***I. J. Computer Network and Information Security*, 2016, 2, 25-31**
Published Online February 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2016.02.03

# Real-Time Encryption/Decryption of Audio Signal

**M.I.Khalil**
Nuclear Research Center, Atomic Energy Authority, Cairo, Egypt.
Currently in a sabbatical leave as an Associate Prof. at Princess Nora Bint Abdurrahman University, Faculty of Computer and Information Sciences, Networking and Communication Dept., Riyadh, Kingdom of Saudi Arabia, Riyadh
E-mail: magdi_nrc@hotmail.com, mikhalil@pnu.edu.sa

***Abstract*—**Encryption is a way to secure and verify data that are traded through public communication channels in the presence of intruder party called antagonists. Consequently, the transmitted or stored message can be converted to unreadable form except for intended receivers. The decryption techniques allows intended receiver to reveal the contents of previously encrypted message via secrete keys exchanged exclusively between transmitter and receiver. The encryption and decryption techniques can be applied equally to a message in any form such as text, image, audio or video. The current paper applies and evaluate two different encryption/decryption algorithms to the real-time audio signal. The first one is the well-known RSA encryption and decryption technique, while the second one is a new suggested algorithm based on symmetric cryptography concept. The Matlab Simulink simulator tool is used for acquiring the real-time audio signal and simulating the proposed algorithms. Considering the mathematical nature of the audio signal, the experimental results showed that the RSA method yields an audio signal with low quality while the suggested algorithm yields audio signal with high quality as exact signal as the original one.

***Index Terms*—**Cryptography, Symmetric, Asymmetric, Encryption, Decryption, RSA, Simulink**.**

## I. Introduction

Confidentiality of precious data can be achieved using cryptography techniques [1-8]. Cryptography is the art of developing and implementing algorithms to encrypt message in such way that it will be impossible for unintended and unauthorized persons to process or reveal the contents of it whether it is in transmitting or storing state. The intended legitimate users who receive the encrypted message can reveal its contents via decryption process using permitted secret keys as agreement between the transmitter and receiver. Various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Procedures and protocols that meet some or all of data confidentiality, data integrity, authentication, and non-repudiation criteria are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs; however, they also include the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems, and not discussing sensitive procedures with outsiders. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. Cryptographic systems can be classified into two categories:

1- Secret-key (Symmetric) cryptosystems [9]. This category uses only a unique key shared between transmitter and receiver to encrypt and decrypt data respectively. Key has great impact in encryption and decryption as the strength of symmetric key encryption depends on the size of the key. Symmetric algorithms are of two types: Block ciphers and stream ciphers. The block ciphers algorithms process the data in groups or blocks. Examples of block ciphers are Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish. On the other side, the stream ciphers algorithms process a single bit at a time as in RC4 cipher algorithm.
2- Public-key (Asymmetric) cryptosystems [10]. Asymmetric key encryption method generates and employees two different keys; private keys and public keys. Both private and public keys are mathematically related and the private one is used for encryption while the public key is dedicated for decryption process. RSA, Rabin and ElGamal are examples of public-key cryptosystems.

Cryptographic system can be characterized by the type of encryption operations used [11-13]:

1- Substitution: Each character of the plaintext is replaced or substituted by other character according to a particular substitution algorithm.
2- Transposition: The characters of the plaintext are rearranged according to predefined permutation table.
3- Product: The cipher text is produced as a result of mixing both the previous two methods.

Most of the cryptography encryption techniques are dedicated for text data while encryption of multimedia data such as audio data has few cryptography techniques. Most of audio signal encryption techniques are based on adding specific noise to the audio signal at the least significant bits before transmitting and extracting this noise at the receiver yielding the original audio signal. Raghunandhan. K. R presents two layer securities, which includes both transposition and substitution cipher. The first stage processes the audio signal with transposition cipher. While in the second stage modulus multiplication is used as substitution cipher, for this the key is generated using Pseudo Random Number Generation (PRNG) [14]. Sheetal Sharma proposed a method where a frequency domain of the wav audio signal is taken for the encryption and decryption. The DFT (Discrete Fourier Transform) is used for transforming the time domain audio signal to frequency domain audio signal. The audio signal is separated into different frequency bins with respect to phase and magnitude values by applying DFT on the audio signal. The RSA technique is applied for the encryption and decryption on the lower frequency bands because not all the frequency regions participate equally in the communication [15-17].

The current paper proposes a new symmetric-based encryption/decryption approach for securing audio signal to guarantee end-to-end secrecy for speech in real time communication systems. The performance of the proposed approach is compared with that obtained when applying the well-known Asymmetric RSA technique. It processes the transmitted audio signal encrypting each acquired sample and decrypting it at the receiver. The technique can be applied equally to both digital and analog audio signals such as GSM, VoIP, Telephone, analogue Radio.

The rest of this paper is organized as follows: Section II illustrates the RSA encryption and decryption algorithms. The proposed method is introduced and implemented in section III. Simulink based simulation of both RSA and the proposed algorithm are illustrated in section IV. The obtained results are discussed and concluded in section V.

## II. RSA Cryptography

Asymmetric key cryptography method uses two separate keys: one private and one public. The main idea behind asymmetric-key cryptography is the concept of the trapdoor one-way function. The most common public-key algorithm is the RSA cryptosystem [13], named for its inventors (Rivest, Shamir, and Adleman). RSA technique employs two keys: public key ***e***, which is used in the encryption process and the other, is private key ***d***, which is used in the decryption process. The generation process of both public and private keys along with the encryption and decryption algorithms are illustrated in List.1.

Using public key (***n***, ***e***), the authorized person can apply the encryption algorithm on the plain message ***x*** yielding the ciphered message ***y***. The encrypted message ***y*** can be computed as following:

$$y = E(x) = x^e \ mod \ n \qquad (1)$$

The ciphered message ***y*** is then transmitted and when another intended authorized person receives it, he can apply the decryption algorithm on it using the private key (***n***, ***d***) as following:

$$D(y) = y^d \ mod \ n \qquad (2)$$

List.1.: RSA Encryption/Decryption Algorithm

***RSA: Choosing keys***

*1. Choose two large prime numbers p, q.*
*(e.g., 1024 bits each)*
*2. Compute n = pq, z = (p-1)(q-1)*
*3. Choose e (with e<n) that has no common factors*
*with z. (e, z are "relatively prime").*
*4. Choose d such that ed-1 is exactly divisible by z.*
*(in other words: ed mod z = 1 ).*
*5. Public key is (n,e). Private key is (n,d).*

***RSA: Encryption, decryption***

*1. Given (n,b) and (n,a) as computed above*
*2. To encrypt bit pattern, m, compute:*
$x = m^e$ *mod n*
*(i.e., remainder when me is divided by n)*
*3. To decrypt received bit pattern, c, compute:*
$m = x^d$ *mod n*
*(i.e., remainder when cd is divided by n)*

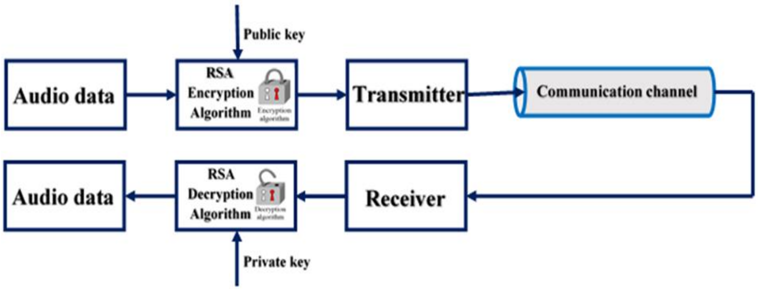

Fig.1. The Block Diagram of the Real-Time Audio Signal Encryption/Decryption using RSA Method

The block diagram of the suggested real-time audio encryption system applying the RSA algorithm is displayed in Fig.1. The acquired audio samples are encrypted using previously generated public key yielding encrypted (or ciphered) samples. The ciphered samples are sequentially transmitted and when received; each sample is then decrypted at the receiver using the private key. It is assumed, for simplicity, that the transmission channel is ideal and has no impairments effects such as noise.

## III. The Suggested System

The block diagram of the proposed system is shown in Fig.2. The acquired audio samples are encrypted using previously generated secret key yielding encrypted (or ciphered) samples. The ciphered samples are sequentially transmitted and when received; each sample is then decrypted at the receiver using the same secret key. It is assumed again, for simplicity, that the transmission channel is free of noise. The work in this paper focuses only on both the encryption and decryption stages. The proposed algorithm is based on symmetric key method and due to the nature of audio signal as real values, the key will be assumed as real number (positive or negative).

Unlike RSA method, both encryption and decryption processes will use the same secret key (***a, b***).

Assuming the value of the plain audio sample = ***p,***

With the condition that: -1 ≤ ***p*** ≤ 1, then the value of the ciphered audio sample ***S*** should be within the upper and lower limits as exactly as ***p***: -1 ≤ ***S*** ≤ 1.

Assuming the secret key = (***a, b***), where ***a*** and ***b*** are real numbers, then applying the proposed encryption method, the value of the ciphered audio sample ***S*** can be calculated as following:

$$S = log_b(a\,p) = log_b(a) + log_b(p) \tag{3}$$

The transmitter sends the ciphered audio sample and assuming that it is purely received (free of noise), we can infer the value of the plain sample as following:

Rearranging Eq.3 yields:

$$log_b(p) = log_b(a\,p) - log_b(a) \tag{4}$$

$$b^{log_b(p)} = b^{[\,log_b(a\,p) - log_b(a)]} \tag{5}$$

$$p = b^{[\,log_b(a\,p) - log_b(a)]} \tag{6}$$

$$p = \frac{b^{log_b(ap)}}{b^{log_b(a)}} = \frac{b^S}{a} = \frac{b^{the\ ciphered\ audio\ sample}}{a} \tag{7}$$

To determine the upper and lower limits of both ***a*** and ***b***:

Assuming $b \in (0, \infty)$, then from Eq.7:

$$a = \frac{b^S}{p} \tag{8}$$

The maximum value of a:

$$a_{max} = \frac{{b_{max}}^{S_{max}}}{|p|_{min}} \tag{9}$$

And the minimum value of a:

$$a_{min} = \frac{{b_{min}}^{S_{min}}}{p_{max}} \tag{10}$$

The absolute minimum value of ***p*** = 0, $\boldsymbol{S_{min}} = \mathbf{-1}$ and $\boldsymbol{S_{max}} = \mathbf{1}$**,** then: $a_{min} = \frac{1}{b}$

Then the proper values of ***a*** and ***b*** are:

$$b \in (0, \infty), \quad a \in (\tfrac{1}{b}, \infty) \tag{11}$$

For more illustration, the block diagrams of both the proposed encryption and decryption methods are separately illustrated in Fig.3 a, b respectively.

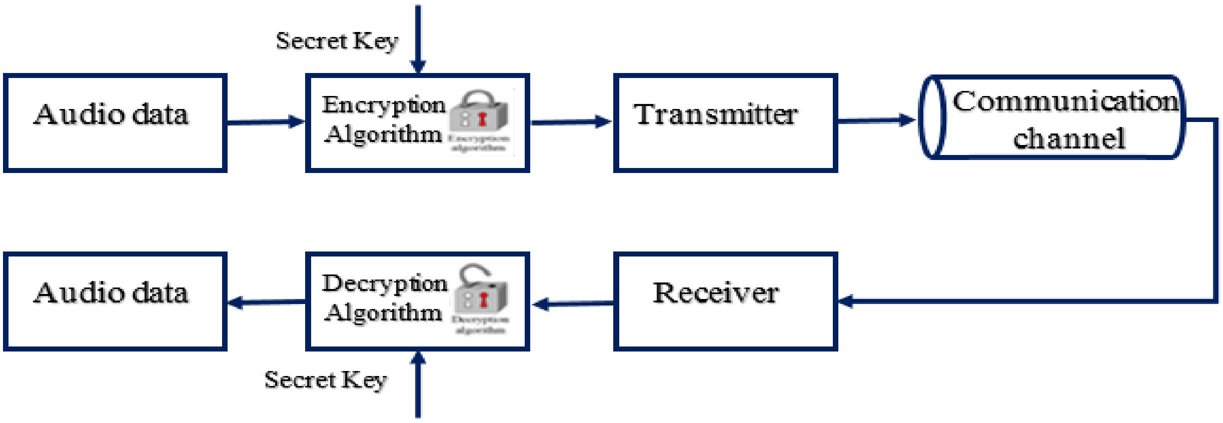

Fig.2. The Block Diagram of the Real-Time Audio Signal Encryption/Decryption using the New Suggested Algorithm

## IV. Implementation And Experimental Results

To evaluate and compare the performance of both RSA and the proposed encryption/decryption methods, the Matlab Simulink software is used as simulation platform.

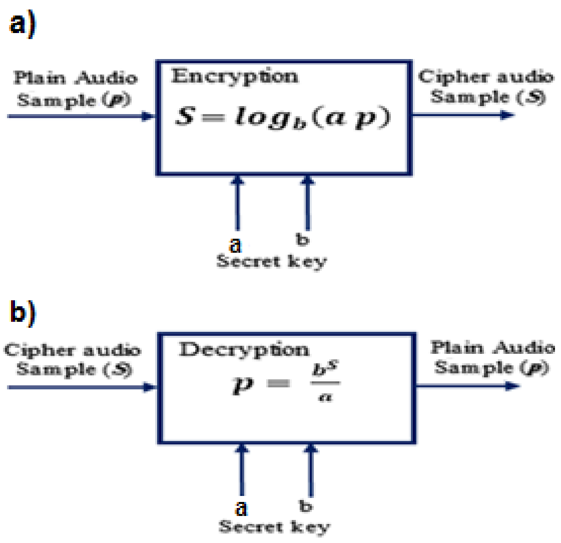

Fig.3. a) Encryption Algorithm b) Decryption Algorithm

### A. Simulation using RSA algorithm

The encryption and decryption of real-time audio signal using RSA method is designed and implemented using Simulink simulator. The block diagram of the simulation scheme is shown in Fig.4 where the real time audio signal is acquired from either a real audio file or real microphone. The encoder block function receives the audio signal ***x*** and encrypts it using (***n, e***) as public key (Eq.1), while the decoder block function decrypts the received ciphered audio signal using (***n, d***) as private key (Eq.2). Both the encryption and decryption functions are implemented as following:

Encryption function: **c = (round(10 *(1+m))^e , n)**
Decryption function: **y = (mod(c1^d , n)) / 10 -1**

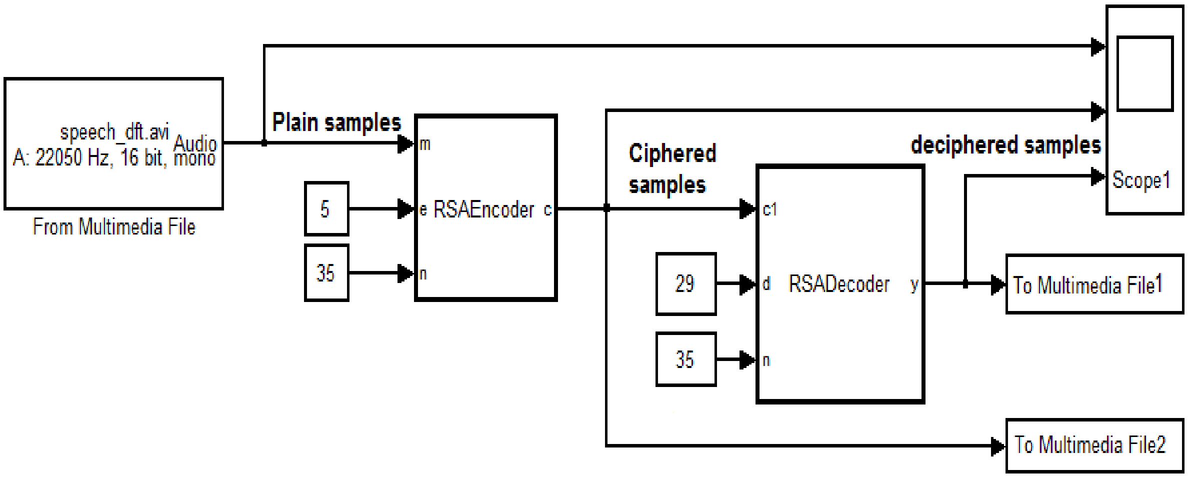

Fig.4. Matlab Simulink Scheme for Encryption and Decryption of Real-Time Audio Signal using RSA method

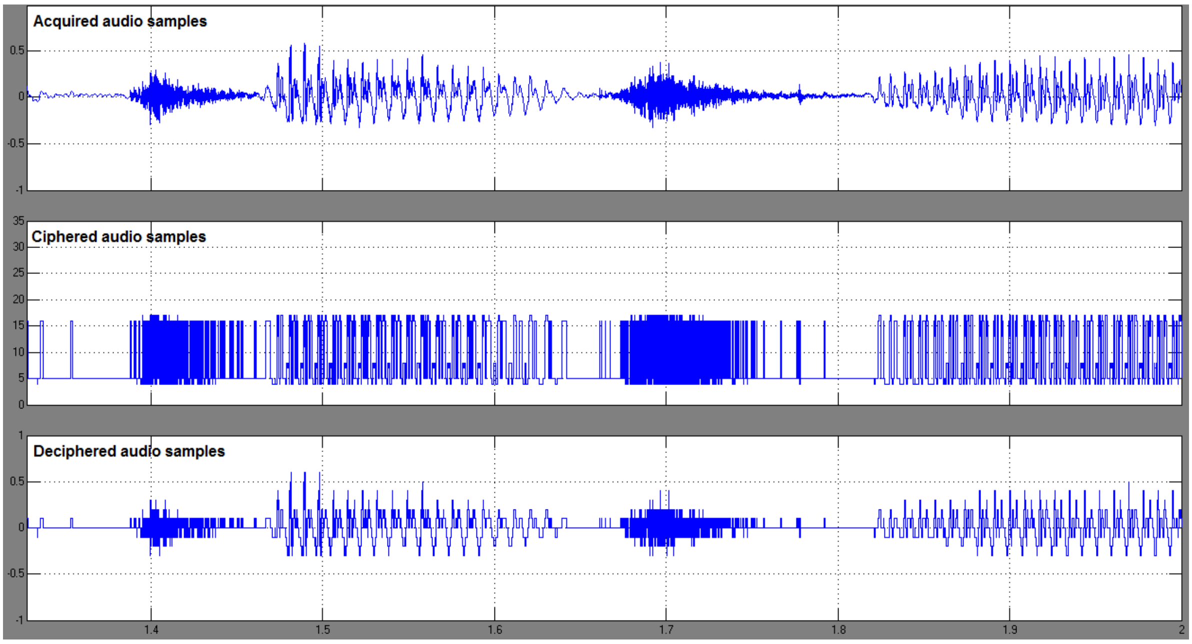

Fig.5. Simulation Results for Encryption and Decryption of Real-Time Audio Signal using RSA Method

As an example, in this simulation, variables ***n, e*** and ***d*** are set as ***35, 5*** and ***29*** respectively. The simulation process yields the plotted diagrams as shown in Fig.5. The upper part represents the acquired signal (plain audio samples); the middle part represents the ciphered signal, while the down part represents the deciphered signal. For comparison purpose, both the ciphered and deciphered audio signals have been stored to multimedia files. The live hearing of both files articulates the impossibility of understanding the words of the first file while there is some difficulty to understand the contents of the second file. This result can be explained due to the rounding of the audio sample value to the nearest integer and shifting it to positive level to be able to undergo the RSA algorithm, which dictates that the value of the ciphered message (audio plain sample in current case) must be positive integer.

### *B. Simulation using the proposed algorithm*

The encryption and decryption of real-time audio signal using the proposed algorithm is implemented using Simulink simulator. The block diagram of the simulation scheme is shown in Fig.6 where the real-time audio signal is acquired using either a real audio file or real microphone. The encryption block receives the audio signal ***p*** and encodes it using (***a, b***) secret key (Eq.3) while the decoder block decrypts it using the same secret key (Eq.7). In this simulation, input variables ***a*** and ***b*** are set as 0.0003 and 300000 respectively. The simulation process yields the plotted diagrams as shown in Fig.7. The upper part represents the acquired signal (plain audio samples); the middle part represents the ciphered signal, while the down part represents the deciphered signal. Both the ciphered and deciphered signals have been stored to multimedia files. The live hearing of both files articulates the impossibility of understanding the words of the first file (ciphered samples in Fig.6) while hearing the second file (deciphered samples) is exactly clear as the original file.

Both the encryption and decryption functions are implemented as following (Fig.6):

Encryption function: $S = \frac{\log_{10} p}{\log_{10} b} + \frac{\log_{10} a}{\log_{10} b}$

Decryption function: $p = \frac{b^S}{a}$

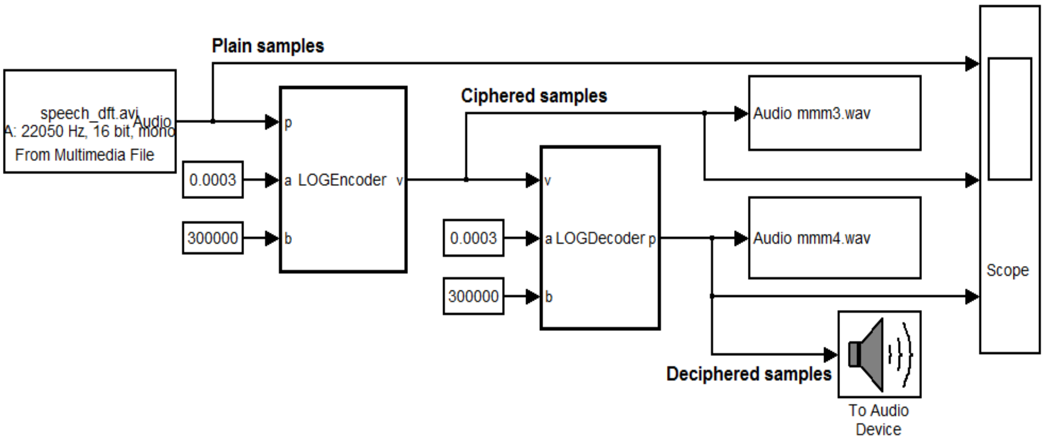

Fig.6. Simulink Scheme for Encryption and Decryption of Real-Time Audio Signal using Proposed Method

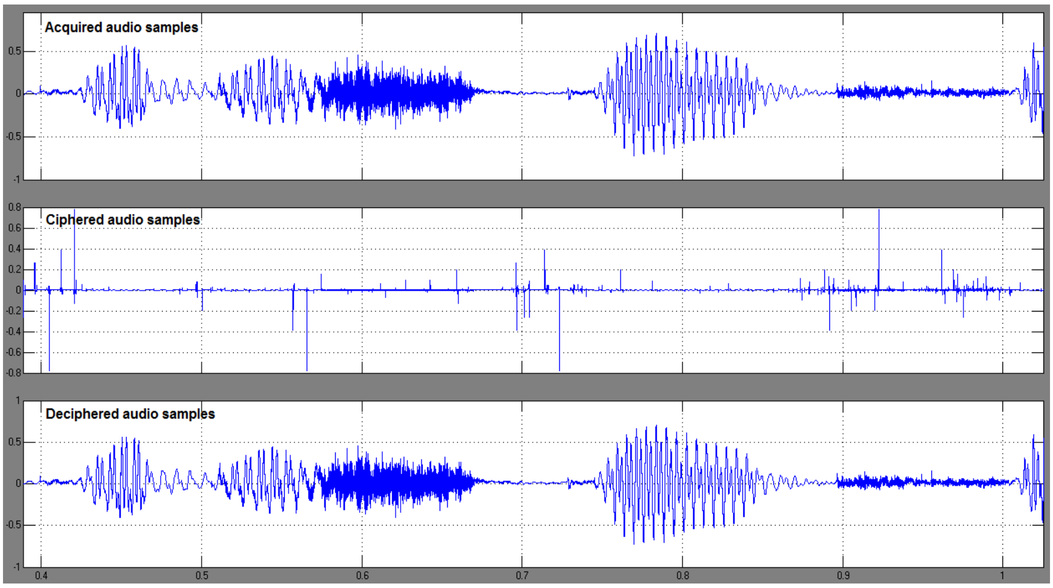

Fig.7. Simulation Results for Encryption and Decryption of Real-Time Audio Signal using the Proposed Method

### *C. Simultaneous simulation using both the RSA and the proposed algorithms*

Both the RSA and the proposed algorithms have been tested simultaneously (Fig.8) using the same input signal yielding the plotted diagrams shown in Fig.9. The input signal is a real mono audio file with sampling rate of 22050 Hz, 16 bit, simultaneous simulation coincides with that obtained for both RSA and proposed algorithm separately in 4.A and 4.B sections respectively. It is noticed that the amplitude of the ciphered audio samples using RSA methods is magnified compared to the amplitude of the corresponding acquired samples which makes it impracticable application. At the same time, the amplitude of the ciphered audio samples using the proposed methods coincides with the original samples. The error rate is determined for both methods by comparing the original acquired samples with those obtained after ciphering stage. The obtained measurements biased extremely to the proposed method (error rate = 0.00017) compared to the RSA method (error rate = 0.9737).

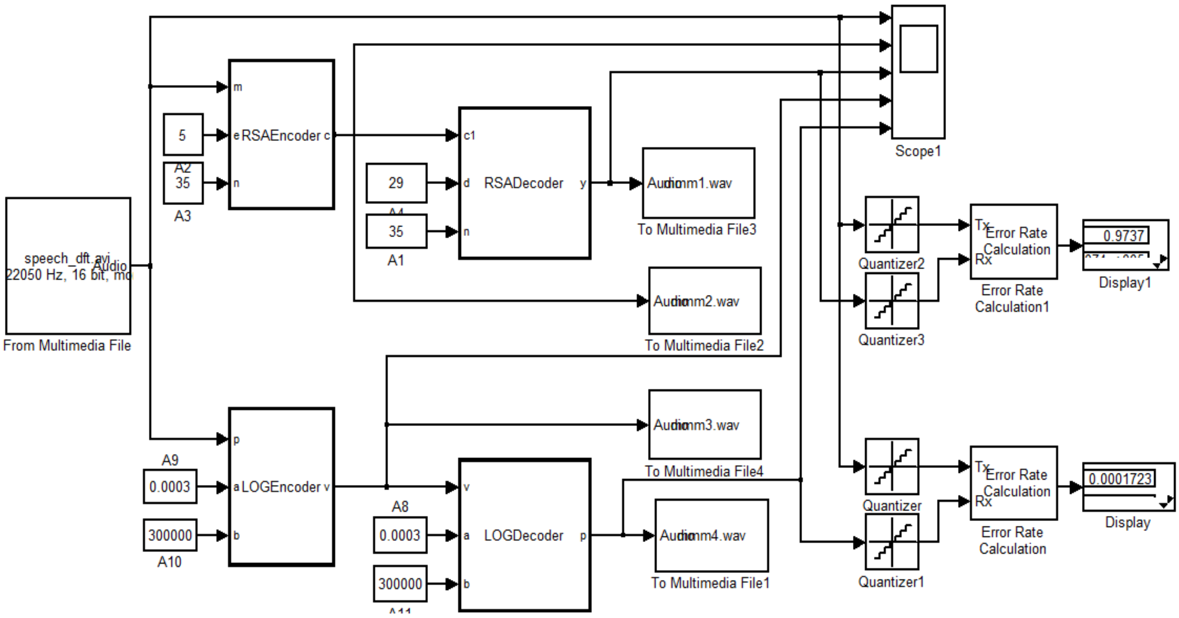

Fig.8. Simulink Scheme for Encryption and Decryption of Real-Time Audio Signal using Both Methods

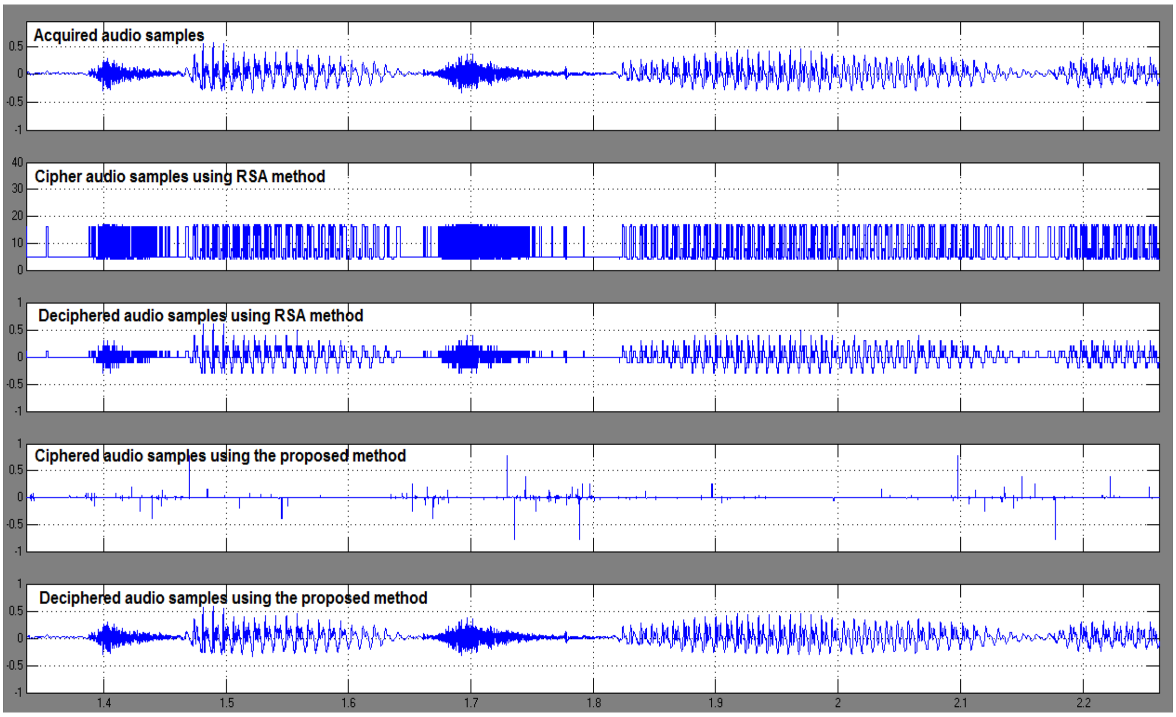

Fig.9. Simulation Results for Encryption and Decryption of Real-Time Audio Signal using Both Methods

## V. Conclusion

The current paper applied and evaluated two different encryption/decryption algorithms to a real-time audio signal. The first one is the well-known RSA encryption and decryption technique, which is classified as an asymmetric cryptography system while the second one is a new suggested algorithm based on symmetric cryptography. The Matlab Simulink software tool is used for implementing and simulating the two methods via acquiring real-time audio signal and applying the encryption and decryption algorithms. The ciphered and deciphered audio samples are traced and compared with the original acquired signal. The experimental results showed that the RSA method yields audio signal with low quality while the suggested algorithm yields as exact signal as the original one. The error rates are measured for both RSA method and the proposed method as well. The obtained results showed that the error rate in the case of the proposed method is extremely low compared to that obtained in the RSA case. The suggested cipher method can be more developed to be applied to video signal.

## References

[1] Jingli Zheng, Zhengbing Hu, Chuiwei Lu, “A Light-weight Symmetric Encryption Algorithm Based on Feistel Cryptosystem Structure”, IJCNIS, Vol. 7, No. 1, December 2014, pp. 16-23.

[2] Mamta. Juneja, and Parvinder S. Sandhu, “A Review of Cryptography Techniques and Implementation of AES for Images”, International Journal of Computer Science and Electronics Engineering (IJCSEE) Volume 1, Issue 4 (2013) ISSN 2320-401X; EISSN 2320-4028.

[3] Koumal Kaushik and Suman, “An Innovative Approach for Video Steganography”, IJCNIS, Vol. 7, No. 11, October 2015, pp. 72-79.

[4] Anupam Mondal and Shiladitya Pujari, “A Novel Approach of Image Based Steganography Using Pseudorandom Sequence Generator Function and DCT Coefficients”, IJCNIS Vol. 7, No. 3, February 2015 pp.42-49.

[5] Habutsu T., Nishio Y., Sasase I., and Morio S., “A secret key cryptosystem by iterating chaotic map,” Lect. Notes comput. Sci, Advances in Cryptology-EuroCrypt’91, 1991, vol. 547, page(s): 127-140.

[6] Pichler F. and Scharinger J., “Finite dimensional generalized baker dynamical systems for cryptographic applications,” Lect. Notes in Comput. Sci, 1996, vol. 1030, pp. 465-476.

[7] T. ElGamal, “A prublic key cryptosystem and a signature scheme based on discrete logarithms”, in Advances in Cryptology (CRYPTO ’84), Springer, 1985, vol. 196, pp. 10–18.

[8] Yen J. C. and Guo J. I., “A new chaotic image encryption algorithm,” Proc. 1998 National symposium on Telecommunications, Dec. 1998, page(s): 358-362.

[9] Yen J. C. and Guo J. I., “Efficient hierarchical image encryption algorithm and its VLSI realization,” IEEE Proceeding Vis. Image Signal Process, April, 2000, vol. 147, no.2, page(s): 430-437.

[10] Ueli Maurer and Björn Tackmann, “On the Soundness of Authenticate-then-Encrypt: Formalizing the Malleability of Symmetric Encryption”, Proceedings of the 17th ACM Conference on Computer and Communication Security, ACM, pp. 505–515, Oct 2010.

[11] Ueli Maurer and Stefano Tessaro, Basing {PRF}s on Constant-Query Weak {PRF}s: Minimizing Assumptions for Efficient Symmetric Cryptography Advances in Cryptology — ASIACRYPT 2008, Lecture Notes in Computer Science, Springer-Verlag, vol. 5350, pp. 161–178, Dec 2008.

[12] Ritesh D.Yelane, Nitiket. N. Mhala and B. J. Chilke, “Security Approach by Using Visual Cryptographic Technique”, ijarcsse, Vol. 5, No. 1, January 2015.

[13] Z. M. Wang, G. R. Arce and G. Di Crescenzo, “Halftone visual cryptography via error diffusion,” In IEEE Transaction on Information Forensics & Security, vol.4, no.3, pp. 383-396, Sep.2009.

[14] R.Gnanajeyaraman, K.Prasadh , Dr.Ramar, Audio encryption using higher dimensional chaotic map, International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009.

[15] Sheetal Sharma and Lucknesh Kumar, Encryption of an Audio File on Lower Frequency Band for Secure Communication, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013 ISSN: 2277 128X.

[16] Ali M. Meligy, Mohammed M. Nasef, Fatma T. Eid, “An Efficient Method to Audio Steganography based on Modification of Least Significant Bit Technique using Random Keys”, IJCNIS Vol. 7, No. 7, June 2015, pp. 24-29.

[17] Thiruppathy Kesavan, V, “Secret Key Cryptography based Security Approach for Wireless Sensor Networks”, Recent Advances in Computing and Software Systems (RACSS), 2012 International Conference, IEEE.

## Authors’ Profiles

**Dr. Magdi Ibrahim Khalil El-Sharkawy**, Egyptian, male, has obtained his B.Sc degree in Computer and Automatic Control Engineering from Faculty of Engineering, Ain Shams University, Cairo, Egypt, in 1983, M.Sc degree in Computer Engineering from Faculty of Engineering, Tanta University, Tanta, Egypt, in 2003 and Ph.D degree in Computer Systems Engineering from Faculty of Engineering, Benha University, Cairo, Egypt, in 2005. He is currently working as Associate Professor in Department of Networking and Communication systems at the Faculty of Computer and Information Sciences, Princess Noura Bent Abdulrahman University, Riyadh, KSA. He has 15 years of previous experience at the Reactor Physics Department, Nuclear Research Center (NRC), Egyptian Atomic Energy Authority Cairo (EAEA), Egypt in the field of Data Acquisition and Interface Design. His main research interests focus on: Digital Signal Processing, Wireless Sensor Networks, Personal and Mobile Communications. So far, he has twelve years of teaching experience and has published more than twenty-five papers in repute journals and proceedings of conferences in fields of the data acquisition, digital signal processing, image processing and neural networks.