RSA and RC4 Cryptosystem Performance Evaluation Using Image and Text File

Akinyele A. Okedola, Yekini N. Asafe

Abstract— The process of transforming plaintext data into cipher text in order to conceal its meaning in case it fall to hand of unauthorized recipient is refers to as encryption. The systems that perform the encryption processes are known as cryptosystems, there are several cryptosystem algorithms: RSA, RC4, DES, 3DES, Blowfish, AES, IDEA, Skipjack, DSA, ElGamal, etc. The major features that identify and differentiate one cryptosystem algorithm from another are its ability to secure the protected data against attacks and its speed/efficiency. In this paper: application software was designed to implement RSA, and RCA encryption algorithms with advanced features of visual Basic 6 for the front end interface. Microsoft Access is used to design backend of the application, and the Macromedia Flash was also used to incorporate dynamic features that enhance the appearance of the application. The program was used to compare the performance of RSA and RC4. The encryption operation was carried out for both RSA and RC4 using five text files and five graphic files of different sizes 10, 50, 100, 150, and 200 kilobyte respectively. The major factor considered for measuring the performance of the algorithms (RSA and RC4) is the speed of execution using time of execution (TE) as parameter for the evaluation. The performance result was presented and analyzed. We discovered that the RC4 is better compare to RSA algorithm based on the experimental facts presented and the result analysis of the two evaluated algorithms.

Index Terms: cipher text, cryptosystems, encryption, decryption, RSA algorithm, RC4 algorithm,

1 INTRODUCTION

ONE of means of protecting information as it is stored on communication paths is cryptography. A cryptography system provides the following services: Confidentiality-It ensures that no unauthorised parties can access information except the intended receiver. Authenticity-validating the source of the message to ensure the sender is properly identified; Integrity-provides assurance that the message was not modified during transmission, accidentally or intentionally and Non-repudiation-This means that a sender cannot deny sending the message at a later date and the receiver cannot deny receiving it [1]. Cryptography does refer to as "the study of secret" in that case cryptosystem performs two functions: Hidden plain text from intruders i.e., converting plain text to cipher text (encryption), and unhidden the data to the authentic users (decryption). Fig.1 shows the simple flow of commonly used encryption algorithms [2].

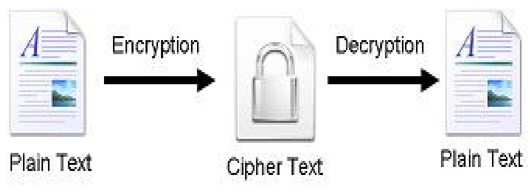

Fig.1 Encryption-Decryption Flow

Cryptography system must focus on the following: Authentication: The process of proving one's identity. This means that before sending and receiving data using the system, the receiver and sender identity should be verified, Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver. Usually this function is how most people identify a secure system. It means that only the authenticated people are able to interpret the message content and no one else, Integrity: Assuring the receiver that the received message has not been altered in any way from the original. The basic form of integrity is packet check sum in IPv4 packets, Non-repudiation: A mechanism to prove that the sender really sent this message. Means that neither the sender nor the receiver can falsely deny that they have sent a certain message, and Service Reliability and Availability: Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users. Such systems provide a way to grant their users the quality of service they expect [3].

As the importance and the value of exchanged data over the Internet or other media types are increasing, the search for the best solution to offer the necessary protection against the intruders' attacks along with providing these services under timely manner is one of the most active subjects in the security related communities. In order to evaluate the performance of the compared algorithms, the parameters that the algorithms must be tested for must be determined.

Since all algorithms has the security features to protect the data against intruder. The major factor to determine the performance is the algorithm's speed to encrypt/decrypt data blocks of various sizes. This paper present a fair comparison between the two most common and used algorithms (RSA and RC4) in the data encryption field. Our main concern here is the performance of these algorithms under different settings; the presented comparison takes into consideration the behavior and the performance of the algorithm when different data loads are used, and the major criteria used is speed of processing with particular reference to execution time.

1.2 Aim and Objectives of the Study

The aim of this study is to develop an application for encryption of image and text using RC4 and RSA Algorithm.

The specific objectives to be met are:

- To design a model for RC4 and RSA algorithm.
- To develop application for the model and evaluate the performance of RC4 and RSA Algorithms using text and image file.

1.2 Statement of the Problem

In a network scenario where data are to be transmitted from one medium to another, the transmitting data may be hijacked by intruder. Several cryptosystems algorithm are available to make data become useless to hijacker or intruders. Hence there is need to evaluate performance analysis in other to choose the best of among the algorithms.

1.3 Scope of the Study

This work will focus on:

- Theoretical Analysis of RSA and RC4 algorithms will be defined and analyzed on paper mathematically to achieve image and text encryption and decryption.
- Practice: The theoretical mathematical algorithm defined above will be used practically to demonstrate the implementation of image and text encryption and decryption for evaluation purposes.

1.4 Significance of the Study

The significant of this study are to contribute:

- To choose a standard encryption to serve as a reference point upon which other encryptions should be benchmarked.
- To ensure and assure integrity of the data being protected.

2 Literature Review

2.1 Cryptography Goals

There are five (5) main goals of security system which includes: Authentication: This means that before sending and receiving data using the system, the receiver and sender identity should be verified; Secrecy or Confidentiality: Usually this function (feature) is how most people identify a secure system. It means that only the authenticated people are able to interpret the message (date) content and no one else; Integrity: Integrity means that the content of the communicated data is assured to be free from any type of modification between the end points (sender and receiver). The basic form of integrity is packet check sum in IPv4 packets; Non-Repudiation: This function implies that neither the sender nor the receiver can falsely deny that they have sent a certain message; Service Reliability and Availability: Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users [4].

2.2 Performance Parameters of Encryption Techniques

Some of the parameters on which encryption techniques are evaluated are [5]: Visual Degradation (VD): This criterion measures the perceptual distortion of the image data with respect to the plain image; Compression Friendliness (CF): An encryption scheme is considered compression friendly if it has no or very little impact on data compression efficiency. Format Compliance (FC): The encrypted bit stream should be compliant with the compressor and standard decoder should be able to decode the encrypted bit stream without decryption. This property is important because it allows preserving some features of the compression algorithm used (e.g., scalability); Speed (S): In many real-time applications, it is important that the encryption and decryption algorithms are fast enough to meet real time requirements; Cryptographic Security (CS): Cryptographic security defines whether encryption scheme is secure against brute force and different plaintext-cipher text attack; Encryption Ratio (ER): This criterion measures the amount of data to be encrypted. Encryption ratio has to be minimized to reduce computational complexity. The encryption ratio is given byER=ne/n.

2.3 RC4 Algorithms and its Features

In cryptography, RC4 is the most widely used software stream cipher and is used in popular protocols such as Transport Layer Security (TLS) (to protect Internet traffic) and WEP (to secure wireless networks). RC4 is a stream cipher, symmetric key algorithm. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent of the plaintext used. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table. The state table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream which is XORed with the plaintext to give the cipher text [6].

RC4 Steps

The steps for RC4 encryption algorithm is as follows:

- Get the data to be encrypted and the selected key.
- Create two string arrays.
- Initiate one array with numbers from 0 to 255.
- Fill the other array with the selected key.
- Randomize the first array depending on the array of the key.
- Randomize the first array within itself to generate the final key stream.
- XOR the final key stream with the data to be encrypted to give cipher text.

2.4 RSA Algorithms and its FeaturesCopyright Form

In RSA technique, two keys are required, first is e and N (n bits) public and second is a number d that is kept secret. In order for A to send a message to B, A looks up B's public values and, if the message is M (written as a number), then A divides the message into pieces of size less than N and sends

- *AKINYELE Akinleye Okedola Obtained B.Sc. Electronics & Computer Engineering from Lagos State University and M.Sc. in System Engineering from University of Lagos. He is currently with Lagos Polythechnic*
- *Yekini Nureni Asafe obtained his academic qualification as follows: M.Sc. in Computer Science, University of Lagos Nigeria (UNILAG); B.Sc. in Electronic and Computer Engineering, Lagos State University (LASU), and NCE (National Certificate in Education) in Physics Lagos State College of Education Ijanikin (LACOED). Hes is currently with Yaba college of Technology.*

C = Me mod n. Then B decodes by M = Cd mod N. The security of the system lies in the choices of the public and private keys. The original RSA cryptosystem was proposed in 1978 by Rivest, Shamir and Adelman and consists of three parts [7][8], these are:

1. RSA Key generation

The processes of RSA key generation are:

- Generate two different primes p and q of (n/2)-bit each.
- Compute N = pq and O(N) = (p-1)(q-1).
- Choose a random integer 1 < e < O(N) such that gcd(e,O(N)) = 1.
- Next, compute the uniquely defined integer 1 < d < O(N) satisfying ed ≡ 1 (mod O (N)).The public key is <N, e> and the private key <N, d>.

2. RSA Encryption

To encrypt a message X with the public key <N, e>, transform the message X to an integer M in {0,…,N-1} and compute the ciphertext C = Me mod N.

3. RSA Decryption

To decrypt the ciphertext C with the private key <N, d>, compute M = Cd mod N and employ the reverse transformation to obtain the message X from M.

3 Design and ImplementationSections

3.1 Description of the System

The system is designed using traditional mode of operation techniques of RSA and RC4 algorithm earlier discussed in section 2 of this paper. The program flowchart for the system is as shown in the figure below:

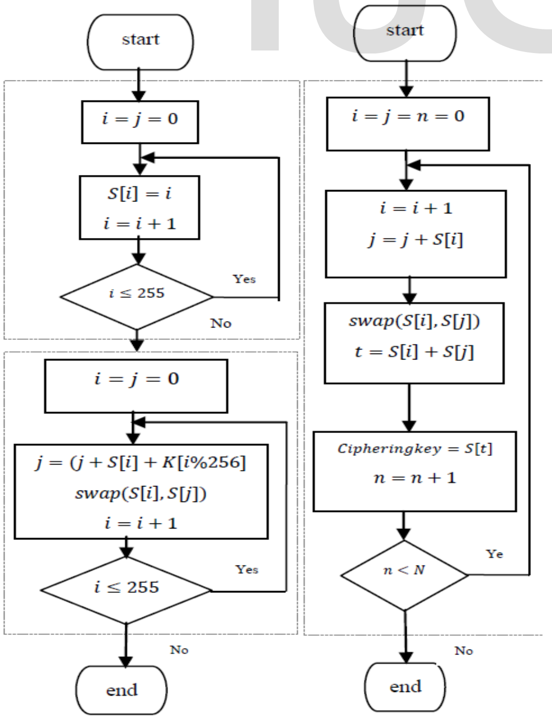

Fig. 2 Cryptosystem Algorithm flow chart for RC4

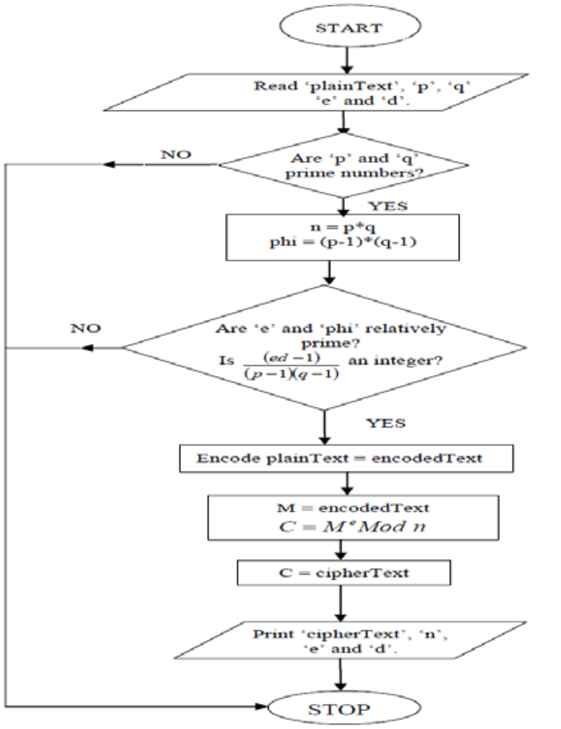
START
Read 'plainText', 'p', 'q' 'e' and 'd'.
NO
Are 'p' and 'q' prime numbers?
YES
n = p*q
phi = (p-1)*(q-1)
NO
Are 'e' and 'phi' relatively prime?
Is $\frac{(ed-1)}{(p-1)(q-1)}$ an integer?
YES
Encode plainText = encodedText
M = encodedText
$C = M^e Mod\ n$
C = cipherText
Print 'cipherText', 'n', 'e' and 'd'.
STOP

Fig. 3 Encryption Algorithm flow chart for RSA

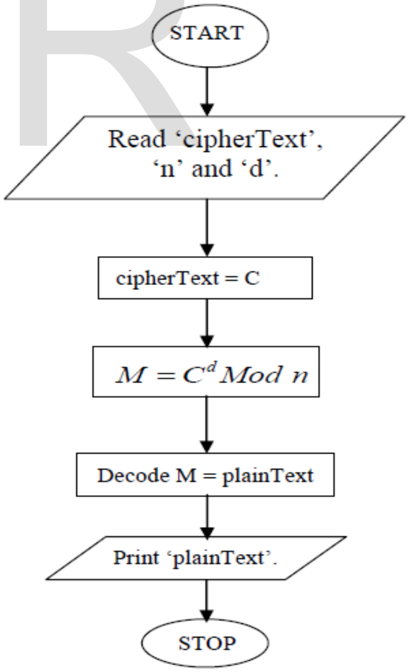

Fig. 4 Decryption Algorithm flow chart for RSA

3.2 Choice of Programming Language

The programming language chosen for implementation of the flowchart for the RSA and RC4 algorithm is Visual Basic 6.0. The programming language was chosen based on the following considerations:

- Its portability, ease of understanding, English-like nature, ease to code.
- It is an ideal programming language for developing sophisticated professional applications for Microsoft windows.
- It makes use of Graphical User Interface for creating robust and powerful applications.
- It uses illustrations for text, which enable users to interact with an application.
- It allows more freedom to the user and developer by presenting greater number of options.
- It features easier comprehension, user-friendliness, faster application development.
- It has powerful database access tools.
- Useful debugger and error-handling facilities
- Sequential and random access files support.

3.3 Implementation and Results Analysis

The encryption operation was carried out for both RSA and RC4 using five text files and five graphic files of different sizes of 10, 50, 100, 150, and 200 kilobyte respectively. The major factor considered for measuring the performance of the algorithms (RSA and RC4) is the speed of execution using time of execution (TE) as parameter for the evaluation. The RSATE and RC4TE were measured for both text file, and the graphic file. The result was tabulated as in table 1, and 2 below.

TABLE I
RSA and RC4 Result With Text Files

Text File No	File Size (Kb)	RSA$_{TE}$ (Sec)	RCA$_{TE}$ (Sec)
File 1	10	1.0	0.5
File 2	50	4.92	2.35
File 3	100	9.24	3.52
File 4	150	13.52	4.58
File 5	200	19.21	6.75

TABLE II
RSA and RC4 Result with Image Files

Text File No	File Size (Kb)	RSA$_{TE}$ (Sec)	RCA$_{TE}$ (Sec)
File 1	10	0.50	0.35
File 2	50	1.82	0.55
File 3	100	2.21	0.68
File 4	150	2.62	0.75
File 5	200	2.64	0.90

The graphical illustration of the results in table I and II is as shown in figure 5 and 6:

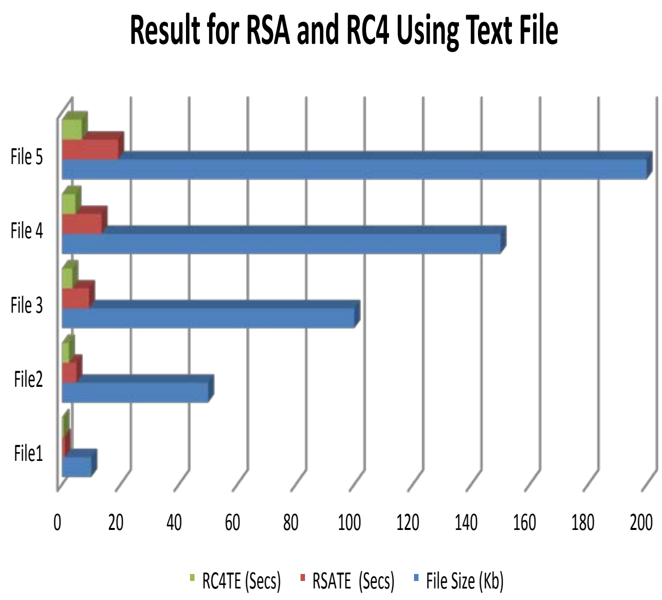

Fig. 5 Performance Evaluation Result with Text Files

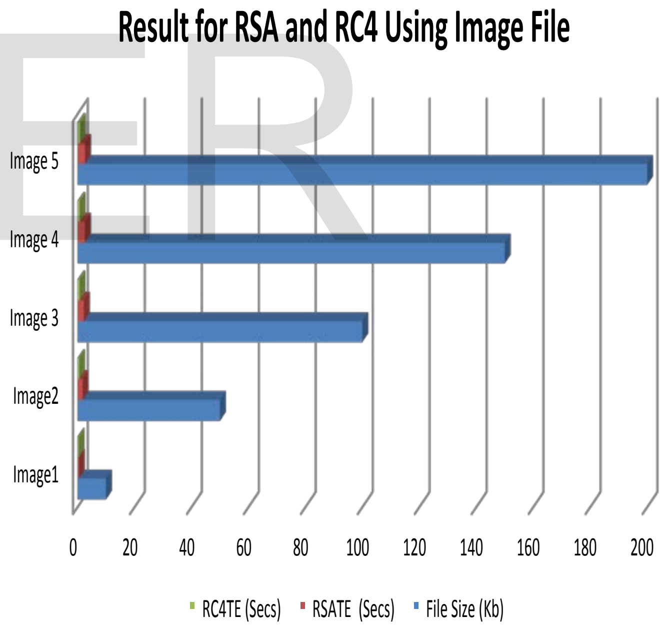

Fig. 6 Performance Evaluation Result with Image Files

4 Conclusion and Recomendation

4.1 Conclusions

From the evaluations of both RSA and RC4 algorithms and the comparison presented, it was concluded that between RC4 and RSA, RSA is the most reliably secure algorithm. However, the RC4 seems to be faster in encryption and decryption process but rather less secure, as it can be broken using a relatively inexpensive device in a short time when compare with RSA.

Although, RC4 is moderately secure. Its key scheduling algorithm is somewhat weak, but this can be corrected. RC4 is faster than RSA. In software, it is roughly one thousand times faster than RSA. RSA is still sufficiently fast for most high-speed applications. By contrast, the slowness of RSA due to the high complexity of modular exponentiation is not usually acceptable for encryption of large files. It is instead often used for small data parcels, such as signatures and keys. All three algorithms are theoretically free, as all the two are in the public domain. There is absolutely no direct monetary cost to implement and use either RSA or RC4. Finally, it was concluded that RC4 is the simplest of the two algorithms to implement. There are no computational optimizations required and the steps are few. RC4 has many steps and operates at the bit level, but each of its operations is straightforward. Algorithm optimization is likely not necessary. RSA has a simple algorithm, but requires substantial optimization, particularly in the exponentiation steps, in order to be practical.

4.2 Recommendations

Based on the analysis and conclusions presented in this report, it is recommended that the RC4 algorithm be used to encrypt real-time wireless and TCP/IP transmissions. Such transmissions require speed, and RC4 is the fastest encryption algorithm considered in this report. As a stream cipher, it is well suited to the near-continuous flow of wireless and TCP/IP transmissions. Also, the algorithm does not have any serious security shortcomings, provided that the protocol and key-scheduling algorithm are adapted to follow the recommendations of the Shamir paper. RC4 is also highly recommended for personal files that are stored locally. The algorithm's simplicity makes it ideal for individuals implementing it on their own. RC4's high speed is also ideal for private individuals, who generally expect quick results. Memory and time requirements of the algorithm are extremely low.

The RSA algorithm is recommended for highly confidential governmental or corporate communications. The security of RSA – due to the difficulty of factorizing large numbers – is very suitable for these sensitive applications. Also, attempts to break the cipher mathematically can typically only be carried out with extensive collaboration, dedicated computers, algorithmic optimizations, and time. The length of the RSA modulus may be chosen to suit security requirements: more sensitive data or data that must remain confidential for a longer time can be encrypted using longer RSA module. The main weakness of RSA is its very low speed. This must be suffered, however, for highly confidential information. Also, RSA requires more human resources than the other algorithms, since without substantial software development to optimize it, the algorithm is too slow to be practical. In addition, RSA is recommended for securing signatures and keys, as the speed of the algorithm is not a significant factor when dealing with small data parcels.

5 FURTHER RESEARCH

This completed works serves as a great improvement to the previous ones. The improvement is actually required in the area of making further evaluation on another set of encryption and decryption algorithms. The research work covered evaluation on the popular RSA and RC4 algorithms. Moreover, no system is perfect in real life situation, therefore, in the future research, it is suggested that whosoever is willing to further research on this topic should work to extend the scope of this project beyond the present scope of study covered. With the improvement of internet services all over the globe, It is therefore, recommended that further research on evaluation of algorithms should please, evaluate algorithm performance that can improve and better present algorithm that can be beneficial for the use of internet to further enhance the security loop holes.

ACKNOWLEDGMENT

The authors wish to thank our wives and children for their endurance during processes of this research, as the tedious work involves does not gives us opportunity to be with them expecially during the design and implementation that ran for almost three weeks.

REFERENCES

[1] Yekini N. Asafe, Aigbokhan E. Edwin, and Okikiola F. Mercy: Cryptography System for Online Communication Using Polyalphabetic Substitution Method. Int. J. Advanced Networking and Applications Volume: 6 Issue: 1 Pages: 2151-2157 (2014) ISSN : 0975-0290

[2] Abdel-Karim Al Tamimi, Performance Analysis of Data Encryption Algorithmswustl

[3] Divya Sukhija, Performance Evaluation of Cryptographic Algorithms: AES and DES International Journal of Computer Science and Mobile Computing, Vol.3 Issue.9, September- 2014, pg. 582-585: IJCSMC, Vol. 3, Issue. 9, September 2014, pg.582 – 585

[4] Earle 2005 "Wireless Security Handbook,". Auerbach Publications 2005

[5] Nadeem 2005 Aamer Nadeem et al, "A Performance Comparison of Data Encryption Algorithms", IEEE 2005

[6] Tsuyoshi Takagi, "Efficiency Comparison of Several RSA Variants", Fachbereich Informatik der TUDarmstadt, March 2003

[7] R. Rivest, A. Shamir, and L. Adleman, "A Method for Ob taining Digital Signatures and Public Key Cryptosystems", Communications of the ACM Vol. 21, No. 2, pp. 120 - 126, 1978.

[8] Allam Mousa and Ahmad Hamad (2006); Evaluation of the RC4 Algorithm for Data Encryption: International Journal of Computer Science and Applications. Vol 3, No 2,

AKINYELE Akinleye Okedola Obtained B.Sc. Electronics & Computer Engineering from Lagos State University and M.Sc. in System Engineering from University of Lagos. He is a Certified Wireless Network Administrator (CWNA), I.T Consultant, Engineer and a Professional Teacher. He was a head of Department of Computer Engineering, Lagos State Polytechnic, and presently the Head, Record and Statistics in the Academic Planning Unit of Lagos State Polytechnic.

Engr. Yekini Nureni Asafe obtained his academic qualification as follows: M.Sc. in Computer Science, University of Lagos Nigeria (UNILAG); B.Sc. in Electronic and Computer Engineering, Lagos State University (LASU), and NCE (National Certificate in Education) in Physics Lagos State College of Education Ijanikin (LACOED). He is a Member Nigeria Computer Society (NCS), International Association of Engineers (IAENG), International Association of Computer Science and Information Technology (IACSIT), and Member Institute of Electrical Electronic (MIEEE). He has co-author, and singular author of several academic/research publications that has features in some revered international journals and conference proceedings both in Nigeria and in abroad. He has written about seventeen textbooks in computer science and engineering