ENCRYPTION USING RANDOM KEYS SEQUENCE – A SCHEME FOR SECURED AUDIO DATA TRANSMISSION

ENCRYPTION USING RANDOM KEYS SEQUENCE – A SCHEME FOR SECURED AUDIO DATA TRANSMISSION

By: Hiba H. Mistareehi

Advisor: Dr. Bassam Harb

Field of specialization - Wireless communication

July 17, 2012

ENCRYPTION USING RANDOM KEYS SEQUENCE – A SCHEME FOR SECURED AUDIO DATA TRANSMISSION

by

Hiba Hekmat Mohammed Mistareehi

B.Sc. Communication Engineering, Yarmouk University, 2012

A Thesis submitted in partial fulfillment of the requirements for the degree of M.Sc. in Communication Engineering Department, Yarmouk University, Irbid, Jordan

Approved by:

Dr. Bassam Harb.........Bassam Harb.................. **Chairman**

Prof. Adnan Al-Smadi.....Adnan....Al-Smadi......... **Member**

Prof. Ahmad Al-Ajlouni................................... **Member**

July 17, 2012

DEDICATION

This thesis is dedicated to my father who has supported me all the way to complete my study. Also, this thesis is dedicated to Dr. Bassam Harb who has been a great source of information.

Finally, this thesis is dedicated to my husband who encouraged and supported me in completing this thesis and took the care of my daughters Jodi & Mariah.

ACKNOWELEDGEMENTS

I want to give my great appreciation and thanks to: Dr. Bassam Harb, Members of the discussion, & all the members of the Communication Engineering Department for their helpful comments, explanations, and suggestions in the thesis stages.

Thanks to my Family who encouraged me to study and succeed in the master program.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

LFSR:	Linear Feedback Shift Registers.
AES:	Advanced Encryption System.
PRNG:	Pseudorandom Number Generator
ASIO:	Audio Stream Input/Output.
PCM:	Pulse Code Modulation.
RNGA:	Random Number Generator Algorithm.
DES:	Data Encryption Standard.
LPC :	Linear Predictive Coding

LIST OF FIGURES

Figure **Page**

LIST OF TABLES

Table **Page**

Abstract

Mistareehi, Hiba Hikmet. Encryption Using Random Keys Sequence – a Scheme for Secured Audio Data Transmission. Master thesis in Yarmouk University.2012 (advisor: Dr. Bassam Harb)

The aim of this thesis is to investigate a method for a secured call that provides maximum security with low complexity. A voice encryption and decryption schemes based on a random key generator are proposed, which includes hardware and software design. The hardware consists of a mobile and a computer. A voice signal is provided by a laptop audio output, connected to the input of a telephone. At the other terminal, the audio signal (encrypted speech signal) received was loaded to a laptop - again using a connector between laptop audio ports and the input of the telephone. A voice encryption/decryption system is programmed using Matlab algorithm as a software application; computer simulations indicate that the restored signal (the decrypted speech signal) has high quality measurements.

In this thesis, the heart of the encryption process is a sequence generator algorithm; the proposed method uses a simple key generation method of random number generation. These keys applied on each block of data voice message (rotation and XOR operation). The result of this process is encrypted voice message. Two schemes for generating a random sequence of encryption keys are presented. Random Key Sequence with Modified Fixed Coefficients and Random Key Sequence with Modified Dynamic Coefficients.

Keywords: Voice encryption/decryption system, Pseudorandom number generator, Linear feedback shift registers, Random key sequence with fixed coefficients, Random key sequence with dynamic coefficients.

CHAPTER ONE: INTRODUCTION

1.1 Introduction

The idea of encrypting messages is probably old as the first secret message sent between humans. In fact, most of the encryption systems were meant to encrypt text messages; the development of encryption systems for voice messages is considered a lot more difficult.

Encryption has been used by militaries (the first approaches for a voice encryption system were invented in the 1920, between World War I and World War II). The governments had to facilitate secure communication; encryption is now commonly used in protecting information within many kinds of civilian systems [1].

Encryption can be used to hide information from unauthorized individuals, either in transit or in storage. For example, the Computer Security Institute reported that in 2008, 71% of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage [2]. Encryption can be used to protect data "at rest", such as files on computers and storage devices (e.g. USB flash drives). In recent years there have been numerous reports of confidential data such as customers' personal records being exposed through loss or theft of laptops or backup drives. Encrypting such files at rest helps protect them [3]. Also it can be used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. There have been numerous reports of data in transit being intercepted in recent years. Data encryption before transferring it also helps to secure data because it is often difficult to physically secure all access to networks [4].

One of the purposes of encryption is to guarantee the confidentiality of transmitted messages. Digital transmission is always much more efficient than analog transmission (in digital encryption it does not matter what kind of signal is encrypted), and it is much easier for digital encryption techniques to achieve much higher degree of security. Any pseudo-random bit stream along with Ex-OR provides a cryptosystem, split the message file into different message blocks, then generate the random key by using random number generator algorithm (RNGA) for each and every message block. After encrypting all the message blocks, shuffle it using another sequence of random numbers. For decryption, we choose the same random numbers and we do the reverse process to get the original message file [5].

Speech is probably the most fundamental form of communication available to us, and our society has become highly dependent on our modern, fast and accurate means of transmitting spoken messages. Usually the main aim of communicators is merely to transmit a message as quickly, cheaply and accurately as possible. There are, however, a number of situations where the information is confidential and where an interceptor might be able to benefit from the knowledge gained by monitoring the information circuit. In such situations, the communicators must take steps to conceal and protect the content of their spoken message. Of course, the amount of protection will vary. On occasions, it is sufficient to prevent the casual listener from understanding the message, but there are other times when it is crucial that even a determined interceptor must not be able to deduce its content.

Voice encryption systems are used to guarantee end-to-end security for speech in communication systems such as telephone. Fig.1 illustrates transmitted data via communication system, where these systems employ data security techniques.

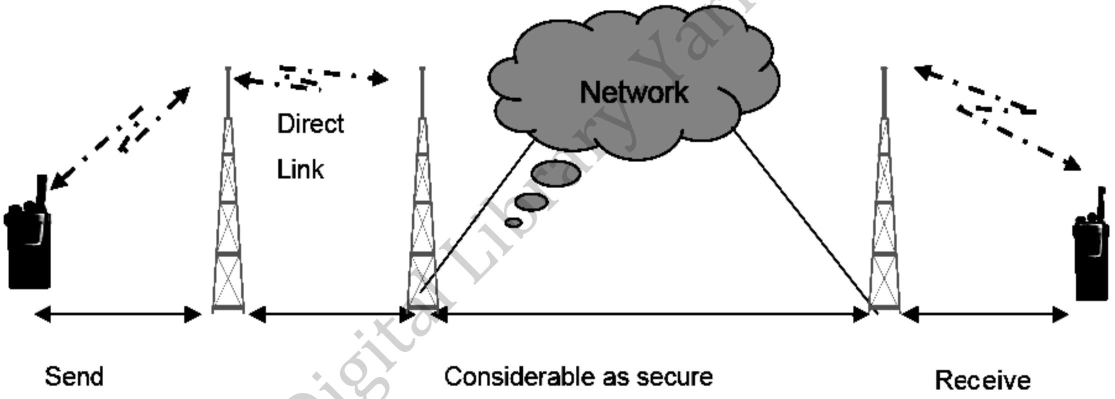


Fig. 1: Secure communication system [1].

1.2 The Human Voice

For the development and understanding of a Voice Scrambling System, it is essential to know some basic parameters of the voice itself. The human voice is simply a sound or audio signal generated by a human to communicate with others. Therefore, a person uses his vocal folds to modulate the air stream, coming from the lungs, into vibrations which make - with the rest of the human sound forming system (like: the mouth hole, the tongue etc) - a sound.

Hence the difference of the anatomy of each human, the voice of two people never sounds the same. The biggest difference is obviously recognized between the voices of men, women and children. This is due to the different fundamental frequencies these three groups usually have. The male vocal cords fundamental frequency are between 85 and 155 Hz, and for woman are between 165 and 250 Hz. Kids have even smaller cords; their fundamental frequency is often about 440 Hz (Babies up to 500Hz) [6].

The human speech consists out of vowels and consonants which both are important for understanding. Vowels are voiced sounds where the vocal cords vibrate while they are produced. Those ones have a very clear, narrow and harmonic spectrum that is at lower frequencies. Some consonants are unvoiced or voiceless sounds which have a wider and higher spectrum as fig. 2 shows the spectrogram of vowels and consonants [1].

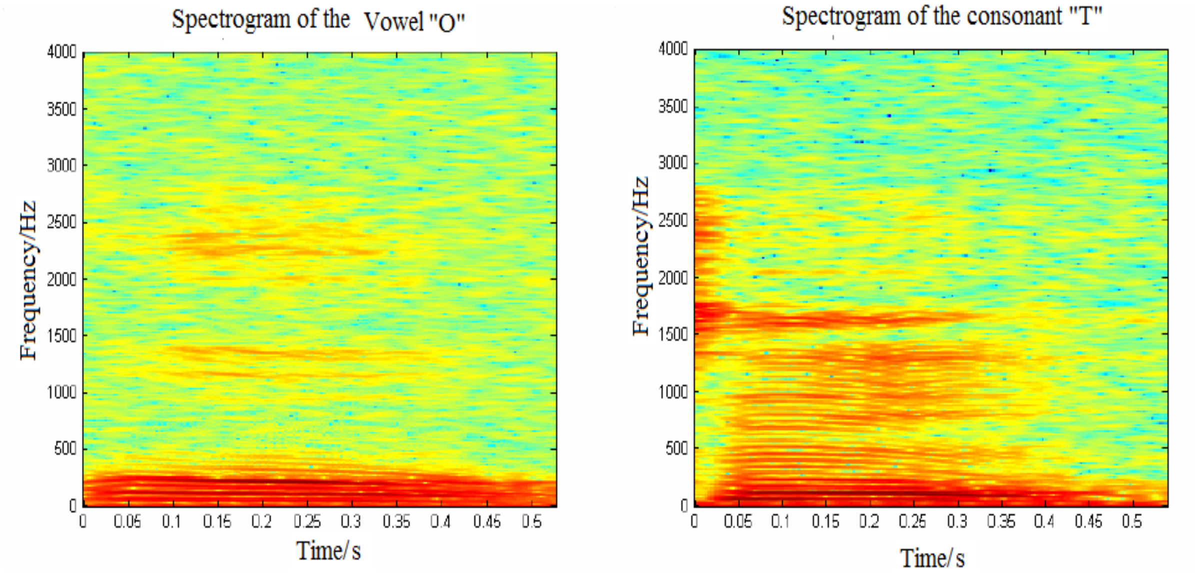


Fig.2: Spectrogram of vowels and consonants [1].

1.3 Applications of Speech Encryption

The issue of the security and privacy of mobile communications affects private individuals, businesses, government agencies, and military personnel. The importance of voice encryption is that everyone may have the ability to [7]:

a) Carry on a personal conversation without fear of being overhead.

b) Make a telephone booking with their Visa card without worrying about someone intercepting their number and address and making fraudulent transactions.

c) Carry out confidential business negotiations over the phone without their competitors recording the details.

d) Plan a robbery over the phone without being arrested.

e) Make an anonymous bomb-warning without getting caught.

1.4 Methods of Voice Security

A scrambler is a device that inverts signals or otherwise encodes a message at the transmitter to make the message unintelligible at a receiver not equipped with the appropriate descrambling device. This data message can be encoded in analog or in digital domain. Whereas encryption usually refers to operations carried out in the digital domain, scrambling usually refers to operations carried out in the analog domain [8].

The developed system is clearly digital system, where its operations are more of an encryption than an analog scrambling.

1.4.1 Scrambling

Scrambling usually refers to operations carried out in the analog domain. Analog voice-scrambling methods typically involve splitting the voice frequency spectrum into a number of sections by means of a filter bank and then shifting or reversing the sections for transmission in a manner determined by switch settings similar to those of a combination lock; the reverse process takes place at the receiver end.

1.4.2 Encryption

Encryption often refers to digital technologies, in fact, if you hear about data security and speech information hiding with modern technologies; you barely talk about digital encryption. Where digital encryption can be seen as a much stronger method of protecting speech communications than analog scrambling, because in digital encryption it does not matter what kind of signal is encrypted.

1.5 Implications of Research

Based on previous work in audio encryption, there are many different methods used for voice encryption. Each method is different from others in complexity, cost, and implementation. In this thesis, we proposed a method which will reduce complexity of the encryption process and achieve a higher level of security.

1.6 The Objective of Thesis

The aim of this thesis is to achieve a voice encryption system with very basic digital signal processing algorithms, where the original speech signal is digitized into a series of bits. In this thesis, the heart of the encryption process is a sequence generator algorithm; the proposed method uses simple keys generation method of random number generation. These keys applied on each block of data voice message (rotation and XOR operation). The result of this process is encrypted voice message, thus reduce the complexity of the encryption process. In order to achieve high level of security, we presented two schemes for generating a random sequence of encryption keys (Random Key Sequence with Modified Fixed Coefficients, and Random Key Sequence with Modified Dynamic Coefficients).

1.7 Thesis Organization

The thesis is organized as follows: A brief introduction and related work is presented in Chapters 1and 2. Chapter 3, describes the Encryption Process. Simulation and results are discussed in Chapter 4. Finally, conclusion and suggested future work are in Chapter 5.

Chapter Two: Related Work

In this master thesis, a voice encryption system with high level of security is desired. The idea is based on a previous work in audio encryption. In [1], Markus Albert Brandau gave an analysis of voice encryption, where its application uses a frequency scrambling technique on an audio signal taken from the computer microphone input and plays it scrambled back to the speakers, or other way around to descramble the signal. The basic idea is to use a frequency channel decomposition through digital signal filtering and down-sampling. Reassembling these sub-bands in a different order, a scrambled voice signal is the result.

In [9], an encryption scheme using a random key generator with memory is presented, this paper proposed a comparative analysis of three different schemes for generating a random sequence of encryption keys. Random Key Sequence with Modified Fixed Coefficients, Random Key Sequence with Modified Dynamic Coefficients, and Multistage Random Key Generation with Feedback. where for Random Key Sequence with Modified Modified Fixed Coefficients the random number sequence can be inferred provided generator coefficients a, and b are known. Therefore, the exhaustive attack would have to find two keys in order to solve the linear equation for a, and b, see appendix-c. Unlike the fixed coefficient scheme where any two key breaks were sufficient to compromise the system, but for Random Key Sequence with Modified Modified Dynamic Coefficients the random number generation coefficients a, and b are continuously modified, see appendix-c. Therefore, the attacker would have to exhaustively search the coefficient spaces. Both the coefficients as well as the constant K must now be determined for inferring the random sequence. A Multistage Random Key Generation with Feedback scheme is an extension of the above idea where the parameter K(N) is continuously changing, this K (N) will be used for generating the random sequences a (N) , and b(N) in the computation of the random key generator for R(N) , see appendix-c. This system is considerably more secure than the previous two schemes. In order to approve this theory, an information-theoretic entropy measured is used to measure the amount of information needed to decipher the ciphertext, where the larger the entropy of the ciphertext is the harder it will be to break it. A multistage random key generation is the best scheme. In [10], Min-sung Koh and Esteban Rodriguez-Marek Proposed method used for voice encryption, based on the Sylvester equation. The encryptor first converts a data vector P into a raw data matrix P using serial-to-parallel converter block, V/M. Matrix P is then multiplied both by matrices F and A, and its result added to form the encrypted output matrix, –C (Sylvester equation). Matrices F and A are both the Hankel matrix S which is an arbitrary vector signal such as random noise. The decrypted information at the receiver is obtained by solving the Sylvester equation. Three theorems are presented that satisfy the Sylvester equation and the QR factorization as valid methods for encryption. The results display excellent performance.

In [11], Hongyu Lei, Yu Zhao, Yuewei Dai, and Zhiquan Wang Proposed a secure voice communication system based on DSP, Firstly, analog voice signal is transformed to PCM voice codes by the CODEC(Coder and Decoder). Then the PCM codes are transferred to DSP and encrypted by DSP. Finally, the encoded data is transmitted to the other side by the ASE (Asynchronous Communications Element). On the other side, the received data is decoded to PCM codes by DSP, and then the PCM codes are transformed by the CODEC to the analog voice signal. Because the transferred data is encrypted, the third party cannot decrypt the data without correct keys. Thus, secure voice communication is done.

In [12], Yucun Yang, Suili Feng, Wu Ye, and Xinsheng Ji Proposed a scheme for encrypted speech transmitting on GSM voice channel. This scheme offers a good method for encrypted speech accessing mobile voice channel by using a proposed special modem called smodem based on Linear Predictive Coding (LPC) technique, Firstly, in transmitting MS, natural human voice is converted by A/D module to PCM as input for GSM vocoder, then it is compressed to a rate of air link well below by a speech codec, as there is a large overhead for the demands of error correction. Then the output bit stream of speech codec is encrypted, modulated to a speech like signal that possesses speech characteristics, and then fed into MS vocoder. MS vocoder encodes it and sends it over the air link as if it were natural human voice. At the receiver, MS module receives the signal from air link, decodes it to a regenerated speech-like signal, and feeds it to the modem in turn. Then the regenerated speech-like signal is demodulated, corrected errors, decrypted, and decoded by the speech codec to recover the voice. In [13], Atef Mermoul and Adel Belouchrani gave a new encryption method for speech encryption. The proposed approach is based on the subspace concept together with the use of nonlinear functions and key signals. An interesting feature of the proposed technique is that only a part of the secret key parameters used during encryption is necessary for decryption. Furthermore, if no plain-text is fed to the encryption algorithm, the latter will provide no contents.

In [14], E. Mosa, Nagy.W .Messiha, and O. Zahran presented an analog speech cryptosystem based on permutation and substitution of speech segments. Permutations processes and substitutions masks are variables which changed with changing the secret key. In the beginning, the first key is applied to the first column of the first matrix from top to bottom. If key bit equal (1) the whole row will shifted circularly to right by offset equal to row number minus one (e.g. row number 14 will be shifted by 13) and if key bit equal (0) the row will remain intact. Second step is applying the same key to the first row of block from left to right. If key bit equal (1) the whole column will shifted circularly to down by offset equal the column number minus one and if key bit equal (0) the column will remain intact. All previous steps are inversed and applied to encrypted signal so divide the continuous signal to fixed size segments that reshaped to blocks. The blocks are inverse permutated and substituted then rearranged again to form the original signal. Computer simulations indicate that the restored signal has good quality measurements. In [15], Gang Chen, and Bo Han proposed an audio scrambling degree measure based on multi-scale average short term entropy. In this scheme, an audio sequence is consisted of amplitude set in different timing points. If scrambling transformation can change the short term property and also the transition properties between neighborhood terms, the original audio information will be hided and the new sequence is not understandable from human auditory system. Thereby, from the scrambling degree measuring based on average short term entropy, randomly selecting consecutive sample points from a given-length audio analysis frame, then compute its short term entropy and then its corresponding mean value. With the increasing length for an analysis frame, the average short term entropy increases as well and finally keeps stable around global entropy for whole audio sequence. During the process, for an updated audio with more chaos, its average short term entropy reaches a big value in an earlier stage and then keeps in this level.

In [16], H. Peyvandi, and S._J. Park proposed a secure scheme for underwater telecommunication networks. In this scheme, the input voice is transformed to the bit stream using a low bit rate encoder. Then, the whole bits are mapped to the predefined symbols, which have been originally designed using hi-fi speech records. Symbols are stored in a lookup table in the both sides of channel. At transmitter side, the prepared signal is windowed, filtered and shaped to transfer over underwater link. The overall bit error rates are as low as that have not any significant effect on quality of speech while, on the other hand, the output noises are quite unintelligible for intruders who try to access to the conversations through the channel of telecommunication network. Produced noises are signals including random scrambled speech-based symbols in which make no any sense to the listener.

In this thesis, a voice encryption and decryption schemes based on a random key generator are proposed. The input voice signal is digitized into a series of bits; the proposed method uses a simple key generation method of random number generation. These keys applied on each block of data voice message (rotation and XOR operation), the result of this process is encrypted voice message. The main feature of the encryption/decryption program implementation is the generation of the encryption key. A symmetric encryption key is used for this application, which means the same key is shared for both encryption and decryption. The technique of generating the key uses two methods: modified fixed random number generation and modified dynamic random number generation. It was shown through experimental results, that the principle of the proposed scheme is implemented with little complex hardware. Computer simulations indicate that the restored signal has good quality measurements.

Chapter Three: Mathematical representation of the proposed method

3.1 Introduction

In cryptography, encryption is the process of encoding the contents of the plaintext in such a way that its contents cannot be deciphered or read by outsiders except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as ciphertext). In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g. software for encryption can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted).

3.2 The voice encryption/decryption system

3.2.1 Encryption

The tasks of encryption require in principle the availability of a long random sequence of numbers. The random sequence must be many millions or over billions of bits in length and the same sequence must be known and synchronized at the transmitter and receiver. Consequently, in most applications, a shorter binary sequence is repeatedly modified and reused in both the transmitter and receiver according to a fixed procedure so as to generate a long sequence. The long sequence so generated is then called a pseudorandom sequence and the short sequence from which it is generated is called the key sequence [17].

Fig.3 and Fig.4 illustrate a process for conversion of data into a form, called a ciphertext that cannot be easily understood by unauthorized people, where, the sender encodes the plaintext into a ciphertext (encrypted message) with the aid of encryption and sends it to the receiver.

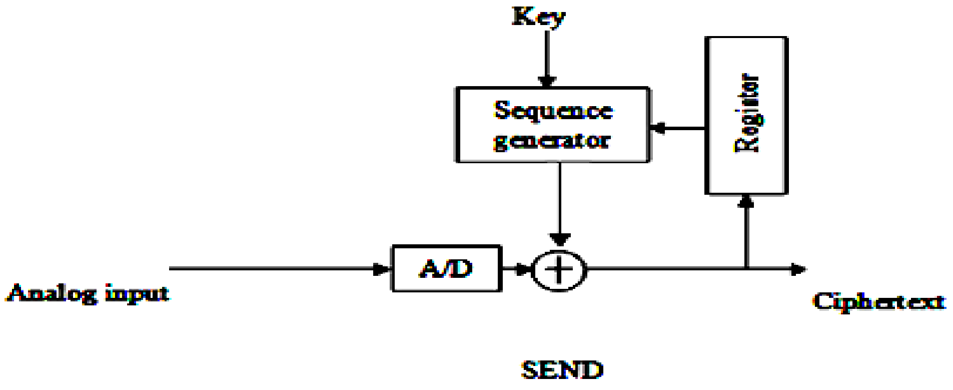


Fig.3: Typical cipher feedback system, transmitter side [18].

The basic idea of a cipher feedback system is shown in Fig.4. The ciphertext is continuously providing one of the inputs to the sequence generator and, consequently, affecting the resulting encipherment.

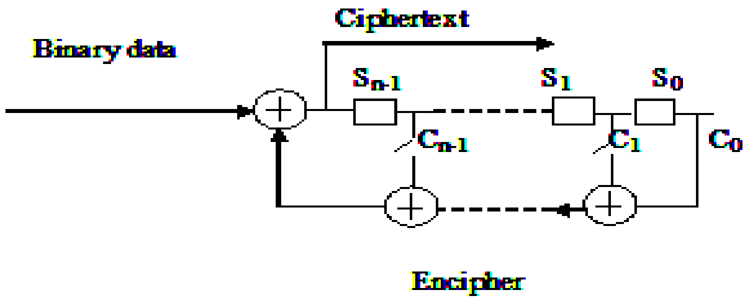


Fig. 4: Cipher system using a linear shift register, transmitter side [18].

The process for conversion data to ciphertext is as follow: Suppose we have such a system and that our key determines the feedback coefficients c_0, c_1... c_{n-1}. If we let the binary message be $m_{0,}$ $m_{1,}$ m_2…m_{n-1} and the corresponding ciphertext bits be e_0,e_1,e_2…e_{n-1} then, if the initial contents of the register are s_0, s_1, s_2… s_{n-1}, when m_0 is fed in, the output e_0 will be given by[18]:

$$e_o = m_0 + \sum_{i=0}^{n-1} c_i\, s_i$$

where, of course, all additions are modulo 2. But now s_o is no longer in the register. In fact, for $1 \leq i \leq n-1$, s_i is now in stage s_{i-1} and e_0 is the new entry in s_{n-1}. Thus, when m_1 is input we get [18]:

$$e_1 = m_1 + \sum_{i=0}^{n-2} c_i\, s_{i+1} + c_{n-1}\, e_0$$

Thus the preceding ciphertext is already affecting the encryption of the second message bit. As the process continues the initial entries in the register will eventually 'disappear' from the register and, after n outputs, each ciphertext bit e_j will depend only on m_j and n previous ciphertext bits. In general, for $h \geq 0$, the enciphering equation is [18]:

$$e_{n+h} = m_{n+h} + \sum_{i=0}^{n-1} c_i\, e_{i+h} \qquad (1)$$

3.2.2 Decryption

The receiver needs to convert the ciphertext back to the plaintext to understand the meaning of the message. Fig.5 and Fig.6 illustrate a process for conversion of the received message to be readable again.

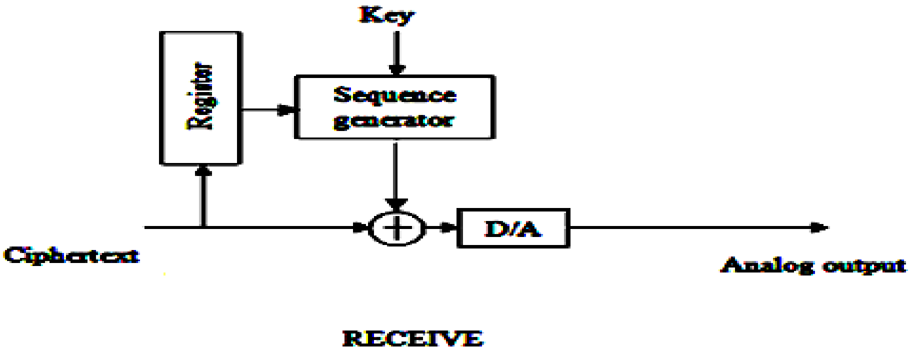


Fig.5: Typical cipher feedback system, receiver side [18].

The basic idea of a cipher feedback system is shown in Fig.6. The ciphertext is continuously providing one of the inputs to the sequence generator and, consequently, affecting the resulting decipherment.

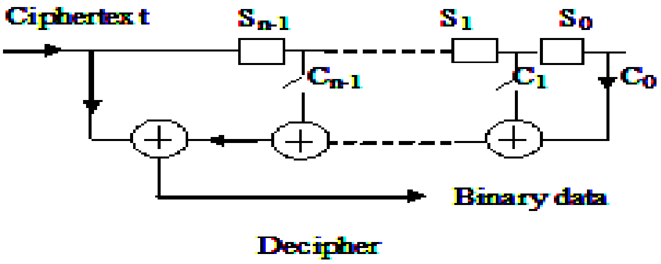


Fig. 6: Cipher system using a linear shift register, receiver side [18].

In order to perform deciphering process, we must assume that the receiver has the correct key, and hence the same feedback coefficients, as the transmitter's, we let s_0*, s_1*... s_{n-1}* denote the initial entries in the receiver's register. If we denote the receiver's input by e_0*, e_1*, e_2*,... e_{n-1}* then, of course, for an error-free channel we will have $e_j^* = e_j$ for all j. if we denote the receiver's output by m_0*, m_1*, m_2*,... m_{n-1}* then, clearly, for correct decipherment we want $m_j^* = m_j$ for all j.

In precisely the same way as the transmitter, at each of the first n inputs one of the initial entries disappears from the register and does not affect the later decipherment. Thus, apart from the first n bits, each m_j* depends only on e_j* and the previous n received bits. More precisely we have [18].

$$m^*_{n+h} = e^*_{n+h} + \sum_{i=0}^{n-1} c_i e^*_{i+h} \qquad \text{for all} \quad h \geq 0 \qquad (2)$$

Thus, if $e_j^* = e_j$ for all i, i.e., if there are no errors during the transmission, from Eq. (1) we get [18]:

$$m^*_{n+h} = e_{n+h} + \sum_{i=0}^{n-1} ci\ e_{i+h} = m_{n+h}$$

In other words the ciphertext is deciphered correctly except that, unless the registers at the transmitter and receiver ends have the same initial contents; the first n bits of the message are lost [18].

3.3 Project implementation

Based on the theory and techniques mentioned earlier and on the Matlab code of cipher system using a linear shift register a voice encryption was programmed. This chapter describes the actual implementation of the system and gives focus on the most important parts.

3.3.1 Overview

Obviously the theory of encryption has to be simply converted into a programming language, but to achieve a voice encryption, it is also necessary to obtain the audio data directly from the hardware respectively from the operation system. Using one of the above mentioned software, Matlab makes this easier.

The proposed method is an efficient, secured way to transmit speech or audio data, hardware system combined with proper software. A block diagram of the proposed system is shown in Fig. 7. Firstly, analog voice signal (clear speech) is recorded to the computer and then Matlab algorithm transforms it to digital data (bits) in which the magnitude of the analog signal is sampled regularly at uniform intervals, with each sample being quantized to the nearest value within a range of digital steps, then the encryption process can begin. After that bits reassembling and the result is encrypted audio signal.

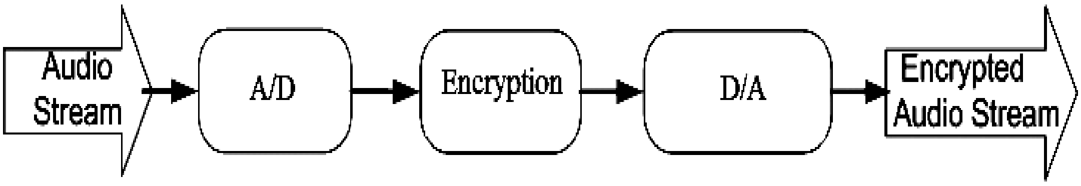
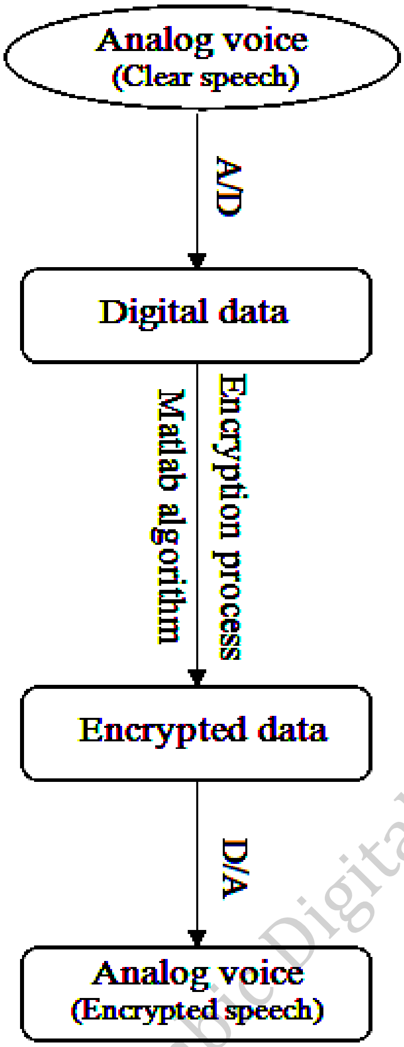


Fig.7: Construction of the proposed system

Then the encrypted data is ready to be sent to the intended receiver. Because the transferred data is encrypted, the third party cannot decrypt the data without correct keys. Thus, secured voice communication is achieved. At receiver side, analog voice (encrypted speech) is converted to digital data, in order to perform decryption process using a Matlab algorithm. Then the decrypted data signal is transformed to analog voice (clear speech). Basic system for transmitting and receiving secured voice signal is shown in Fig. 8, and Fig.9.



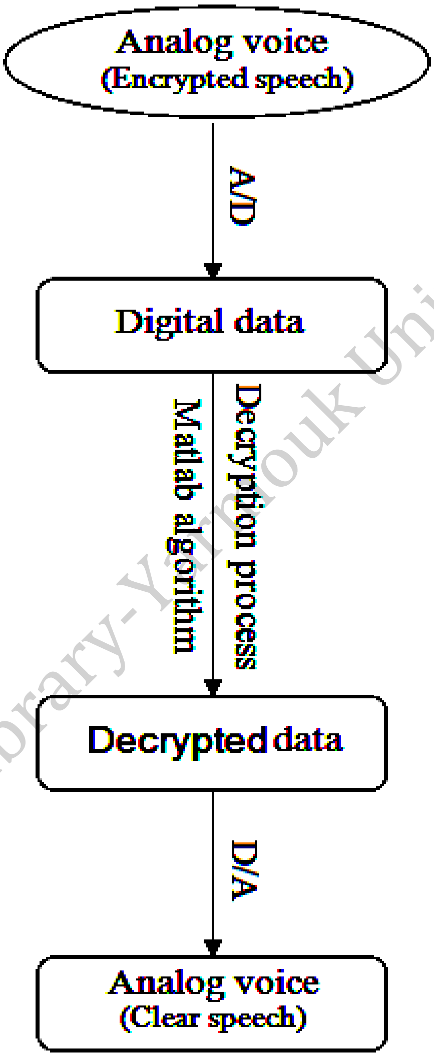


Fig.8: Flow chart of voice encryption system **Fig.9: Flow chart of voice decryption system**

3.3.2 Proposed Algorithm for Voice Encryption and Decryption Process:

Proposed algorithm is summarized in the following steps:

1. PortAudio has to be initialized.

2. The stream has to be managed (started and later stopped).

3. The manipulation of the audio data has to be performed.

4. The stream has to be terminated.

Fig. 10 illustrates voice encryption process and Fig. 11 illustrates voice decryption process.

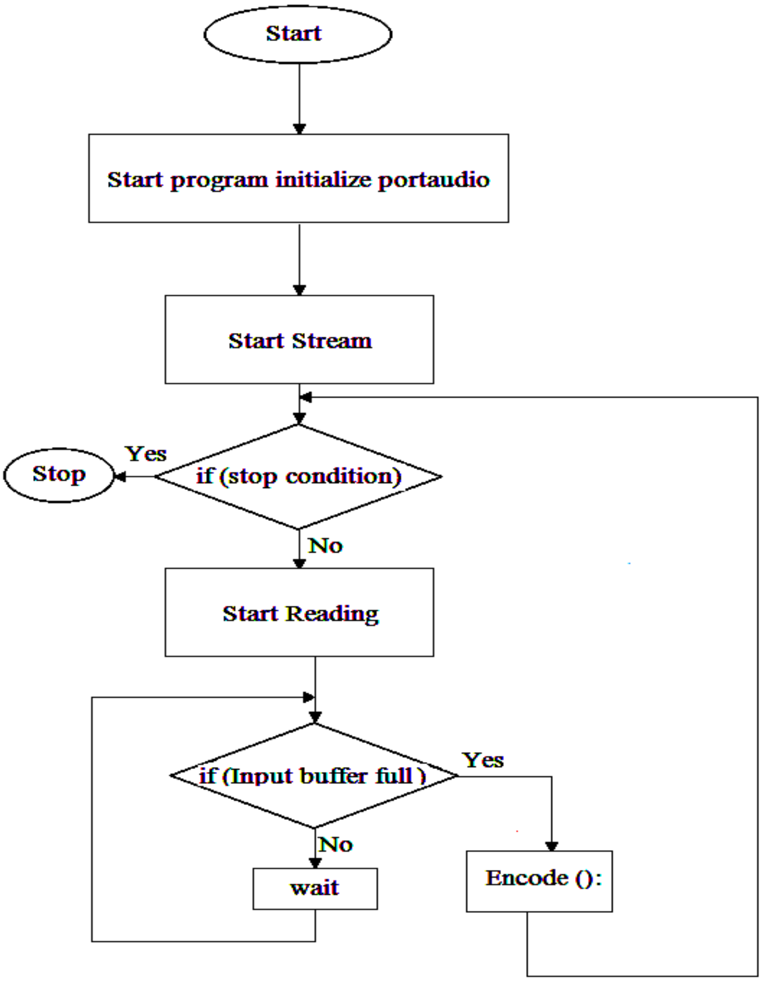


Fig. 10: Flow chart of software program for voice encryption process.

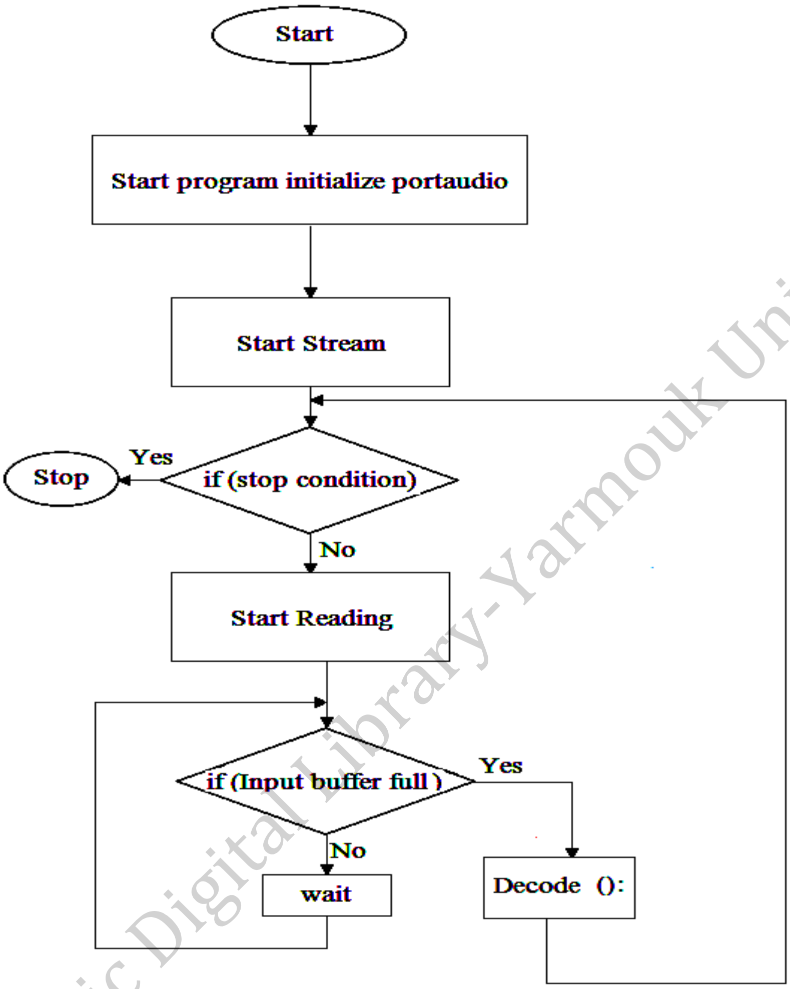


Fig. 11: Flow chart of software program for voice decryption process.

3.3.3 Techniques of Voice Security:

In this thesis, we will develop algorithms that are expected to offer useful encryption algorithms for audio/speech coding. Our problem is to find a scheme that provides high level of security; we present two different schemes for testing which one is considerably more secure than others.

3.3.3.1 First method (Random Key Sequence with Modified Fixed Coefficients)

In encoding process using Modified Fixed Coefficients scheme, shift register initially is filled by initial state (all zeros, 00...0,), and the feedback coefficients c_0, c_1,..., c_{n-1} is any one of 2^n-1 possible state except all zeros, 00...0, where n is number of stages in the shift register, then the process of encryption can be started, see fig. 4, notice after n outputs, each ciphertext bit will depend only on input bit and n previous ciphertext bits, see eq.1.

3.3.3.2 Second method (Random Key Sequence with Modified Dynamic Coefficients)

In this scheme, we use different generators to generate a multisequence of random numbers, i.e. shift register initially is filled by initial state , and the feedback coefficients c_0, c_1,..., c_{n-1} is any one of 2^n-1 possible state (except all zeros) generated by first generator, then it can be used for encryption of the first n-bits of input message data, then the process of encryption begins, and after each n-bits of outputs (encrypted data), the feedback coefficients c_0, c_1,.., c_{n-1} will be any another of 2^n-1 sequence, generated by another generator, (as visible in Fig. 12). Fig. 13 summarizes software program of multistage random key generation. The second method is considerably more secured than the first method, where for true decryption by Random Key Sequence with Modified Fixed Coefficients scheme, you need to know key sequence just one time, because these keys are constant and not altered in every loop of decryption process, but for Random Key Sequence with Modified Dynamic Coefficients scheme, key sequence is altered in every loop of decryption process, so for true decryption, all keys and their sequence must be known.

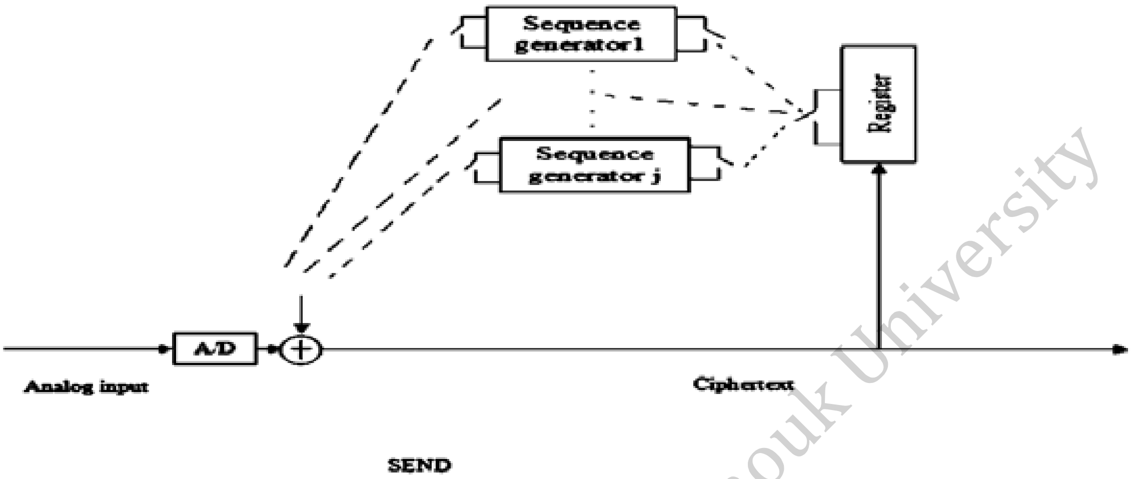


Fig. 12: Typical cipher feedback system with multigenerators.

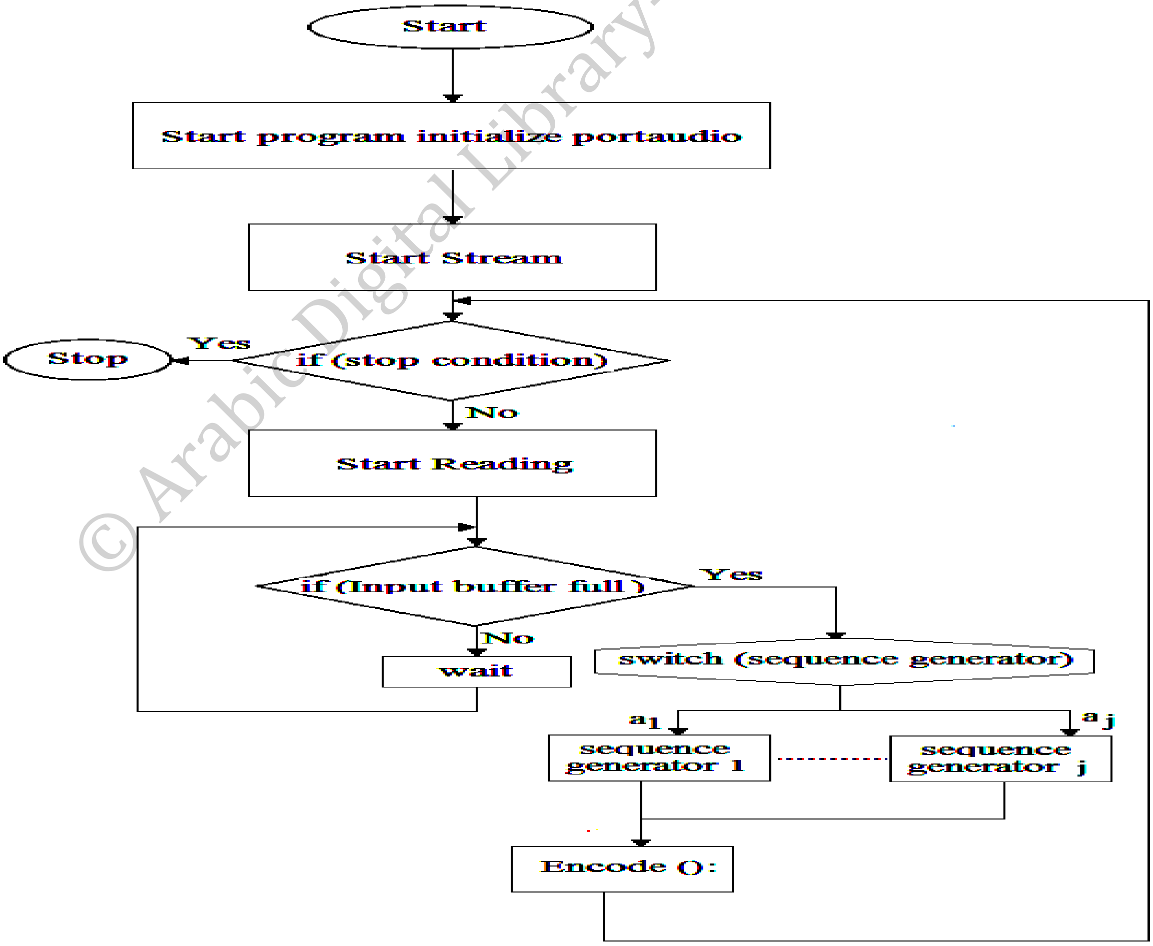


Fig .13. Flow chart of modified dynamic coefficient.

Chapter Four: Analysis and Simulation

4.1 Introduction

Based on previous work in audio encryption, there are many different methods used for voice encryption. Each method is different from others in complexity, cost, and implementation. In this thesis, we proposed a method which will reduce complexity of the encryption process and achieve high level of security.

4.2 Performance Measurement

A common technique is to record voice data for a male or a female speaker for some time. The reference samples consisted of a number of short sentences or phrases of English language speech, typically 8 - 12 seconds in length. The data sampled at 11.025 kHz and a sampling resolution of 16 bits / sample. Human hearing range is up to 20,000 Hz and human speech frequency is in the range of 200 to 7,000 Hz for typical speech activity such as talking, singing, laughing and crying [6]. The signal was sampled at least two times the highest frequency to satisfy the Nyquist Theorem. Increasing sampling rates will also automatically provide signal-to-noise ratio advantage. Therefore, speech recordings that are digitized with high sampling rate are able to effectively represent the information contained in the waveform. The data was stored and manipulated using Matlab algorithm.

In order to assess the impact of transmission, the samples are transmitted through a telephone network. The input samples are provided by a laptop audio output, connected to the input of the telephone. At the other terminal, the audio signal received is loaded to a laptop - again using a connector between laptop audio ports and the input of the telephone Fig.14. Tests were conducted on both unencrypted and encrypted speech.

The main feature of the encryption/decryption program implementation is the generation of the encryption key. A symmetric Encryption key is used for this application, which means the same key is shared for both encryption and decryption Fig.15. A copy of the generated key is saved in a file with extension .mat during the Encryption process and the same key is used as the decryption key to retrieve the encrypted file. The technique of generating the key uses two methods: fixed random number generation and dynamic random number generation.

Table.1: Input parameters

Parameters	**Variables**
Sampling Frequency	11.025 kHz
Sampling Resolution	16 bits / sample
Speech Length	8 - 12 seconds
Speech Segments	55125 samples

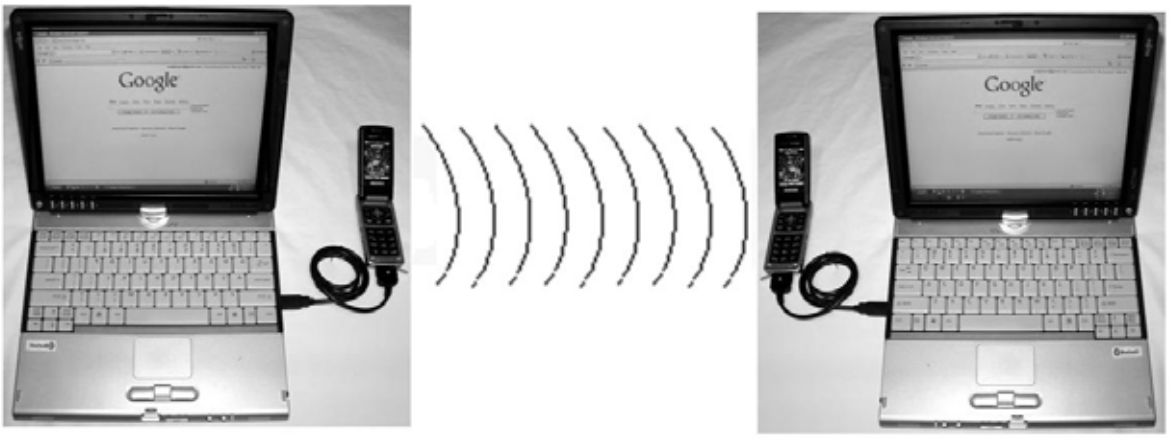


Fig.14: Hardware unit, Transmitter side/ Receiver side.

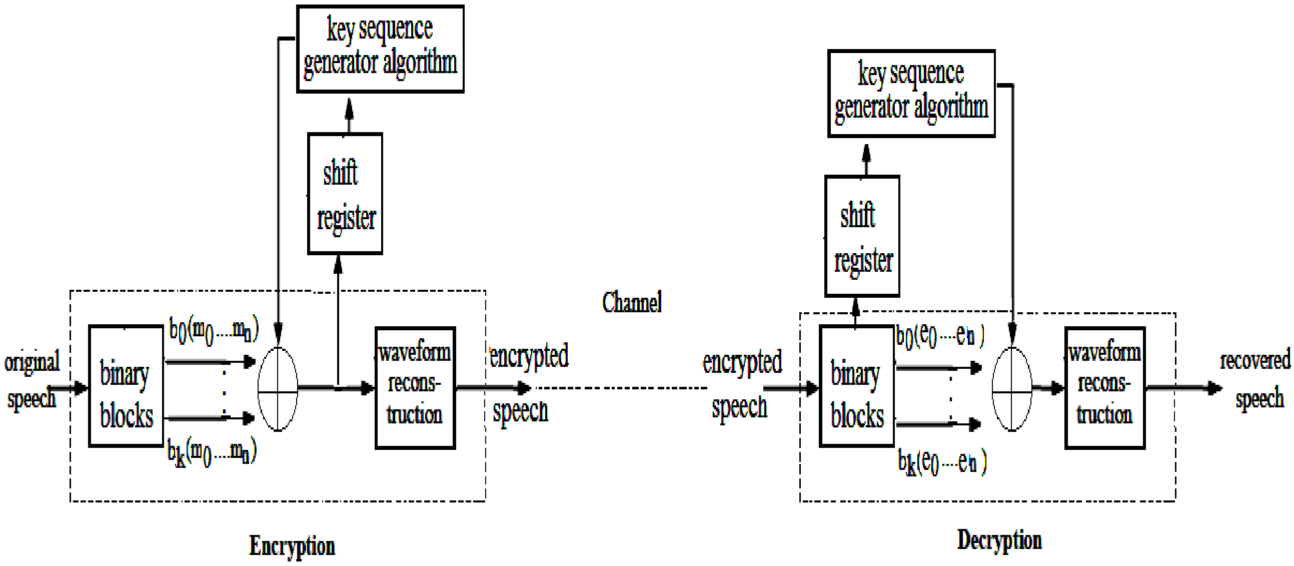


Fig.15: Encryption and decryption schemes of the proposed cryptosystem

4.3 Simulation Results and Discussion

In our simulation, we implement proposed approach using MATLAB (version 7.10). . In order to achieve high level of security, two schemes for generating a random sequence of encryption keys are presented. Random Key Sequence with Modified Fixed Coefficients and Random Key Sequence with Modified Dynamic Coefficient (Multistage Random Key Sequence Generation).

Fig.16 shows that the speech contains voiced part, and unvoiced part. Voiced part contains the maximum speech information whereas the unvoiced part provides the whispering sounds. The sound waveform presented in this figure shows variations over 1300 samples of speech starting from near silence, which consists of a spikes at around 202th and 392th samples and peak resonance in between 8th to 780th samples, where with voiced speech, air pressure from the lungs forces normally closed vocal cords to open and vibrate (The vibration frequencies depending on the person's age and sex) and forms resonance in the vocal track, these resonance peaks are called formants, after 1500th sample time domain samples lose periodicity, because the vocal cords do not vibrate in unvoiced sounds.

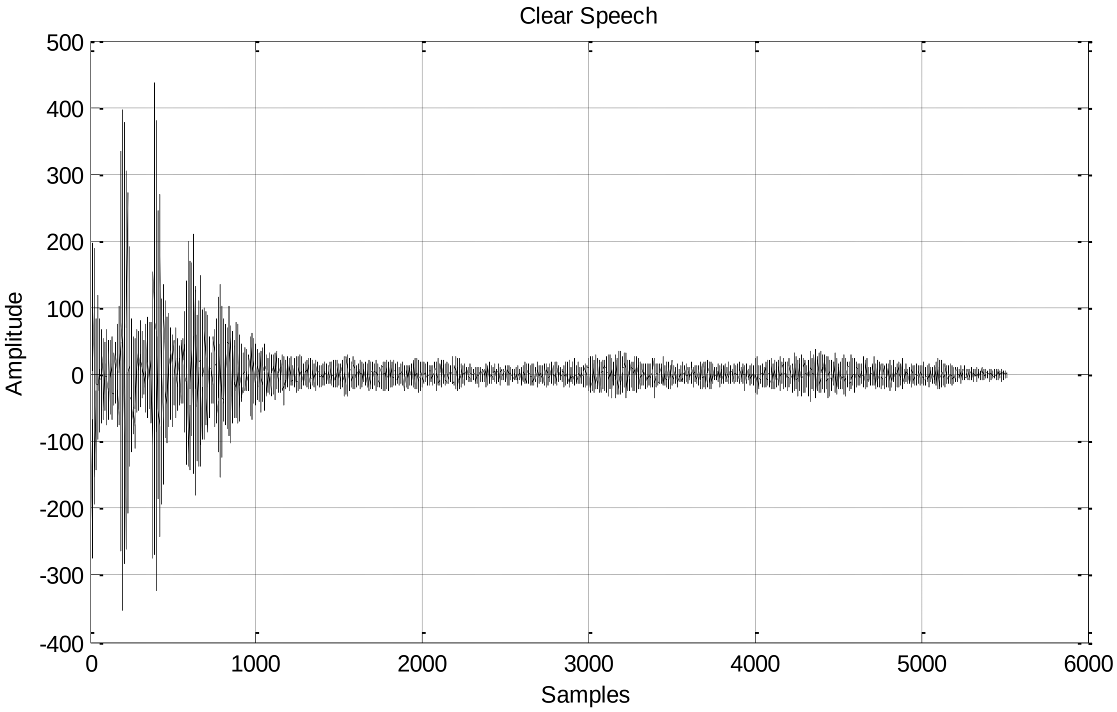


Fig.16: Time domain representation of original speech.

The sound waveform presented in Fig.17 shows regular variations of speech in between 1st to 55125th samples with corresponding amplitude approximately in between -250 to 250. In this case sound is a mixture of voiced sound and unvoiced sound, the result is a noise. Such sounds show little long-term periodicity.

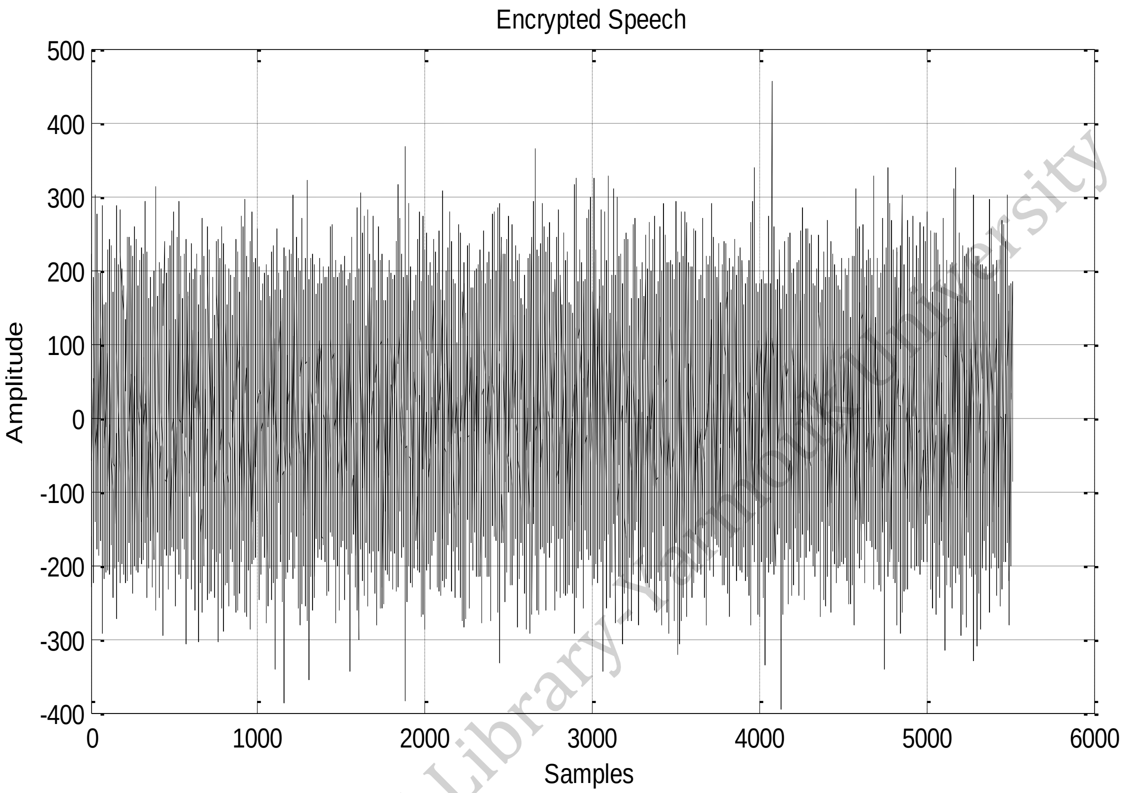


Fig.17: Time domain representation of encrypted speech for random key sequence with Modified Fixed Coefficients scheme.

Fig.18 shows the results of time-domain representation of the decrypted speech for Random Key Sequence with Modified Fixed Coefficients scheme. It is very clear from this figure that the reconstructed speech is similar to the input speech (taking samples randomly from reconstructed speech and original speech the result is the amplitude is the same).

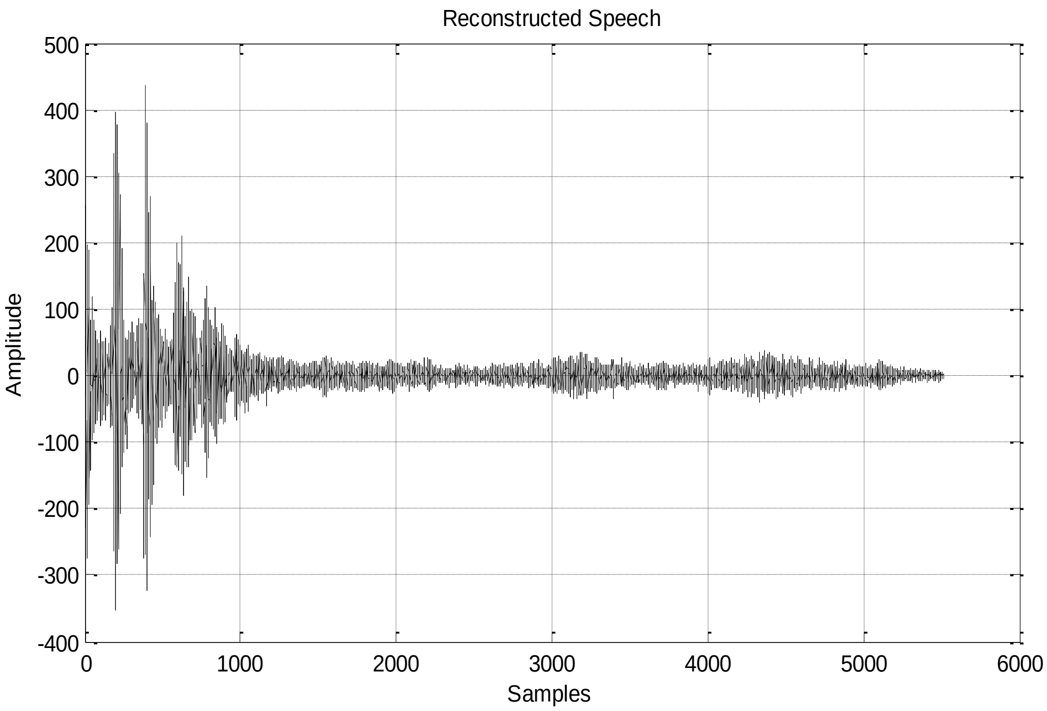


Fig.18: Time domain representation of reconstructed speech.

The Fig.19 shows the results of time-domain representation of the encrypted speech for Random Key Sequence with Modified Dynamic Coefficients scheme. In this figure, the waveform has become chaotic (a very high degree of content destruction). Analysis of the signal subject to encryption mix and exchange voiced speech with unvoiced speech together. Displaying this signal confirms that the signal sounds like a noise, where noise sound exhibit smaller amplitude and faster oscillation compared to voiced sound.

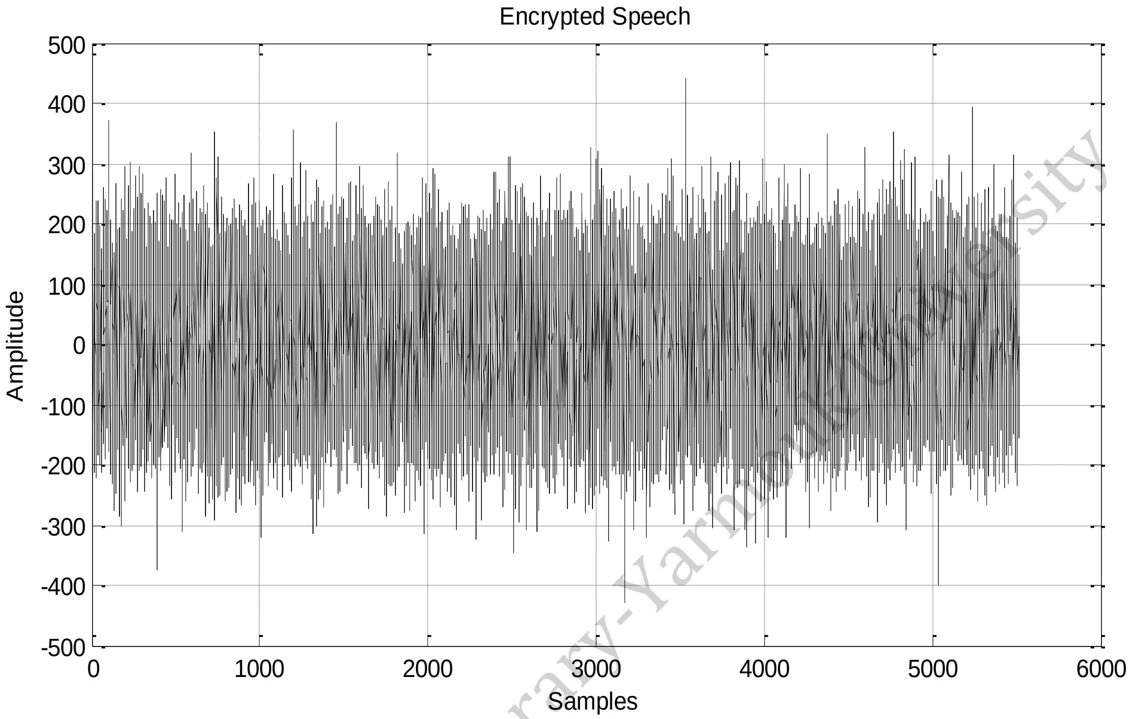


Fig.19: Time domain representation of encrypted speech for random key sequence with Modified Dynamic Coefficients scheme.

Fig.20 shows the results of time-domain representation of the decrypted speech for Random Key Sequence with Modified Dynamic Coefficients scheme. It is very clear from this figure that the reconstructed speech is similar to the input speech. As mentioned earlier speech sounds are created by vibratory activity in the human vocal tract, and it is normally transmitted to a listener's ears or to a microphone through the air, where speech and other sounds take on the form of radiating waves of variation in air pressure, these waveforms can be plotted and analyzed, as visible in this figure.

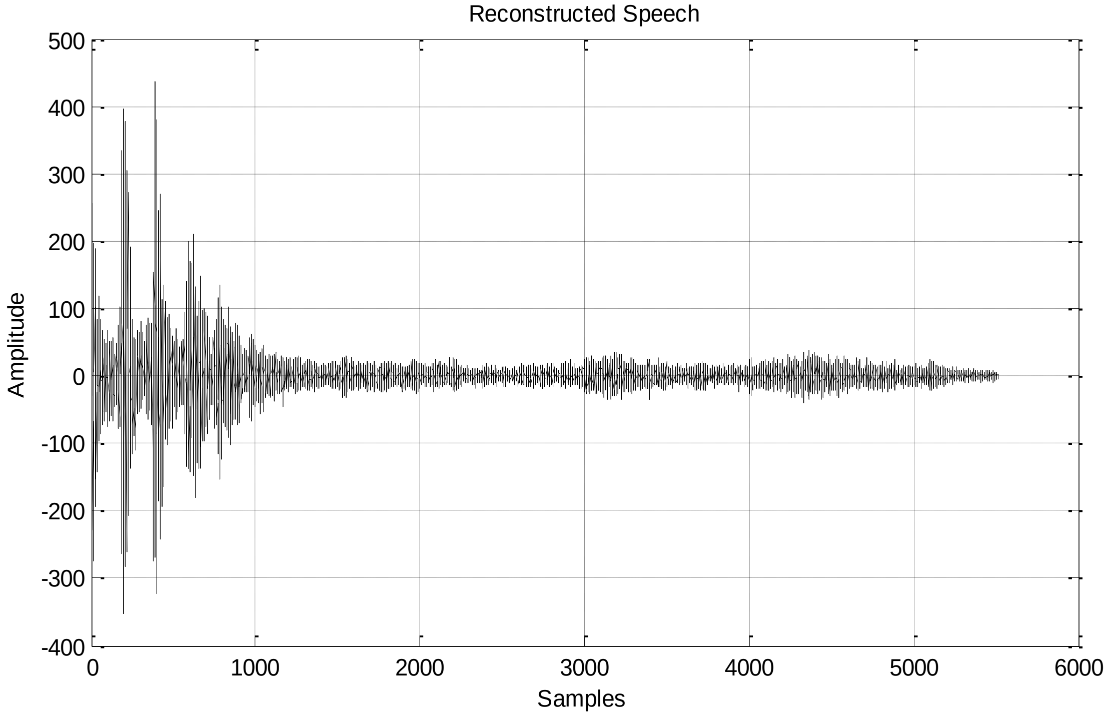


Fig.20: Time domain representation of reconstructed speech.

Power spectral density, *P(f)*, which is a function that maps the frequency (*f*), to the amount of power of the signal containing that frequency. It shows the strength of the variations (energy) as a function of frequency. In other words, it shows at which frequencies variations are strong and at which frequencies variations are weak. Figures 21, 22, and 23 show the result of power spectral density of the original speech, encrypted speech and reconstructed speech for Random Key Sequence with Modified Fixed Coefficients scheme, respectively. The vibration frequencies vary from about 12 to 800 Hz and forms resonance in the vocal track at even harmonics. These resonance peaks are called formants and can be seen in Fig. 21, below.

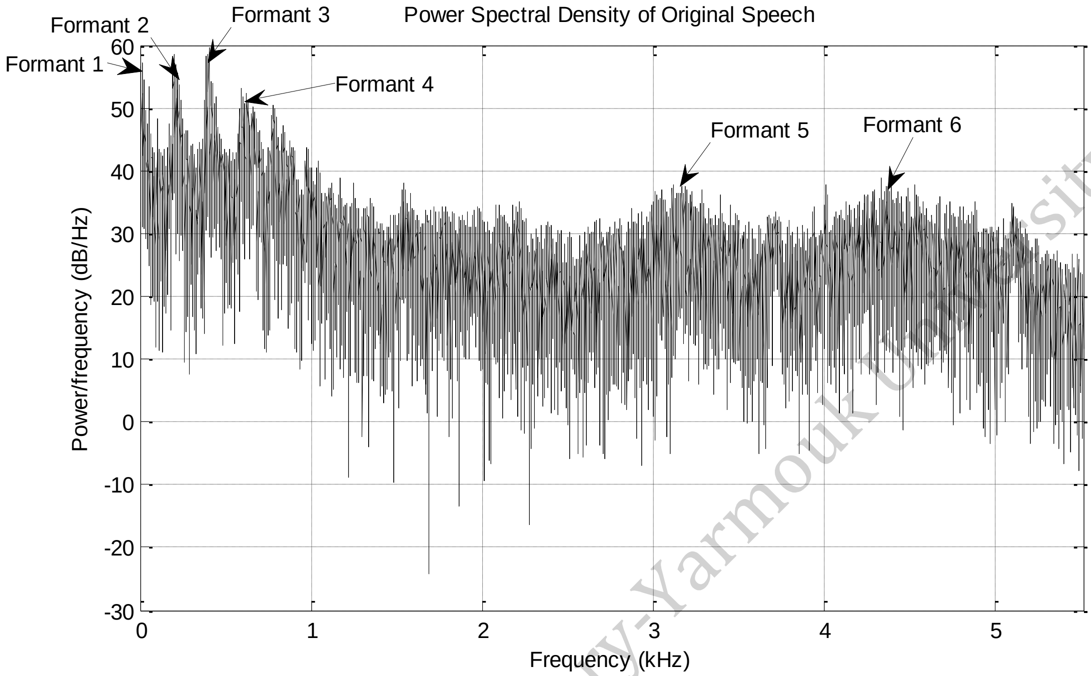


Fig .21: Power density spectrum of original speech.

As visible in Fig. 22 the power spectral density of encrypted speech with Modified Fixed Coefficients scheme does not display the clear resonance peaks that are found in the original speech (i.e. the periodic nature of formant vanished). The encryption scheme completely eliminates the harmonic structure and leaves almost no detectable spectral envelope.

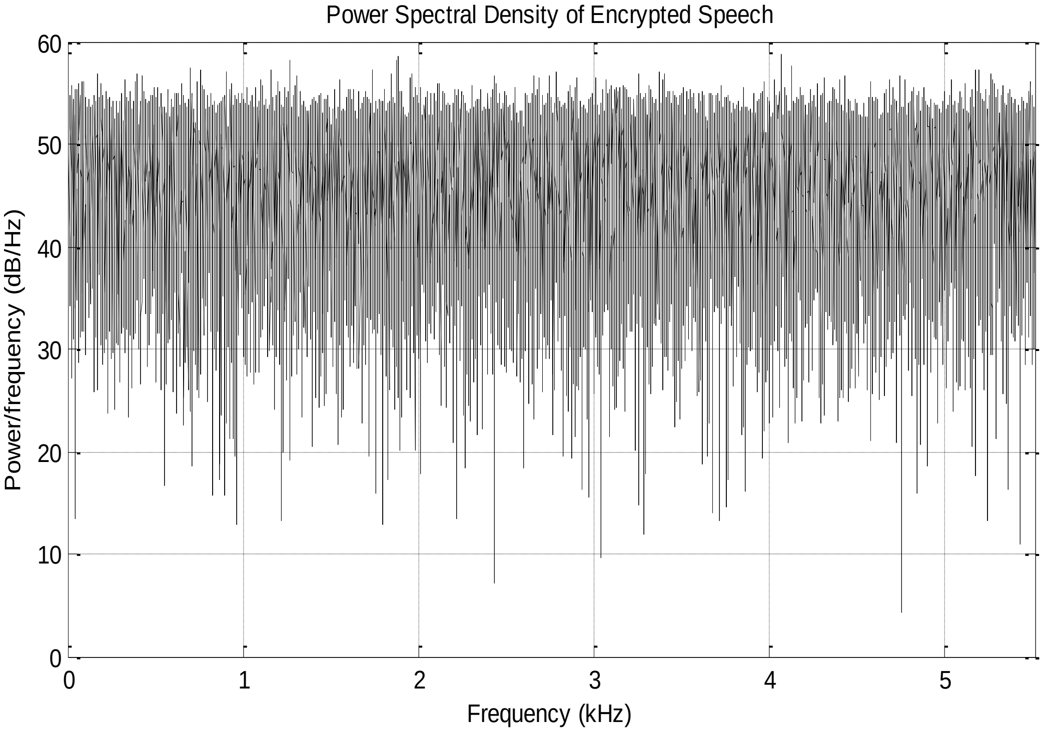


Fig .22: Power density spectrum of encrypted speech for random key sequence with Modified Fixed Coefficients scheme.

It is clear from Fig.23 that the power spectral density of the reconstructed speech with Modified Fixed Coefficients scheme is much similar to that of the original speech (taking samples randomly from reconstructed speech and original speech the result PSD is the same).

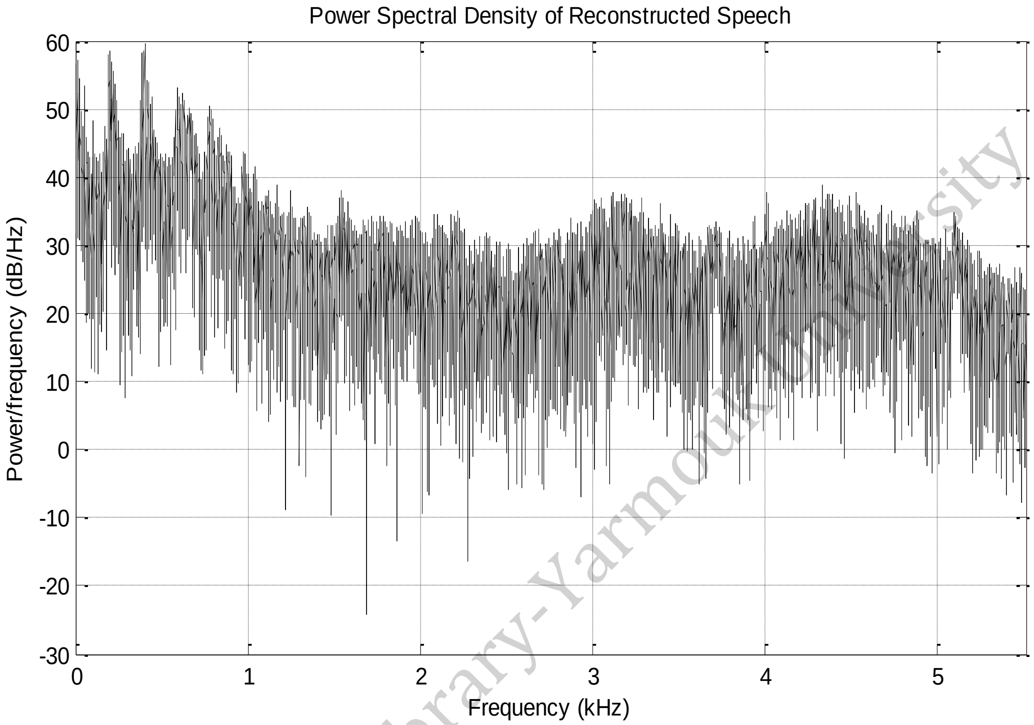


Fig .23: Power density spectrum of reconstructed speech.

Fig.24 shows the results of power spectral density of the encrypted speech for Random Key Sequence with Modified Dynamic Coefficients scheme, in this figure, a sound contains many different components with roughly the same power. This sounds like a noise, where the noise power spectral density is ideally flat with frequency.

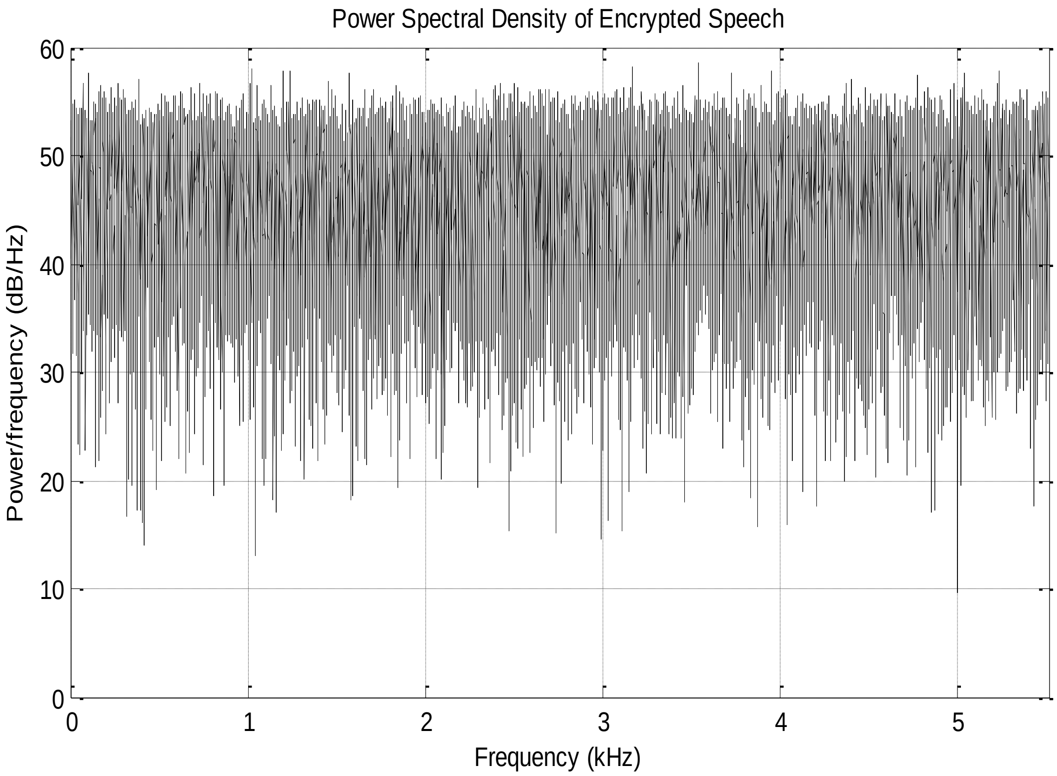


Fig.24: Power density spectrum of encrypted speech for random key sequence with Modified Dynamic Coefficients scheme.

Fig.25 shows the results of power spectral density of the decrypted speech for Random Key Sequence with Modified Dynamic Coefficients scheme. From this figure, it is very clear that the power spectral density of the reconstructed speech is much similar to that of the original speech.

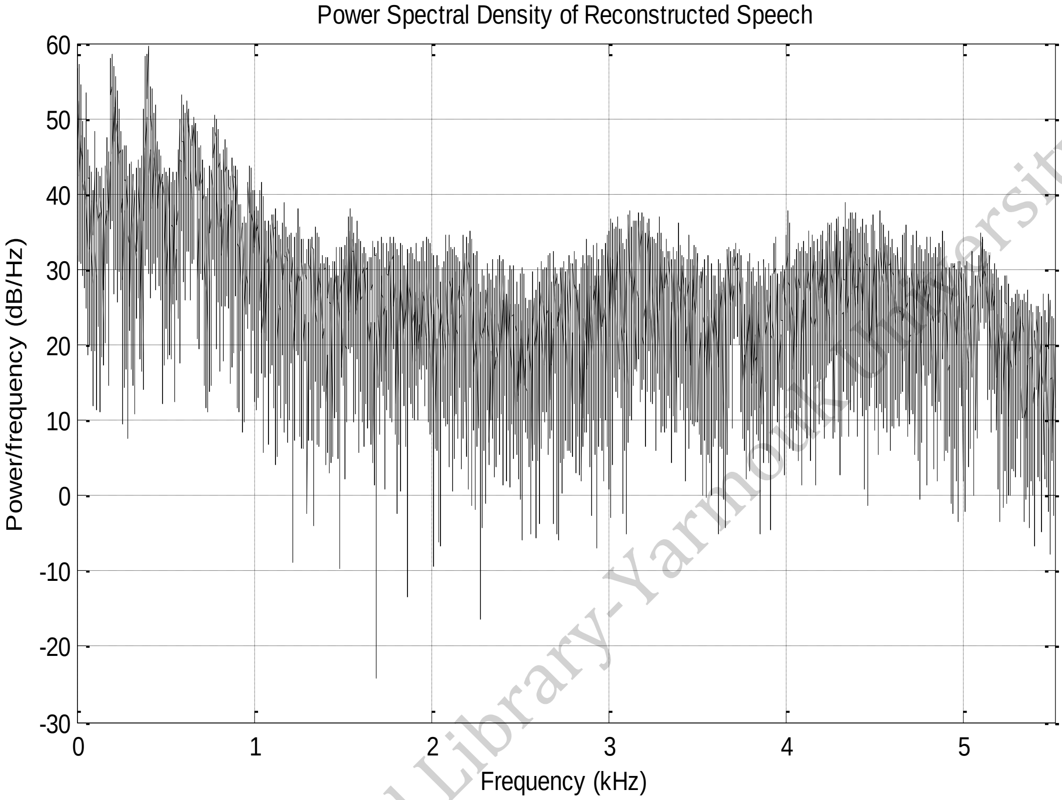


Fig.25: Power density spectrum of reconstructed speech.

Table. 2, shows the magnitude spectrum of the original and encrypted speech. A clear harmonic structure with frequency of approximately 401.6 Hz characterizes most of the spectrum in original speech. For encrypted speech of random key sequence with modified Dynamic Coefficients scheme maximum PSD is 58.55dB/Hz, and it is 58.72dB/Hz in random key sequence with Modified Fixed Coefficients scheme.

For PSD of Modified Dynamic Coefficients diagram a sound contains many different components with roughly the same power which is 55 dB/Hz, but also it contains components with power varies in the range of 23 dB/Hz to 34 dB/Hz and it reaches as minimum as 9.535 dB/Hz. However, from PSD of Modified Fixed Coefficients diagram power varies in the range of 26 dB/Hz to 35 dB/Hz and it reaches as minimum as 4.312 dB/Hz, as in the table below.

Table.2: Power Spectral Density of Original Speech and Encrypted Speech.

Frequency	**PSD of Original Speech**	**PSD of Modified Fixed Coefficients**	**PSD of Modified Dynamic Coefficients**
0.4016KHz	59.62 dB/Hz	44.33 dB/Hz	45.91 dB/Hz
1.69 KHz	-24.3 dB/Hz	40.45 dB/Hz	40.56 dB/Hz
3.537 KHz	31.29 dB/Hz	40.35 dB/Hz	58.55 dB/Hz
4.071 KHz	30.2 dB/Hz	58.72 dB/Hz	41.96 dB/Hz
4.752 KHz	22.06 dB/Hz	4.312 dB/Hz	42.78 dB/Hz
4.994 KHz	25.2 dB/Hz	44.69 dB/Hz	9.535 dB/Hz

A spectrogram is a representation of how the frequency content of a signal changes with time. Time is displayed along the x-axis, frequency along the y-axis, and the amount of energy in the signal at any given time and frequency is displayed as a level of yellow. During regions of silence, and at frequency regions where there is a little energy, the spectrogram appears blue; red regions indicate areas of energy – caused by vocal fold closures, harmonics, or formant vibration in a speech signal.

There are two types of spectrogram for speech: Narrow-band spectrogram is a spectrogram produced using an analysis scheme which emphasizes frequency changes in the signal.

Whereas wide-band spectrogram is a spectrogram produced using an analysis scheme which emphasizes temporal changes in the signal.

Fig.26 shows the spectrogram of original speech. In this one, the frequencies are plotted over the time and the amplitude is marked with the intensity of the color. In this figure narrow and wide-band spectrograms are clearly seen. Narrow-band spectrograms show the harmonics of the vocal fold vibration over very small segments of less than 0.1 seconds. Whereas wide-band spectrograms show the vocal tract resonances (formant) occupying the right of the diagram.

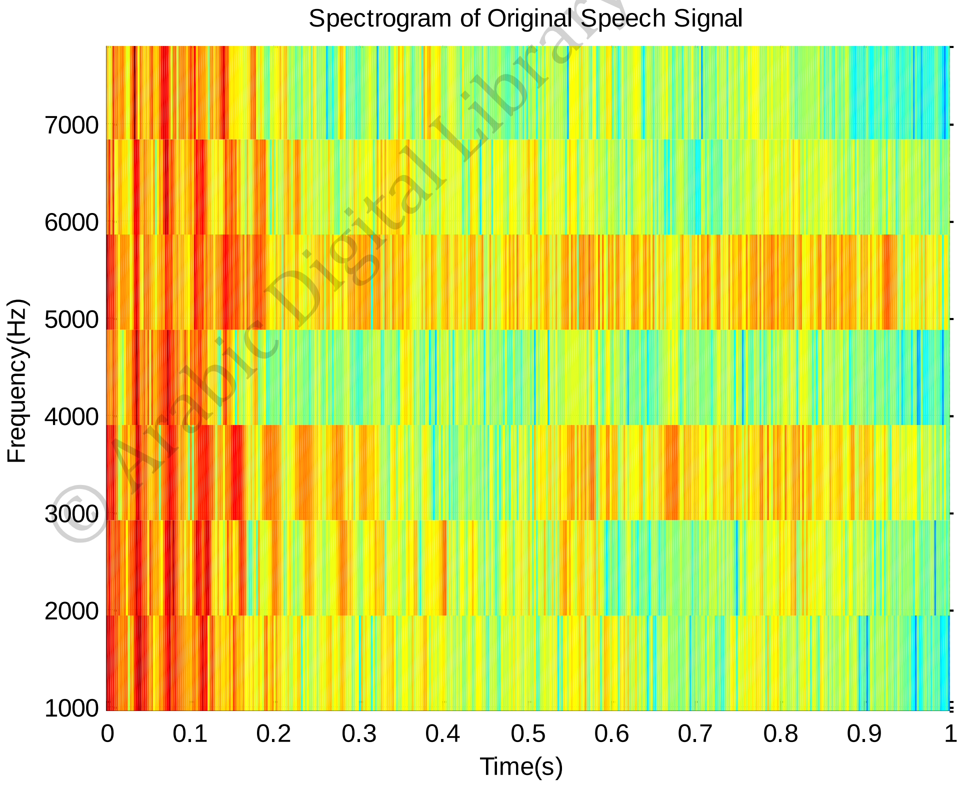


Fig.26: Spectrogram of original speech.

Fig.27 shows fast changes in waveform, and very clear wide-band spectrograms. As we move right along the x-axis we shift forward in time, travelling one spectrum after another.

The lines visible in the spectrogram on this figure each represent 1000 Hz along the frequency axis, so that the spectrogram contains 8000 Hz in total. All of the spectra computed by the Fourier transform are displayed parallel to this vertical or y-axis. The strength of a given frequency component *f* at a given time *t* in the encrypted speech signal is represented by the red, yellow, and blue color of the corresponding point S(t,f).

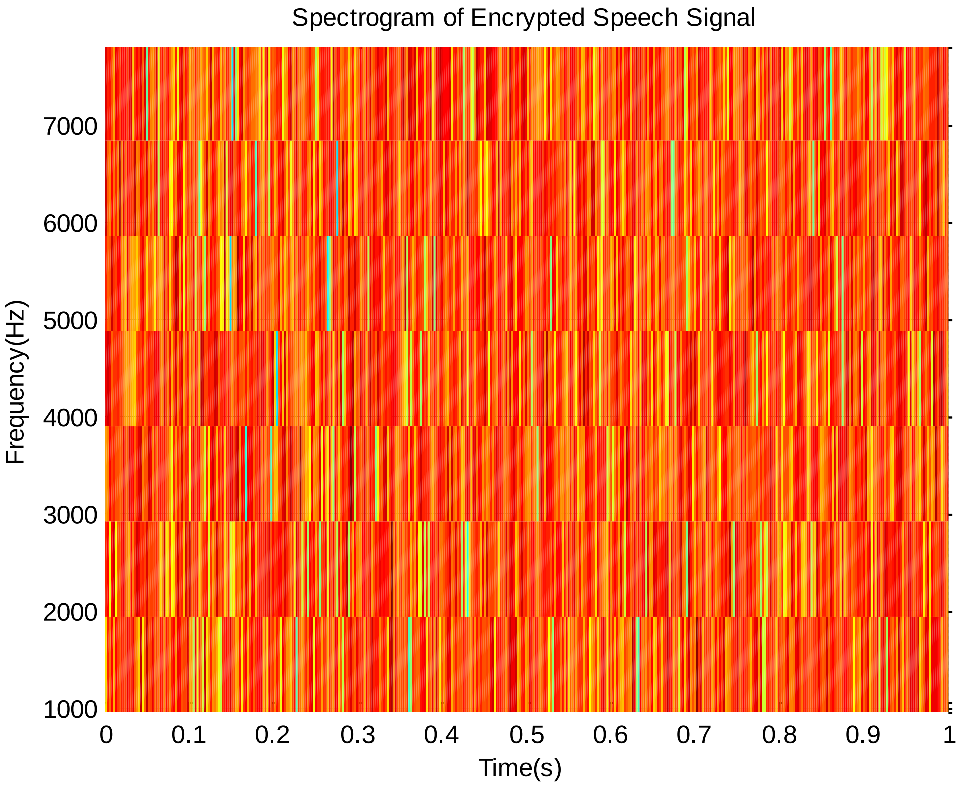


Fig.27: Spectrogram of encrypted speech for random key sequence with Modified Fixed Coefficients scheme

The spectral distribution of sounds can be described in terms of two kinds of spectral structures, one that has a periodic or harmonic spectral distribution and the other that has a noisy spectral distribution. We can utilize from knowing these spectral structures in understanding spectral features of sounds and estimate the complexity of different sounds.

It is obvious that Fig.28 has harmonic spectral distribution, as known speech sounds contain energy at all frequencies in the audible range, although it is thought that most phonetic information is concentrated below 8000 Hz. In the spectrogram in Fig.28 we use shades of red to mean increasing energy along the frequency axis, blue to mean decreasing energy, and yellow to mean amount of energy in the signal at any given time and frequency.

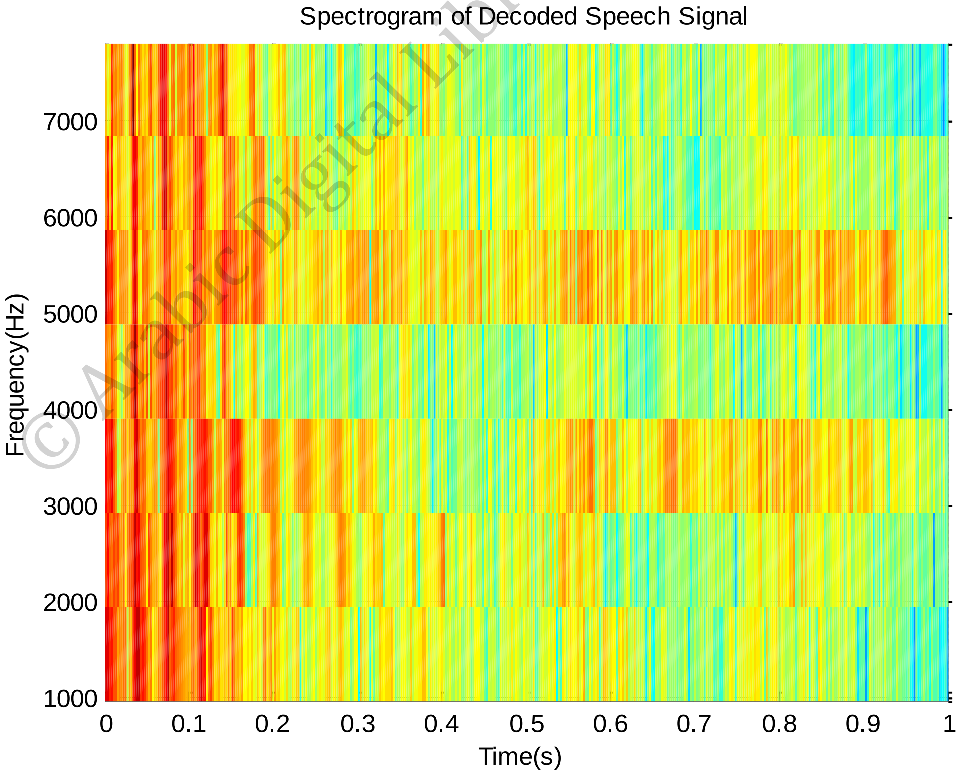


Fig.28: Spectrogram of decoded speech.

The spectrogram is used to present the time-frequency information of a signal. The spectrogram of Fig.29 shows time on the x axis, frequency on the y axis, and sound level in a highlight color (blue is weak, red is strong). In the spectrogram, the harmonics appear as vertical lines. In this figure, the pitch changes, so the frequencies of the spectral lines are variable, and the power of every harmonic increase with time, so the sound becomes louder, it is obvious that this figure has a noisy spectral distribution

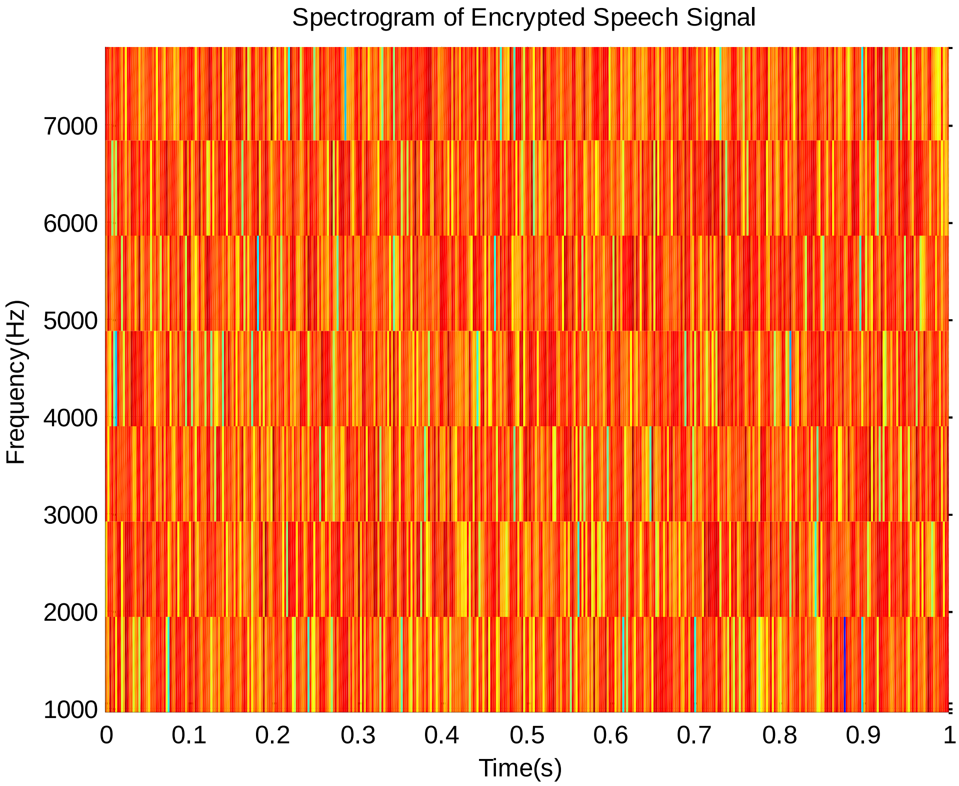


Fig.29: Spectrogram of encrypted speech for random key sequence with Modified Dynamic Coefficients scheme.

From Fig.30 it is very clear that the Spectrogram of reconstructed speech is almost similar to the input speech. With the use of color to highlight the important features of a spectrogram, the bold color of a given point is proportional to the energy at that time and frequency. In our color spectrograms, the formants can be traced by following the yellow bands between the increasing red and decreasing blue bands.

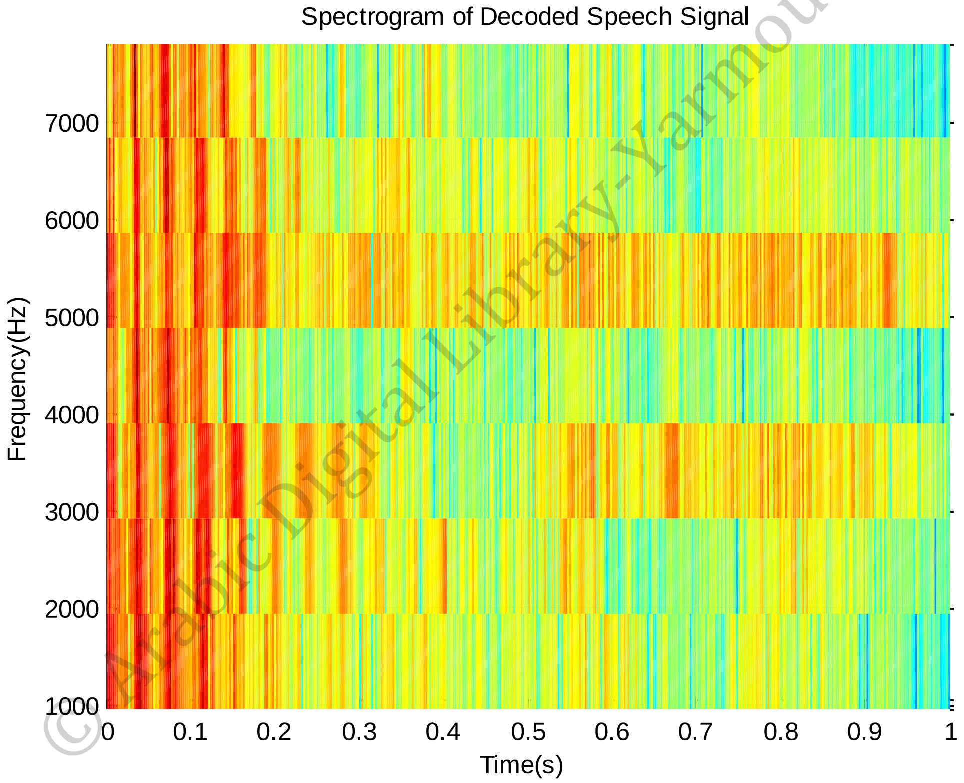


Fig.30: Spectrogram of decoded speech.

Cross-correlation is a measure of similarity of two waveforms as a function of a time-lag applied to one of them. The formula essentially slides one of the waveforms along the time-axis, calculating the integral of their product at each position. When the functions match, the value of product of these waveforms is maximized. This is because when peaks (positive areas) are aligned, they make a large contribution to the integral. Similarly, when troughs (negative areas) align, they also make a positive contribution to the integral because the product of two negative numbers is positive.

It is obvious from Fig.31, and Fig.32 that the cross correlation between clear signal and encrypted signal varies approximately in the range -70 to 70, which has sufficiently lower values than cross correlation between clear signal and decrypted signal, so the clear signal cannot be detected, and that is the desired.

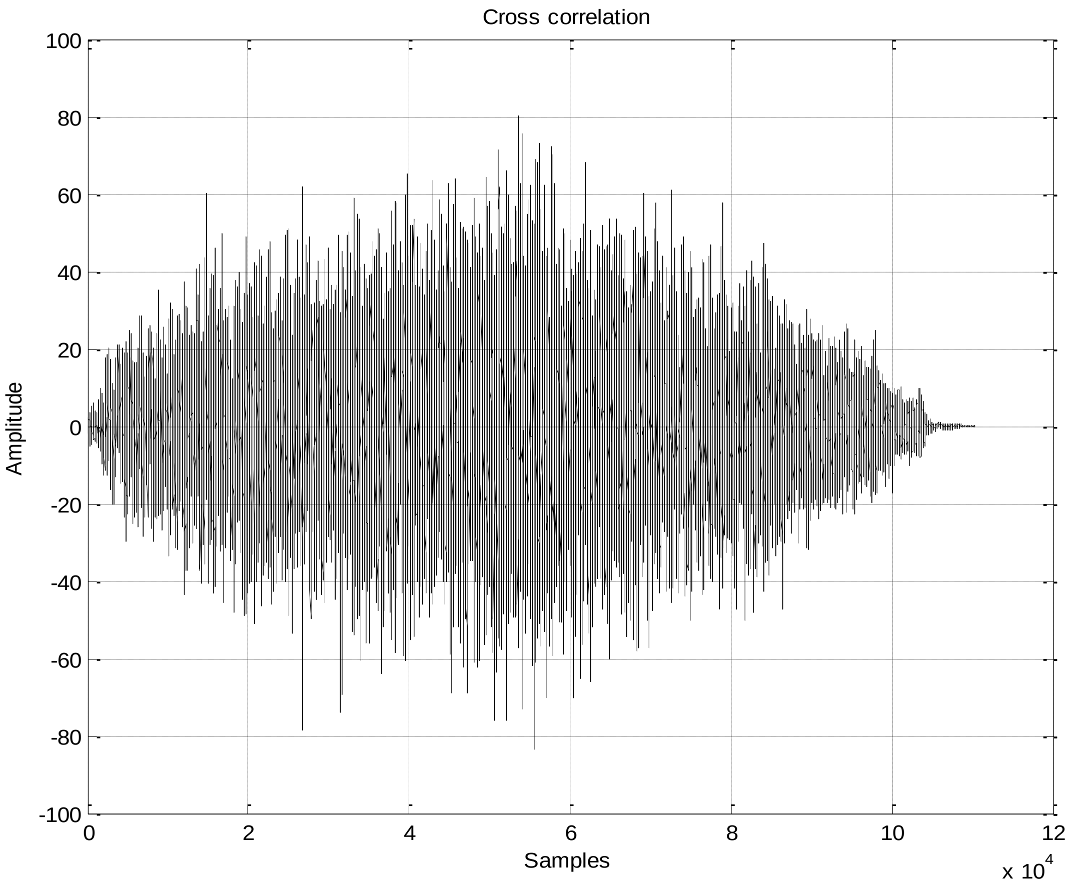


Fig.31: Cross correlation between clear signal and encrypted signal for random key sequence with Modified Fixed Coefficients scheme.

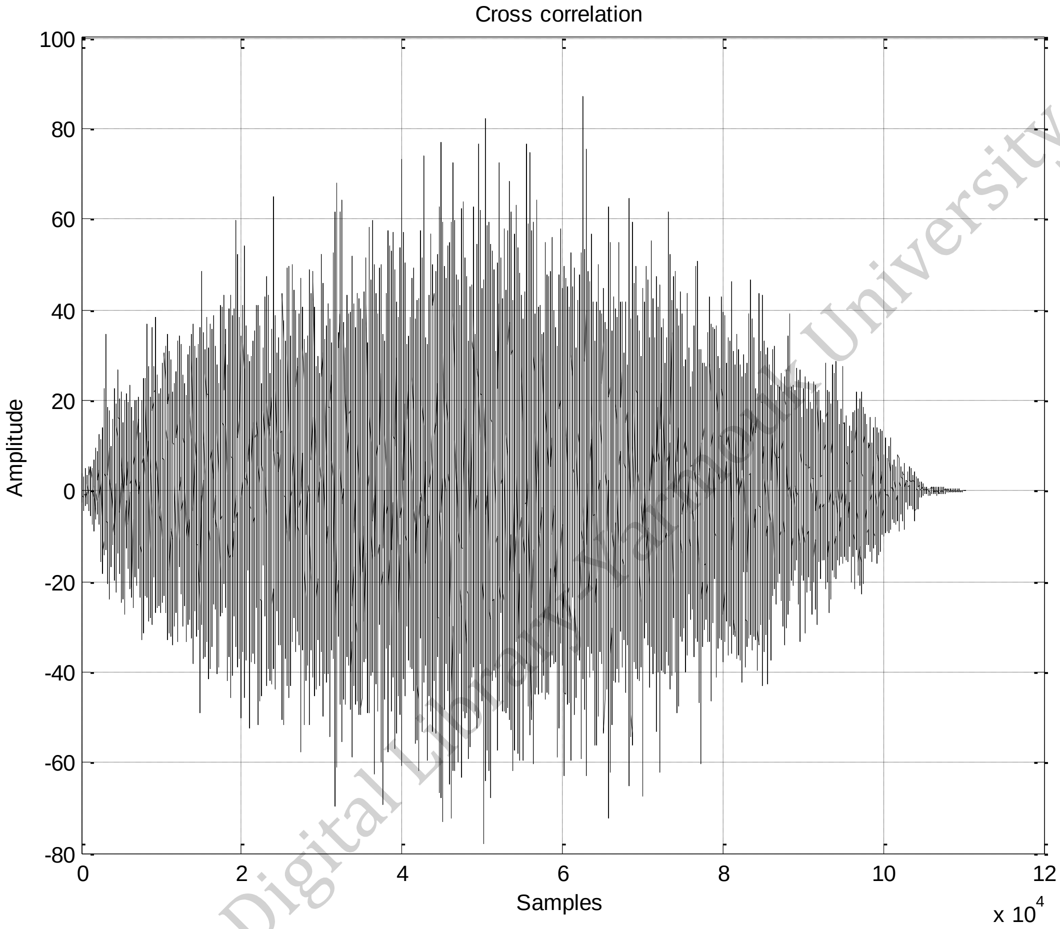


Fig.32: Cross correlation between clear signal and encrypted signal for random key sequence with Modified Dynamic Coefficients scheme.

Fig.33 shows the cross correlation between clear signal and decrypted signal, as mentioned earlier cross correlation is used for measuring the similarity of two signal. This figure shows high similarity, so the clear signal can be detected, and that is the desired.

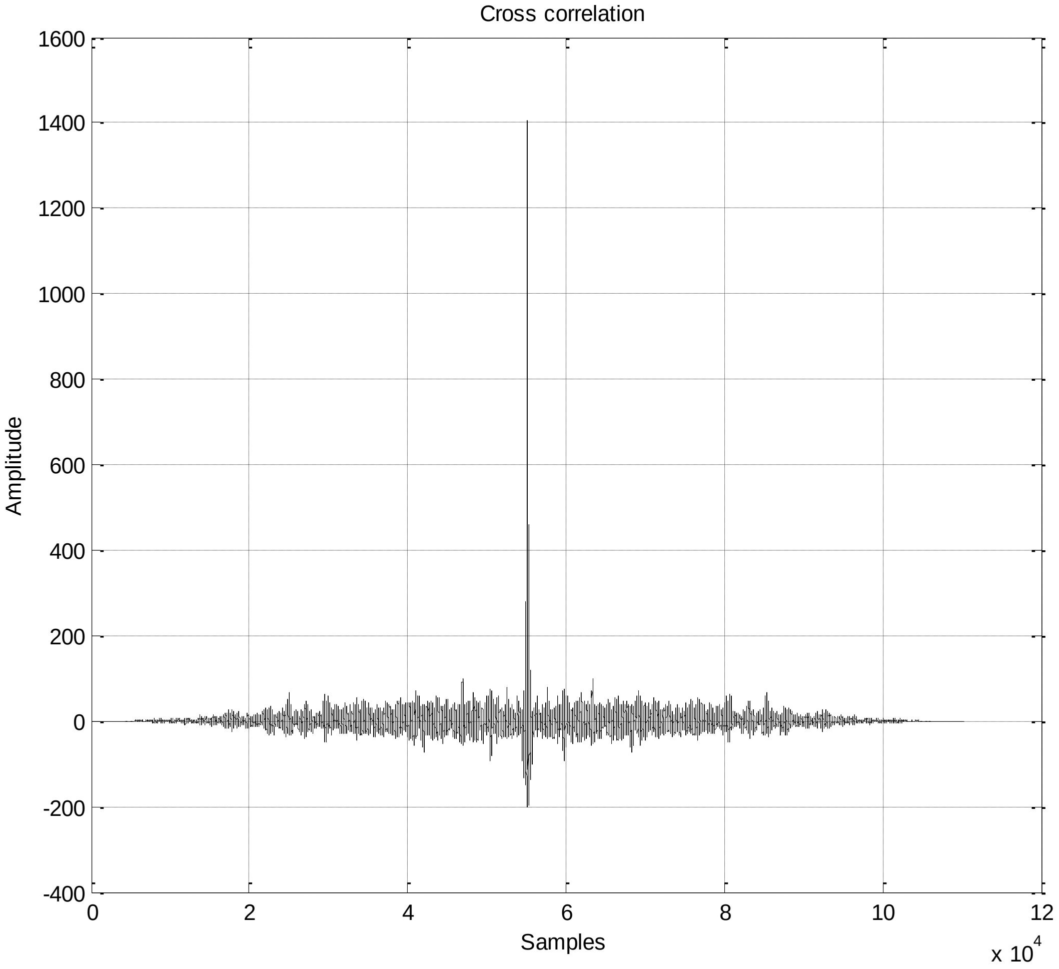


Fig.33: Cross correlation between clear signal and decrypted signal.

The lower the value of the correlation in the cipher, the better the quality of the cryptosystem. The correlation results for the proposed cryptosystems are tabulated in Table. 3. From these results, we can see that both methods produce cipher speech with low correlation between similar segments in the plain and the cipher, which means that they all give a good encryption quality.

Table.3: Correlation measurement of Clear Signal with Decrypted Signal, Clear Signal with Encrypted Signal (Random Key Sequence with Modified Fixed Coefficients, Random Key Sequence with Modified Dynamic Coefficients).

Samples	Decrypted Signal	Modified Fixed Coefficients	Modified Dynamic Coefficients
22000	-15.8643	-6.0837	-1.3979
44000	27.9946	20.1470	1.6840
55010	279.0541	3.2262	7.9311
55450	-39.7272	-11.4881	-17.1402
80000	25.0505	6.8956	4.2508

It is obvious from Tabe.3 that the most similarity between clear signal and decrypted signal occurs at sample 55010 where it is 279. However, correlation between clear signal and encrypted signal for random key sequence with Modified Dynamic Coefficients scheme is 7.9 at this sample, and it is 3.2 for random key sequence with Modified Fixed Coefficients scheme.

Taking sample 80000, correlation between clear signal and encrypted signal for random key sequence with Modified Dynamic Coefficients scheme is 4.2, and it is 6.8 for random key sequence with Modified Fixed Coefficients scheme. However, it is 1.68 and 20.1 at sample 44000 for random key sequence with Modified Dynamic Coefficients scheme and random key sequence with Modified Fixed Coefficients scheme, respectively. The lower the values of the correlation of these schemes are due to waveforms of these schemes don’t match the original speech waveform.

Chapter Five: Conclusion and Future Work

In this thesis, a scheme for encrypted speech transmission directly on mobile voice channel is proposed to guarantee the end to-end secure communication over mobile networks. The proposed scheme based on pseudorandom technique is a good solution for encrypted speech accessing mobile voice channel and transmitting over the mobile networks. Various random key generation schemes based on the pseudo-random generator have been proposed and evaluated. Such as a multistage random key generator which is established by increasing the number of generators of random keys the complexity to know these keys in order to use it in decryption process is increased, where the casual listener cannot decrypt the data without correct keys. Thus, secure voice communication is achieved.

The design and implementation of an efficient and low complexity algorithm for providing secured speech transmission is being presented. It was shown through experimental results, that the principle of the proposed scheme is implemented with little complex hardware. Computer simulations indicate that the restored signal has good quality measurements.

For future enhancement to this application a new simple tool (Quick Basic) will be created and applied with Matlab encryption/decryption algorithm, where Matlab encryption/decryption algorithm interface with the encryption and a decryption buttons. Quick Basic is good software operated under Microsoft window because of the flexibility of this program's advanced features integration such as double clicks on the encryption/decryption buttons, the process of the encryption/decryption begins without need to see Matlab code, see appendix-b.

Simplicity and availability of these programs proves that they are a tool that can be used to fit the needs of any one to secure his audio data without the need to purchase expensive software from the market.

There are no limitations of the type of files accepted for encryption in this application, which means for future work any type of a file such as data files, audio files, video files or image files can be encrypted by the application. This is because all the files are encrypted at the binary level.

References

1. Markus Albert Brandau. "*Implementation of a real-time voice encryption system*", master thesis, Information Engineering,University of Applied Sciences Cologne. de Catalunya, EUETIT .2008.

2. Robert Richardson, 2008 CSI Computer Crime and Security Survey at 19. Online at http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf.

3. Samba Sesay, Zongkai Yang, Jingwen Chen and Du Xu." *A Secure Database Encryption Scheme*". Consumer Communications and Networking Conference, CCNC, pp.49 – 53, 2005.

4. Irma B. Fernandez, Candidate E, and Wunnava V. Subbarao. " *Encryption based Security for ISDN Communication: Technique & App.lication*". IEEE Southeastcon '94, pp.70 – 72, 1994.

5. F.Sheeja, and Mary." *Erratic Cryptosystem for Elevated Message Security*". Fourth International Conference on Information Technology, ITNG '07, pp.967 – 969, 2007.

6. Wikipedia, Human Voice, http://en.wikipedia.org/wiki/Human_Voice.

7. David G. W. Birch and Ian J. Shaw. " *Mobile Communications Security- Private or Public*". Security and Cryptography App.lications to Radio Systems, pp.5/1 - 5/6, 1994.

8. Lin-shan Lee, and Ger-chih Chou. "*Asynchronous Speech Encryption - Formulation and Simulation*". IEEE Military Communications Conference, MILCOM 1983, Volume 3, pp.791 - 795, 1983.

9. Praduemn K. Goyal and Eduardo B. Fernandez. " *Encryption using random keys-a scheme for secure communications* ". IEEE Aerospace Computer Security App.lications Conference, pp.410 - 412, 1988.

10. Min-sung Koh and Esteban Rodriguez-Marek.“ *A highly Adaptive Novel Symmtric Encryption Method Using The Sylvester Equation with An App.lication Example For Lossless Audio Compression*”. IEEE Military Communications Conference, MILCOM, Volume 3, pp.1891 – 1897, 2005.

11. Hongyu Lei, Yu Zhao, Yuewei Dai, and Zhiquan Wang.“ *A Secure Voice Communication System Based on DSP* ”.8th International Conference on Control, Automation, Robotics and Vision, ICARCV, Volume 1, pp.132 – 137, 2004.

12. Yucun Yang, Suili Feng, Wu Ye, and Xinsheng Ji.“*A Transmission Scheme for Encrypted Speech over GSM network*”. International Symposium on Computer Science and Computational Technology, ISCSCT '08, Volume 2, Pp.805 – 808, 2008.

13. Atef Mermoul and Adel Belouchrani. “*A subspace-Based Method for Speech Encryption*”.10th International Conference on Information Sciences Signal Processing and their App.lications, ISSPA, pp.538 – 541, 2010.

14. E. Mosa, Nagy.W .Messiha, and O. Zahran. “*Random Encryption of Speech Signal*”. International Conference on Computer Engineering & Systems, ICCES 2009, pp.306 – 311, 2009.

15. Gang Chen, and Bo Han. “ *An Audio Scrambling Degree Measure Based on Information Criteria*”. 2nd International Conference on Signal Processing Systems, ICSPS, Volume 1, pp.181 – 185, 2010.

16. H. Peyvandi, and S._J. Park. “*Security in Data Communication and Privacy in Converstions for Underwater Wireless Networks using Scrambled Speech Scheme*”. OCEANS 2011, pp.1 – 3, 2011.

17. Richard E. Blahut. “*Digital transmission of information*”. Addison-Wesley, pp. 479-501, 1990.

18. Henry J. Beker and Fred C. Piper. “ *Secure speech communications*”. Academic press, INC. London, pp. 227-237, 1985.

19. Martin, Luther. “ *Introduction to Identity-Based Encryption*. Artech House, 2008.

20. Majdi Al-qdah, and Lin Yi Hui. “*Simple Encryption/Decryption App.lication*”. International Journal of Computer Science and Security, IJCSS, Volume 1, pp.33 – 40, 2007.

21. Alister Burr. “*Modulation and coding*”. Pearson Education Limited, 2001.

22. Ankit Fadia, and Jaya Bhattacharjee. “*Encryption*”. Vikas publishing house pvt. ltd, pp. 1-18, 2007.

23. Andrew J. Viterbi, and Jim K. Omura. “ *Principles of digital communication and coding*”. Mc Graw-Hill, Inc, pp. 47-96, 1979.

24. E. Biglieri, and G. Prati. “ *Digital communications*”. *Elsevier Science Publishing Company*, Inc, pp. 3-21, 1986.

25. Borujeni,S.E.,and Nezhad,M.R.R. “*Voice privacy in wireless phone, mobile, communication by pseudo random number generator and tompkin-paig algorithm*”. International Symposium on Wireless Systems And networks, ISWSN'03, 2003.

26. C. J. Weinstein, J. W. Forgie, " *Experience with Speech Communication in Packet Networks,"* Communications- IEEE Journal, Volume 1, 1983.

27. D.W.Davies, and W.L.Price. “*Security for computer networks*”. John Wiley and Sons Ltd, 1989.

28. Dr.M.Mohamed Sathik, and A. Kalai Selvi.“*Secret sharing scheme for data encryption based on polynomial coefficient*”. IEEE International Conference on Computing Communication and Networking Technologies, ICCCNT, pp.1 - 5, 2010.

29. David L. Pepyne and Yu-Chi (Larry) Ho, and Qinghua Zheng.“ *SPRiNG: Synchronized Random Numbers for Wireless Security*”. IEEE Wireless Communications and Networking, WCNC 2003, Volume 3, pp.2027 – 2032, 2003.

30. Da-Peng Guo, and Qiu-Hua Lin. “*Fast Decryption Utilizing Correlation Calculation for BSS-based Speech Encryption System*”. Sixth International Conference on Natural Computation, ICNC, Volume 3, pp.1428 – 1432, 2010.

31. Gao Bingkun, Li Wenchao, and Hu Yue.“ *The app.lication research of Hyperchaos encryption in security communications*”. Control and Decision Conference, CCDC '09, pp.1278 – 1281, 2009.

32. http://www.enterprisenetworkingplanet.com/_featured/article.php/3792771/PGPs-Universal-Server-Provides-Unobtrusive-Encryption.html.

33. H. Nijmeijer, I.I. Blekhman, A.L.Fradkov, and A. Yu. Pogromsky.“ *Self-Synchronization and Controlled Synchronization*”. 1st International Conference on Control of Oscillations and Chaos, Volume 1, pp.36 – 41, 1997.

34. Howard M. Heys.“ *An Analysis of the Statistical Self-Synchronization of Stream Ciphers*”. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2001, Volume 2, pp.897 – 904, 2001.

35. John G. Proakis, and Masoud Salehi. “*Digital Communications*”. McGraw-Hill, 2008.

36. John Bellamy. “*Digital Telephony*. John wiley and sons, Inc, 1982.

37. Jing Dong and Tieniu Tan. “ *Security Enhancement of Biometrics, Cryptography and Data Hiding by Their Combinations*”. 5th International Conference on Visual Information Engineering, VIE 2008, pp.239 – 244, 2008.

38. Natasa ZIVIC, Obaid Ur REHMAN and Christoph RULAND. “*Analysis of Serial and Parallel Soft Input Decryption schemes over a Wireless Channel*”. International

Symposium on Performance Evaluation of Computer & Telecommunication Systems, SPECTS 2009, Volume 41, pp.282 – 288, 2009.

39. Paul A.Lynn, and Wolfgang Fuerst. “ *Introductory digital signal processing*”. John Wiley and Sons Ltd, 1998.

40. Raju Ramaswamy, " *A Key Management Algorithm for Secure Communication in Open Systems Interconnection Architecture*," Computers & Security – International Journal, Volume. 9, pp. 77-84,1990.

41. Sanjay Sharma. “*Digital communications*”. S.K.Kataria and Sons, pp.394-454, 2007.

42. T. M. Chen, J. Walrand, and D. G. Messerschmitt, *" Dynamic Priority Protocols for Packet Voice,"* Communications- IEEE Journal, Volume. 7, pp. 632-643, 1989.

43. W. Montgomery, *" Techniques for Packet Voice Synchronization,"* Communications- IEEE Journal, Volume1, pp. 1022-1028, 1983.

44. Yang Lu and Jiguo Li., and Junmo Xiao.“ *Forward-Secure Certificate-Based Encryption:Definition and Generic Construction*”. International Conference on E-Business and Information System Security, EBISS, pp.1 - 5, 2009.

APPENDICES

APPENDIX A- Terminology

A/D: Transform analog information, such as audio signals into a form suitable for digital handling, which might involve any of these operations: processing by a computer or by logic circuits, including arithmetical operations and code conversion.

PCM: Pulse - code modulation is a digital representation of an analog signal, in which the magnitude of the analog signal is sampled regularly at uniform intervals, with each sample being quantized to the nearest value within a range of digital steps.

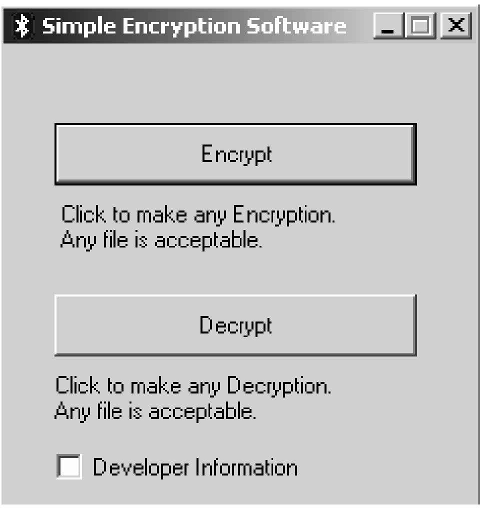
Plaintext: Is information a sender wishes to transmit to a receiver.

Ciphertext: Is the result of encryption performed on plaintext using an algorithm, called a cipher.

LFSR: Linear feedback shift register is a shift register whose input bit is a linear function of its previous state. The most commonly used linear function of single bits is the exclusive-or (XOR) of some bits of the overall shift register value.

PRNG: Peseudorandom number generator is algorithm that produces a sequence of bits that are uniquely determined from an initial value called a seed.

APPENDIX-B

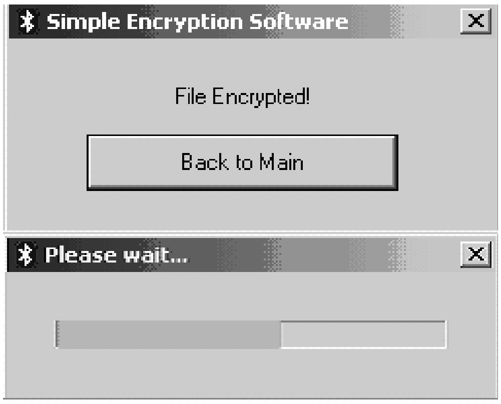


Click to make any Encryption.
Any file is acceptable.

Click to make any Decryption.
Any file is acceptable.

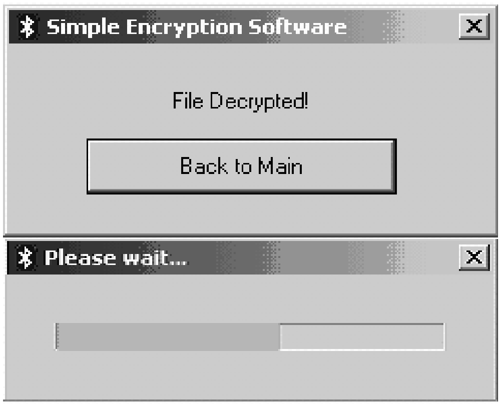
□ Developer Information

The Encryption/Decryption interface [20].



File Encrypted!

A successful encryption and the encryption progress bar [20].



File Decrypted!

Successful decryption and the decryption progress bar [20].

APPENDIX-C

Random Key Sequence Generated by a Fixed Coefficient Generator

$R(N)=(a.R(N-1)+b) \bmod n$

where a, b, and n are constants.

Random Key Sequence with Modified Dynamic Coefficients

$a(N)=f\,[a(N - l), R(N- 1),K]$

$b(N)=f\,[b(N - 1) , R(N - 1) , K]$

$R(N)=[a(N).R(N - 1) + b\,(N)] \bmod n$, K is a constant

The parameters a(N), and b(N) are continuously changing.

Multistage Random Key Generation with Feedback

$K\,(N) = [\, c(N-1) \,.\, K(N-1) + d\,(N-1)] \bmod n$

$c(N) = g\,[\, c(N - 1) , K(N- 1)]$

$d(N) = h\,[\, d(N – 1), K(N - 1)]$

The parameter K(N) is continuously changing, where K (N) will be used for generating the random sequences a (N) , and b(N) in the computation of the random key generator for R(N).

الملخص

مستريحي، هبه حكمت. التشفير باستخدام سلسلة متعاقبة من المفاتيح العشوائية -- مخطط لتأمين سرية انتقال البيانات الصوتية رسالة ماجستير بجامعة اليرموك.2012. (المشرف: الدكتور بسام حرب)

الملخص: الهدف من هذه الرسالة هو تحري طريقة اتصال آمنه بحيث تضمن اكبر قدر من السرية باقل تعقيد، تم مناقشة مخطط التشفير وفك التشفير الصوتي باستخدام طريقة المفاتيح العشوائية ، والتي تتضمن معدات وبرمجيات. المعدات هي التلفون والكمبيوتر،اشارة الصوت تُحمَل من مخرج الصوت في laptop الموصول مع التلفون. على الطرف الاخر، اشارة الصوت (اشارة الصوت المشفرة) المستلمة تُحمل الى laptop عن طريق وصلة بين مخرج الصوت في اللاب توب ومدخل الصوت في التلفون. وتمت برمجة نظام تشفير/فك التشفير للصوت باستخدام Matlab algorithmكتطبيق على البرمجيات، تشير نتائج تنفيذ البرنامج على الحاسوب ان الاشارة المسترده (اشارة الصوت بعد فك التشفير) تمتلك مقاييس عالية الجودة.

في هذه الرساله، قلب (اهم جزء) عملية التشفير هو توليد سلسلة رقمية عشوائية، المخطط المقترح يقدم طريقة بسيطة لتوليد سلسلة متعاقبة من المفاتيح العشوائية، هذه المفاتيح تستخدم مع كل جزء من اجزاء الرساله الصوتيه(rotation XOR operation and) النتيجه هي رساله صوتيه مشفره .قدم مخططين يتعلقان بطريقة توليد سلسلة متعاقبة من مفاتيح التشفير العشوائية. مفاتيح عشوائية متعاقبة مع معاملات ثابتة ، و مفاتيح عشوائية متعاقبة مع معاملات متغيرة.

كلمات البحث: نظام تشفير / فك التشفير للصوت، مولد الأرقام العشوائيه، مخزن خطي للتغذيه الراجعه، مفاتيح عشوائية متعاقبة مع معاملات ثابتة ، و مفاتيح عشوائية متعاقبة مع معاملات متغيرة.