Asian Journal of Engineering and Applied Technology
ISSN: 2249-068X (P) Vol.10 No.2, 2021, pp.19-24

DOI: https://doi.org/10.51983/ajeat-2021.10.2.3058

Fast Implementation of the Rivest-Shamir-Adleman (RSA) Algorithm with Robust Packet Data Loss Detection Function

Issah Mubasir, Alhassan Abdul-Barik and Alhassan Salamudeen
Department of Computer Science, University for Development Studies, Tamale, Ghana
E-mail: barik75@yahoo.com, mubasir18@gmail.com, salamprog@yahoo.com
(Received 6 June 2021; Accepted 25 July 2021; Available online 6 August 2021)

Abstract - **Encryption is the process of protecting information from unauthorized parties by converting such information into an unreadable form. Packet data is a method of transferring data, broken into bits called packets which travel over a network. Packet losses occur when packets fail to reach their destination devices as a result of network congestion, faulty routers or as a result of an attack. Encryption is the standard method for making a communication private. In sending a private message to another user, it is first encrypted (termed encipher), the intended recipient alone knows how to correctly decrypt (decipher) the message. There are several algorithms developed for the purpose of encryption which provides data security and integrity. This paper proposes the use of the Rivest-Shamir-Adleman (RSA) algorithm to implement a system for encrypting text files of any length (by breaking long messages into valid blocks and encrypting each block) capable of being transmitted using a Simple Mail Transfer Protocol (SMTP). Probable primes, 3048 bits in length are generated to be used in the generation of public, private key pairs for encryption and decryption. The proposed scheme is better because the route taken during transmission of data is recorded and packet losses are also checked for during transmission of encrypted files as compared to known state-of-the-art schemes.**
Keywords: **Cryptography, Encryption, Decryption, Packet Loss, Public Key, Private Key, Modulus**

I. INTRODUCTION AND BACKGROUND

The internet is composed of a large number of interconnected computers, making it easy for people and corporations to communicate (including sharing of files and media) at a very fast speed. This helps in speeding up business processes and daily activities of people. However, the issue of privacy and security comes to play when sensitive information is being transmitted. This is because such information has to be communicated through routers and computers whose security level is not known to the sending party. Transmitting information through such insecure connections could lead to the leakage of sensitive information to the general public, stealing of data or the alteration of information by third parties for malicious purposes. This research seeks to solve this problem in two phases.

Firstly, information being transmitted is in plain text. How can such information be kept hidden even when intercepted? This can be solved by using a secure encryption algorithm such as the Rivest-Shamir-Adleman (RSA) algorithm as used in this research. The security of this algorithm is derived from the difficulty of factoring large integers that are the product of two large primes [1].

Secondly, is it possible to determine if data/information reaches its destination? The scheme allows for the detection of how many packets are dropped if there were packet losses and which particular router the losses occurred. It therefore enables encrypting and decrypting of text as well as the generation of cryptographic keys and also checking for packet losses.

II. REVIEW OF LITERATURE

This section discusses various research works undertaken by researchers in the field of Rivest-Shamir-Adleman (RSA) cryptosystems. Thangavel *et al.*, [2] proposed an improved system based on the use of four prime numbers rather than the usual RSA algorithm, which uses two huge prime numbers. Encryption (*E*) and Decryption (*D*) values are derived from the product of four prime numbers (*N*), making the system extremely safe. The key generation time is however increased as compared to the traditional RSA algorithm while [3] seeks to improve the speed of the RSA decryption and signature (which is a mathematical scheme for authentication of messages or documents). It proposes a different form of the RSA cryptosystem where modules and private exponents are reduced in modular exponentiation. Sinjan and Vincent (2015) also implements the traditional RSA encryption algorithm where two random prime numbers and an Euler totient function are used to generate public and private keys in the C Programming Language [4&5] proposes an improved and updated RSA cryptosystem based on *n* unique prime numbers.

To perform double encryption-decryption, two separate public and private keys created from a significant factor of the variation *N* are utilised, providing better security. The RSA cryptosystem is used for digital signatures which increases security [6]. In [7], the security of data is enhanced by using a modified RSA cryptosystem based on *n* prime numbers. This is a new technique to provide maximum security for data over the network as '*n*' prime number is not easily breakable. Packet loss occurs when data sent from one networked device fails to arrive at the destination device.

A variety of reasons account for the loss of packets and the effect of this is noticeable when streaming media and in online gaming where quality is affected. Packet loss is measured as a percentage of packets lost with respect to packets sent [8]. Packet loss is typically caused by network congestion. Packets travel through various links to get to the destination device. When one of these links is at full capacity, then the arriving packets will have to wait (queue) before being sent. However, if a network device is falling far behind, there is no option than to drop packets [9].

In a computer network, a ping test is a way of sending messages from a computer to another. Aside from checking if the computer is connected to a network, ping also gives indications of the reliability and general speed of the connection [10]. In [11] two redundant moduli, $\{2^{2n}-3\}$ and $\{2^{2n}+1\}$ are added to detect errors as well as correct them in encrypted and compressed data as applied in Redundant Residue Number System (RRNS).

III. PRESENTATION OF RESULTS AND DISCUSSION

In this section, the methodologies including the Iterative waterfall model and the Rivest-Shamir-Adleman (RSA) Algorithm is presented. It also includes how these methodologies are used for results simulation and discussion.

A. The Iterative Waterfall Model

The iterative waterfall model of the Software Development Life Cycle is used in the development of the system. Java Programming Language is used in the implementation of the system using its Big Integer library functions. The Big Integer library provides functions such as modular arithmetic, Greatest Common Divisor (GCD) calculation, primality testing, prime generation, and bit manipulation among others.

Simple Mail Transfer Protocol (SMTP) is used in the email function of the developed system using the javax. mail package of the java programming language. In the encryption of texts, messages longer than the modulus are divided into relatively equal blocks such that each block is smaller than the modulus. Each block is then encrypted and appended to an ArrayList of the java.util class. Each block of text (cipher text) is decrypted and concatenated to give the original text.

B. The Rivest-Shamir-Adleman (RSA) Algorithm

1. Create two huge random prime numbers p and q of about equal size that their product $n = pq$, has the needed length.
2. Calculate $n = pq$, and $z = (p-1)(q-1)$.
3. Choose an integer d, $1 < d < z$, such that $\gcd(d, z) = 1$.
4. Determine the secrete exponent f, $1 < f < z$, such that $df = 1$.
5. The Public key is (n, d), while the Private key is (f, p, q).

Where the modulus is known as *n*; the public exponent is known as *d*; and the secrete exponent or the decryption exponent is known as *f*.

During transmission of mail, packet losses are checked for as well as the number of hops and the route taken to the destination. These statistics are stored in a file generated upon initiation of the transmission.

IV. RESULTS AND DISCUSSION

The system is developed and tested on a computer with the following specifications.

TABLE I SYSTEM SPECIFICATIONS

Component	System Specifications
Operating System	Windows 7 Ultimate service pack 1
RAM	6.00GB
System Type	64bit
Processor	Inter(R) Celeron(R) CPU 900 @2.20GHz 2.19GHz
Rating	3.3 Windows Experience Index

The development of the system consisted of several windows, each performing a specific function. The Key Generator window is used for the generation of 2048 bit length public and private keys. The Encoder and Decoder windows are for the encryption and decryption of text respectively. The Email window is used for emailing encrypted files and also checks for packet losses during transmission.

V. KEY GENERATION

Key generation is the process of generating cryptographic keys. A key is used in the encryption and decryption of data.

TABLE II TIME VARIATIONS IN KEY GENERATION

Bit Length	Time taken for Public key length (ms)			Average Time taken (ms)
	4 digits	5 digits	7 digits	
1024	1003	1418	615	1012
2048	6649	4033	3197	6400.25
3072	23990	45633	102715	57446

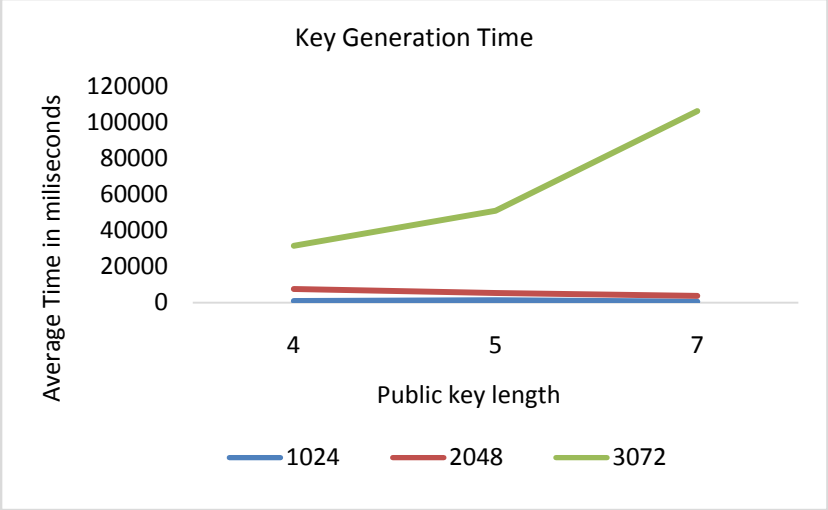

Fig. 1 Key Generation Time Variation

Encryption of text files takes different execution times in milliseconds depending on the file size and the system the encryption is run on. Some text files decrease in size after encryption while others increase in size. For example, a file of type *.pdf* with an original size of 1820*kb* decreased in size to 154*kb* after encryption with an execution time of 433*ms*. However, a file of type *.txt* with an original size of 24.9*kb* increased to 77.1*kb* after encryption with an execution time of 110*ms*.

A. Description of Implemented System

1. Packet Loss Detector Window

This is used to perform further packet loss checks based on information gathered from the generated log file. Echo requests allows user to specify the number of packets to send. The radio button labelled 'Ping until Stopped' sends packets continuously until the user stops it.

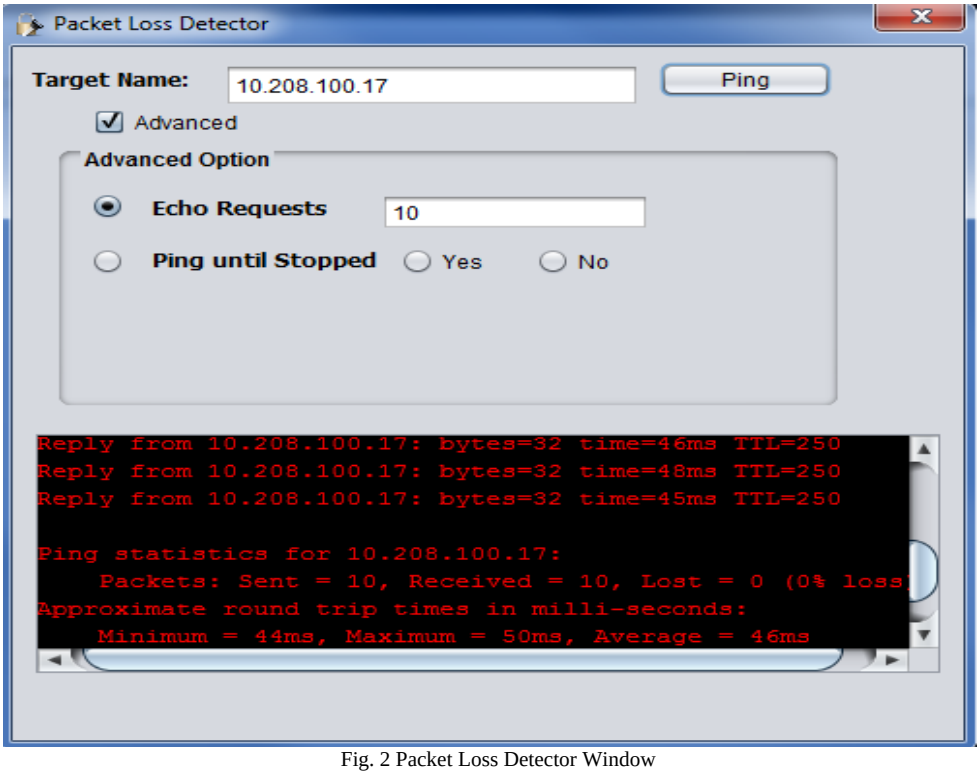

Fig. 2 Packet Loss Detector Window

2. Generated File showing Trace Route and Packet Loss

This log file is generated while mail is being sent.

It shows the results of pinging the mail server to detect packet losses. It also traces the route taken to the mail server.

```
2018/05/28 09:41

Sending Message...


Tracing route to gmail-smtp-msa.l.google.com [108.177.15.108]
over a maximum of 30 hops:

  1      1 ms      1 ms      1 ms  192.168.43.1
  2      *         *         *     Request timed out.
  3      *       802 ms    782 ms  10.208.23.97
  4    105 ms     99 ms      *     10.208.84.34
  5      *         *         *     Request timed out.
  6     66 ms     79 ms     85 ms  10.208.100.17
  7   1253 ms    369 ms    316 ms  196.201.61.221
  8    376 ms    460 ms    665 ms  41.181.247.0
  9    370 ms    674 ms    413 ms  41.181.189.66
 10    153 ms    162 ms    174 ms  72.14.198.110
 11      *       717 ms    473 ms  108.170.246.144
 12    427 ms    442 ms    398 ms  216.239.58.133
 13    488 ms    392 ms    429 ms  209.85.253.196
 14    364 ms    417 ms   1183 ms  209.85.240.155
 15      *         *         *     Request timed out.
 16      *         *         *     Request timed out.
 17      *         *         *     Request timed out.
 18      *         *         *     Request timed out.
 19      *         *         *     Request timed out.
 20      *         *         *     Request timed out.
 21      *         *         *     Request timed out.
 22      *         *         *     Request timed out.
 23      *         *         *     Request timed out.
 24      *         *         *     Request timed out.
 25    446 ms    464 ms    465 ms  wr-in-f108.1e100.net [108.177.15.108]

Trace complete.
error (if any):


Pinging gmail-smtp-msa.l.google.com [64.233.167.109] with 32 bytes of data:
Reply from 64.233.167.109: bytes=32 time=504ms TTL=38
Reply from 64.233.167.109: bytes=32 time=333ms TTL=38
Reply from 64.233.167.109: bytes=32 time=322ms TTL=38
Reply from 64.233.167.109: bytes=32 time=431ms TTL=38

Ping statistics for 64.233.167.109:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 322ms, Maximum = 504ms, Average = 397ms
error (if any):

********************************************************************************
```

Fig. 3 Generated File Showing Trace route and Packet Loss

3. Encryption Window

The encoder window is used for the encryption of data. The browse button allows the user to select a file to be encrypted. Data can also be written into the plaintext text area for encryption. Public key and modulus are inputted into their respective text fields. After encryption, cipher text can be saved to a file on the local computer by clicking the 'Export to file' button.

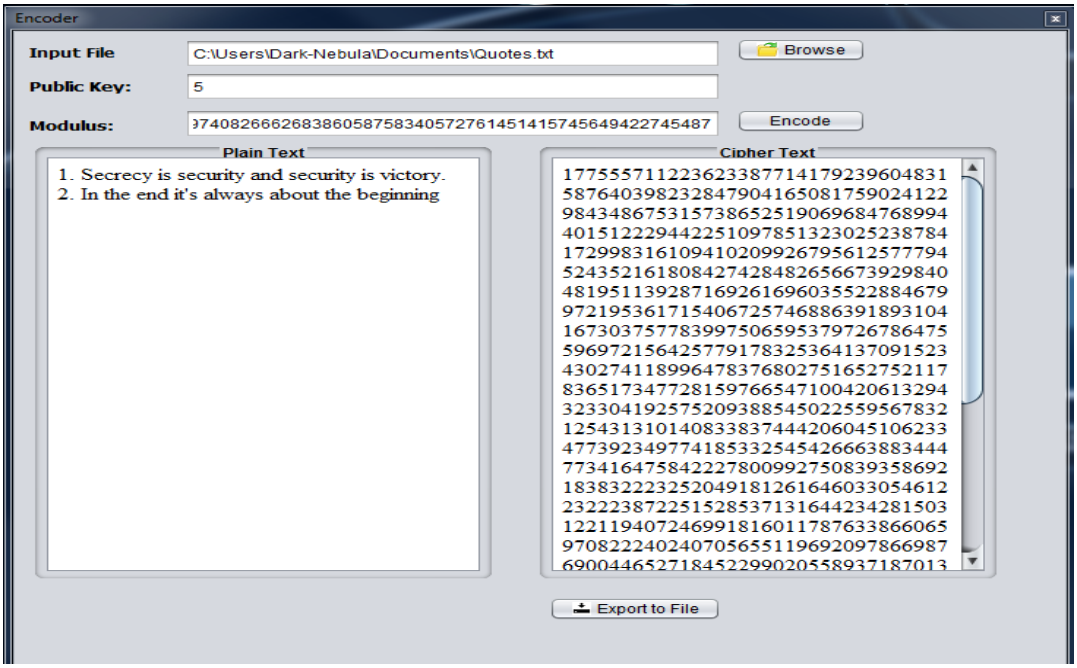

Fig. 4 Encryption Window

4. Decoder Window

Cipher text can be inputted from the local disk using the browse button to import a file. Cipher text can also be inputted into the cipher text area. Private keys and modulus are provided to decrypt the data into plaintext which can be saved to file using the 'Export to File' button.

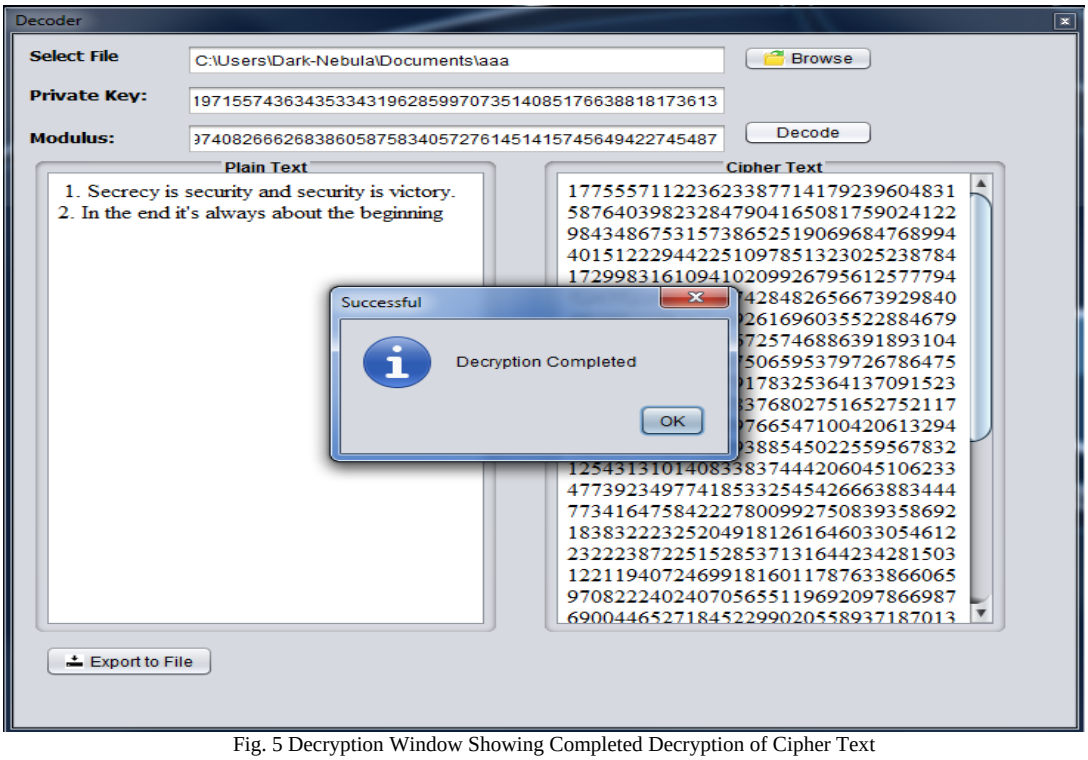

Fig. 5 Decryption Window Showing Completed Decryption of Cipher Text

5. Cryptographic Key Generator Window

The key generator window generates the keys needed for encryption and decryption. An initial public key is inputted and an appropriate prime is generated as the new public key together with the private key and the modulus. The public and modulus are used together for encryption, and private and modulus are used for decryption. Keys generated are 2048 bits long, enhancing the encryption process.

Fig. 6 Cryptographic Key Generation Window

VI. CONCLUSION

The research has proposed a new scheme that is simple, easy and inexpensive to encrypt data securely over insecure networks such as the internet. It utilises the Rivest-Shamir-Adleman (RSA) algorithm which is one of the efficient encryption algorithms. Public and private keys of 2048 bits in length which are large prime numbers are generated and used in both encryption and decryption. Encrypted/ decrypted files can be stored on the local disk securely. Encrypted files can also be sent by mail using the mailing feature of the developed system. Packet losses are checked for using the ping and trace route networking tools. Checking of packet losses during transmission helps to

determine the status of packets during transmission. It can also help in determining faulty routers and also compromised routers where packets are dropped. The system has a user-friendly interface easing its usage. The limitation of this system is that it only encrypts text files.

VII. EXTENSION FOR FUTURE WORKS

Digital signatures which are mathematical schemes for representing the authenticity of messages could be incorporated into the scheme as this will improve security and authenticity of information. The scheme could also be extended to encrypt image, audio and video files.

REFERENCES

[1] RSA algorithm. November 2014. [Online]. Available: http://searchsecurity.target.com/definition/RSA

[2] M. Thangavel, P. Varalakshmi, P. M. Murrali, and K. Nithya, "An Enhanced and Secured RSA Key Generation Scheme (ESRKGS)," *Journal of information security and application*, Vol. 20, pp. 3-10, February 2015.

[3] Y. Li, Q. Liu, and T. Li, "Design and Implementation of an Improved RSA Algorithm," *International conference on E-Health Networking Digital Ecosystems and Technologies*, 2010.

[4] C. Sinjan, K. Vincent, "A Study and Implementation of RSA Cryptosystem," arXiv:1506.04265[cs: CR], 13 June 2015.

[5] M. A. Islam, Md. A. Islam, N. Islam, and B. Shabnam, A Modified and Secured RSA Public Key Cryptosystem Based On "N" Prime Numbers. *Journal of Computer and Communication*, Vol. 6, pp. 78-90, 2018. [Online]. Available: http://doi.org/10.4236/jcc. 2018.63006.

[6] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Communication of the association for computing machinery*, pp. 120-126, 1978.

[7] B. Persis, U. Ivy and P. Mandiwa, "A Modified RSA Cryptosystem Based on 'n' Prime Numbers," *International Journal of Engineering and Computer Science*, Vol. 1, No. 2, pp. 63-66, November 2012.

[8] Packet loss, 6th July 2018, In Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/packet_loss.

[9] H. Mike, "4 Causes of Packet Loss and How to Fix Them," April 28, 2015, [Online]. Available: https://www.annese.com/blog/what-causes-packet-loss.

[10] P. Boyana, *What Is a Ping Test?*, 18th April, 2013, [Online]. Available https://www.websitepulse.com/blog/what-is-ping-test.

[11] A. B. Alhassan, K. A. Gbolade and E. K. Bankas, "A Novel and Efficient LZN-RNS Scheme for Enhanced Information Compression and Security," *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET)*, Vol. 4, No. 11, pp. 1450-4019, 2015.