryptography is seen as a technological methods that offer security to data being conveyed on information and communications systems. A cryptography system that offers two accompanying functions, decryption and encryption is known as cryptosystem. Cryptosystems utilize encryption algorithms to define the encryption method, the required software components, and the key to implement the encryption and decryption of the data (Schneier and John, 1996). Cryptography techniques are constantly used to secure critical and confidential information against malicious attack from the invaders. There are two major categories of cryptographic algorithms: asymmetric key and sysmmetric key cryptography (Stalling, 2006). There exist various cryptographic methods and algorithms that are well-defined in the literature such as RSA, DES and AES (Schneier and John, 1996).

In the field of cryptography, encryption can be described as the process of altering information (known as plaintext) employing an algorithm (termed a cipher) to make it illegible to anyone apart from those who have unique knowledge, normally represented as a key. The outcome of the method is encrypted information (in cryptography, known as cipher text). The inverse procedure, that is to render the encrypted information legible again is known as decryption, in other words to render it unencrypted (Fouché and Helen, 1956).

Encrypted data transmitted across network guarantees confidentiality, even if it is successfully retrieved from the network by attackers who compromise some security measures, the confidentiality of the file data is maintained, as the data is stored in encrypted format. Encryption is simply a process of keeping data private or confidential.

Encryption has been used ever since by governments and militaries to aid confidential communication and transmission. Presently encryption is often used in safeguarding information in various types of civilian for instance. For instance, according to the account of Computer Security Institute in 2007, 71% of the companies considered applied encryption for most of their data in transit, furthermore 53% employed encryption for most of their data in storage. Encryption is able to safeguard data "at rest", like files on computers and backup drives (for example USB flash drives). In modern times there have been various reports of secret data for example customers' private files

being unprotected via damage or thievery of laptops or storage drives. Encrypting such files at rest aids safeguard them, incase physical security measures collapse. Digital rights management systems which block illegitimate usage or imitation of patent material and safeguard software against reverse engineering are to some extent a discrete instance of applying encryption on data at rest (Fouché and Helen, 1956)

In this work, we implemented a cryptosystem for text document data encryption/decryption by combining the features of both symmetric key and asymmetric key cryptography. Using the combination of symmetric algorithm (public key) and asymmetric algorithm (private key) increases the overall encryption speed and equally provides the same level of security as the asymmetric technique when used alone. Since the resulting system will combine the speed and strength of the symmetric algorithm with the robustness and key management capability of the asymmetric algorithm, thereby producing an enhanced encryption algorithm which is the motivation for this work.

This paper is organized as follows: in the next Section, we give a brief review of related works; Symmetric and Asymmetric Encryption are presented. In section 3, we discussed briefly the algorithms development of both symmetric and asymmetric encription employed in this work. Section 4 discusses the results and discussion and we conclude the paper in Section 5.

2.0 Related work

RSA encryption is most commonly used for the transport of symmetric-key encryption algorithm keys and for the encryption of small data items. But this algorithm is very slow compare to the commonly used symmetric-key encryption algorithms such as DES (Menezes and Vanstone, 1996). In Subasree and N. K. Sakthivel (2010), a Dual-RSA scheme using Chinese Remainder Theorem (CRT) for its Decryption that improved roughly ¼ times faster performance of RSA in terms of computation cost and memory storage requirements was developed. The Omar *et al*.(2012) proposed a framework for the combination of both Symmetric and Asymmetric Cryptographic Techniques for a secured communication.

2.1. Symmetric and Asymmetric Encryption

Encryption is one of the strongest and the safest way in securing data. Encryption systems are divided into two major parts, symmetric and asymmetric. Symmetric encryption is known as secret key or single key, The receiver uses the same key which the sender uses to encrypt the data to decrypt the message,. This system was the only system used before discovering and developing the public key., A safe way of data

transfer must be used to moving the secret key between the sender and the receiver in symmetric encryption. Figure 2.1 shows how the system works. Symmetric encryption occurs either by substitution transposition technique, or by a mixture of both. Substitution maps each plaintext element into cipher text element, but transposition transposes the positions of plaintext elements.

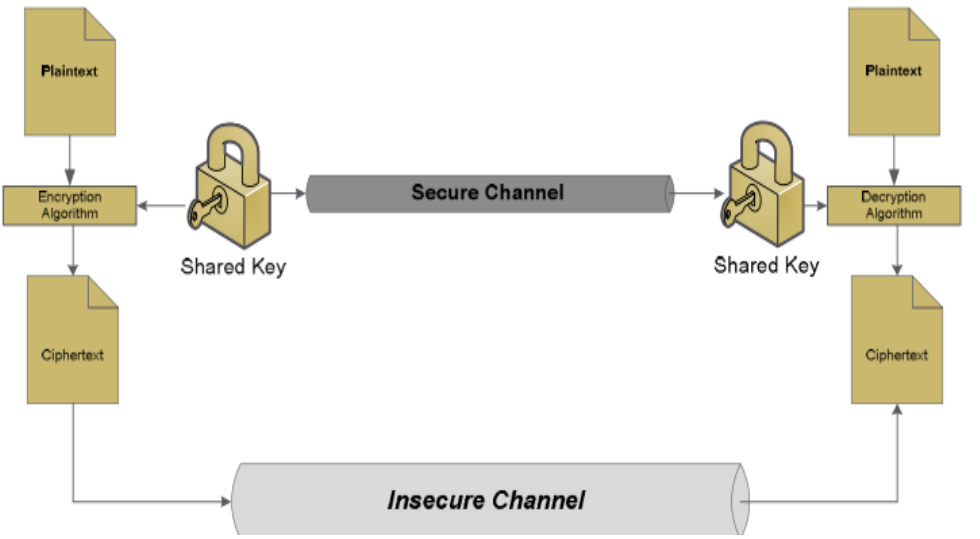

FIGURE .2.1 : Simplified model of conventional encryption (Mohammed *et al.*, 2011)

In 1976 Diffie and Helman invented new encryption technique called public key encryption or asymmetric encryption; Asymmetric encryption is the opposite of symmetric encryption in safety, since it doesn't require sharing the secret key between the sender and the receiver. And this is the main difference between symmetric and asymmetric encryption, the sender has the public key of the receiver. Because the receiver has his own secret key which is extremely difficult or impossible to know through the public key, no shared key is needed; the receiver is responsible for establishing his private and public key, and the receiver sends the public key to all senders by any channel he needs, even unsecured channels to send his public key, asymmetric key can use either the public or secret key to encrypt the data. Also it can use any of the keys in decryption, asymmetric encryption can be used to implement the authentication and non-repudiation security services, and also it can be used for digital signature and other

application that never be implemented using symmetric encryption. Figure.2.2 shows how the system works.

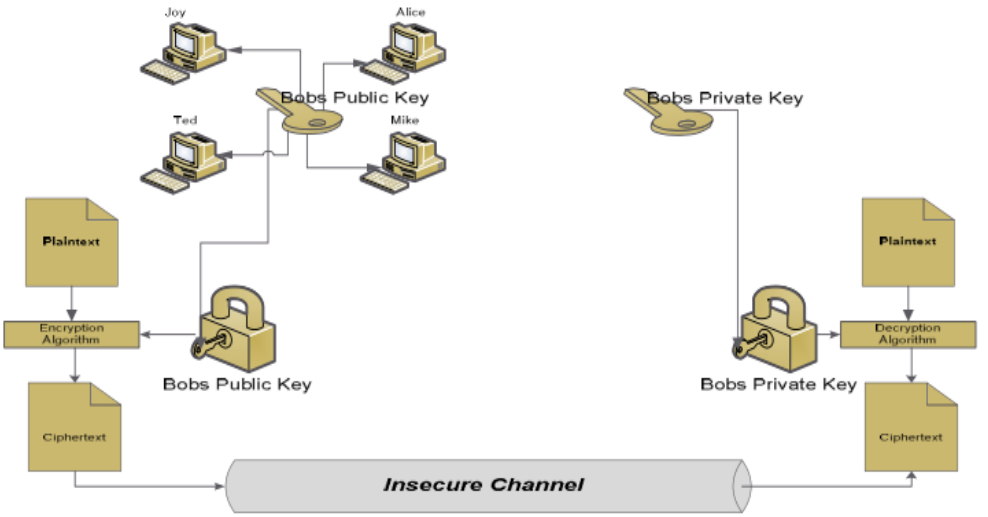

FIGURE 2.2 : Simplified model of asymmetric encryption (Mohammed *et al.*, 2011)

Asymmetric encryption is slower and very complicated in calculations than symmetric encryption. Therefore, asymmetric encryption deals with plaintext as a group of numbers which are manipulated in mathematics, while the plaintext in symmetric encryption deal as group of symbols and characters, the encryption process may permute these symbols, or may substitute one symbol by another. So the nature of the data determines the system of encryption type. And every system has its own uses. For example, asymmetric encryption may be used in authentication or in sending secret key for decryption. Before stated the algorithm in section two, we will explain the following three definitions (Douglas,2006):

Definition 1*:* Let a, n are relatively prime(gcd(a,n)=1), then there is at least one integer m that satisfies a^m mod n=1. m is referred as the order of a (mod n).

Definition 2: If p is a prime number. An element α having order p-1 is called a primitive element modulo p

Definition 3: Let p be a prime number and α is a primitive element modulo p. any element $\beta \in Z_p$ can be written as $\alpha^i = \beta, 0 \le i \le p-2$ in a unique way i.e., $\alpha^i \equiv \beta (\text{mod}) p$, i is called the unique **discrete logarithm.**

3.0 The Algorithms Development

Since the symmetric algorithm is not suitable for network used by itself unless it is being used with the asymmetric algorithm because of its poor key management technique (Paul, 2004), a combination of both techniques was used in this work. The asymmetric algorithm was used for the key encryption and decryption process because it provides a means to deliver keys on a secure channel (Bruce and John, 1996). While, the data to be sent will be encrypted and decrypted using the symmetric algorithm.

This justifies the selection of the RSA encryption algorithm for the asymmetric technique and the DES encryption algorithm for symmetric technique. In this work, the algorithm design is divided into two parts;

i. The key generation process using the asymmetric encryption technique.
ii. The encrypting and decryption process using the symmetric encryption technique.

3.1. RSA Algorithm (Key generation process using asymmetric encryption technique)

RSA can be described as an Internet authentication and encryption system that applies an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman (RSA). RSA algorithm is known to be the best frequently employed encryption and authentication algorithm. The algorithm makes use of the fact that, it is simple to produce a dual huge prime numbers and multiply them but very tough to determine the product. In the RSA algorithm, designing the key generating technique involves taking a dual grand prime numbers, say p and q that are independently and randomly chosen such that they have about 200 decimal digits (but not less than 150) each. Multiply these two numbers to give a new number, N. Also get another value Q by multiplying $(p-1)$ with $(q-1)$. The mathematical expression is given below:

$$N = p * q$$
$$Q = (p-1)*(q-1) \quad 2.1$$

Next, a random integer e known as the "encryption exponent" is selected between 1 and Q such that gcd (e, Q) = 1 (i.e. the Greatest Common divisor of e and Q). This is expressed below;

gcd (e, Q) = 1 such that **(1 < e < Q)**

Then, using the extended Euclidean algorithm, a unique integer for d will be computed as follows:

$e\,d = 1 (\text{mod } Q)$ such that **(1 < d < Q)**

This implies that $d = e^{-1} (\text{mod } Q)$

2.2

This generates the public key which is (N, e) and the private key d.

The public and private keys are thus (N, e) and d respectively, where p = the first prime factor chosen, a nonnegative integer and q = the second prime factor chosen, and a nonnegative integer and N is the modulus.

gcd (e, Q) = Greatest Common divisor between e and Q.

e = encryption exponent.

d = decryption exponent.

(N, e) = the public key.

d = the private key.

By making each of the primes about 200 decimals digits long, the product of **p** and **q** can be calculated easily in a fraction of a second. However, factoring **N** is extremely difficult to achieve, even schroeppel, the fastest known algorithm when used would requires billions of years at the rate of one step per microsecond to arrive at the answer (Davies *et al*., 1991). Using a computer might be faster, but for decimal digit of about four hundred (400) and larger, it will run for approximately Ten thousands, one hundred and seventy six (10176) times the life of the universe to determine the product of **p** and **q** supposing a computer can test one million (1,000000) factorizations for every second in the lifespan of the universe (The universe's lifespan is about 1018 seconds; 18 digit number). The use of large primes for **p** and **q** is the strength of this method (Bellare *et al.*, 1998).

Therefore, the RSA algorithm steps are stated below:

RSA Algorithm Steps:

- Every user generate a public/private key duo by choosing two huge primes arbitrary p, q
- Computing modular value $n = p * q$
- Calculating the Euler's function $\varphi(n) = (p-1)(q-1)$
- Selecting at randomly the public encryption key e, where $1 < e < \varphi(n)$ and e is prime relative to the $\varphi(n)$.
- Solving the following equation to find private decryption key d:
  - $e * d = 1 \text{ mod } \varphi(n)$. such that $(0 \le d \le n)$
- Publishing their public encryption key: $P_K = (e, n)$
- Keeping secret private decryption key: $P_R = (d, n)$
- At the encryption side the sender uses encryption mathematical equation $C = P^e \text{ mod } n$

- At the decryption side the reciever uses decryption mathematical equation $P = C^d \bmod n$

3.1.1 The key encryption and decryption processes

A Key encryption process

Since we now have our public and private keys, the next step is to encrypt the key.

The key to be encrypted can be represented by **m**, where **m** is an integer in the interval (0, **N**-1). We can calculate the cipher text, **C** (encrypted data format) employing the formula below.

$\mathbf{C} = \mathbf{m}^e \bmod \mathbf{N}$

where **C =** the cipher text (encrypted data) and

m = representation of the key in integer

B. Key decryption process

The recipient gets an encrypted key that is of no value unless it is decrypted. For the original data **m** to be retrieved from the cipher text **C,** The private key is used to perform the decryption: $\mathbf{m} = \mathbf{C}^{\mathbf{d}} \bmod \mathbf{N}$.

The illustration shown below explains the process that occur using RSA algorithm,

Illustration

Let **p** = 2357 and **q** = 2551

N = p * q = 2357 * 2551 = 6012707

Ø = (p - 1) * (q - 1) = (2357 - 1) * (2551 - 1) = 6007800

Choosing e = 3674911 and using the Euclidean algorithm to find **d** we have that;

$\mathbf{d} = e^{-1} \mathbf{(mod\ Ø)} = 3674911^{-1} \pmod{6007800} = 422191$

This generate a public key, **N =** 6012707 and e = 3674911, where **d is** the private key

To encrypt, say message, **m** = 5234673;

The cipher text **C** will be $\mathbf{C} = \mathbf{m}^e \bmod \mathbf{N} = 5234673^{3674911} \bmod 6012707 = 3650502$

To decrypt, the original message is recovered at the recipient end by decryption using the formula below:

$\mathbf{m} = \mathbf{C}^{\mathbf{d}} \bmod \mathbf{N} = 3650502^{422191} \bmod 6012707 = 5234673.$

3.2 The encryption and decryption process using symmetric technique

DES utilities series of procedures involving various substitution and permutation primitives to encrypt a data block. These primitives are later employed to invert the encryption operation. *Horst Feistel algorithm* described a range of substitution and permutation primitives which are repeatedly applied to data blocks for a particular number of times, each set of primitive operations is referred to as a "round". The DES algorithm employs 16 rounds to certify that the data are appropriately scrabbled

to meet up with the security goals. DES is a block product and also a figure 2.1 shows a typical implementation of the DES algorithm.

i. *The Initial Permutation (IP):* This is the initial stage. The 64-bit plaintext is permuted built on an Initial Permutation table, that restructures the bits and generates the permuted input. After IP phase, then the next step which is made up of 16 rounds of corresponding function **F().** The procedures involved in each of the rounds is described by these formulas.

Li = Ri – 1o

Ri = Li – 1 XOR F (Ri -1, ki)

where **Ri** = i numbers of rounds.

Li = i numbers of left circle shift.

Ki = i numbers of permutation choice.

XOR = XOR operation.

F () = function involving both permutation and substitution.

ii. *Permuted Choice One (P1):* The Permuted Choice One (P1) implements permuted choice of 64 bits and returns 56 bits, the remaining 8bits are used for parity (error checking) bit.

iii. *Left Circular Shift (LCS):* The 56-bit output from permutated choice one (P1) is divided into 28-bit block cipher (Shah *et al.,* 2005). The flow chart in blocks each. After having these two 28-bit blocks, the dual now go through a circular left shift of their bits, the number of shifts stated from a list of shifts for each of the rounds.

iv. *Permuted Choice Two (P2):* Following LCS and every one round, a new permuted choice is executed, which leads to the production of a 48-bit sub-key. The *P2* procedure iterates up util sixteen (16) 48-bit sub-keys are generated.

v. *32-bit Swap:* The 64 bits of output from round 16 has left 32 and right 32 bits. These left and right 32 bits blocks are swopped.

vi. *Inverse Permutation (IP^{-1}):* This particular stage is the reverse of the inverse permutation. It gets the input of 64 bits, and alters their sequence again to get a cipher text.

vii. *Encryption and decryption:* DES works on 64-bit "plaintext" data blocks, passing them under the manipulation of a 56-bit key to generate 64 bits of encrypted cipher text as shown in figure 3.1. Likewise, the DES decryption technique runs on a 64-bit cipher text block employing the same 56-bit key to generate the initial 64t plaintext block. This is a reverse of the encryption process (Kavitha *et al*., 2008).

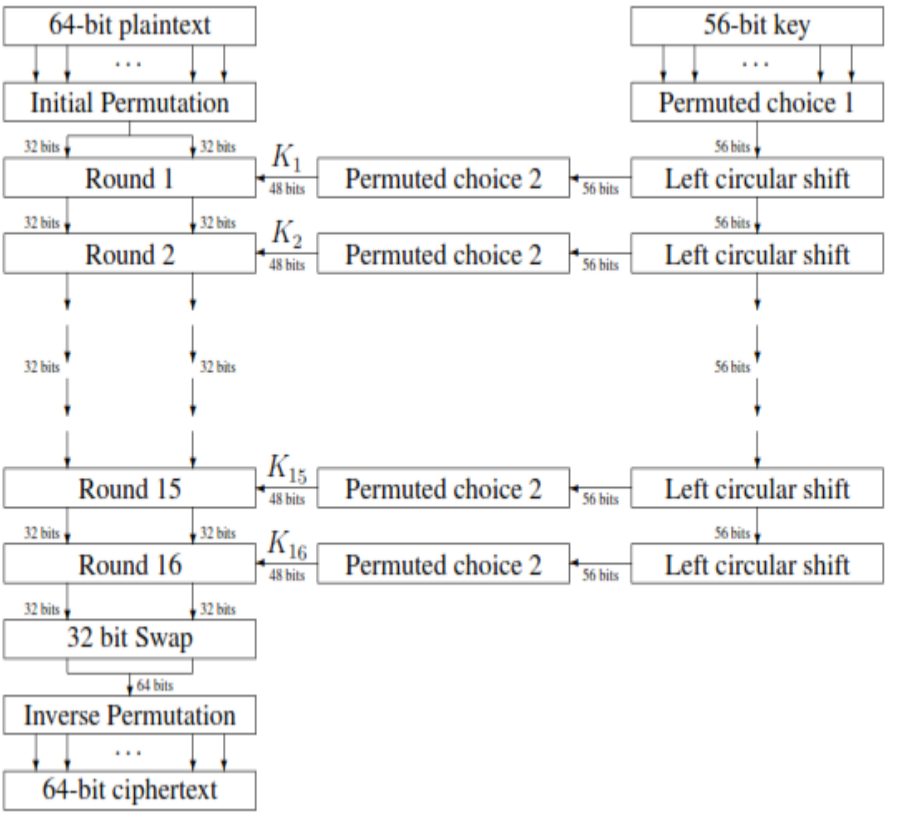

Fig 3.1: General Depiction of DES Encryption Algorithm for encrypting data (Bellare *et al.*, 1998)

4.1 Results and Discussion

4.1.1 Results

The Design implementation for this work is divided into two parts, namely;

The Communication Client implementation

The Communication Server implementation

Both implementations, the Communication client and the Communication server implementation uses Sockets for communication between each other which enables the sending and recipient of data between both ends. The transport protocol used in the implementation design is the Transmission/Transfer control Protocol (TCP). Also, threading and cryptographic function of .NET was used for the implementation. The role of the two implementations is described in the following as follows:

A. The Communication Client Implementation

In this implementation, which is the client side, files are selected, encrypted and sent by specifying the Server`s Internet Protocol (IP) address. The communication client implementation is shown in Fig 4.1 below and its different components explained below;

i. The File Type Combo Box: Here the file type is specified. in this work, the file type can be either .txt or .doc document.

ii. The File Text Box: This displays the name of the selected file using the "browser button" located on its right side.

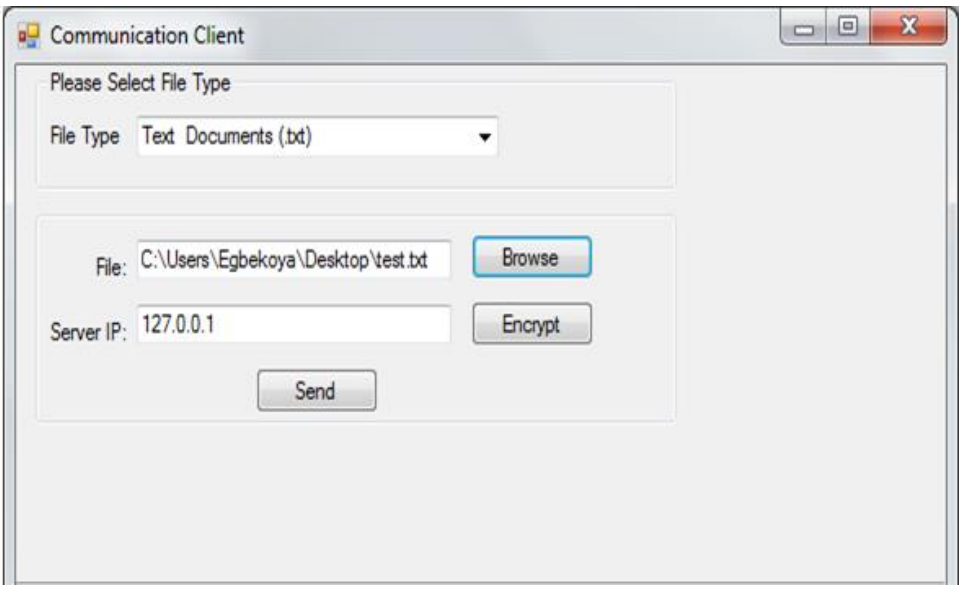

Fig 4.1 : Communication Client implementation

iii. The Browse Button: This is used to browse file for selection.

iv. *The Encrypt Button*: This encrypts the file displayed in the "file text box" using the enhanced algorithm (combination of RSA and DES).

v. The Server IP Textbox: Here the IP address of the server is specified.

vi. The Send Button: This sends the encrypted file to the specified server IP address.

B. Communication Server Implementation

This is the module at the server end. Here the encrypted file is received and decrypted using the required keys. Also, the server is started and stopped here. The communication server module is displayed in Fig

4.2 below and its component described.

i. *The Start Server Button*: This button starts the server and creates the "NCEUploads folder" on the primary hard drive the first time it is run. If the folder already exists, it does not create a new folder but uses the existing one.
ii. *The stop Server Button*: This button stops the server.
iii. *The Reset Button*: This is used to reset the counter, although not usually used.
iv. *The Clear Screen Button*: This is used to clear the progress information displayed in the text area below it.
v. *The Text Area*: It displays progress information about the received files from the client end. Above the text area is the "server IP address". Below the text area is the value of the "file size acquired" and the value of the "last block size read".
vi. The Browse Buttons: This is used to select the encrypted file and the two keys (RSA and DES) for the decryption.
vii. *The Decrypt Button*: This button decrypt the selected file with the selected keys as specified in "vii" above.

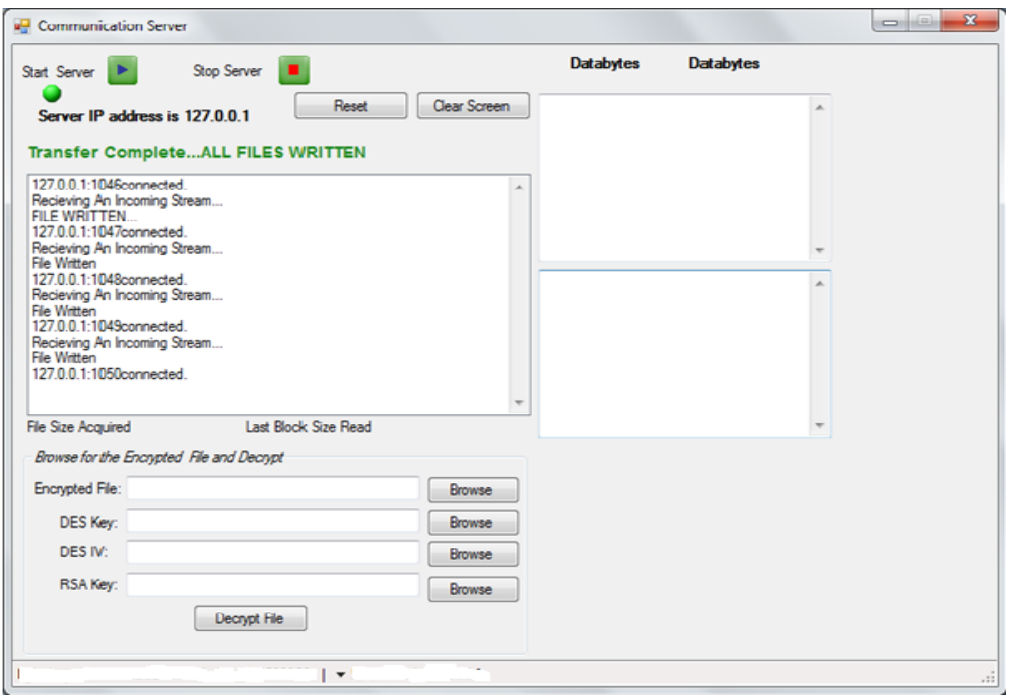

Fig 4.2 Communication Client Implementation

4.1.2 Discussion

After exploring the modules and its components above, The client and server applications are run and the server started, this creates the "NCEUploads" and NCEKeys folder in the primary hard drive where all transferred file will be stored.

On the client module, the file type is selected and the browse button is used to browse to the desired file which will be selected. The selected file is encrypted with the encryption button and sent to the typed-in IP address by clicking the send button.

On the server end, the transfer progress is displayed as in fig 4.2 above. When the transfer is completed, a pop-up indicates "file transfer successful" and the last line on text areas displays "file written". Using the browse button on the server end, select the received (encrypted) file, and the decryption keys by pressing the "decrypt button", decrypt the file which gives us back the original file.

5. Conclusion

Information Security is a means by which an organization can protect or extend a competitive advantage over others, this involves ensuring that access to the network is controlled, and that data is not vulnerable to attack during transmission across the network. Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. Confidentiality means nobody can understand the received message except the one that has the decipher key, and "data cannot be changed" that is, the original information would not changed or modified. In this work we implemented both symmetric and asymmetric encryption techniques. The asymmetric algorithm was used for the key encryption and decryption process, while the data to be sent will be encrypted and decrypted using the symmetric algorithm. The enhanced encryption algorithm used in this work combines the strength of the asymmetric and symmetric algorithm and balances their weaknesses. This technique provides a better security compared to the asymmetric or symmetric algorithm when used alone. This was implemented in Microsoft visual basic .NET

References

Bellare et al. Bellare M., Canetti R., and Krawczyk H. (1998). A modular approach to the design and analysis of authentication and key exchange protocols, *13th Symposium on Theory of Computing (STOC), ACM,* New York, 419–428.

Bellare et al., Bellare M., Desai A., Pointcheval D., Rogaway P. (1998) Relations Among Notions of Security for Public- Key Encryption Schemes, *Crypto' 98, LNCS*

Springer-Verlag, Berlin, 1462, 26–45

Bruce Schneier, John Wiley & Sons, (1996). ISBN 0-471-11709-9.

Davies, D. W. (1991). Advances in Cryptography – *EUROCRYPT'91*, *LNCS* 547, 205-220, Springer-verlag.

Douglas R. Stinson (2006). *CRYPTOGRAPHY Theory and Practice*.

Fouché Gaines, Helen (1956 (1939)). *Cryptanalysis - a study of ciphers and their solution*. Dover. ISBN 0-486-20097-3.

Kavitha Ammayappan, V. N. Sastry, Atul Negi (2008). Cluster based Multihop Security Protocol in MANET using ECC, *TENCON, IEEE Conference*.

Menezes P. and Vanstone S. (1996). Handbook of Applied Cryptography. CRC Press.

Mohammed Abutaha, Mousa Farajallah, Radwan Tahboub & Mohammad(2011). Odeh Survey Paper: Cryptography Is The Science Of Information Security. *International Journal of Computer Science and Security (IJCSS)*, 5(3).

Omar M.Barukab, Asif Irshad Khan, Mahaboob Sharief Shaik , MV Ramana Murthy (2012). Secure Communication using Symmetric and Asymmetric Cryptographic Techniques, *I.J. Information Engineering and Electronic Business*, 2, 36-42.

Paul Reid (2004). Biometrics for Network Security. *Prentice Hall*, ISBN: 0-13-101549-4

Shah, M. H., Khan, S. and Xu, M. (2005). A Survey of Critical Success Factors in E-Banking, European, *Mediterranean & Middle Eastern Conference on Information Systems*, Cairo Egypt, 7-8.

Schneier B. and John Wiley & Sons (1996). Applied Cryptography: *Protocols, Algorithms, and Source Code in C*.

Stalling W (2006). Cryptography and Network Security: *Principles and Practices*. Prentice Hall,.

Subasree S. and Sakthivel N. (2010). Design of a new security protocol using hybrid cryptography algorithms, *IJRRAS*, 2.