DEVELOPMENT OF IMPROVED RIVEST SHAMIR AND ADLEMAN (RSA) ALGORITHM FOR SECURING DATA ON TRANSMISSION AND STORAGE.

[1]ADEJUMOBI, O.K., [2]SADIQ, M.O. [3]BARUWA, ABIODUN A. AND [4]AKINTOYE, N.O.

[1]Department of Computer Engineering, The Polytechnic, Ibadan.
[2,4]Department of Elect./Elect., The Polytechnic, Ibadan. [3]Departmentnof Elect./Elect. Engineering, Osun Sate College of Technology, Esa-Oke, Osun State.

Abstract

In present times, the high growth in the networking technology leads to the practice of interchanging digital data frequently. The data in both the private and public sectors are increased which requires, Availability, Authentication, Confidentiality and Integrity. The security of this confidential data from unauthorized access can be done by a process called Cryptography. This is achieved by converting Plain text into Cipher text (encryption). The original message is then recovered by a process called decryption. However, many encryption techniques are available. This Paper therefore reviews most popular and effective algorithms of encryption that are currently used. It focuses mainly on different kinds of encryption techniques, their advantages and disadvantages. The Paper also developed an Improved Rivest Shamir and Adleman (RSA) Algorithm for Securing Data on Transmission and Storage. Recommendations were also drawn for improved cryptography.

Keywords: *Algorithm, Cryptography, Encryption, Decryption, Plain Text, and Cipher Text.*

Introduction

With high growth in network technology information of any form can transmitted over the internet. Unfortunately, some of these information are unprotected and can be accessed by unauthorized users, also called hackers. Therefore, when information is transmitted, it has to be protected. However, there are different encryption techniques used to protect the confidential information from unauthorized users. Encryption is the most effective way to

achieve data security although new encryption techniques are discovered every day.

This Paper reviews some of the recent encryption techniques and their security issues.

Basic Terms Used in Cryptography

(1) Plain Text- The original message that is readable by humans. This is refered to a message before encryption or after decryption.

(2) Cipher Text- In cryptography, cipher text is data that has been encrypted. This text is unreadable until it has been converted into plain text with a key.

(3) Encryption- It is security tool for computer network. It is the process of converting information (known as plain text) using an algorithm to make it unreadable (known as cipher text) to anyone except those processing special knowledge, usually referred to as a key. It is the most efficient method to achieve data security. Encryption can protect confidentiality of message. .For data encryption, a secret key is used. Encrypted data is called cipher text and decrypted data is called plain text.

(4) Decryption- It is process of taking encoded or encrypted text and converting it back into original text. Decryption is used for un-encrypting the data with keys or algorithm. Cryptography uses the decryption technique at the receiver side to obtain the original message from non-readable message (Cipher Text). The decryption process requires two things- a Decryption algorithm and a key. A Decryption algorithm indicates the technique that has been used in Decryption. Usually, the encryption and decryption algorithm are same.

(5) Key- A key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption work on the plain text and at the time of decryption work on the cipher text. The selection of key plays vital role in cryptography process as the security of encryption algorithm fully depends on it. For example, if ‘A’ uses a key of ‘2’ to encrypt the Plain Text “University” then Cipher Text produced will be “wpkxgtkva” [1].

Goals of Cryptography

Due to the great security demand, cryptography is widely used today. The following are the various goals of cryptography;

- **Confidentiality**

Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

- Authentication- The identity of the sender is checked to assure that the information received by any system is from an authorized person or a false identity.

- **Integrity**

Assuring the receiver that the received message has not been altered in any way from the original. Only the authorized user is allowed to alter the transmitted information.

- **Non - Repudiation**

This ensures that neither the sender, nor the receiver of message should be able to deny the transmission.

- **Access Control**

Only the authorized parties are able to access the given information [2].

Data Security Techniques

There are three major data hiding techniques that are popular namely; Watermarking, Steganography and Cryptography.

Watermarking

A watermark is a recognizable image or pattern that is impressed onto paper, which provides evidence of its authenticity [2, 3]. Watermark appears as various shadesof lightness or darkness when viewed in transmitted light. Watermarks are often seen as security features to bank-notes, passports, postage stamps and other security papers [3]. Digital watermarking is an extension of this concept in the digital world.

A watermarking system's primary goal is to ensure robustness, i.e, it should be impossible to remove the watermark without tampering the original data. Digital watermarking is a passive protection tool. It just marks the data, but does not degrade it nor controls access to data [4].

Steganography

Steganography is a practice of hiding/concealing the message, file, image within other message, file or image. The word, steganography is of Greek origin and means "covered writing" or "concealed writing". In other words, it is the art and science of communicating in a way which hides the existence of the communication. The goal is to hide messages inside other harmless messages in a way that does not allow enemy to even detect that there is a second message present [5]. Steganography focuses more on high security and capacity. Even small changes to stegomedium can change its meaning. Steganography does not alter the structure of the secret messageSteganography masks the sensitive data in any covermedia like images, audio, video over the internet [6].

Cryptography

Crypt means “hidden or secret” and graphein means “writing”. The term has been derived from Greek language. Cryptography is an art of transforming data into an unreadable format called cipher text. The receiver at other side, deciphers or decrypt the message into plain text.

Cryptography is an important tool for the protection of multimedia content. All the multimedia files are encrypted before being distributed over the internet. Due to the encryption of the file, it is useless to all the persons who do not have access to the keys. So the key for the decryption of the content should not be disclosed to anyone else other than the content provider.

Encryption is a way to protect information from unwanted attacks by changing it into a formthat cannot be recognized by any attackers. Data encryption mainly is changing of the data, such as text, image, audio, etc. so that it is unreadable, invisible or impenetrable during the transmission. So in order to recover the original data, the receiver just inverses data encryption known as data decryption (see Figure 1).

The encryption process can be described as follows;

$C = E (P, K)$

Where, P = Original data

E = Encryption Algorithm

K = Encryption Key

C= Cipher message, which is transmitted and can be subject to attack

The decryption procedure can be described as;

$P= D (C, K)$

Where, C = Cipher message; D= Decryption Algorithm

K= Decryption Key; P= Recovered data

Classification of Cryptography

The encryption algorithms are classified into two broad categories: Symmetric Key and Asymmetric Key encryption as shown in Fig. 2. All the classical cryptosystems that were developed before 1970 are examples of symmetric key cryptosystems. Besides that, most of the cryptosystems developed after 1970 are symmetric [7].

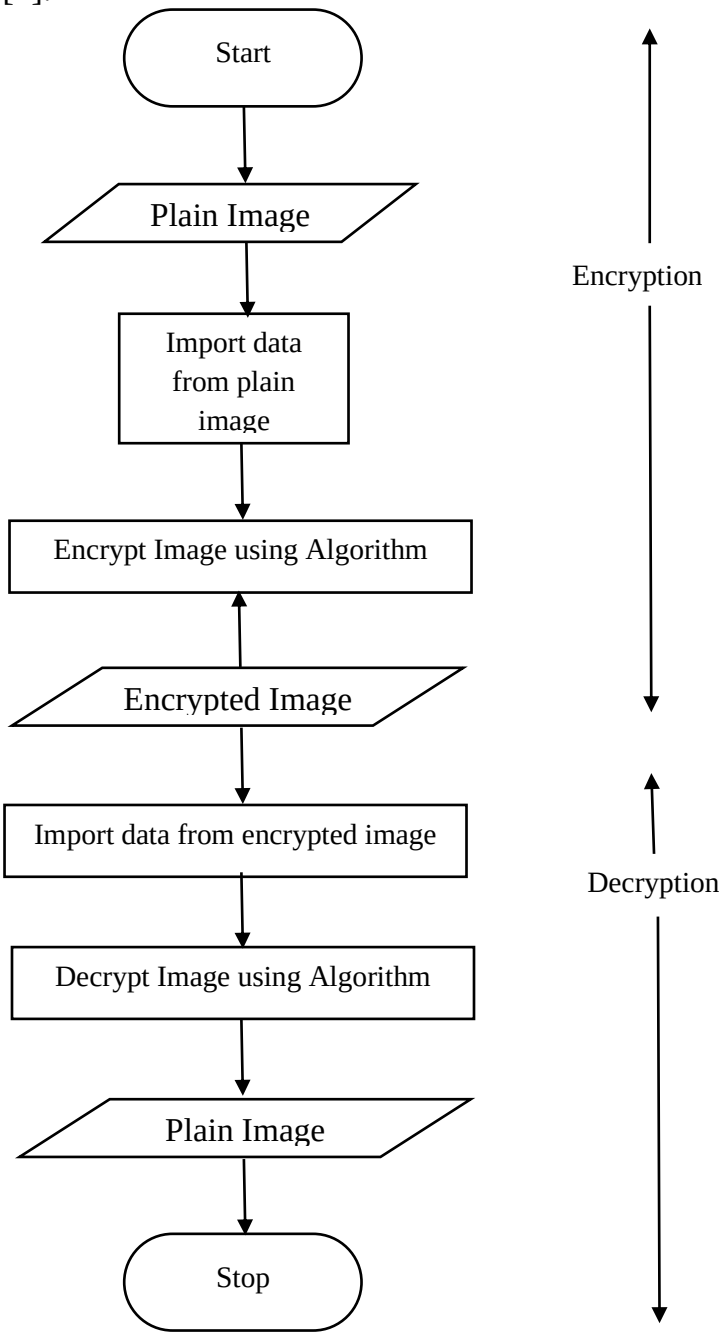

Figure 1: Encryption - Decryption Process

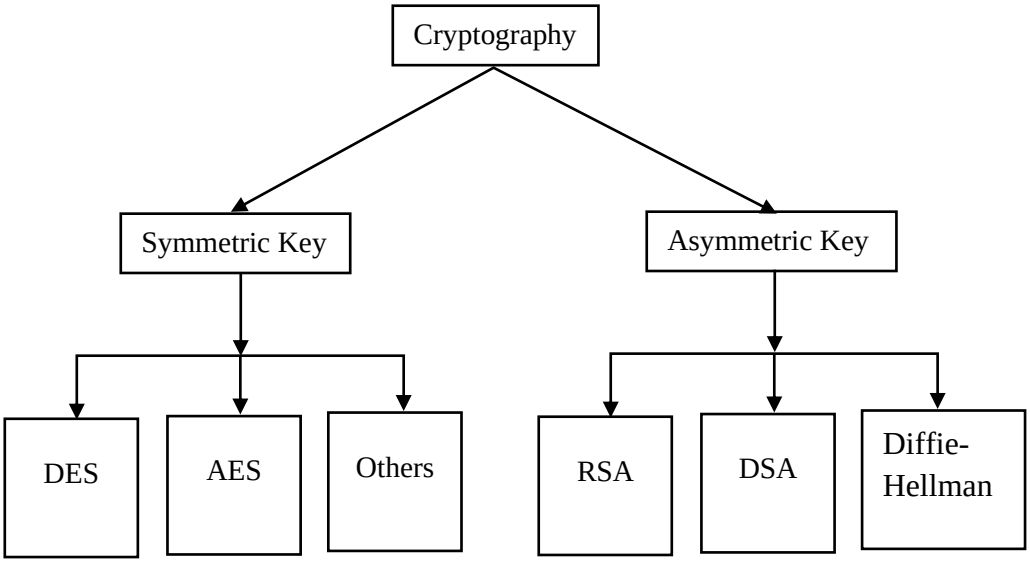

Figure 2: Overview of Most Common Encryption Algorithms

A. Symmetric Encryption

This type of cryptography uses a single key, which is used for encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. At the receiver side, same key will be used to decrypt the message and get the plaintext. Because there is common key used for encryption and decryption processes, the secret key cryptography is also known as symmetric encryption. This was the only type of encryption method widely known until June 1976. There are various symmetric key algorithms such as DES, TRIPLE DES, AES, RC4, RC6, and BLOWFISH [S]. The disadvantage of symmetric key is that it is not able to handle a large network of communication. On the other hand, the symmetric key requires a smaller size for the same level of security as public key cryptosystems, thus, making the communication faster and memory required smaller [9].

B. Asymmetric Encryption- Public-key Cryptography

Here, key used to encrypt a message is different fromthe key used to decrypt the message. In asymmetric or public-key cryptography, two cryptographic keys: a private key and a public key are used. The private key is kept secret, while public key may be distributed. Messages are encrypted with recipients' public key and decrypted with private key. Some commonly used asymmetric

cryptography techniques are RSA (Rivest Shamir and Adleman), Diffie-Hellman, and DSA (Digital Signature Algorithm).

A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating parties must, ideally, share a different key, and perhaps each cipher text exchanged as well. The number of keys required increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all straight and secret [9].

2.3.2 Analysis of different Techniques

A. RSA (Rivest Shamir and Adleman) Algorithm

RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem [10]. In RSA, user firstly creates and then publishes the product of two large prime numbers and their public key asan auxiliary value [10]. These prime numbers must be kept secret. Public keycan be used by anyone to encrypt a message.The RSA algorithm involves three steps:

- Key generation
- Encryption
- Decryption

B. Digital Signature Algorithm

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient cause to believe that the message was created and sent by a known sender; such that the sender cannot refuse having sent the message (authentication and non-repudiation) and that the message was not altered in transmission (integrity)[11]. Digital signatures are commonly used for financial transactions, software distribution, and in many other cases where it is important to detect forgery or tampering. Digital signatures are often used to implement electronic signatures, which refer to any electronic data that carries the intent of a signature. It is not true that all electronic signatures use digital signatures.

Digital signatures employ a type of asymmetric cryptography. For messages sent through a nonsecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender [12]. Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult

to forge than the handwritten type. Digital signature schemes in the sense used here are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid. Digitally signed messages may be anything representable as a bit string: examples include electronic mail, or a message sent via some other cryptographic protocol.

C. Diffie–Hellman Algorithm

Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys [13]. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two unknown parties to jointly establish a shared secret key over an insecure communications channel [14]. This key can be used to encrypt subsequent communications using a symmetric key cipher. The method was followed shortly afterwards by RSA, an implementation of public key cryptography using asymmetric algorithms.

D. Data Encryption Standard

The DES algorithm is the most widely used encryption algorithm in the world. For many ears, and among many people, "secret code making" and DES have been synonymous. The DES was published by the United States' National Bureau of Standards in January 1977 as an algorithm to be used for unclassified data (information not concerned with national security). DES applies a 56-bit key to each 64-bit block of data. This process can run in several modes and involves 16 rounds. Although this is considered "strong" encryption, many companies use "triple DES", which applies three keys in succession. This is not to say that a DES-encrypted message cannot be "broken." [15].

E. AES (Advanced Encryption Standard)

The Advanced Encryption Standard (AES) is an encryption algorithm for securin sensitive but unclassified material by U.S. Government agencies and, as a likely consequence, may eventually become the de facto encryption standard for commercial transactions in the private sector. It is robust replacement for the Data Encryption Standard (DES) and to a lesser degree Triple DES. The specification called for a symmetric algorithm using block

encryption of 128 bits in size, supporting key sizes of 128, 192 and 256 bits, as a minimum. The algorithm was required to be royalty-free for use worldwide and offer security of a sufficient level to protect data for the next 20 to 30 years. It's hardware and software implementation is easyeven in restricted environments (for example, in a smart card) and also offers good protection against various attack techniques.

Table 1: Performance Analysis and Comparison of Symmetric and Asymmetric Key Cryptography [16].

Method	DES	RSA
Approach	Symmetric	Asymmetric
Encryption	Faster	Slow
Decryption	Faster	Slow
Key distribution	Difficult	Easy
Complexity	O(Log N)	O (N3)
Security	Moderate	Highest
Nature	Closed	Open
Inherent Vulnerabilities	Brute Forced, Linear and differential cryptanalysis attack	Brute Forced and Oracle Attack
Vulnerabilities cause	Weak key usage	Weak Implementation
Secure Services	Confidentially	Confidentially, integrity, non repudiation

F Improved RSA (Montgomery Modular Multiplication)

The improved RSA is used for file security using Montgomery method for encryption of text files on MATLAB platform. The Montgomery method uses Public exponent, Private exponent and Modulus exponent generated for the encryption and decryption of messages. Figure 3 shows the flow Chart of both Encryption and the Decryption processes.

The Automation of the developed system was coded and built in a non-user interactive environment called the M file.

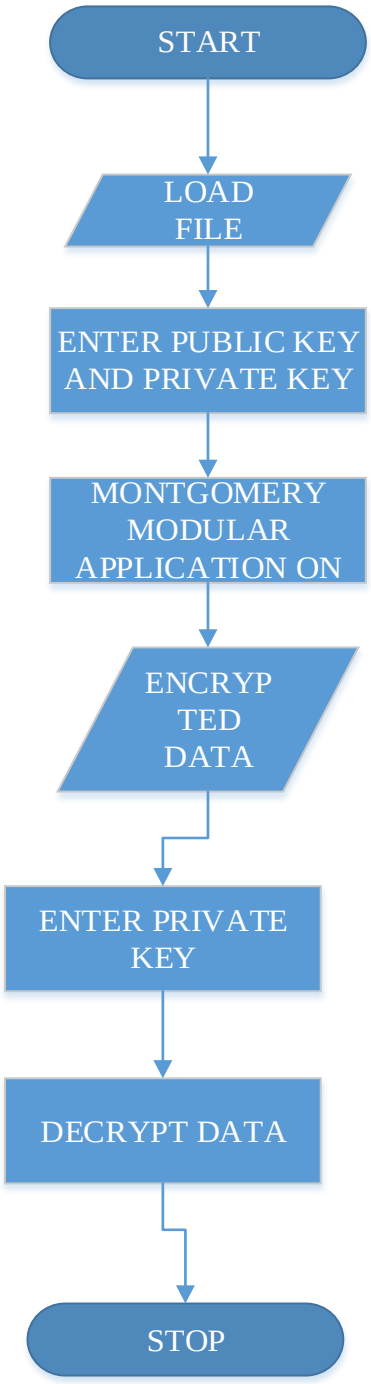

Figure 3: Flow Chart of Encryption and Decryption Processes

Improved RSA - Experimental Data and Software Testing

This is divided into Encryption and decryption Processes.

1. Encryption Process

Firstly, the Matlab Program is loaded after which the M-file of the Montgomery Algorithm is loaded (see Figure 4). The text file is then loaded on the platform for encryption by clicking 0n the 'Load Text file' (see Figure 5).

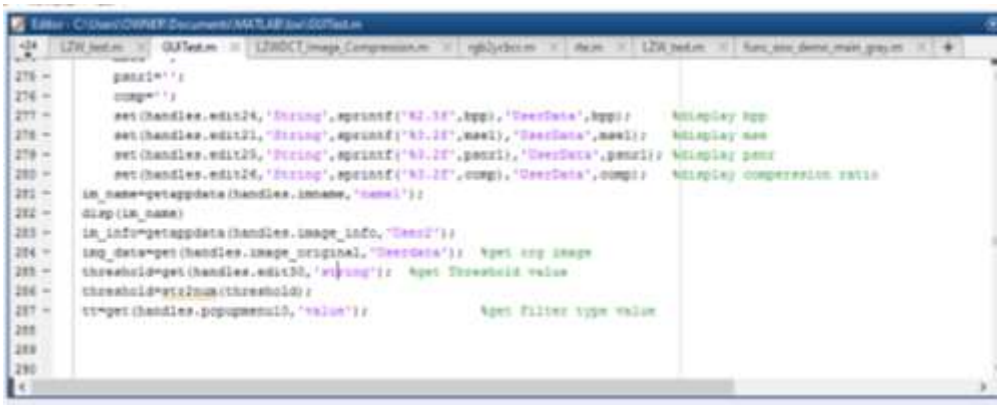

Figure 4: The Matlab M File

The encryption process is initiated by clicking the 'encrypt' button (see Figure 5), which in turns generates the Public, Private and Modulus exponents for the encryption of the loaded message (Plaintext). For the loaded message, a Modulus of 5723 was generated, a Public exponent of 5 and a Private exponent of 3341 were generated. Encryption time which is the CPU execution processing time was displayed (see Figure 6). The encrypted message is shown in Figure 7.

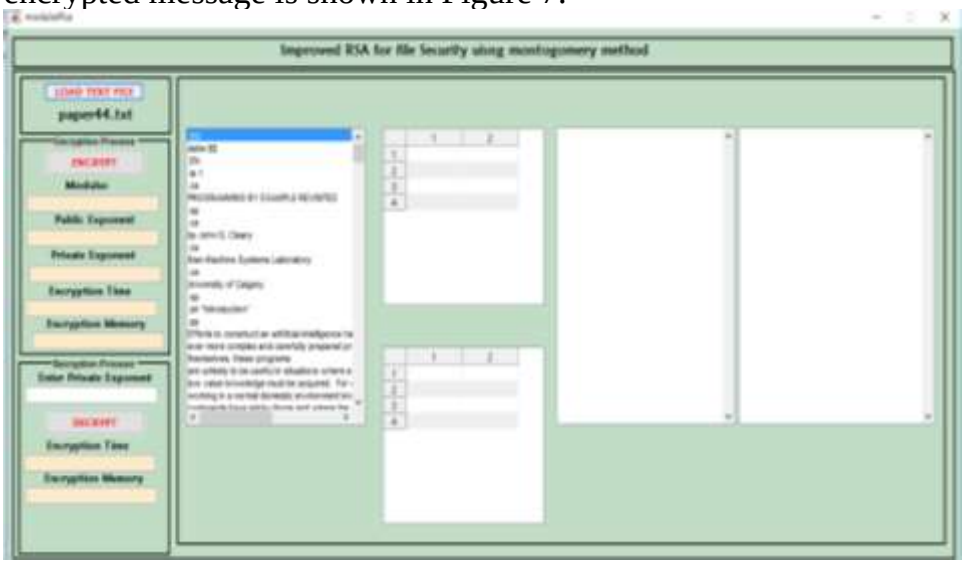

Figure 5: Loading the Text File

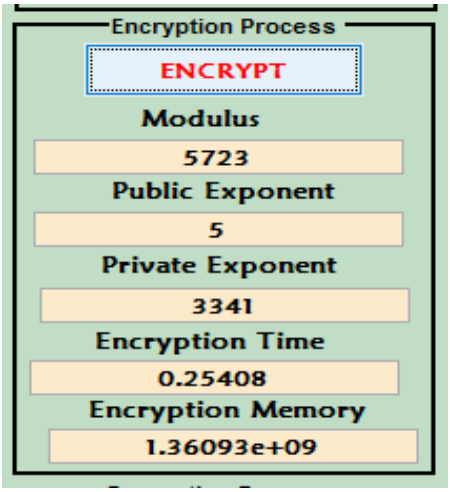

Figure 6: Encryption Output

Figure 7: Encrypted Message

Decryption Process

Here, it should be noted that the recipient of the transmitted encrypted message must also have Matlab and the Montgomery M-File on his or her Computer system. The Decryption Process is triggered by the correct supply of the Private Key (see Figure 8). If the Key entered is incorrect, the process of decryption will be terminated (see Figure 9). However, Figure 10 shows the decryption time and memory after the correct supply of Private exponent.

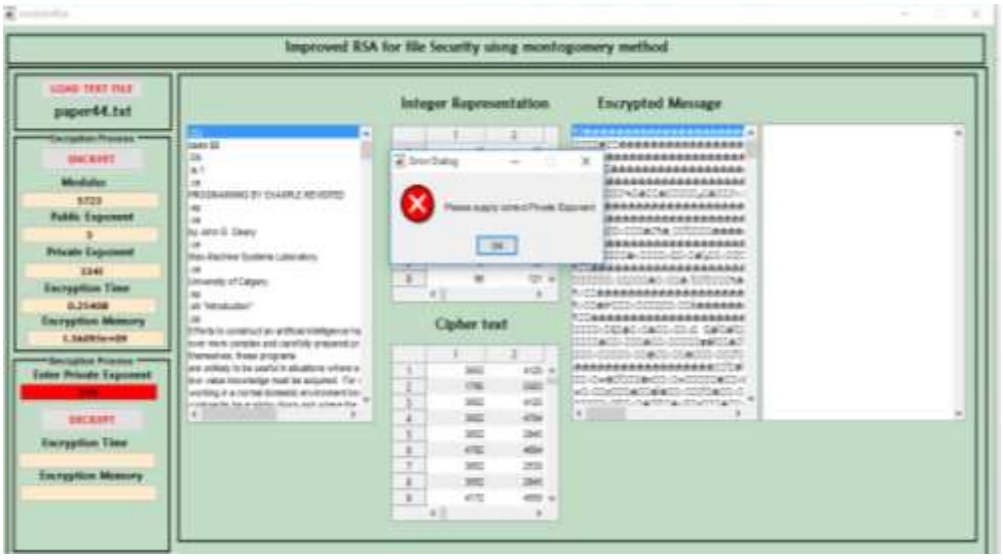

Figure 8: Supply of Incorrect Private Key during decryption

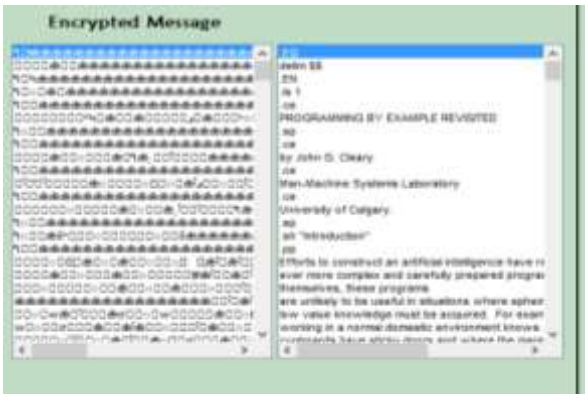

Figure 9: Decrypted Message

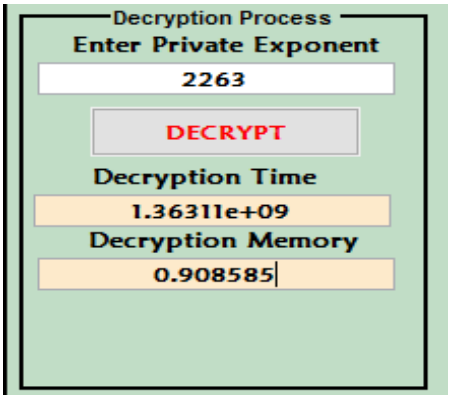

Figure 10: Decryption Output

Conclusion and Recommendation

Cryptography plays important role in securing digital data both at storage and transmission. It is used to achieve the security goals of confidentiality, integrity, authentication, and non-repudiation of information. This Paper reviews different types of encryption techniques, their advantages and disadvantages. However, an Improved RSA (Montgomery Multiplier Algorithm) was implemented. The most admirable features of this Algorithm are its simplicity, in terms of application and quick response time in terms of encryption and decryption time. Its high beneficial outputs in term of security cannot be ignored.

It is however recommended that for better security of data on transmission, the Montgomery Algorithm can be modified by increasing the prime number system used.

References

[1]. Richa Gupta, Sunny Gupta, Anuradha Singhal (2014): 'Importance and Techniques of Information Hiding : A Review'. International Journal of Computer Trends and Technology (IJCTT) – volume 9 Number 5. Pp 260-265.

[2] Saranya K , Mohan Priyar, and Udhayan J (2014). A Review on Symmetric Key Encryption Techniques in Cryptography, International Journal of Science, Engineerin and Technology, Volume 3, Issue 3.

[3] Kayarkar H. and Sugata Sanyal (2015). A Survey of Data Hiding Techniques and their Comparative Analysis.

[4] Sabu M Thampi (2004): 'Information Hiding Techniques: A Tutorial Review, ISTE-STTP on Network
Security & Cryptography, LBSCE.

[5]. PandeA. and Ambreno, J (2013). Advances in Multimedia Encryption. In: Embedded Multimedia
Security Systems. London: Springer-Verlag, pp. 11-22. [Online] Available at:
http://www.springer.com/cda/content/document/cda_downloaddocument/9781447144588-c2.pdf?SGWID=0-0-45-1345406-p174549534 [Accessed 11 10 2015].
[6] Mangesh Ghonge, Ankita Dhawale, atul Tonge, P. (2014): Review of Steganography Techniques, International Journal of Advent Research in Computer &Electronics, Vol. 1, No.1.
[7]. Ramesh G, Umarani. R," Data Security In Local Area Network Based On Fast Encryption Algorithm",International Journal of Computing Communication and Information System(JCCIS) Journal Page 85-90. 2010v
{8]. Emanuil Rednic; and Andrei Toma (2016): ftware Analysis: Security Management In A Multimedia System, Vol.4, N0. 2. Pp. 237-247.
[9] National Bureau of Standards, " Data Encryption Standard," FIPS Publication 46, 1977.
[10] A. Perrig, J. Stankovic, and D. Wagner (2004) ,"Security In Wireless Sensor Networks," ACM,Vol. 47, No.653.
[11] ErfanehNoorouzil et al (2011) "A New Digital Signature Algorithm", International Conference on Machine Learning and Computing, IPCSIT,vol.3, Pp 43-47.
[12]William-Stallings,http://williamstallings.com/Extras/Security Notes/lectures/authent.html, Dated: 13-dec-2012at 14:05.
[13] Wikipedia,"http://en.wikipedia.org/wiki/Diffie%E2%80%93Hell man_key_exchange," Dated: 13-dec-2012 at10:33
[14] Simon Blake Wilson et al., "Key Agreement Protocols and Their Security Analysis,"9-sep-1997.
[15] The DES 15 years of Public Scrutiny. Dorothy e Denning.
[16] Yogesh Kumar, Rajiv Munjal and Harsh Sharma (2011): "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures". IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03. Pp 60 - 63.