Vol 8. No. 3 – September, 2015

African Journal of Computing & ICT

www.ajocict.net

A Hybrid Cryptosystem Using Elgamal Algorithm and Matrix Encryption

N.J. Mamvong
ICT Directorate
University of Agriculture
Makurdi, Benue State, Nigeria.
joemamvong@gmail.com; joemamvong@uam.edu.ng; 08065746622

T. Aboiyar & T. Gbaden
Department of Mathematics/Statistics/Computer Science
University of Agriculture
Makurdi, Benue State, Nigeria.
t.aboiyar@uam.edu.ng; t_aboiyar@yahoo.co.uk; gbaden2014@gmail.com; 07037381034; 07069121825

ABSTRACT

The increasing use of electronic means in data communication from one point to another, coupled with the growth of networking comes with a corresponding increase in vulnerability of privacy. Modern cryptography entails the study of mathematical techniques of encryption and decryption to solve security problems in communication. This research work harnessed the advantage of speed of implementation in a secret cryptosystem and the component advantage that allows strangers to exchange messages in a public key cryptosystem, thereby forming a suitable hybrid cryptosystem which guarantees a secure communication between communicating parties. This is achieved by integrating the Elgamal public key algorithm and matrix encryption technique to achieve the hybrid cryptosystem. This hybrid cryptosystem combines advantages of 'speed of implementation' over typical public key cryptosystems, as well as the advantage of 'secure key distribution' over typical secret key cryptosystems. A network bandwidth analysis showed the practical limitation of the typical Elgamal algorithm as a public key encryption scheme. The hybrid cryptosystem provides an alternative to this limitation as it utilizes its matrix encryption component to step down to a secret key scheme after the first contact of intending users, thereby showing a superior advantage over typical implementation of the Elgamal and matrix encryption schemes as separate entities.

Keywords – Encryption; decryption; key, Network; bandwidth.

African Journal of Computing & ICT Reference Format:
N.J. Mamvong, T. Aboiyar & T. Gbaden (2015): A Hybrid Cryptosystem Using Elgamal Algorithm and Matrix Encryption.
Afr J. of Comp & ICTs. Vol 8, No. 3. Pp 43-50.

1. INTRODUCTION

More than ever before, people are connected in one way or the other, such that even the entire world has become a single community. The increasing use of electronic means in data communication from one point to another, coupled with the growth of networking comes with a corresponding increase in vulnerability of privacy for the communicating persons [Goshwe, 2013]. A principal goal of cryptography is to allow two people to exchange confidential information, via a channel that is being monitored by an adversary [Adewumi and Garba, 2003]. A typical example of such insecure environments that may require the technique of cryptography to guarantee privacy is the well-known internet.

Although the use of cryptographic systems (cryptosystems) in achieving communication security has been in existence, the two broad categories of cryptographic systems viz: secret key cryptography (SKC) and public key cryptography (PKC) have evolved along with their limitations in the implementation front, viz 'secure key distribution' and 'speed of implementation' respectively [Goldreich, 2004]. This paper presents a method which harnessed the advantage of speed of implementation in a secret cryptosystem and the component advantage that allows strangers to exchange messages in a public key cryptosystem, thereby forming a suitable hybrid cryptosystem which guarantees a secure communication between strangers and yet makes up for the respective limitations stated above

2. METHODOLOGY

According to [Hoffstein*et al*, 2008], Cryptographic methods are aimed at applying an encryption scheme by a message sender to a *plaintext* to transform it into a *ciphertext* before sending, and the reverse process of applying a decryption scheme by the receiver to the *ciphertext* in order to recover the original *plaintext* as illustrated in the figure below:

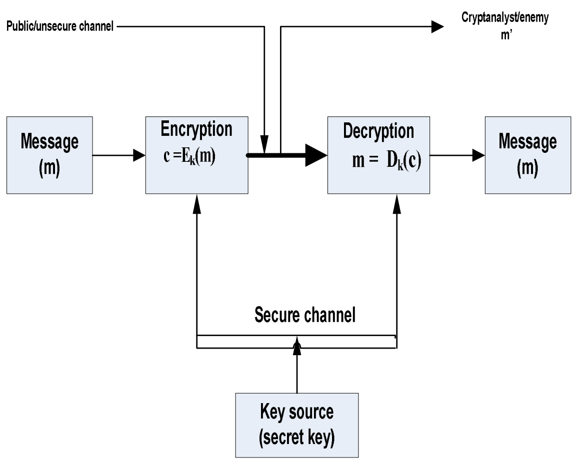

Figure 1.Schematic illustration of a Cryptosystem showing Encryption and Decryption in an unsecure channel.

For the purpose of this paper, we considered the methods of matrix encryption from the family of secret key cryptosystems, the Elgamal algorithm from the family of public key cryptosystems to form a hybrid method that is made of the combination of Elgamal algorithm and matrix encryption [Yan, 2013]. Also, taking into cognizance, the fact that these three methods require that the message to be encrypted is converted into an integer before it is made suitable for the mathematical operations embedded in these algorithms, we hereby consider the first twenty six English alphabets, the number digits from zero through nine, and some characters which we deem as most frequently use (our arbitrary choice) to form a character to numeric value transformation figure as shown below:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
R	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
8	**9**	**=**	**/**	**+**	**-**	**“**	**?**	**‘**	**!**	**%**	**#**	**(**	**)**	**@**	**_**	**space**
35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51

Figure 2: Character to numeric-value transformation table.

2.1. The Elgamal Algorithm

According to (Yan, 2013), The Elgamal public key cryptosystem can be described as follows:

1. A prime q and a generator $g \in F_q$ is made public.
2. BOB chooses a private key at random$a \in \{1,2,\dots,q-1\}$

   This$a$ is the private decryption key. The public encryption key is$\{g, q, g^a \, mod \; q\}$
3. Suppose now that ALICE wishes to send a message to BOB, he chooses a random number $b \in \{1,2,\dots,q-1\}$ and sends to BOB the following pair of elements of F_q:

   g^b, Mg^{ab} where M is the message.
4. Since BOB knows the private decryption key a, he can recover M from this pair by computing$g^{ab} \; (mod \; q)$ and divides this result into the second element. That is,$M \equiv Mg^{ab}/(g^b)^a (mod \; q)$.

The mathematical basis for the security of the Elgamal public key cryptosystem is rooted in the discrete logarithm problem of finding the private key a, by solving the DLP:

$$a \equiv \; log_g \, x \; (mod \; q-1),$$

such that

$$x \equiv g^a (mod \; q).$$

Anyone who can solve the discrete logarithm problem inF_q breaks the cryptosystem by finding the secret decryption key g^a[Yan, 2013]. In theory, there could be a way to use knowledge of $g^a$and $g^b$to find g^{ab} and hence break the cipher without solving the discrete logarithm problem, but there is no known way to go from $g^a$and $g^b$to g^{ab} without essentially solving the discrete logarithm problem and hence, the security basis of the Elgamal public-key cryptosystem.

2.2. Matrix Encryption

According to [Yan, 2013], the matrix encryption method utilizes the block enciphering method to achieve the process of encryption. The block enciphering method suggests that the plaintext to be encrypted be broken into groups of letters, and performing the encryption and decryption on the blocks of letters, as compared to other monographic methods where the encryption is done on the single letters of the plaintext. This principle of splitting the plaintext into groups before performing encryption is called block ciphering [Stallings, 2005]. The matrix encryption is a process of performing an encryption on each of these blocks (groups of letters) using any arbitrarily chosen matrix.

We carry out this process using the procedure outlined below:

(i) Split the message M into blocks of n-letters, say $M_1, M_2, \dots, M_j$;each block M_i, for $1 \le i \le j, i = 1,2,\dots,j$ is a block consisting of n letters.

(ii) Translate the letters into their numerical equivalents and form the cipher-text: $C_i \equiv AM_i(mod\ N), i = 1,2,\dots,j$Where A is the key, and is an invertible $n \times n$matrix with: $gcd[det(A), N] = 1$,

$$C_i = (C_1, C_2, \dots, C_n)^T and\ M_i = (M_1, M_2, \dots, M_n)^T$$

Using matrix encryption, we shall consider an arbitrary matrix A, and perform $C_i = AM_i(mod\ 52)$ as the encryption algorithm. To decrypt the message, we use the decryption function: $M_i = A^{-1}C_i(mod\ N)$, where A^{-1} is the inverse of the arbitrarily chosen encryption matrix -A. We shall consider the decryption function: $M_i = A^{-1}C_i(mod\ 52)$

2.3. The Hybrid Cryptosystem

In this section, we put up an encryption algorithm that combines the Elgamal public-key cryptosystem and the matrix encryption. This hybrid cryptosystem combines advantages of 'speed of implementation' over typical public key cryptosystems, as well as the advantage of 'secure key distribution' over typical secret key cryptosystems. The Algorithm is given below:

Algorithm 1: Mathematical Description of the Hybrid Cryptosystem

1. An arbitrary prime $p$and a generator $g \in F_q$are first published.
2. BOB chooses a private key at random: $a \in \{1,2,\dots,p-1\}$. This a is the private decryption key. The public encryption key is $\{g, p, g^a mod\ p\}$
3. Suppose now that ALICE wishes to send a message to BOB, she chooses a random number $b \in \{1,2,\dots,p-1\}$ and sends to BOB the following pair of elements: g^b, Mg^{ab} where M is precisely the matrix encryption formular: $E = AM, D = INV(A)\ C$
4. Since BOB knows the private decryption key a, he can recover M from this pair by computing: $M \equiv Mg^{ab}/(g^b)^a(mod\ p)$
5. Having recovered M ($E = AM, D = INV(A)\ C$), ALICE and BOB can now proceed to exchange messages using the algorithm described in M as follows:
6. Split the message M into blocks of n-letters, say $M_1, M_2, \dots, M_j$; each block M_i, for $1 \le i \le j, i = 1,2,\dots,j$ is a block consisting of n letters.
7. Translate the letters into their numerical equivalents and perform the Encryption: $C_i \equiv AM_i(mod\ N = 52), i = 1,2,\dots,j$ where A is the key, and is an invertible $n \times n$ matrix.
8. Decrypt encrypted messages by performing the reverse operation: $M_i = A^{-1}C_i(mod\ N = 52)$, where A^{-1} is the inverse of the arbitrarily chosen encryption matrix –A.

www.ajocict.net

Example

Given that $p = 14197 \; and \; g = 137$. The following operation is an example of the communication between ALICE and BOB using the mathematical algorithm of the hybrid cryptosystem:

- Suppose BOB chooses $a \in \{1,2,\dots,p-1\}$. This a is the private decryption key. The public encryption key is $\{g, p, g^a mod\ p\}$

  Take $a = 5$, the Bob's message to Alice is :

$$\{137, 14197, 2550\} \; where$$
$$2550 = 137^5 mod\ 14197$$
$$= 48261724457 \; mod\ 14197$$

Cryptanalysis on 2550 without the knowledge of $a = 5$ is as follows:

$$2550 = g^x$$

$a \equiv log_{137} x (mod\ q - 1)$, Such that

$$x \equiv g^a (mod\ q).$$

- Suppose ALICE chooses $b = 3 \in \{1,2,\dots,p-1\}$. And sends

$\{g^b, Mg^{ab} = 1696, 16365845431432463230 11\} \; where$

$1636584543143246323011 = 2550^3 mod\ 14197 * (M = [E = AM.D = INVAC] = 537113404379142213)$

$= 3047 * 537113404379142213$

Upon receiving Alice's message, BOB recovers M by computing

$$M \equiv Mg^{ab} / (g^b)^a (mod\ p)$$
$$\Rightarrow \frac{1636584543143246323011}{1696^5 mod\ 14197} = 537113404379142213$$
$$= M = [E = AM.D = INVAC]$$

With M being successfully exchanged, Alice and BOB can exchange encrypted messages using the knowledge of M, which is now the secret key component of the hybrid cryptosystem.

3. RESULTS AND DISCUSSION

We used the C# programming language to code the hybrid cryptosystem and we tested it on a campus area network (CAM) of the University of Agriculture Makurdi which follows a hierarchical design topology and runs on a network bandwidth of 45mbps (megabits per seconds) uplink and downlink as at the time this test was conducted.

3.1 Public Key Exchange and Network Bandwidth Analysis

A measure of the network throughput is taken before the commencement of the public key exchange procedure of the hybrid cryptosystem.

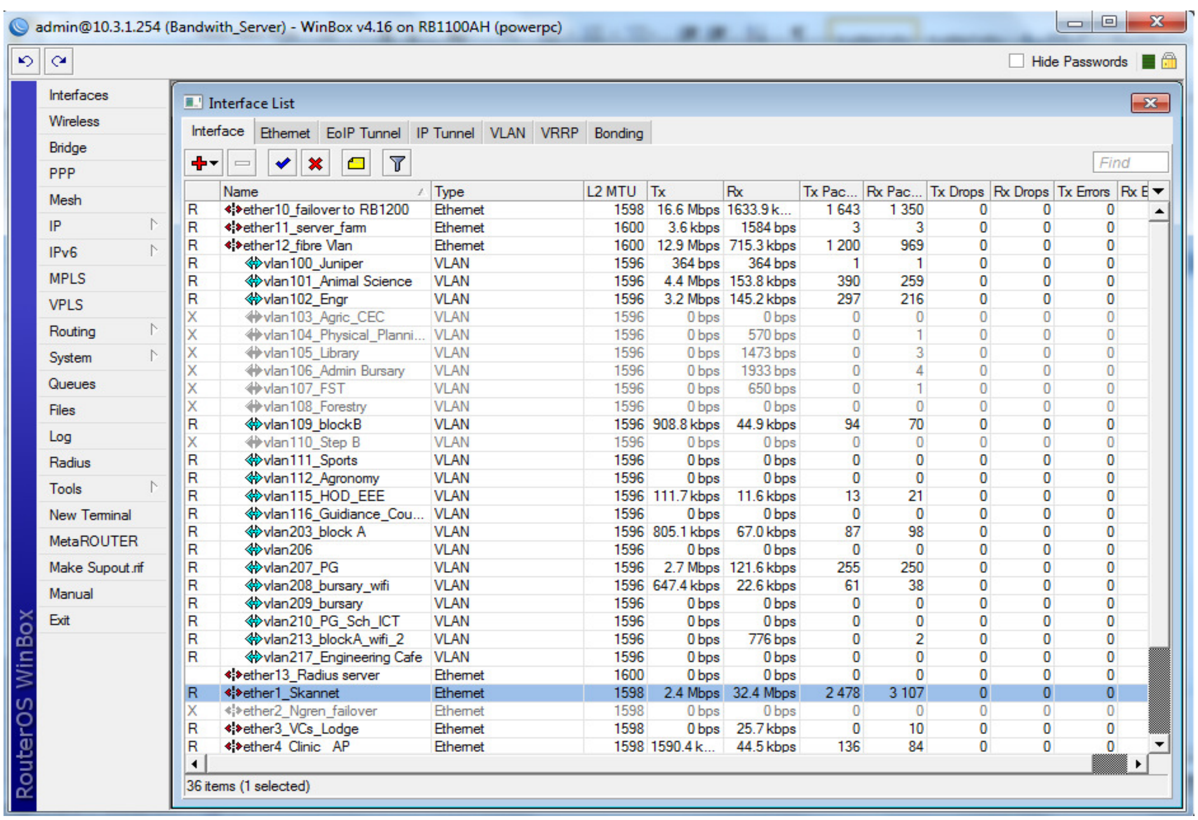

Figure 3: Capture of the bandwidth manager before commencement of public key exchange.

Alice makes a choice of a private decryption key which is kept secret, and computes and sends her first message to Bob, Using the knowledge of the known published prime number for the public key procedure:

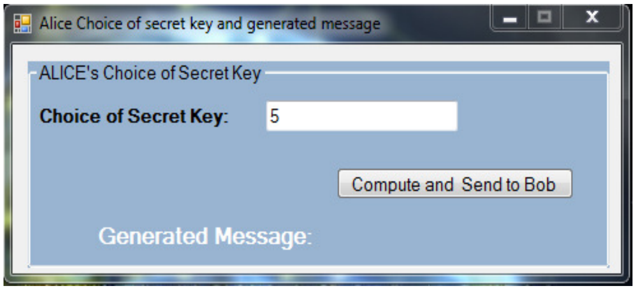

Figure 4: Capture of Alice's choice of a secret decryption key and the first computed message to Bob.

In a similar fashion, Bob makes a choice of a private decryption key which is kept secret, and computes and replies Alice's message, using the knowledge of the known published prime number for the public key procedure.

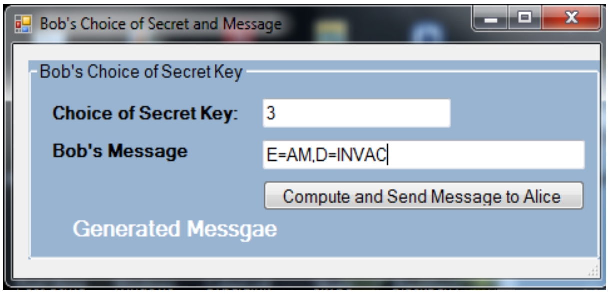

Figure 5: Capture of Bob's choice of a secret key together with the message reply to Alice.

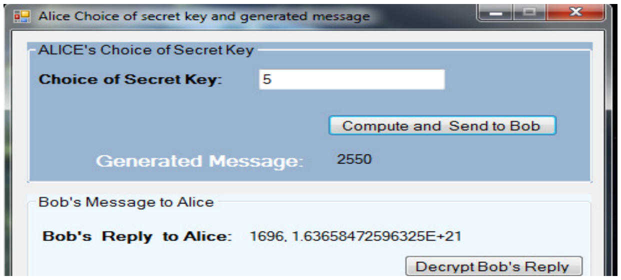

Figure 6. Capture of the message reply from Bob to Alice.

Upon receiving Bob's reply, Alice clicks the 'decrypt Bob's reply' to get the mesasge which is the key to be used for the secret Key cryptosystem, -a component of the hybrid cryptosystem that utilizes matrix encryption for message encryption and decryption.

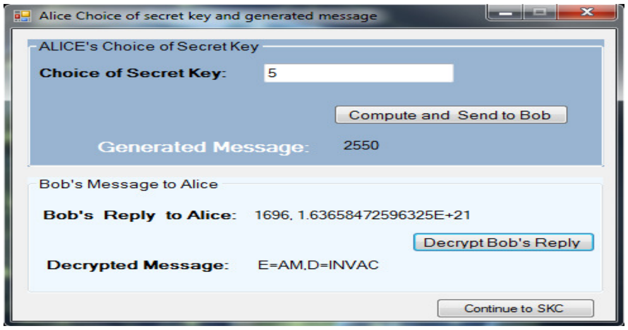

Figure 7: Capture of Alice's decryption of Bob's Public key message.

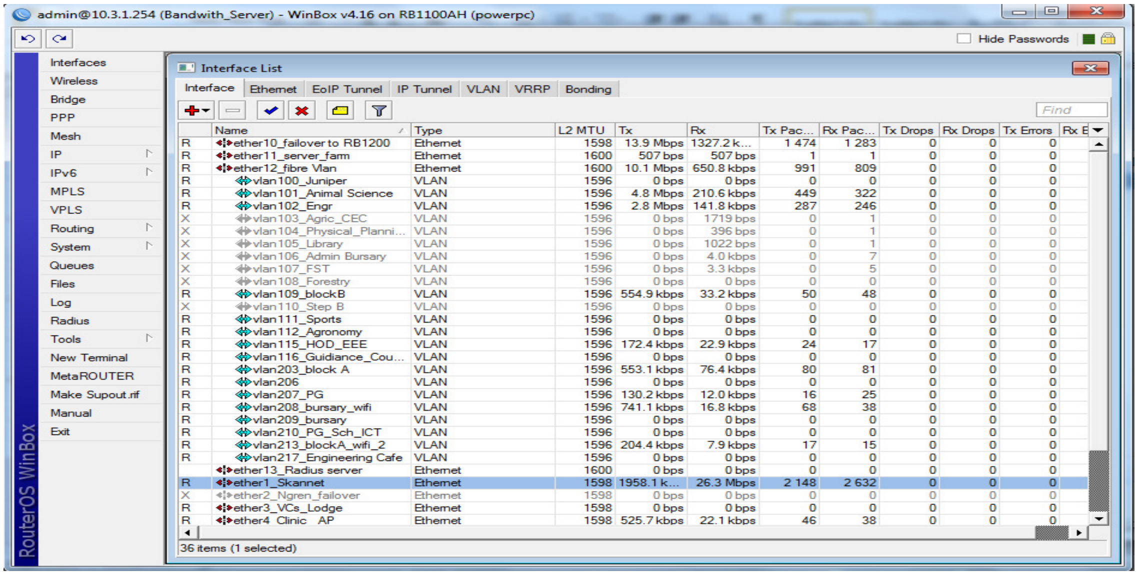

Figure 8: Capture of the bandwidth manager at the completion of public key message exchange.

The table below shows a measure of the change in network speed before the commencement of the public key exchange procedure and after the completion of the key exchange procedure. We notice a speed drop of about 6mbps. This is exposes the practical implementation challenge with typical public key schemes.

Table 1: Table Showing the Change in Network Link Speed during Public Key Exchange.

Link speed before commencement of Public key message exchange.	**Link speed after completion of Public key message exchange**	**Change in the link Speed**
32.4mbps	26.3mbps	6.1mbps

Source – [Field Survey]

Secret Key cryptosystem established after a successful exchange of the secret key using the public key procedure. Subsequent exchanges of messages using the cryptosystem now uses this established secret key system, which depends on very little or no bandwidth resources as compared to typical public key schemes.

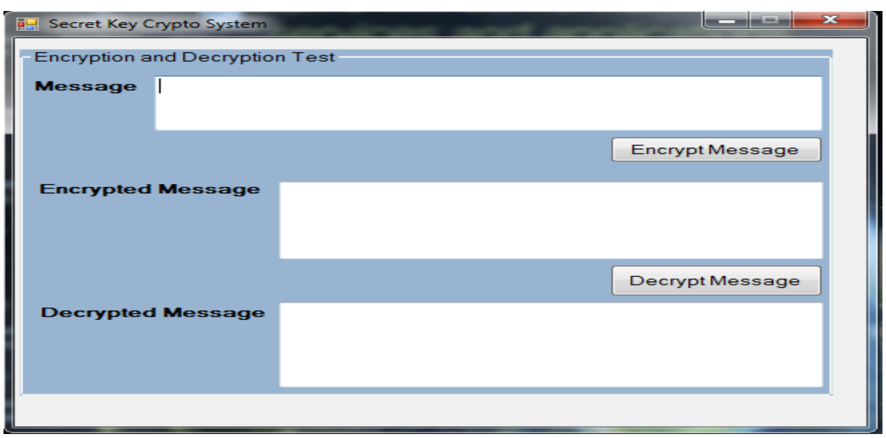

Figure 9: Capture of the established Secret-key Cryptosystem after a successful key exchange message.

Messages are either typed or copied and pasted into the message field of the established secret key system and clicking the ‘encrypt’ button executes the secret key component of the hybrid cryptosystem.

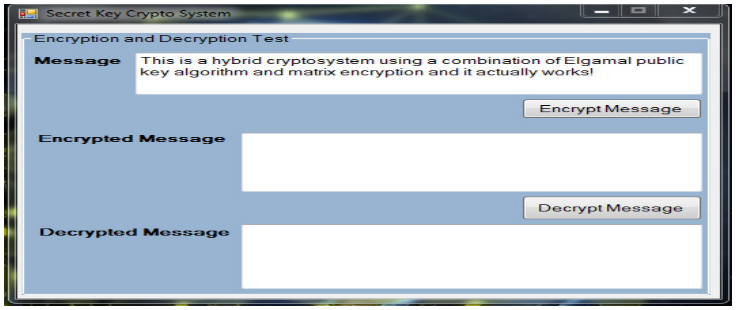

Figure 10. Capture of the secret key cryptosystem with a sample plaintext for encryption.

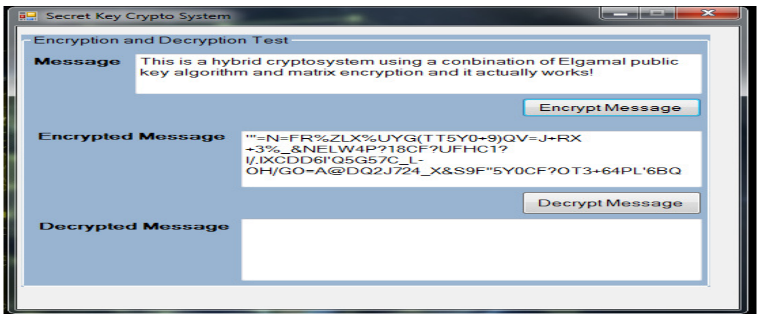

Figure 11: Capture of the secret key cryptosystem with a sample plaintext and the corresponding encrypted ciphertext.

Clicking the ‘decrypt’ button upon receiving and encrypted message recover’s the original message (plaintext):

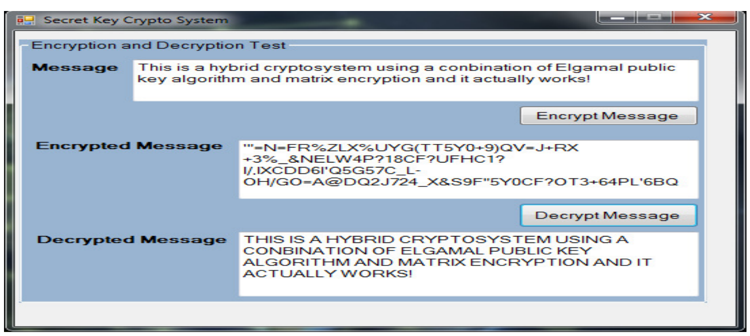

Figure 12.Capture of the secret key cryptosystem showing the decrypted message from the ciphertext.

Cryptanalysis of the hybrid cryptosystem first poses the challenge of solving the discrete logarithm problem during the public key exchange procedure:

$$a \equiv \log_g x \,(mod\ q - 1),$$

such that

$$x \equiv g^a (mod\ q),$$

followed by computing:

$$M_i = A^{-1} C_i (mod\ N = 52),$$

where A^{-1} is the inverse of the arbitrarily chosen encryption matrix –A.

Figure 13: .**Capture of the encrypted message that EVE gets from eavesdropping on the communication line.**

3.2 Analysis of Implementation Speed for the Hybrid Cryptosystem

We begin this analysis with Reference to Table 1 (Showing the change in network link speed during public key exchange). It is note-worthy that because the public-key process of this hybrid cryptosystem depends largely on network factors (such as bandwidth and throughput) other than just the computing power of the local host, we observed the link speed before the commencement of the exchange of key, as well as the link speed at the completion of the exchange of keys.

This is critical because the Elgamal public key component of the hybrid cryptosystem which guarantees a secure contact between intended users who may not have met before requires a network resource to ride on. Consequently, a fast and reliable network link only translates to speed and guarantee respectively, of a successful completion of the key exchange process, and hence, the relative speed of the hybrid cryptosystem. Figure 3 (Capture of the bandwidth manager before commencement of public key exchange) shows this link speed on ether1_skanet to be 32.4mbps (megabits per second).

Figure 8 (Capture of the bandwidth manager at the completion of public key message exchange) shows the link speed on the same ether1_skanet to be 26.3mbps (megabits per second). Column three of Table 1 shows the change in the link speed to be 6.1mbps (megabits per seconds). Like many other typical implementations of public key cryptosystems, the Elgamal algorithm known to have the challenge of slow implementation. However, the stepping down to matrix encryption (by design) of this hybrid cryptosystem limits the challenge to only the first contact of communicating parties, after which subsequent encryptions and decryptions of messages are handled by the matrix encryption component of the hybrid cryptosystem shown in Figure 9 (Capture of the established Secret-key Cryptosystem after a successful key exchange message) and hence, showing the unifying advantage of the hybrid cryptosystem.

4. CONCLUSION

In this paper, a hybrid cryptosystem was presented. It was successfully implemented and tested on a campus area network, with which message encryption and decryption can be achieved. An attacker who intercepts a message for malicious reasons is faced with the challenge of solving a discrete logarithm problem together with accompanying function to find meaning to the message. This cryptosystem - which combines the advantages of ‘secure key distribution’ and ‘speed of implementation’, guarantees secure exchange of messages (like emails, and text messages) in insecure network environments like the internet or intranets which has become a part of our daily routine, and therefore provides a viable option to maintaining communication privacy even in insecure communication environments.

REFERENCES

[1] S.E. Adewumi and E.J.D. Garba, “A crytosystems algorithm using systems of non-linear equations”,Iranian Journal of Information Science and Technology, vol 1, pp. 43 – 55, June 2003.

[2] D. E. Denning, Cryptography and Data Security, Canada: Addison-Wesley Publishing Company, 1982.

[3] O.Goldreich, Foundations of Cryptography, United States of America: Cambridge University press, 2004.

[4] N. Y. Goshwe, “Data encryption and decryption using RSA algorithm in a network environment”,International Journal of Computer Science and Network Security, vol13, pp. 9-13, July 2013.

[5] J. Hoffstein, J. Pipher, and J.H. Silverman, An introduction to mathematical cryptography,USA: Springer,2008.

[6] W. Stallings, Cryptography and network security principles and practices, United States of America: Prentice Hall.2005.

[7] S. Y. Yan, Computational number theory and modern cryptography, John Wiley & Sons Singapore pte. Ltd. 2013.