ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Musical Cryptography Using Multiple Note Substitution Algorithm

Ajay Raghav [1], Baby John [2]

M. Tech Student, Department of Electronics and Communication Engineering, GISAT Engineering College, Kottayam, Kerala, India[1]

HOD and Professor, Department of Electronics and Communication Engineering, GISAT Engineering College, Kottayam, Kerala, India[2]

ABSTRACT: Music and its attributes have been used in cryptography from early days. Musical symbols and musical notes have been used as substitution cipher. The algorithms applied to musical cryptography use predefined set of notes and rules for the synthesis of musical patterns. The main task in the musical cryptography is to generate musical cryptograms which in turn are good sequence of musical patterns soothing to ear. The traditional methods used in musical cryptography limits the length of the plaintext to be encrypted. In this paper, a multiple note substitution algorithm is proposed to overcome the limitation to the number of letters in plaintext. The application of the algorithm produce cryptic message which not only hide the message as musical piece but it also reduces the chance of cipher message to be detected as cipher.

KEYWORDS: cryptography, musical cryptography, substitution cipher, symmetric key cryptography, plaintext, cipher text.

I. INTRODUCTION

In this era of digital word, the traditional communication has been transformed to digital communication with the use of Internet and its technologies. In the digital communication keeping message private is a serious issue to be addressed. To cope with this challenge cryptography is used in information security. Messages rather the information to be exchanged is generally in a specific language that we people use, anyone who understands the language can get the message. The messages to be transmitted are generally called as plain text message. Cryptography is the art of changing a plain text message into unintelligible or unreadable message. Figure 1.1 shows the simplified model of cryptography.

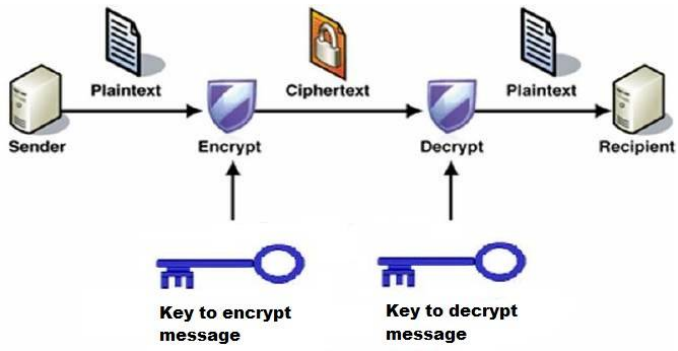

Figure 1.1: Simplified Model of Cryptography

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

As shown in Figure 1.1, cryptography uses an encryption algorithm to convert a plaintext message into cipher text and a decryption algorithm to convert the cipher text back into plaintext message. The encryption algorithm takes the plain text message along with the encryption key as input and converts the message into an unintelligible message known as cipher text as an output.The decryption algorithm takes cipher text message and the key used to decrypt the message.

Transposition and substitution are the simplest transformation that has been used from the very beginning of the cryptography. Transpositions shuffles or jumbles the letters of the plain text message depending on the pre-agreed manner, i.e. the first letter of the plain text message may be placed at the tenth position in the cipher text. Substitution algorithms substitute a particular character of messages with other character or symbols, a particular word may be replaced by another word; a prior mapping scheme is to be agreed in this type of system, this mapping may be encoded as a dictionary of words or table of alphabets or symbols.

Depending on the key used to encrypt and decrypt the cipher algorithms are categorized as symmetric key and asymmetric key algorithms. Symmetric key algorithm uses them same key to encrypt and decrypt the message, while the asymmetric key algorithm uses two different keys for encryption and decryption. Here a public key is used to encrypt the message while the private key is used to decrypt the cipher text. In context to the public key cryptography, public key is known to the public while private key is private to the receiver of the message.

Musical cryptography techniques convert the plain text message into musical notes or musical symbols. Musical cryptography uses music and its features to encode the message into a cipher message. The main task in the musical cryptography is to generate musical cryptograms which in turn are good sequence of musical patterns soothing to ear. The traditional methods used in musical cryptography limits the length of the plaintext to be encrypted. In this paper, a multiple note substitution algorithm based symmetric key cryptography is proposed to overcome the limitation to the number of letters in plaintext.The application of the algorithm produce cryptic message which not only hide the message as musical piece but it also reduces the chance of cipher message to be detected as cipher.

The remaining part of this paper is organized as follows:section 2 covers the literature review, section 3 describes about the cryptanalysis,section 4covers the proposed system, section 5 shows the simulation results and finally section 6 concludes this paper.

II. LITERATURE REVIEW

Cryptography is the transformation of readable data into a form which cannot be understood by any undesired persons in order to secure data. Information security is an important issue, for some applications such as ecommerce, e-banking, e-mail, medical databases, and so many more, all of them require the exchange of private information [1].

Main objectives of cryptography are: Confidentiality, Integrity, Authentication and Access Control [2].The two basic encryption techniques are substitution and transposition. In substitution technique letters of plaintext are replaced by other letters or by numbers or symbols. Transpositions shuffles or jumbles the letters of the plain text message depending on the pre-agreed manner [3] [4].

Based on the Key used cryptography algorithms can be classified as Symmetric Key Cryptography and Asymmetric Key Cryptography. In the symmetric key encryption, same key is used for both encryption and decryption process. Symmetric algorithms not consuming too much of computing power and it works with high speed in encrypt them. Asymmetric key encryption is the technique, in which the different keys are for the encryption and the decryption process. One key is public and second is kept private. Asymmetric cryptographic algorithms depend on very large complex mathematical computation, so it is considered as slow algorithm [5] [6].

The chance for malicious insertion and modification is higher in symmetric key cryptographic techniques. By analysing the traffic flow an intelligent attacker may decode the plain text and allows a counterfeit or new message that may look genuine to be placed in place of the original. The asymmetric key cryptographic algorithms involve large mathematical calculations and therefore the time complexities are quite high [7].

Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis. Some cryptanalysis techniques are Ciphertext-only attack, Known-plaintext attack, Chosen-plaintext attack, Man-in-the-middle attack, Correlation attack, Attack using the underlying hardware and Faults in

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

cryptosystems [8]. So two requirements for secure use of conventional encryption: strong encryption algorithm and a strong, secured key [9].

Music and musical attributes can be used cryptography. Use of music notes in encrypting any message is not in wide use. Dutta [8] in his work, 26 alphabets and 10 numbers are randomly positioned and then they are assigned with the numbers -12 to 23. These numbers have to be converted into vector and the MATAB function sound sends the signal in vector to the speaker available on a computer.

Yamuna [9] in her work, apply two levels of encryption. First convert a normal text into traditional Indian music note and then convert the text into western music notes. It uses two designing tables one for Conversion to Indian Musical Notes and another for Conversions to Western Musical Notes. These two tables will be the key for encryption and decryption.

Dutta [10] in his work converts the plain text message into a musical piece by substituting the text characters of the message by mathematically generated musical notes. A musical note consists of fundamental frequency, its amplitude (volume) and its shape. For a simple sound we can use a simple sine wave. The transition table serves as the encryption and decryption key where, a unique note is assigned to every cell. The generated musical sequence is then saved as a (.wave) file.

Kumar [11] in his work of musical cryptography for every character in the plaintext there will be more than one candidate notes. Then find the different combination of candidate notes for each character. The Genetic algorithm will find the best combination of the candidate notes. The musical notes are represented with octave and channel number.

Zad [12] in his work of automatic music composing using Genetic Algorithm considers entropy of the notes distribution as a factor of fitness function. The fitness function of this project plays a great role for accepting the best song

Entropy is a measure of the uncertainty of a random variable and gives the average amount of information contained in the transmitted message. It is a quantity based on the concept of probability of occurring a symbol in the transmitted message [13]

III. CRYPTANALYSIS AND ATTACKS ON CRYPTOSYSTEMS

Typically, the objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext.. There are two general approaches to attacking a conventional encryption scheme:

Cryptanalysis: Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

Brute-force attack: The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

If either type of attack succeeds in deducing the key, the effect is catastrophic: All future and past messages encrypted with that key are compromised.Figure 3.1 shows the Model of Symmetric Cryptosystem. The intruder can receive the ciphertext transmitted by the sender and either can make corrections in the ciphertext or simply read and given to the ciphertext. This is achievable either by observing the traffic, obtaing the key etc.

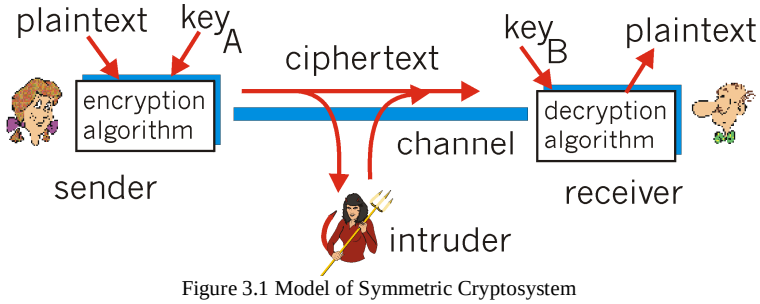

Figure 3.1 Model of Symmetric Cryptosystem

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Some of the cryptanalytic attack techniques are discussed below:

Ciphertext-only attack: In this case the attacker does not have any information about the original message, all information that the attacker has is the encoded text only. In such a scenario, the attacker makes an intelligent guess as to what can be the plaintext by guessing the fixed format headers. In the past, many attacks have been made by examining the frequency analysis of the ciphertext.

Known-plaintext attack: In this type of attack, the attacker either has a partial knowledge of what the plaintext is, or he can make a guess for some part of the plaintext. The remaining plaintext is obtained by this piece of information. The attacker can determine the key that has been used in the encrypting process and thus crack the code.

Chosen-plaintext attack: In this attack, the attacker attacks the encrypting device by sending any plaintext to the machine and then analyzing the encrypted output. Using a very intelligent reasoning, he can very well guess what the key used is and hence succeed in decoding the message.

Man-in-the-middle attack: A technique called packet sniffing is there which can assist the attacker in decoding any information. This is a process in which attacker machines on a network sniff the packets (capture the packet or the data streams) over a network. The sniffed packet can be used by the "man in the middle" to obtain the key(s) that two parties are sharing and thus he can very easily decode the entire message without either of the parties having information about this.

Correlation attack: This attack technique uses the stastical property of correlation between the input (the public key) and the output (the private key or the secret key). The obtained information is used to generate the function that is used in the encrypting process.

Attack using the underlying hardware: There can be an attack on the hardware also. Very intricate examination of the hardware yields characteristics such as the timings of the device, power consumption, radiation patterns etc. These characteristics can later be correlated to obtain the encrypting function. At times, the information can even yield the secret key.

Attack using Faults in cryptosystems: In this condition, there exists some fault in the cryptosystem which might have been the mistake of the programmer. Attackers can thus attack this shortcoming and obtain the necessary information regarding the encrypting function.

Brute-force attack: It involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

There are two requirements for secure use of conventional encryption:

1. Need a strong encryption algorithm.
2. Need a strong and secured key.

Strong encryption algorithm means, the opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key. The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.

IV. PROPOSED SYSTEM

Musical cryptography techniques convert the plain text message into musical notes or musical symbols. Musical cryptography uses music and its features to encode the message into a cipher message, the cipher message can be symbolic, verbal or instrumental .The main task in the musical cryptography is to generate musical cryptograms which in turn are good sequence of musical patterns soothing to ear. In this paper, a multiple note substitution algorithm based symmetric key cryptography algorithm is proposed to obtain an optimal sequence of musical patterns as a cipher message with no limitation to the length of plaintext.

The twelve chromatic notes used in Indian classical music are "Sa, re, Re, ga, Ga, ma, Ma, Pa, da, Da, ni, Ni". The ciphertextof the proposed system is a combination of these notes on a prescribed rule. The musical note Sa1.1 means the note Sa will be played in octave 1 and channel 1. Octave means a range of frequencies and the same note when played in different channel the amplitude will be different.

This cryptographic system use a symmetric key .The key is a matrix with 12 columns and 19 rows. Figure 4.1 shows the Key matrix used for encryption. In the figure each cell of the key has a numeric value, which represents the ASCII

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

values of letters, numbers and special characters. In the key matrix a single character is placed at a minimum of 2 and maximum of 3 cells. Thus we can have multiple notes to substitute for a letter. This type of arrangement is provided to give additional security to the cryptographic system. The row and column in which a letter appears decides which note should be played in which octave and channel. For example the ASCII code for the letter A is 65 and this appear in 3 cells, they are (3, 9), (11, 12) and (17, 1).So for the letter A in (3, 9) the note is da3.1, in (11, 12) the note is Ni3.5 and in (17, 1) the note is Sa7.3.

'Sa'	're'	'Re'	'ga'	'Ga'	'ma'	'Ma'	'pa'	'da'	'Da'	'ni'	'Ni'
[33]	[34]	[35]	[36]	[37]	[38]	[39]	[40]	[41]	[42]	[43]	[44]
[45]	[46]	[47]	[48]	[49]	[50]	[51]	[52]	[53]	[54]	[55]	[56]
[57]	[58]	[59]	[60]	[61]	[62]	[63]	[64]	[65]	[66]	[67]	[68]
[69]	[70]	[71]	[72]	[73]	[74]	[75]	[76]	[77]	[78]	[79]	[80]
[81]	[82]	[83]	[84]	[85]	[86]	[87]	[88]	[89]	[90]	[91]	[92]
[93]	[94]	[95]	[96]	[97]	[98]	[99]	[100]	[101]	[102]	[103]	[104]
[120]	[106]	[107]	[108]	[109]	[110]	[111]	[112]	[113]	[114]	[115]	[116]
[121]	[118]	[119]	[120]	[121]	[122]	[123]	[124]	[125]	[126]	[127]	[32]
[122]	[33]	[34]	[35]	[36]	[37]	[38]	[39]	[40]	[41]	[42]	[43]
[105]	[44]	[45]	[46]	[47]	[48]	[49]	[50]	[51]	[52]	[53]	[54]
[117]	[55]	[56]	[57]	[58]	[59]	[60]	[61]	[62]	[63]	[64]	[65]
[123]	[66]	[67]	[68]	[69]	[70]	[71]	[72]	[73]	[74]	[75]	[76]
[124]	[77]	[78]	[79]	[80]	[81]	[82]	[83]	[84]	[85]	[86]	[87]
[125]	[88]	[89]	[90]	[91]	[92]	[93]	[94]	[95]	[96]	[97]	[98]
[126]	[99]	[100]	[101]	[102]	[103]	[104]	[105]	[106]	[107]	[108]	[109]
[127]	[110]	[111]	[112]	[113]	[114]	[115]	[116]	[117]	[118]	[119]	[69]
[65]	[71]	[75]	[78]	[82]	[98]	[100]	[32]	[104]	[108]	[111]	[115]
[66]	[68]	[83]	[86]	[103]	[97]	[107]	[114]	[116]	[118]	[120]	[99]
[70]	[72]	[76]	[77]	[88]	[85]	[105]	[109]	[112]	[119]	[117]	[122]

Figure 4.1: Key matrix

Plain text message is the message to be encrypted, which can be a combination of letters, numbers and special characters. In the encryption section, at first all possible musical notes corresponding to each letters in the plaintext are found with the help of the key matrix. There is a minimum of two possible substitutions for a letter and maximum of three possible substitutions for a letter .Then combinations of each note are obtained. Even though there is more than one combination of musical note for the plaintext, only one combinations of musical note is used for the creation of ciphertext. The best combination of musical notes can be obtained by calculating the entropy of each combination and choosing the combination with highest entropy. Figure 4.2 shows the model of encryption section. From the figure it is clear that the inputs to the encryption are the plaintext and the key. Also the output of the encryption section is a media file which is very smoothing to the ear.

Entropy is a concept widely used in Information theory .Entropy calculates the average amount of information carried out in the transmitted message. It is a quantity based on the probability. As the assigned probability changes different combinations of musical notes are obtained for the same plaintext message. It is calculated as follows:

$$\text{Entropy, } H(x) = P(x) \times \log (1/P(x))$$

Where p(x) is the probability

In this cryptosystem unique probability is assigned randomly to each musical note in an octave and channel. This random assignment of probability provides additional security to the cryptosystem. Now the combinations of musical notes are converted into sine waves. The amplitude values of sine waves are restricted to the range [-1, +1], because Amplitude values outside the range [-1, +1] are clipped prior to writing. Now the ciphertext is represented as sine waves and the final ciphertext is obtained by writing these sine waves into media file using the MATLAB function wavwrite. This ciphertext can be transmitted to the receiver through email, as message in Facebook, through Bluetooth etc.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

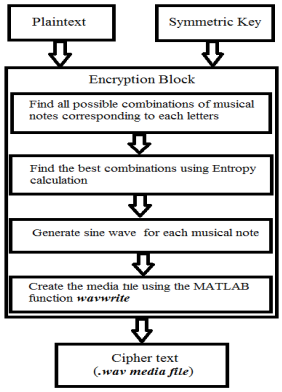

Figure 4.2: Model of encryption section

The encryption algorithm can be briefly described as:

1. Find all possible combinations of musical notes corresponding to each letters of the plaintext.
2. Find the best combinations of musical notes by finding the combinations of musical note with maximum entropy.
3. Generate unique sine waves corresponding to each musical notes of the best combination.
4. Create the media file using the inbuilt MATLAB function wavwrite.

The receiver receives the media file which is very smoothing to the ear. In the decryption section, at first the media file is converted into matrix using the MATLAB function wavread. The values in the matrix are the values of the sine waves. Then the amplitude and frequency of the sine waves are obtained.Figure 4.3 shows the Model of decryption section. From thefigure it can be seen that the input to the system are the ciphertext which is the media file and the key. Since the system is symmetric system the key used for encryption is given as the key in decryption. The output of the decryption section will be the original plaintext message transmitted.

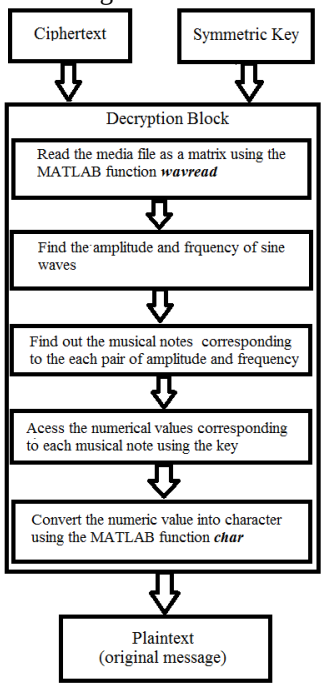

Figure 4.3: Model of decryption section

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

For finding the frequency of sine wave Discrete Fourier Transform is used. The values of the Fourier transform are sorted in the descending order. Index of the highest Fourier is used to calculate the frequency. The MATLAB code for finding the frequency is given below.

Let s be the variable containing the values of sine waves

```
dft=fft(cell2mat(s));
[a,index] = sort (abs (dft),'descend');
b=index (1);
Fs = 1000;
freq=((b-1)/100)*Fs;
```

freq is the variable containing the frequency

Fs is the sampling frequency

For finding the amplitude of sine wave the values of the matrix are sorted in the descending order. The first value in the sorted matrix is the amplitude of the sine wave, The MATLAB code for finding the amplitude is given below.

Let s be the variable containing the values of sine waves

```
[a,x]= sort (cell2mat(s)'descend');
g=a (1)*10;
amp =int64(g);
```

amp is the variable containing the amplitude

Now using the amplitude and frequency the corresponding musical notes are found out. Using these musical notes the row and column represented by key matrix is obtained. By using the row and column a numerical value can be accessed from the key matrix, which represents an ASCII value of an alphabet, number or special character. When converting the numerical value into character using the MATLAB function char the original plaintext will be obtained.

The decryption algorithm can be briefly described as:

1. Convert the media file received into matrix of values between -1 and 1.
2. Find the amplitude and frequency of the sine wave with the help of Fourier transform.
3. Find out the musical note corresponding to each pair of amplitude and frequency.
4. Access the ASCII value from the key matrix using the musical note.
5. Convert the numerical value into character or letter or special character using the MATLAB function char
6. The character text obtained from the above step is the original message transmitted

IV. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed algorithm was implemented in MATLAB. In the encryption section the text which is to be transmitted is read from the user. Consider the following example

Plaintext message is: **Hello**

The possible musical notes for **H**:

ga4.1 pa3.5

The possible musical notes for **e**:

da6.1 ga5.5

The possible musical notes for **l**:

ga7.1 ni5.5 Da7.3

The possible musical notes for **l**:

ga7.1 ni5.5 Da7.3

The possible musical notes for **o**:

Ma7.1 Re5.7 ni7.3

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

The possible combinations of musical notes are:

ga4.1	**da6.1**	**ga7.1**	**ga7.1**	**Ma7.1**
ga4.1	**ga5.5**	**ni5.5**	**ni5.5**	**Re5.7**
ga4.1	**NONAL**	**Da7.3**	**Da7.3**	**ni7.3**
pa3.5	**da6.1**	**ga7.1**	**ga7.1**	**Ma7.1**
pa3.5	**ga5.5**	**ni5.5**	**ni5.5**	**Re5.7**
pa3.5	**NONAL**	**Da7.3**	**Da7.3**	**ni7.3**
NONAL	**da6.1**	**ga7.1**	**ga7.1**	**Ma7.1**
NONAL	**ga5.5**	**ni5.5**	**ni5.5**	**Re5.7**
NONAL	**NONAL**	**Da7.3**	**Da7.3**	**ni7.3**

NONAL means No Notes Available

Ciphertext message is:

ga4.1ga5.5ni5.5ni5.5Re5.7

In the decryption side the name of the received media file is obtained from the user. The decryption for the above transmitted ciphertext is given below.

Enter the name of the media file:**music file**

Frequency:

21604320624062404000

Amplitude:

6 8 8 89

Music ciphertext:

ga4.1 ga5.5ni5.5ni5.5 Re5.7

Accessed value from key matrix:

72 101 108 108111

Character corresponding to accessed value:

H e l lo

The Decrypted message is:

Hello

By implementing the proposed algorithm in MATLAB and by stimulating the code for encryption and decryption the transmitted massage is successfully decrypted.

This cryptosystem do not put any restriction to the length of the message to be transmitted securely. This is a great achievement of this cryptosystem. Figure 5.3 shows the Encryption and Decryption time comparison. From the figure it is clear thatthe time required for encryption is somewhat higher than the time required for decryption. This is because of the fact in the encryption side the number of functions are higher. Also as the length of the message increases the both the encryption and decryption time goes on increasing.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

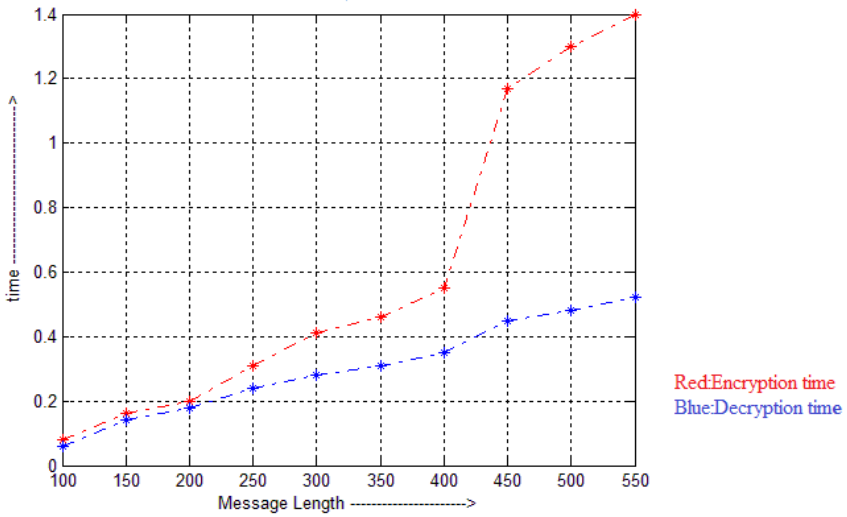

Figure 5.3 Encryption and Decryption time comparison

The received music file is very smoothing to the ear. Anyone who receives the file can listen the music, but do not get any idea of the message behind it. For getting any idea about the message he/she want to know the frequency, amplitude and the key matrix. Thus it provides high level of security to the transmitted message. The resultant musical piece is hard to break as the key is usually like a one-time pad and guessing or producing the key is nearly impractical. The proposed algorithm does not use any cover file to hide the message so there is no such payload problem as happens with steganography. Steganography techniques which generally use least significant bits or the control messages for the replacement; rather the proposed algorithm generates musical notes for each character on its own.

VI. CONCLUSION

Music is like a language. Hiding messages in music makes it a private cipher language. The application of multiple note substitution algorithm based symmetric key musical cryptography produce cryptic message as musical piece which are smoothing to ear and don't felt to be created artificially. The resultant musical piece is hard to break as the key is usually like a one-time pad and guessing or producing the key is nearly impractical. Also the proposed algorithms do not put any limitation to the number of letters in plaintext. The application of the algorithm produce cryptic message which not only hide the message as musical piece but it also reduces the chance of cipher message to be detected as cipher Thus the cryptosystem using genetic algorithm allows a very strong secure communication with less chance for trying to eavesdropping the communication.

A better cryptic algorithm is demanded in future, which may generate musical sequence as real world music and with less encryption and decryption time.

REFERENCES

[1] Mohammed AbuTaha, MousaFarajallah, RadwanTahboub and Mohammad Odeh, "Survey Paper: Cryptography Is The Science Of Information Security," International Journal of Computer Science and Security (IJCSS), Volume (5): Issue (3): 2011.
[2] Rajdeep Bhanot1 and Rahul Hans," A Review and Comparative Analysis of Various Encryption Algorithms", International Journal of Security and Its Applications Vol. 9, No. 4 (2015).
[3] Anupama Mishra, "Enhancing security of caesar cipher using different methods", International Journal of Research in Engineering and Technology", Volume: 02 Issue: 09 Sep-2013
[4] William Stallings, "Cryptography and network security principles and practice", 5th edition
[5] RituTripathi and Sanjay Agrawal, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques" International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 6, June 2014.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

[6] Omar M.Barukab, AsifIrshad Khan, MahaboobShariefShaik and MV Ramana Murthy, "Secure Communication using Symmetric and Asymmetric Cryptographic Techniques," I.J. Information Engineering and Electronic Business, 2012.
[7] Swapna B Sasi, Dila Dixon, Jesmy Wilson," A General Comparison of Symmetric and Asymmetric Cryptosystems for WSNs and an Overview of Location Based Encryption Technique for Improving Security", IOSR Journal of Engineering (IOSRJEN) Vol. 04, Issue 03 (March. 2014)
[8] SandipDutta ,SoubhikChakraborty and N.C.Mahanti, "A Novel Method of Hiding Message Using Musical Notes", International Journal of Computer Applications Volume 1 – No. 16 2010
[9] M. Yamuna, Krishna Pandey and Nikhil Choudhary, "Cryptography using music notes", Journal of Global Research in Computer Science, 4 (4), April 2013, 100-102.
[10] SandipDutta, Chandan Kumar and SoubhikChakraborty, "A Symmetric Key Algorithm for Cryptography using Music" International Journal of Engineering and Technology (IJET) Vol 5 No 3 Jun-Jul 2013
[11] Chandan Kumar, SandipDutta and SoubhikChakborty, "Musical Cryptography using Genetic Algorithm", International Conference on Circuit, Power and Computing Technologies 2014.
[12] Damon DaylamaniZad ,Babak N. Araabi and Caru Lucas," A Novel Approach to Automatic Music Composing Using Genetic Algorithm"
[13] Thomas M. Cover and Joy A. Thomas," Elements of information theory" John wiley& sons publication, Second Edition, 2006