ISSN: 2454-1907
DOI: https://doi.org/10.29121/ijetmr.v5.i7.2018.259

IJETMR
International Journal of Engineering Technologies and Management Research
A Knowledge Repository

ENCRYPTION AND DECRYPTION OF AUDIO SIGNAL BASED ON RSA ALGORITHN

Sura F. Yousif [*1]
[*1] Department of Chemical Engineering, Collage of Engineering, University of Diyala, Iraq

Abstract:
One of the most important methods to protect and verify information that are exchanged over public communication channels in the existence of third party called antagonists is encryption. 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 current work applies the well-known RSA algorithm for audio signal encryption and decryption. The performance of the presented algorithm has been tested via experimental implementation which show that the Cpestral Distance Measure (CD), Linear Predicative Code Measure (LPC) and Segmental Spectral Signal to Noise Ratio (SSSNR) reach to 6.8781, 4.9614 and -21.5563 dB respectively 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; Decryption; Cryptography; Symmetric Key Cryptosystem; Asymmetric Key Cryptosystem; RSA Algorithm.

Cite This Article: Sura F. Yousif. (2018). "ENCRYPTION AND DECRYPTION OF AUDIO SIGNAL BASED ON RSA ALGORITHN." *International Journal of Engineering Technologies and Management Research*, 5(7), 57-64. DOI: https://doi.org/10.29121/ijetmr.v5.i7.2018.259.

1. Introduction

The most important aspect in our daily life is data communication. The main issue in data communication is data security to preserve its availability, integrity, proper access control as well as confidentiality. Therefore, Data protection is essential from misuse. The necessity to protect communication today in the e-age from intruders has become greater than ever before (Rahman et.al, 2012). Data protection 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. Cryptography can be defined as the science of implementing and developing techniques to encrypt a message in a way that could be impossible for intruders and illegal persons to detect or modify its contents whether it's being in storing or sending case. Only the intendent user can recover the content of the encrypted message by decryption operation using secret key which is shared between the transmitter and receiver. Cryptosystems refer to set of protocols and procedures that are associated with aspects of data

ISSN: 2454-1907
DOI: 10.5281/zenodo.1341956

security like authentication, confidently, integrity and non-repudiation (Khalil, 2016, Christina C et.al, 2016).

Fundamentally, cryptosystems can be categorized to two main types based on the way in which encryption and decryption processes are carried out in the cryptosystem: symmetric key (secret key) cryptosystems and asymmetric key (public key) cryptosystems. In symmetric key cryptosystems, the same key is shared between the transmitter for encryption and the receiver for decryption the data. The strength of symmetric algorithms depends on the size of the secret key. Blowfish, Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are examples of symmetric key encryption techniques. In asymmetric key cryptosystems, each user in the system has two different keys: private which is used for encryption at the transmitter and public which is used for decryption at the receiver. Although these two keys are different but they are mathematically related. 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 (Rahman et.al, 2012, Khalil, 2016).

New techniques have been presented recently for data encryption using RSA algorithm. As examples, the researchers in (Rahman 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. In (Khalil, 2016), 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 produce an audio signal of high quality as the original signal. In (Christina C et.al, 2016), 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. In (El Bakry et.al, 2016), 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. In (Sayyad et.al, 2017), 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. In (Sharma & Rani, 2017), 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.

ISSN: 2454-1907
DOI: 10.5281/zenodo.1341956

Finally, genetic algorithm is applied for optimization purpose. The results are evaluated in sense of MSE and PSNR.

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.

This scheme is organized as following: Section 1 has been already presented. RSA algorithm with its encryption and decryption techniques is briefly illustrated in section 2. The proposed methodology and its implementation are introduced in section 3. Section 4 gives the measurements criteria that used to evaluate the presented audio cryptosystem. Experimental results and discussion are explained in section 5 and finally the main conclusions of this work are summarized in section 6.

2. RSA Algorithm

RSA is basically an authentication system and Internet encryption method. This algorithm was developed by its inventors in 1977 (Ron Rivest, Adi Shamir and Leonard Adleman). It is one of the most common asymmetric key cryptosystems that it is included as a part from Netscape and Microsoft of the Web browsers. Initially, two large prime numbers are chosen and multiplied in this algorithm to create the public and the private keys pair which are further used in the encryption and decryption operations. There is no need to send the private key throughout the Internet if RSA algorithm is used. The private key is utilized to decrypt the secret message at the receiver which has been ciphered or encrypted by using the public key at the transmitter. Everyone can know the public key which is used to encrypt the messages, but the encrypted messages by the public key can be decrypted only with the private key. Three steps are involved in RSA which are key generation, encryption and decryption processes (El Bakry et.al, 2016, Priyanka & Hemalatha, 2016).

- **Key generation:** The following steps illustrate the key generation in RSA algorithm:
- Choose two large prime integers p and q. The modulus n can be computed from these two numbers, $n = p * q$.
- Calculate Euler's totient function $\emptyset \; for \; n$ from the equation: $\emptyset(n) = (p-1)(q-1)$.
- Choose a third integer number e such that gcd $(\emptyset(n), e) = 1$. i.e. $\emptyset(n) \; and \; e$ are coprime, where e represents the public exponent.
- Compute an integer number d using the formula $d = e^{-1} mod \; \emptyset(n)$, where d represents the private exponent.

The number pair (n, e) which represents the modulus and the encryption or public exponent is referred to the public key while the number pair (n, d) which represents the modulus and the decryption or private exponent that should be kept secret is referred to the private key. $p, q \; and \; \emptyset(n)$ have to be kept secret because these parameters may be utilized to compute d (Sayyad et.al, 2017, Kaur & Singh, 2013).

ISSN: 2454-1907
DOI: 10.5281/zenodo.1341956

Encryption Process: The public key (n, e) is used to encrypt the plain message M at the transmitter to produce the cipher message C by using the formula:

$$C = M^e mod\ n \qquad (1)$$

Then, this ciphered or encrypted message C is transmitted to the intended receiver.

Decryption Process: The private key (n, d) is used to decrypt the ciphered message C at the receiver to produce the plain message M by using the formula (Khatri et.al, 2016):

$$M = C^d mod\ n \qquad (2)$$

3. The Proposed Methodology

The proposed methodology consists of two stages: 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. The block diagram of the presented methodology is shown in Figure 1.

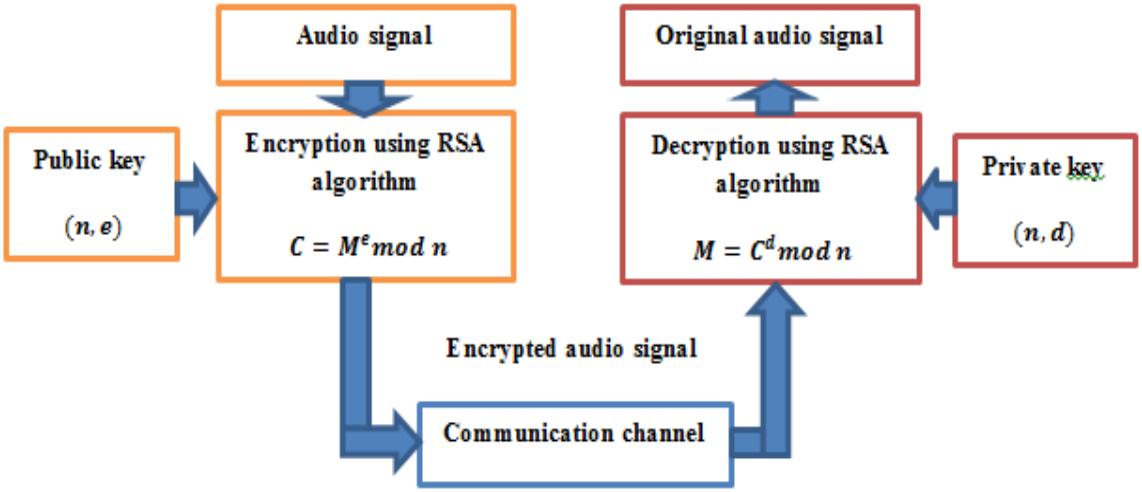


Figure 1: Block diagram of the presented methodology

4. Measurements 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 (Abdullah et.al, 2015):

ISSN: 2454-1907
DOI: 10.5281/zenodo.1341956

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:

$$CD = 10log_{10}\left[2\sum_{n=1}^{p}\{C_x(n) - C_y(n)\}^2\right]^{\frac{1}{2}} \qquad (3)$$

Where $C_x\ and\ C_y$ represent the cepstral vectors of the original and encrypted audio signals respectively (Al-saad & Hashim, 2013).

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

$$d_{lpc} = \ln\left(\frac{AVA^T}{BVB^T}\right) \qquad (4)$$

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 (Mahdi et.al, 2016).

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

$$SSSNR_i = 10\ log\frac{\sum_{n=1}^{N}|X_i(n)|}{\sum_{n=1}^{N}[|X_i(n)| - |Y_i(n)|]} \qquad (5)$$

Where $X_i\ and\ Y_i$ represent the DFT for the original and the encrypted audio signals respectively (Abdullah et.al, 2015).

5. Simulation Results and Discussion

The test results are presented and discussed in this part for evaluating the performance of the presented work. 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. 2 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. (2b) 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.

ISSN: 2454-1907
DOI: 10.5281/zenodo.1341956

(2c) is precisely evident as the original signal in Fig. 2a. MATLAB (R2013a) is used as a programming language to implement all the simulations in the presented cryptosystem.

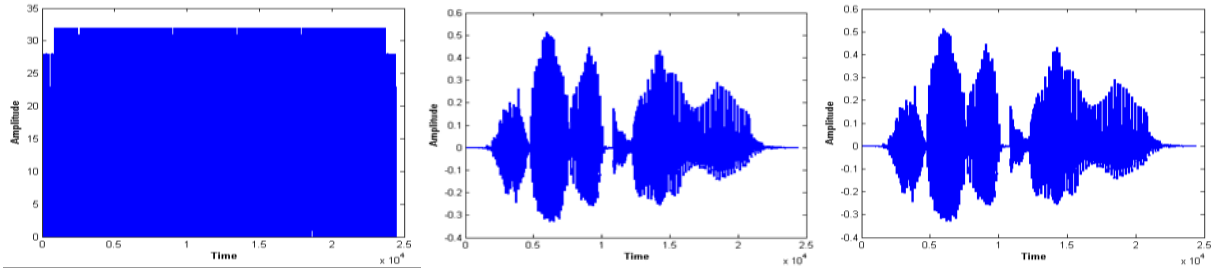


Figure 2 (a): Original audio signal, (b) Ciphered audio signal, (c) Deciphered audio signal

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 (Al Saad & Hato, 2014). 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 (c) 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 (Al-saad & Hashim, 2013). 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

ISSN: 2454-1907
DOI: 10.5281/zenodo.1341956

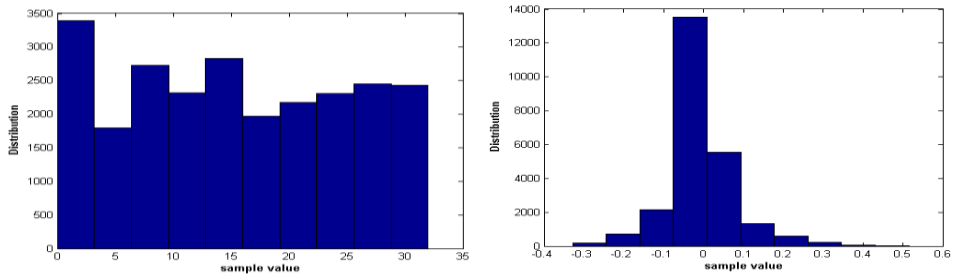
Histogram analysis: Histogram represents the distribution of information values in the system. The analysis of histogram is made by testing distribution of information in various fields. Encrypted information is represented as numbers in the histogram in the encryption practices. If the distributions of these numbers are close, then the performing of encryption process is good (Abd Elzaher et.al, 2016). The histograms of the original and encrypted audio signals are presented in Figs. 3a and 3b 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.

6. Conclusions

Accessibility, reliability, confidentially and secrecy of data 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.

Acknowledgements

I would like to thank the college of engineering, University of Diyala for their supporting and encouragement to write this paper.



(a) (b)

Figure 3 (a): Histogram of the original audio signal, (b) Histogram of the encrypted audio signal

References

[1] 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.

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

ISSN: 2454-1907
DOI: 10.5281/zenodo.1341956

[3] 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.
[4] 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.
[5] 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.
[6] 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.
[7] 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.
[8] 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.
[9] 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.
[10] 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.
[11] Al-saad, S. N. and Hashim, E. H. A Speech Scrambler Algorithm Based on chaotic system, Al-Mustansiriyah J. Sci., Vol. 24, No 5, 2013, 357-372.
[12] 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.
[13] 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.
[14] 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.

*Corresponding author.
E-mail address: sura.fahmy@ yahoo.com