International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 8 Aug 2021, pp: 638-644 www.ijaem.net ISSN: 2395-5252

Design Implementation of Security System for Audio Streaming

Hadeel M. EL Helou[1], Ihab ELAFF[2]
[1]Cyber Security department,USUKDAR University, Istanbul, Turkey
[2]Computer engineering department,USUKDAR University,Istanbul, Turkey
Corresponding Author: Hadeel M. EL Helou

Submitted: 01-08-2021 Revised: 10-08-2021 Accepted: 13-08-2021

ABSTRACT: This research paper is about securing audio streaming usingRSA encryption algorithm. To ensure maximum security level while streaming audio in real-time, some parameters are controlled includingencryption key size, bandwidth of communication channel, audio sampling rate and packet size.

The critical point which provides maximum security with real time sound streaming has been detected according to some selected setting.

KEYWORDS: Cryptography, RSA, Algorithm, encryption, decryption, Security.

I. INTRODUCTION

At this time in our life, we use the networks and the internet so much to communicate with others and we don't imagine our life without communication so the digital life is very important for us. So when communicate with others, this communication should be secure and safe.

On the other hand, digital life has a lot of risks if we don't protect ourselves from these risks and study and analyse these risks such as attacking, so we should use cryptography to securely communicate without any problems.

With the fast growth of communication technology, protection of audio from the hackers became a critical task for the technologist. So, there is always a need for a more secure and faster audio encryption technique [1]. Thisresearchfocuses on audio encryption for streaming audio in real-time. Over the years several encryption techniques have been implemented. But most of the techniques encrypt only text data, a very few techniques are proposed for multimedia data such as audio data. The techniques which encrypt text data can also be applied to audio data but have not achieved satisfactory results. Various encryption techniques are implemented for audio data. Some of which are inefficient to meet real time requirements and some are naive to meet the security requirements. Encryption of audio data is Difficult and complex process than the techniques used for text data.

II. AUDIO CRYPTOGRAPHIC ALGORITHMS

There are lots of encryption algorithms (encryption standards) in the field of cryptography. These are symmetric and asymmetric encryption algorithms. Some basic symmetric encryption algorithms are studied and detailed below:

DES is a block cipher. It encrypts the plaintext data in a block of 64 bits and produces 64-bit cipher text. The cipher key length is 56 bits and round key length is 48 bits [2].

AES algorithm can encrypt and decrypt the plaintext and cipher text of 128-bits. It uses a variable length key of size 128,192,256 bits [3].

3DES / Triple DEA is a symmetric-key block cipher which applies the DES cipher algorithm three times to each data block and encrypts and decrypts data using three 56-bit keys into 64-bit blocks [4].

Some basic asymmetric encryption algorithms are studied and detailed below:

RSA is a public-key cryptosystem that is widely used for secure data transmission. RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers [5].

ALAGAMMAL is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange[6].

Diffie-Hellman is a method of securely exchanging cryptographic keys over a public

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 8 Aug 2021, pp: 638-644 www.ijaem.net ISSN: 2395-5252

channel and was one of the first public-key protocols [7].

Playfair ismanual symmetric encryption technique and was the first literal diagram substitution cipher [8].

II. LECTURE REVIEW

Paper id	Name	Authors	Year	Methods	Results
[9]	ENCRYPTION AND DECRYPTION OF AUDIO SIGNAL BASED ON RSA ALGORITHM	Sura F. Yousef	2018	RSA	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
[10]	A SURVEY ON DIFFERENT ENCRYPTION TECHNIQUES FOR IMAGE, VIDEO, AUDIO AND DOCS	Arjun Poduval, Nandini Rai, Parvez Khan, Atish Sane	2021	AES, DES, RSA, Blowfish	The results show that RSA uses a lot time encryption and decryption compared to others. Blowfish spend the least amount of time, The results show that AES requires the highest number of bits to be encrypted and DES requires the least number of bits to be encrypted correctly
[11]	Performance Analysis of RSA and ElGamal for Audio Security	TIN ZAR NWE1 , SU WAI PHYO	2014	ElGamal, RSA	results, encryption and decryption time of RSA algorithm are significantly faster than ElGamal algorithm
[12]	Real-Time Encryption/Decryption of Audio Signal	M.I.Khalil	2016	RSA	The current paper applied and evaluated two different encryption/decryption algorithms to a real-time audio cryptography
[13]	A Study on Current Scenario of Audio Encryption	Rashmi A. Gandhi, Atul M. Gosai	2015	DES,3DES,AES, Blowfish, RC4	Design and implementation of a new algorithm for audio encryption based on above

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 8 Aug 2021, pp: 638-644 www.ijaem.net ISSN: 2395-5252

					parameters
[14]	Encrypt Audio File using Speech Audio File As a key	Najwan A Hassan, Farah Saad Al-Mukhtar and Esraa H Ali	2020	AES	The results for all tested audio files shows that the proposed algorithm for audio files is secured because of its, uniform histograms, large keys space, low correlation, and low PSNR, showed that the proposed algorithm for encryption of audio file is a very good choice in same time is a very good security to audio transmission
[15]	LITERATURE SURVEY ON RECENT AUDIO ENCRYPTION TECHNIQUES	Srividya L, Dr. P.N. Sudha	2016	DES, 3DES, RC2, RC4, RC6, Blowfish	Audio file is considered as a stream and encryption is dependent on both data and key. Brute force attack is impossible on encrypted audio file which are typically large. It is also resistive to statistical attacks. It is not suitable for low quality audio files as they will be prone to statistical attacks.

III. METHODS

Audio streaming is the practice of delivering real-time audio through a network connection. This type of data transmission requires certain protocols for handling the chronology of data packets or other transmission types, to provide the end-user with on-demand content.

In general, audio streaming utilizes a buffering system and a secure data stream platform to allow end users to listen to full audio files without interruption.

Much of today's audio streaming is done through sophisticated mobile devices made to handle higher amounts of data streaming, along with voice communications and more, with high-tech regional networking systems to support this data use. Equipped with ultra-modern microprocessors and new operating systems, today's class of mobile devices are some of the most elaborate and high-powered devices available on today's consumer market, and accommodating good audio and video streaming is a major engineering component for dominant device makers .

Audio sampling

Digital audio uses pulse-code modulation (PCM) and digital signals for sound reproduction. This includes analog-to-digital conversion (ADC), digital-to-analog conversion (DAC), storage, and transmission. In effect, the system commonly referred to as digital is in fact a discrete-time, discrete-level analog of a previous electrical analog. While modern systems can be quite subtle in their methods, the primary usefulness of a digital system is the ability to store, retrieve and transmit signals without any loss of quality.

Sampling rate

A commonly seen unit of sampling rate is Hz, which stands for Hertz and means "samples per second". As an example, 48 kHz is 48,000 samples per second.

When it is necessary to capture audio covering the entire 20–20,000 Hz range of human hearing,[14] such as when recording music or many types of acoustic events, audio waveforms are typically sampled at 44.1 kHz (CD), 48 kHz, 88.2 kHz, or 96 kHz[15]. The approximately double-rate requirement is a consequence of the Nyquist theorem. Sampling rates higher than

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 8 Aug 2021, pp: 638-644 www.ijaem.net ISSN: 2395-5252

about 50 kHz to 60 kHz cannot supply more usable information for human listeners. Early professional audio equipment manufacturers chose sampling rates in the region of 40 to 50 kHz for this reason.

The Audio Engineering Society recommends 48 kHz sampling rate for most applications but gives recognition to 44.1 kHz for Compact Disc (CD) and other consumer uses, 32 kHz for transmission-related applications, and 96 kHz for higher bandwidth or relaxed anti-aliasing filtering.

CD-DA, the standard audio CD, is said to have a data rate of 44.1 kHz/16, meaning that the audio data was sampled 44,100 times per second and with a bit depth of 16. CD-DA is also stereo, using a left and right channel, so the amount of audio data per second is double that of mono, where only a single channel is used.

For example, the bit rate of a CD-DA recording (44.1 kHz sampling rate, 16 bits per sample and two channels) can be calculated as follows:

Bit rate= sample rate*bit depth*channels
=44.100*16*2=1411.2 kbit/s

Real-time-audio meaning

The transmission of live voice. It implies that there is no delay at the receiving side, or at most, imperceptible delays. Although an audio broadcast that is streamed live may be considered real-time audio, there is an intentional, buffered delay at the receiving end. True real-time audio capability is required in a two-way conversation such as voice over IP (VoIP).

In my paper I used RSA algorithm to achieve audio streaming with real time and high security.

RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys Public Key and Private Key. As the name describes, the Public Key is given to everyone and the Private Key is kept private.

The RSA Algorithm

The RSA algorithm works by utilizing the prime factorization to achieve asymmetric encryption. Fundamentally, RSA cryptography relies on the difficulty of prime factorization as its security method. Using a very simplified example with limited math described, the RSA algorithm contains 4 steps.

Key Generation – During this step, a user can employ a random number generator or simply pick 2 very large prime numbers (called p and q). These numbers must be kept secret. Compute n=pq where "n" is the modulus for both public and private keys and its length is known as the key length. Make "n" public. For key sizes equal to or larger than 1024 bits, there is no efficient method for solving this algorithm (factoring the very large number "n") efficiently. Even the largest supercomputer in the world would take thousands of years to solve it. This is known as the RSA problem, and if solved, would compromise all RSA-based cryptosystems.
Key Distribution – Bob wants to send Alice secret information so the following steps occur.
Bob must know Alice's public key to encrypt the message.
Alice must know her private key to decrypt the message.
For Bob to be able to send his encrypted message, Alice send her public key to Bob.
Alice never distributes her private key.
Encryption – After Bob obtains Alice's public key, he can send a message (M) to Alice. First, he turns (M) (at this point a plaintext message) into an integer (m) through using a agreed upon padding scheme. He then computes the cipher text using Alice's public key and transmits (c) to Alice.
Decryption – Alice can recover the message (m) from the cipher text (c) by using her private key. She can then recover the original message (M) by reversing the padding scheme from (m).

Additionally, RSA encryption allows for digitally signing messages, which is paramount to crypto currencies and is a key component of Bit coin's UTXO transaction model. Alice can digitally sign a message to Bob to verify that she sent it (by validating that her private key was used) through producing a hash value of the message and attaching it to the message. This value can be verified by Bob who uses the same hash algorithm in conjunction with Alice's public key and compares the resulting hash value with the message's actual hash value.

I programmed RSA code by using TCL language and this language has a lot of properties easy to design the security networks also Rapid development in many cases you can implement applications 5-10x faster with Tcl than with other languages, especially if the application involves GUIs, string-handling, or integration.

TCLis an ideal language to use for automated hardware and software testing, and it may well be the dominant language used for this

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 8 Aug 2021, pp: 638-644 www.ijaem.net ISSN: 2395-5252

purpose. With TCLyou can easily connect to testing hardware or internal APIs of an application, invoke test functions, check the results, and report errors.
it has a rich and powerful event-driven programming model that makes network programming easy, allowing clients and servers to be created with just a few lines of code.
Also it's easily include Tcl as an embedded scripting language in an application, or make existing C, C++, or Java code look like it was built right into TCL.

The main idea in my thesis improve the security with real time when I communicate with any one by voice in any application by using RSA algorithm and develop the code and made list of prime numbers with different length of bits range start from [4-32] bits for these numbers and choose the sample per packet 250 bytes and the bitrate 1Mb/s means one million bits per second and add send plain data randomly
And add encryption data and decryption data and add time for three parts

Encryption time (T2-T1):

This time after sender obtains receiver public key, he can send a message (M) to receiver. First, the sender turns (M) (at this point a plaintext message) into an integer (m) through using a agreed upon padding scheme. He then computes the cipher text using the receiver's public key and transmits (c) to the receiver.

IV. RESULTS

From the curve and the table and the time for every two prime numbers with different size the

Transfer time:

The time it takes to transmit or move data from one place to another in the first I calculated it by using this formula:bytes_per_Packet =byte_per_sample* sample_per_Packet

Then Trans _Time =bytes_per_Packet * 10.0 / BaudRate]

Decryption time (T4-T3):

This time gets it when the receiver can recover the message (m) from the cipher text (c) by using her private key. The receiver can then recover the original message (M) by reversing the padding scheme from (m).

Then calculate the transaction time (encryption _time & transfer _time &decryptiontime) from all this operation to achieve my goal which point give us real time and high security in communicate audio

I noticed after testing the Real time with a quarter of a second delay is acceptable when packet per sample 250 bytes and by using straight equation at time 1000 ms and noticed what the length of bits for n which produced it from multiplication two prime number

To achieve maximum security withreal time in communicating voice.

critical point appears when the time equals 1000ms and find out the intersection between the x-axis representing N and the y-axis representing time.
By using the straight equation:

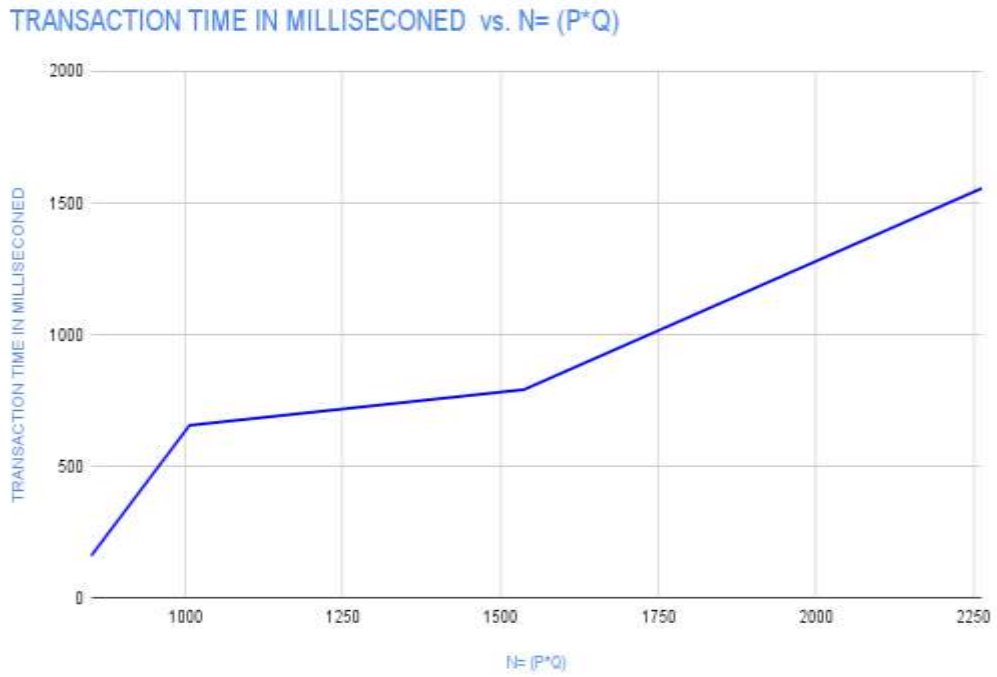
M=y1-y0/x1-x0 = 1556.544153706 - 792.15606 / 2263 – 1537 = 764.388/726=1.052876033057851

So when N=726 the length of bits equals 10 bits and this number produced from multiplication two prime numbers and at this point achieved the highest security and real time with a quarter of second delay for audio streaming .

SL.NO	N= (P*Q)	TRANSACTION TIME IN MILLISECONED
1	851	160.72806
2	1007	656.72406
3	1537	792.15606
4	2263	1556.54406
5	3127	3308.28006

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 8 Aug 2021, pp: 638-644 www.ijaem.net ISSN: 2395-5252

6	5723	9423.41206



V. CONCLUSION

This paper studied how we can improve audio streaming security and make balance between the security and real time streaming using RSA algorithm and control in parameter for prime numbers to show where the critical Point achieved and what are the N(p*q) values

Produce the highest security and get the acceptance real time with quarter of second delay so from this operation we can protect thecommunication voice from any attacker.

In the Future work I recommend other researchers to test and practice audio streaming security in other algorithms like AES and DES and choose other bytes for sample per packet and detect another critical point to achieve highest security and real time in communication operation also practice this idea in other media such as video.

REFERENCES

[1]. Rashmi A. Gandhi, Atul M. Gosai," A Study on Current Scenario of Audio Encryption", International Journal of Computer Applications (0975 – 8887) , April 2015.

[2]. Thida Soe, Soe Soe Mon, Khin Aye Thu, Performance Analysis of Data Encryption Standard (DES), Faculty of computer systems and Technology, University of Computer Studies, Hinthada, Myanmar, August 2019

[3]. AkoMuhamad Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data", Department of Applied Mathematics & Computer Science, June 16, 2017

[4]. NouraAleisa, "A Comparison of the 3DES and AES Encryption Standards", International Journal of Security and Its Applications, No.7 (2015).

[5]. ShireenNisha, Mohammed Farik, RSA Public Key Cryptography Algorithm , INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 6, ISSUE 07, JULY 2017

[6]. Mike Rosulek (2008-12-13). "Elgamal encryption scheme". University of Illinois at Urbana-Champaign, 2016-07-22.

[7]. ManojRanjanMishra1, Jayaprakash Kar2, "A STUDY ON DIFFIE-HELLMAN KEY EXCHANGE PROTOCOLS", 2Department of Computer Science and Engineering, No. 2 2017.

[8]. Salman A. Khan, Design and Analysis of Play fair Ciphers with Different Matrix Sizes, Computer Engineering Department,

College of Information Technology, Sept. 2015.

[9]. Sura F. Yousif, ENCRYPTION AND DECRYPTION OF AUDIO SIGNAL BASED ON RSA ALGORITHM, Department of Chemical Engineering, College of Engineering, University of Diyala, July 2018.

[10]. Arjun Poduval, Nandini Rai, Parvez Khan, Atish Sane, A SURVEY ON DIFFERENT ENCRYPTION TECHNIQUES FOR IMAGE, VIDEO, AUDIO AND DOCS, International Journal of Engineering Applied Sciences and Technology, 2021.

[11]. TIN ZAR NWE1,SU WAIPHYO2, Performa nce Analysis of RSA and Elgamal for Audio Security, 2Dept of IT, June2014.

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

[13]. Rashmi A. Gandhi, Atul M. Gosai, Ph.D., A Study on Current Scenario of Audio Encryption, International Journal of Computer Applications ,7, April 2015.

[14]. Najwan A Hassan, Farah Saad Al-Mukhtar and Esraa H Ali, Encrypt Audio File using Speech Audio File As a key, Baghdad, Iraq, AL-NAHRIAN UNIVERSITY, DEPARTMENT OF COMPUTER SCIENCES, 2020.

[15]. Srividya L, Dr. P.N. Sudha, LITERATURE SURVEY ON RECENT AUDIO ENCRYPTION TECHNIQUES, International Journal of Electronics and Communication Engineering and Technology, November-December 2016.

[16]. Self, Douglas (2012). Audio Engineering Explained. Taylor & Francis US. pp. 200, 446. ISBN 978-0240812731.