# Performance Analysis of RSA Algorithm for Audio Data Security in Communication Networks

Okonkwo Joshua I., Ozor Godwin O., Okoye Francis A.
*Computer Engineering, Enugu State University of Science and Technology, Nigeria*

*Abstract:* - **Data security and confidentiality is an important aspect of communication system that has always been a focus for exchanging information among parties at location physically apart. One of the most important techniques to protect and verify information that are exchanged over communication channels in the existence of third party called antagonists is cryptography. The stored or transmitted message is transformed in the encryption process to unreadable or gibberish form. The reverse process in which the intendent recipient can reveal the encrypted message content is called decryption. The encryption and decryption processes are achieved using secret keys that are exclusively exchanged between the sender and recipient. This method can be applied to any form of message such as audio, video, image or text data. The study presents the application of the well-known RSA algorithm for audio data encryption and decryption. The performance of the presented algorithm has been tested via experimental implementation using Matlab simulations. The results on the presented technique validated that it is secure, reliable and efficient to be applied in secure audio communications as well as it performed high intelligibility of the recovered audio signal.**

*Keywords:* **encryption, audio, RSA, communication**

## I. INTRODUCTION

Data communication is the most important aspect in our daily life. The main issue in data communication is data security to preserve its availability, integrity, proper access control as well as confidentiality. Data security has been traditionally ensured with cryptography which plays a major role throughout many applications such as e-commerce, e-mail, mobile phone communication, Pay-Tv, sending financial information and so forth. Therefore, one of the most important technique to protect and verify data that are exchanged over communication channels in the existence of third party called antagonists is cryptography. Cryptography gives the means to construct a secure logical channel over an insecure physical connection [1]. One of the methods of cryptography is encryption of data, prepared to be transferred in encrypted way and decrypted when the data is to be used. Encryption is the process of transforming plaintext (original message) into cipher text (hidden message) to conceal its meaning thereby preventing any unauthorized recipient from retrieving the original data [2]. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any antagonist that can see the cipher text should not be able to determine anything about the original message. Encryption works by running the data through a special encryption formula called a key [3]. Decryption is the reverse process of converting encrypted data to its original un-encoded form.

The aim of cryptography is not to hide the existence of a message, but rather to hide its meaning, through a method of encryption. The act of converting a plain text message to its cipher text form is called enciphering. Reversing that act (i.e., cipher text form to plain text message) is deciphering. Enciphering and deciphering are more commonly referred to as encryption and decryption, respectively.

There are two basic types of cryptographic techniques namely; Symmetric cryptographic technique and asymmetric cryptographic technique. Symmetric technique uses a single key for both encryption and decryption of data. Data encryption standard (DES), advance encryption standard (AES), Carlisle Adams and Stafford Tavares (CAST) Algorithm, Blowfish, Twofish, international data encryption algorithm (IDEA) and Secure and Fast Encryption Routine (SAFER) are some examples of symmetric technique [6]. In an asymmetric technique, two different keys that are mathematically related are used. It uses one key (public key) for encryption and another (private key) for decryption. The public key is widely distributed while the private key is secret, which is known to the receiver only. Thus, reconstructing of the original message by decrypting it is feasible. Asymmetric cipher has several advantages over conventional symmetric ciphers. It means that if the opponent can have both the algorithm of encryption and the public key, he will still need to the private key to decrypt the original message which is available only with the intendent recipient. The disadvantage of this type of encryptions is that they are need more computations than symmetric ciphers. Hence, encryption and decryption processes may take longer time. For a short message, this is not suitable, but for bulk data encryption, it certainly does. RSA is an example of asymmetric key encryption methods [4] [5].

## II. RELATED WORKS

Rahman, M. D *et al*(2012), presented a new idea to implement RSA algorithm on speech encryption/decryption. Different speech words were saved in a wave file after they were recorded from different speakers. Encryption and decryption processes are performed in this method on the extracted data from those words after saving them as integer data in a text file.Khalil, M.I. (2016), presented two different encryption and decryption techniques are applied to an audio signal. RSA algorithm is the first one while a new suggested technique that depends on the concept of symmetric cryptography is the second one. The suggested method gives better results than RSA method since it produces an audio signal of high quality as the original signal. Christina C, M. S., *et al* (2016), presented a Video Encryption and Decryption using RSA Algorithm. The RSA algorithm is used to encrypt video data while transmitting it over the internet. The video will be encrypted via public key after converting it to several bytes then it will be sent to the receiver in the text form. The receiver will decrypt the encrypted video via private key after applying paging technique to accelerate encryption and decryption processes.El Bakry, H. M., *et al*(2016) presented Implementation of an Encryption Scheme for Voice Calls. Voice calls are encrypted using RSA encryption approach to maintain the security. The voice call is converted in this method from analog to digital from after receiving it from the microphone via analog to digital converter circuit. Then, the output signal is sent to digital to analog converter circuit to convert it again to its analog form after encrypting it using RSA. The receiver will apply the reverse processes in decryption to get the original voice call.

Sayyad, S. N., *et al*(2017), presented Dual-layer Video Encryption & Decryption using RSA Algorithm. Video encryption scheme that based on Pseudo Noise (PN) sequence and RSA is introduced. Two layers of encryption are utilized on the source after separating the video and audio components to increase the security. The first encryption layer is RSA while the second one is Pseudo Noise (PN) sequence. Sharma, Er. J. and Rani, J. (2017), presented an Efficient Hybrid Approach for Secure Speech Cryptography. A hybridization algorithm that based on three layers of encryption algorithms is proposed to improve speech data security. The first layer is RSA and the second is DES while the third is a combination of both RSA and DES algorithms.

The current work presented a new encryption/decryption technique to ensure end to end secrecy and security of the audio signal, as well as to preserve the good quality of the recovered signal while storing or transmitting throughout any communication system by applying the RSA asymmetric key algorithm.

## III. DESIGN METHODOLOGY

The proposed methodology consists of three stages: keys generation, encryption and decryption of the audio signal using RSA algorithm. Public and private keys are generated previously and then the public key is used to encrypt the acquired speech or audio samples at the transmitter. The ciphered or encrypted audio samples are sent to receiver sequentially through a communication channel who will decrypt each sample by employing the private key. For simplicity, it is assumed that the transmission or communication channel is ideal or free of noise.

*Stage 1: Key generation*

A flow chart of the key generation is given in Figure 1. The following steps illustrate the key generation in RSA algorithm:

a) Random numbers were first generated by the program using Pseudo random number generator.
b) The algorithm selects two distinct large prime numbers p and q.
c) These chosen numbers were checked whether the numbers is a prime using primality test. If p and q passes the primality test, then the algorithm proceed to stage (iii), otherwise, it returns to stage (ii) to select another p and q.

After p and q have passed the primality test, the algorithm moved to the next step, that is, stage (d)

d) the product of p and q were computed and attributed to n, that is, $n= p \times q$
e) the Euler's totient function was also computed,
$$\Phi\ (n) = (p - 1) \times ( p - 1) \quad (1)$$
f) the algorithm then chooses an integer e (encryption key), such that $1 < e < \Phi\ (n)$ , and $\gcd (e, (n)) =1$.
The RSA encryption algorithms with small exponent e , are significantly faster [1].
g) after a value for e, have been successfully chosen, the algorithm computes the private (decryption key) d , to satisfy the Extended Euclidean Algorithm given as $d \times e = 1 \bmod (\Phi\ (n))$ . From the expression,
$$d = e^{-1} \bmod(\Phi\ (n)) \quad (2)$$

VIII. The pubic key is (n, e) and the private key is (n, d).

The values of d, e, p, d and $\Phi(n)$ must be kept secret because these parameters may be utilized to compute [8] [11].

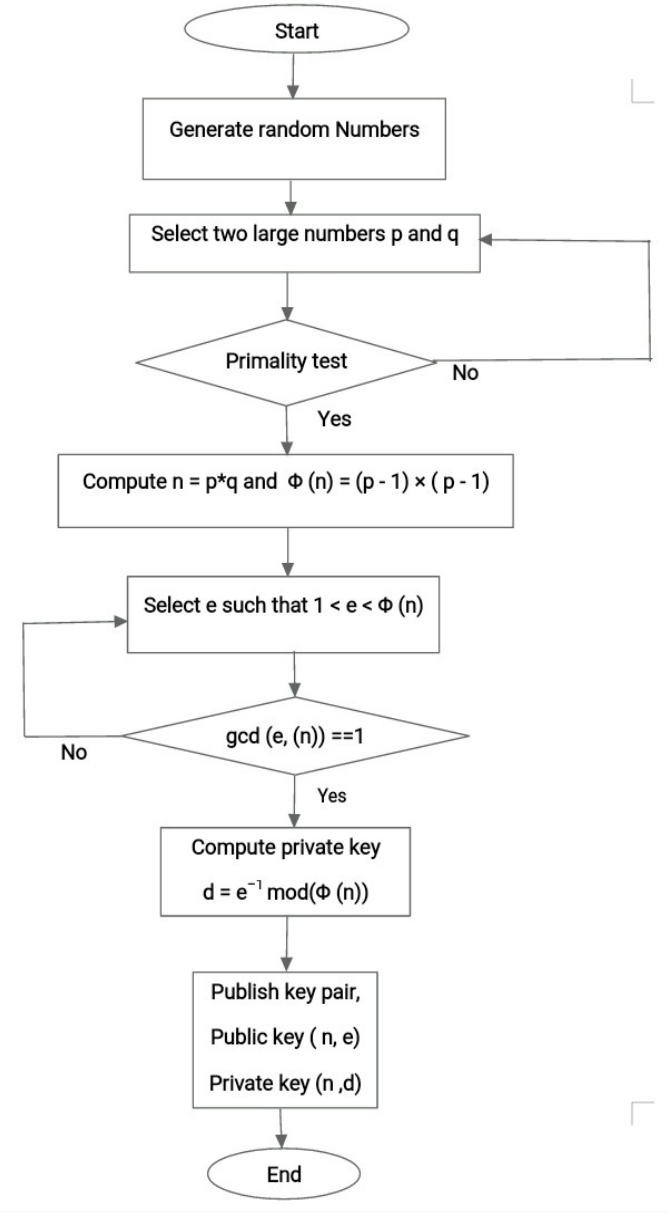

Fig 1: A flowchart of RSA Algorithm Key Generation

### Stage 2: Encryption

For encrypting any message, the algorithm converts the given message into an integer number by using a suitable padding scheme. Then following formula is used to generate encrypted message **C:**

$$C = M^E mod(N) \quad (3)$$

### Stage 3: Decryption

The following formula is used to decrypt the encrypted message M:

$$M = C^D mod(N) \quad (4)$$

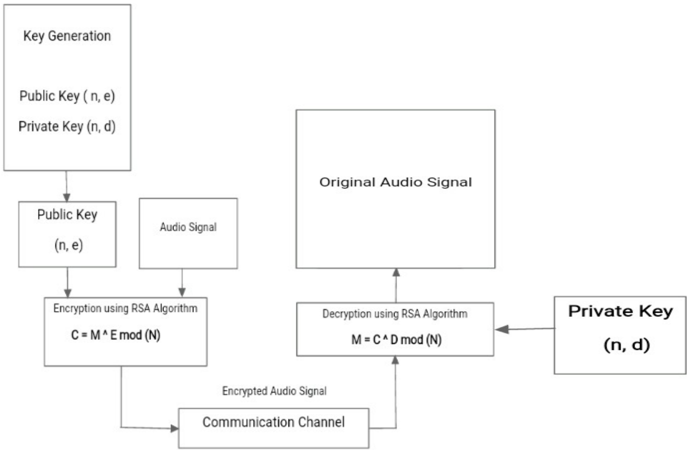

Fig 2: A block diagram of the design methodology

### Step 4: Measurement Criteria

The performance of the presented methodology can be evaluated using number of common quantitative metrics which are Cpestral Distance Measure (CD), Linear Predicative Code Measure (LPC) and Segmental Spectral Signal to Noise Ratio (SSSNR). These metrics are summarized briefly as follows [13]:

**Cpestral Distance Measure (Cd):** The estimation of the log-spectrum distance between the original and the encrypted audio signal is called Cepstrum Distance (CD). It can be computed from the equation:

$$d_{tpc} = \ln\left(\frac{AVA^T}{BVB^T}\right) \quad (5)$$

Where $\mathbf{C_x}$ and $\mathbf{C_y}$ represent the cepstral vectors of the original and encrypted audio signals respectively [14].

**Linear Predicative Code Measure (LPC):** Linear predictive code measure can be defined using the formula:

$$SSSNR_i = 10log\frac{\sum_{n=1}^{N}|X_i(n)|}{\sum_{n=1}^{N}[|X_i(n)|-|Y_i(n)|]} \quad (6)$$

Where **A** and **B** represent the vectors of LPC coefficients for the original and the encrypted audio blocks respectively, and V represent the autocorrelation matrix for the original audio block [15].

**Spectral Signal to Noise Ratio (SSSNR):** Segmental Spectral Signal to Noise Ratio (SSSNR) can be calculated using the equation:

$$CD = 10log_{10}\left[2\sum_{n=1}^{P}\{C_x(n)-C_y(n)\}^2\right]^{\frac{1}{2}} \quad (7)$$

Where $\mathbf{X_i}$ and $\mathbf{Y_i}$ represent the DFT for the original and the encrypted audio signals respectively [13].

## IV. SIMULATION RESULTS AND DISCUSSION

The test results of the performance of the algorithm is presented and discussed in this part. The audio signals which are used in this simulation are extracted from TIMIT database which have sampling frequency of 16 KHz and signal duration of 1.5250 seconds (24400 samples), 2.4850 seconds (39760 samples), 3.9250 seconds (62800 samples) and 4.1950 seconds (67120 samples) respectively and also, all the silence periods are eliminated from them. Different values were tested of p and q to produce the key pair. In this simulation, the values of p and q that were used to compute encryption and decryption keys are set as 3 and 11 respectively because they produced better results for encryption. The encryption key value e is selected to be 7. Hence, the public and the private keys (n , e) and (n , d) will be (33, 7) and (33, 3) respectively. The plotted diagrams shown in Fig. 3 are yielded from the simulation process in the presented work that represent the original, ciphered and deciphered audio signals respectively. It is obvious from Fig. (3b) that the original information has been completely destroyed in the ciphered signal because it is impossible to understand the words by live hearing while hearing the deciphered signal in Fig. (3c) is precisely evident as the original signal in Fig. 3a. MATLAB (R2018a) is used as a programming language to implement all the simulations in the presented cryptosystem.

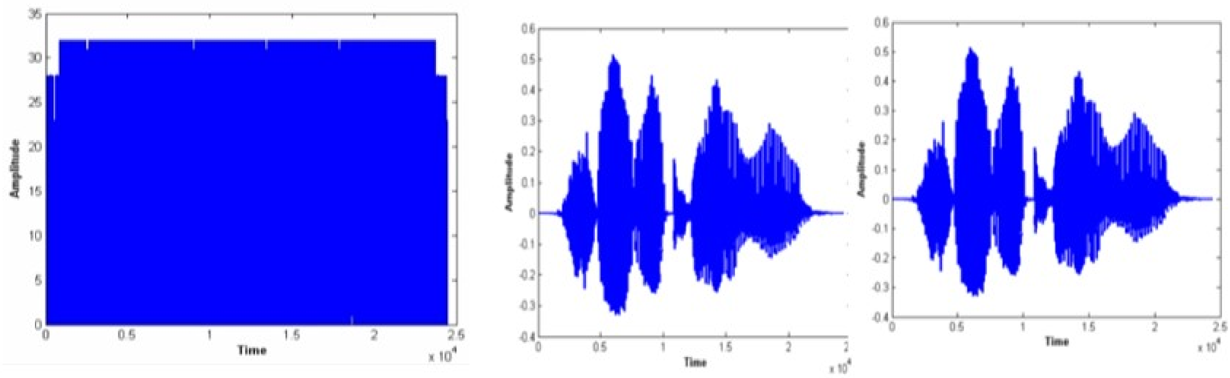

Figure 3 (a): Original audio signal, (b) Ciphered audio signal, (c) Deciphered audio signal

**Quality of audio encryption:** The residual intelligibility of the encryption algorithm is measured using three quality metrics which are CD, $d_{LPC}$ and SSSNR. The better is the audio encryption quality as the value of the SSSNR is decreased, and the values of CD and $d_{LPC}$ are increased [16]. The results of the introduced cryptosystem are explained in Table 1. From the results given in this table, it can be observed that the SSSNR value is very low (negative value) while the CD and $d_{LPC}$ values are high for all ciphered audio files. This means that the residual intelligibility in the presented cryptosystem is low which indicates the high security at the encryption process.

**Quality of audio decryption:** The same three quality metrics are used to measure the quality of the decryption algorithm which are CD, $d_{LPC}$ and SSSNR. The better is the audio decryption quality as the value of the SSSNR is increased, and the values of CD and $d_{LPC.}$ are decreased [14]. The results of the introduced cryptosystem are listed in Table 2. It can be noticed from Table 2, that the SSSNR value is very high (positive value) while the CD and $d_{LPC}$ values are low for all decrypted audio files. This means that the recovered audio signal is of good precision and high quality.

**Table 1:** Results of quality metrics for encryption process

| File name | CD | $d_{LPC}$ | SSSNR (dB) |
|---|---|---|---|
| arctic_a0098.wav | 6.8781 | 4.9614 | -21.5563 |
| arctic_a0497.wav | 5.8812 | 4.9251 | -23.6007 |
| arctic_b0189.wav | 6.2877 | 2.4912 | -21.5213 |
| arctic_a0211.wav | 4.9800 | 3.2795 | -21.6429 |

**Table 2:** Results of quality metrics for decryption process

| File name | CD | $d_{LPC}$ | SSSNR (dB) |
|---|---|---|---|
| arctic_a0098.wav | -0.9644 | -7.4452× 10−13 | 118.4235 |
| arctic_a0497.wav | -1.0197 | -6.1617× 10−14 | 116.4555 |
| arctic_b0189.wav | -0.9424 | -1.0547× 10−14 | 118.5244 |
| arctic_a0211.wav | -0.9618 | 2.3537× 10−14 | 118.3664 |

**Histogram analysis:** Histogram represents the distribution of information values in the system. The analysis of histogram is made by testing distribution of information in various fields. Encrypted information is represented as numbers in the histogram in the encryption practices. If the distributions of these numbers are close, then the performing of encryption process is good [17]. The histograms of the original and encrypted audio signals are presented in Figs. 4a and 4b respectively. From these figures, it can be noticed that the histogram of the encrypted audio signal using RSA algorithm is significantly different from that of the original one and it's fairly uniform. This means that the presented cryptosystem provides good encryption quality which demonstrates high level of security.

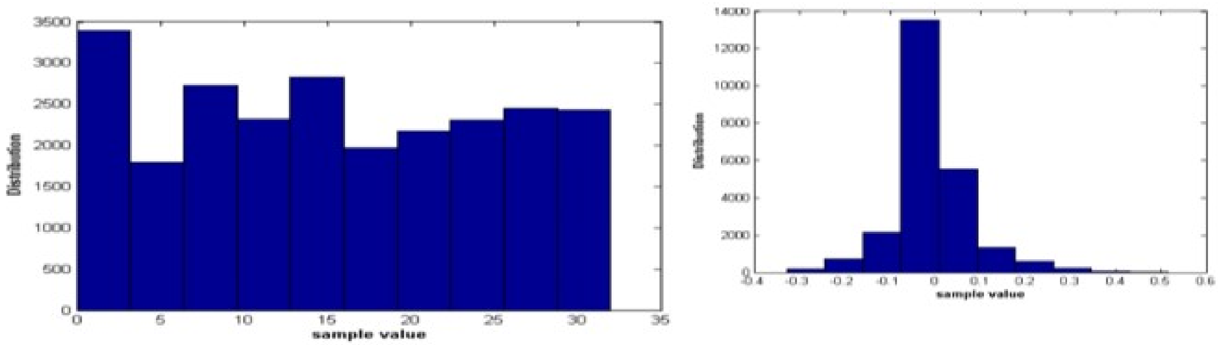

Figure 4 (a): Histogram of the original audio signal, (b) Histogram of the encrypted audio signal

## V. CONCLUSIONS

Dataaccessibility, reliability, confidentially and secrecy are the main aspects that should be maintained in audio security. Protecting audio systems from modification, disruption, extermination as well as the illegal access is the main goal of audio security. A secure and efficient communication system for audio signals that based on RSA public-key cryptosystem is designed in this work. The presented cryptosystem is implemented and its performance is evaluated using different audio quality metrics in both encryption and decryption processes. The results obtained demonstrated that the residual intelligibility in the encrypted audio signal is low while the quality of the recovered audio signal is maintaining good with a satisfying level which confirm the suitability, reliability, high security and effectiveness of the introduced scheme to be applied in practical applications like audio data encryption/decryption.

## REFERENCES

[1]. T. Charomie, "Implementation of Hybrid Encryption Method using Caesar Cipher Algorithm", Dissertation submitted to Faculty of Computer System & Software Engineering Universiti Malaysia Pahang (UMP), Malaysia, 2010.

[2]. A. Naser, H. Fatemeh and K. Riza, "Developing a new hybrid cipher using AES, RC4 and SERPENT for encryption and Decryption", International Journal of Computer Applications, vol. 69, no. 8, pp.53-62, 2013.

[3]. S. William, "Cryptography and Network Security", 4th Edition, Prentice-Hall Inc., pp.58-309, 2005.

[4]. Rahman, Md. M., Saha, T. K. and Bhuiyan, Md. A. Implementation of RSA Algorithm for Speech Data Encryption and Decryption, IJCSNS International Journal of Computer Science and Network Security, Vol.12 No.3, March 2012, 74-82.

[5]. Khalil, M.I. Real-Time Encryption/Decryption of Audio Signal, I. J. Computer Network and Information Security, 2016, 25-31.

[6]. Christina C, M. S., Karthika, M., Vasanthi, M. and Vinotha, B. Video Encryption and Decryption using RSA Algorithm, International Journal of Engineering Trends and Technology (IJETT), Vol. 33 No. 7, March 2016, 328-332.

[7]. El Bakry, H. M., Taki El Deen, A. E. and El Tengy, A. H. Implementation of an Encryption Scheme for Voice Calls, International Journal of Computer Applications, Vol. 144, No.2, June 2016, 24-27.

[8]. Sayyad, S. N., Sutar, P. S., Pise, R. S., Raut, V. H. and Nalawade, C.V. Dual-layer Video Encryption & Decryption using RSA Algorithm, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 4, April 2017, 7661-7668.

[9]. Sharma, Er. J. and Rani, J. An Efficient Hybrid Approach for Secure Speech Cryptography, International Journal of Computer Science and Mobile Computing, Vol.6 Issue.1, January, 2017, 23-29.

[10]. Priyanka, S. and Hemalatha, B. Speech Data Encryption and Decryption Using Elliptic Curve Cryptography", International Journal of Research in Computer Science, Vol. 3, Issue 1, 2016, 48-53.

[11]. Kaur, J. and Singh, Er. K. P. Comparative Study of Speech Encryption Algorithms Using Mobile Applications, International Journal of Computer Trends and Technology (IJCTT), Vol. 4, Issue 7, July 2013, 2346-2350.

[12]. Khatri, S., Mathur, A. and Sharma, S. Parallel Implementation of Cryptographic Algorithm for Image Encryption", International Journal for Technological Research in Engineering, Vol. 4, Issue 2, October 2016, 424-426.

[13]. Abdullah, H. N, Hreshee, S. S. and Jawad, A. K. Design of Efficient Noise Reduction Scheme for Secure Speech Masked by Chaotic Signals, Journal of American Science, 2015, 49-55.

[14]. Al-saad, S. N. and Hashim, E. H. A Speech Scrambler Algorithm Based on chaotic system, AlMustansiriyah J. Sci., Vol. 24, No 5, 2013, 357-372.

[15]. Mahdi, A., Jawad, A. K. and Hreshee, S. S. Digital Chaotic Scrambling of Voice Based on Duffing Map, International Journal of Information and Communication Sciences, 2016, 16-21.

[16]. Al Saad, S. N., and Hato, E. A Speech Encryption based on Chaotic Maps, International Journal of Computer Applications, Vol. 93, No 4, May 2014, 19-28.

[17]. Abd Elzaher, M. F., Shalaby, M. and El Ramly, S. H. Securing Modern Voice Communication Systems using Multilevel Chaotic Approach, International Journal of Computer Applications, Vol. 135, No.9, February 2016, 17-21.