Genetic Algorithm Based Cryptographic Approach Using Karnatic Music

Surya .S[1], Muhammad Ilyas .H[2]

[1]*PG Scholar, Dept. of Computer Science and Engineering, College of Engineering Cherthala, Kerala, India*
[2]*Assistant Professor, Dept. of Computer Science and Engineering, College of Engineering Cherthala, Kerala, India*

Abstract -*Music and its attributes have been used in different area of world. Music can be used as a language communicable. Music notes have been used in the field of stenography and cryptography in early days. A piece of data is hide within a musical note and send to the destination. Musical symbols and musical notes have been used as the substitution cipher. The main goal of the musical cryptography is to generate different musical cryptograms. In this paper a Genetic Algorithm based symmetric key musical note generation is used to obtain the optimum solution. The application of Genetic Algorithm for producing cryptic message doesn't only hide the message as musical piece but it also reduces the chance of cipher message to be detected as cipher.*

Key Words: **Musical Cryptography; Genetic Algorithm; raga Analysis; Encryption and Decryption.**

1. INTRODUCTION

In this era of digital world, with the use of Internet and its other technologies our traditional communication has been converted into digital communication. In this digital era, keeping message secret is a major issue to be addressed. To cope with this challenge cryptography is used in information security. The messages rather information to be transmitted to destination generally we people use specific language for the transmission. Their ultimate goal is anyone who doesn't understand the piece of information they hide. The message to be transmitted is generally called as plain text message. Cryptography is the art of changing the text or data into a coded format or any other encrypted form [1],[2].

A cryptographic approach use two algorithm: encryption Algorithm for encrypts the data into corresponding coded format and a decryption algorithm which transforms the coded message into its original message. The basic idea of cryptography approach is to apply transformations to the plain text and such that the message no longer remains intelligible to an intruder without applying the reverse transformation. These transformations are based on some permutation and combinatorial or any other mathematical transformation. Transposition and substitution that has been used from the very beginning stage of 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 on the tenth position in the cipher text. Substitution algorithm substitutes a particular character of messages with other characters or symbols. i.e. a particular word is replaced by another word.

Depending on the key used to encrypt and decrypt the cipher algorithms are categorized as symmetric key and asymmetric key algorithms. Symmetric key algorithms use the same key for encryption and decryption process. Asymmetric Key algorithm uses different key for encryption and decryption. Symmetric Key is also known as private key cryptography a secret key is being agreed upon prior transfer of messages, depending on the key the sender side encrypts the message and receiver side decrypts the message. In this paper, Musical cryptography concepts convert the plain text message into musical notes or musical symbols. In musical cryptography music and its attributes to encode the plain text into its corresponding cipher text. The cipher messages can be symbolic, verbal or instrumental notes. All applications of stegnography such as Invisible links and Microdots are applicable here.

2. RELATED WORKS

Music and musical attributes has been used in early days of cryptography. The data's are encode in the form of musical notations. Eric Sam's [5] in his article has mentioned that many of the cryptologists were notable musicians. Many composers used to hide messages in their musical compositions; Elgar and Schumann are one of them. Schumann used a three lines eight notes cipher system which was derived from Klubers work. Elgar and Schumann are one of them. Hooper and Kluber [7] used a cipher wheel to encrypt messages using musical notes.

Tractus varii medicinal [5] used five different pitches in five different ways to produce 25 symbols to make an alphabetic cipher. Each of the pitches taken by Tractus had a certain notation and a stem direction. Athanius Kircher [8] a polymath gave an idea of using orchestra in musical cryptography. Kircher used six different instruments with four notes from each to encode 26 letters.

Dutta et al [6] have used 36 numbers by taking twelve musical notes each from three different octaves and encrypted the plain text message using musical notes. Dutta et al [7] in his work was able to encrypt 26 character literals and 10 numerals. Dutta et al [6] have used Indian raga Raga Malkhauns, where they have first found the transition probabilities for transition of musical notes and used the transition probability to encrypt the message.

MIDI was developed for the communication of digital Instruments and it is a Digital Interface standard established in 1983. MIDI has instructions and commands which are sent to the devices for the playback of musical notes. MIDI files [11] contain MIDI streams and MIDI commands. A standard MIDI file can contain more than one MIDI stream along with time information for each of the MIDI events. MIDI file have song, sequence, tempo and time signature information. Each note in a MIDI contains the following data structure.

The onset tells the time a particular note starts to play. Onset time is provided in Beats and Seconds. The duration tells us about how long the note will play. Midi channel denotes the channel number in which the note will play. It has 16 channels or octaves in which musical notes can be played simultaneously. Sa, re, Re, ga, Ga, ma, Ma, Pa, da, Da, ni, Ni are the twelve chromatic notes used in Indian classical music whose corresponding western notation is" CDbDEbEFGAbABbB". The velocity tells that how loud or soft a particular note will play.

3. PROPOSED WORK

The proposed work deals with the encryption and decryption process within the help of musical notes. Here the data is hiding with in the musical notes such as candidate notes and send to the receiver side. Here a plain text and a transition table or transition matrix are available in the sender side. First process done here is creating a transition probability matrix based on a particular raga. We are here to choose raga sankarabharanam. Select some musical notes based on these ragas and count the probability from one note to another note and take the total probability from each row and represented into a matrix form. Then represent it into a state diagram. Here states are swara's. We are here to select 12 swaras and which are sates of the state diagram. Then apply Bayesian probability approach we will get the exact probability matrix of the rendering raga. Then generate candidate notes of the message and apply GA and we will choose a cut of value and value below the fitness are selected as the best music. Finally we get one gene for the best music then map the each gene with corresponding transition table letter we get the exact plain text message.

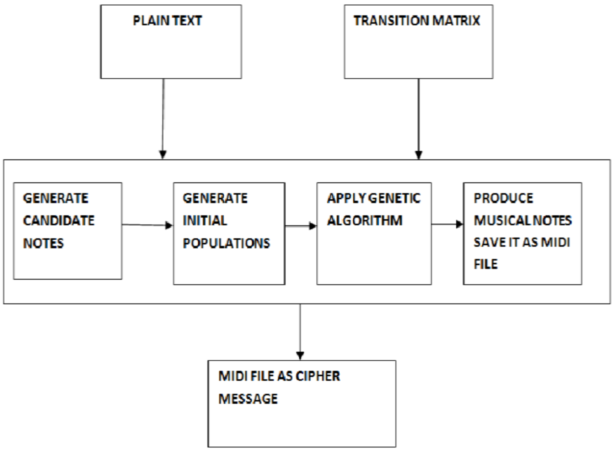

PLAIN TEXT
TRANSITION MATRIX
GENERATE CANDIDATE NOTES
GENERATE INITIAL POPULATIONS
APPLY GENETIC ALGORITHM
PRODUCE MUSICAL NOTES SAVE IT AS MIDI FILE
MIDI FILE AS CIPHER MESSAGE

Fig-1: System Model of Encryption Process

3.1. Sender Side Processing

The sender side processing means encryption technique is doing here. The secret data is hiding within a piece of musical notes and that to be thrown to the destination side. A plain text is needed for the encryption process which is to be converted into the corresponding cipher text after the encoding process. Here a transition matrix is used as a key matrix. In this paper, we generate the transition matrix with the help of Karnatic Raga 'Sankarabharanam'.The candidate notes are generated by using the transition table. The generation of transition table [3] is described below section. Randomly select each candidate notes and assign each one to corresponding data in the plain text. Calculate the cross products of the generated candidate notes, as a result, we collect huge amount of data sets. These data sets are the initial population of our genetic algorithm. Selection, Crossover and Mutation are the main three operations of the Genetic Algorithm. Which are to be used here with the initial population. The encrypted note or encoded note is save it as a MIDI file which is the cipher text.

3.2. Encryption Algorithm

***ALGORITHM: INPUT** (plain text message, transition Table/ key matrix **OUTPUT** (Musical Sequence)*

Step 1: Select the transition table of swaras.

Step 2: Assigns the first seven characters into the first octave.

Step 3: Assigns the next seven characters into the next octave and so on.

Step 4: Select the character to be encoded from the octaves and find the swara corresponding to that particular letter.

Step 5: Encrypt the letter with candidate notes

Step 6: Obtain the final musical sequence as encrypted message.

3.4. Receiver Side Process

The encrypted musical note is decoded in the receiver section. The decryption will be done simply by searching the tones in the transition table starting with the first note in the selected start row. The second and so on notes will be found as the transition of last character to the present note by reverse engineering the determination of candidate notes in the encryption process.

***ALGORITHM: INPUT** (cipher text message, transition Table/ key matrix **OUTPUT** (plain text)*

Step 1: Select the transition table of swaras.

Step 2: Determine the notes (genes) from the encrypted message.

Step 3: Select the first gene from the encrypted message and identify which row contains that gene in the transition table.

Step 4: The above note is mapped with the letter to be decrypted.

Step 5: Plain text is generated

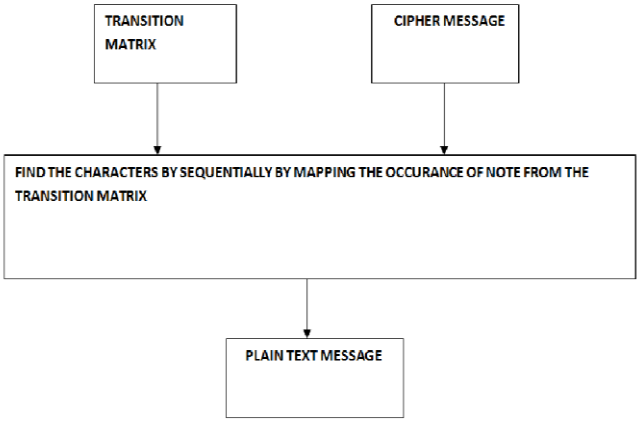
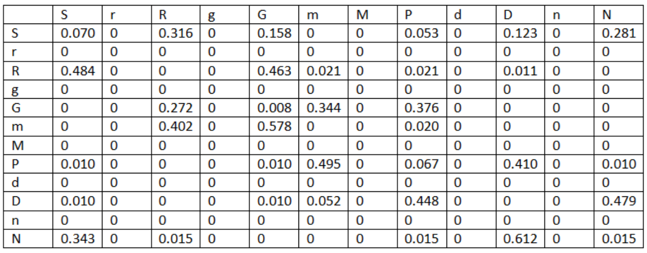

TRANSITION MATRIX
CIPHER MESSAGE
FIND THE CHARACTERS BY SEQUENTIALLY BY MAPPING THE OCCURANCE OF NOTE FROM THE TRANSITION MATRIX
PLAIN TEXT MESSAGE

Fig-2: System Model of Decryption Process

3.5. Generation of Transition Matrix and Transition Table

We represented each raga in the form of a matrix that quantified the transitions between the swaras, which represents as Transition Probability Matrix (TPM). Narayan Srinivasan [3] explains it in Hindustani raga representation. Here, we lost some information's about the octave where the musicians preferred to sing or play certain combination of swaras. We were able to find out the transitions from one swara to another swara which was our primary interest irrespective of the octave information. To create the matrix, we considered all 12 swaras of Karnatic music scale even though rarely any raga uses all 12 swaras. A typical transitional probability matrix for the notes of a raga Sankarabharanam using all the twelve natural notes is given below Fig.3.

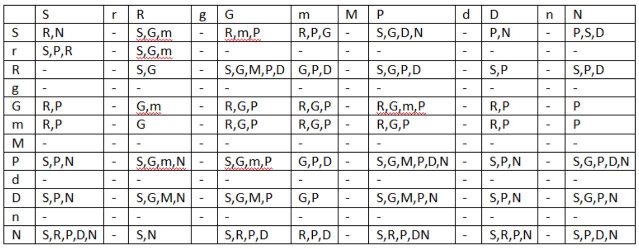
After created a corpus of swaras transcribed from each raga, we determined how often any one particular swara was followed by another swara by counting the exact number of transitions from one swara to the other swaras. We repeated this procedure for all 12 swaras such that we calculated the frequency of transitions from every swara to each of the 12 swaras, which included transition to the same swara too. We then divided that number by the sum of all the transitions originating from any one particular swara. This depicted the probability of appearance of a swara conditioned on the transition originating swara.



	S	r	R	g	G	m	M	P	d	D	n	N
S	0.070	0	0.316	0	0.158	0	0	0.053	0	0.123	0	0.281
r	0	0	0	0	0	0	0	0	0	0	0	0
R	0.484	0	0	0	0.463	0.021	0	0.021	0	0.011	0	0
g	0	0	0	0	0	0	0	0	0	0	0	0
G	0	0	0.272	0	0.008	0.344	0	0.376	0	0	0	0
m	0	0	0.402	0	0.578	0	0	0.020	0	0	0	0
M	0	0	0	0	0	0	0	0	0	0	0	0
P	0.010	0	0	0	0.010	0.495	0	0.067	0	0.410	0	0.010
d	0	0	0	0	0	0	0	0	0	0	0	0
D	0.010	0	0	0	0.010	0.052	0	0.448	0	0	0	0.479
n	0	0	0	0	0	0	0	0	0	0	0	0
N	0.343	0	0.015	0	0	0	0	0.015	0	0.612	0	0.015

Fig-3: Transition Probability Matrix of Raga

The transition table is the key matrix of our system. These are generated from the above created transition matrix. Transition table [3] contains different candidate notes. A particular note is assigned with different candidate note according to their probability. The highest probability notes are to be selected from different octaves. The below figure shows the transition table for the given raga.



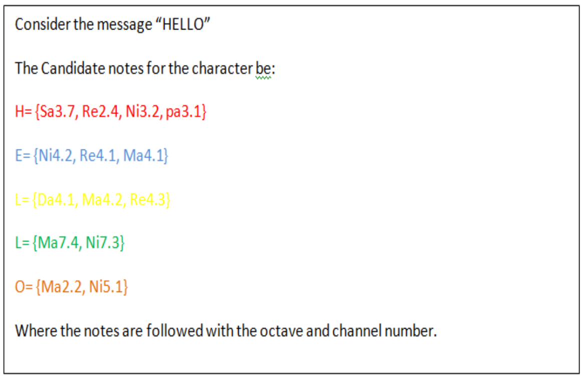
	S	r	R	g	G	m	M	P	d	D	n	N
S	R,N	-	S,G,m	-	R,m,P	R,P,G	-	S,G,D,N	-	P,N	-	P,S,D
r	S,P,R	-	S,G,m	-	-	-	-	-	-	-	-	-
R	-	-	S,G	-	S,G,M,P,D	G,P,D	-	S,G,P,D	-	S,P	-	S,P,D
g	-	-	-	-	-	-	-	-	-	-	-	-
G	R,P	-	G,m	-	R,G,P	R,G,P	-	R,G,m,P	-	R,P	-	P
m	R,P	-	G	-	R,G,P	R,G,P	-	R,G,P	-	R,P	-	P
M	-	-	-	-	-	-	-	-	-	-	-	-
P	S,P,N	-	S,G,m,N	-	S,G,m,P	G,P,D	-	S,G,M,P,D,N	-	S,P,N	-	S,G,P,D,N
d	-	-	-	-	-	-	-	-	-	-	-	-
D	S,P,N	-	S,G,M,N	-	S,G,M,P	G,P	-	S,G,M,P,N	-	S,P,N	-	S,G,P,N
n	-	-	-	-	-	-	-	-	-	-	-	-
N	S,R,P,D,N	-	S,N		S,R,P,D	R,P,D	-	S,R,P,DN	-	S,R,P,N	-	S,P,D,N

Fig-4: Transition Table /Key Matrix

3.6. Genetic Algorithm For Selection Of Best Music

The Genetic Algorithms (GAs) [20],[21] are exploration Algorithms based on the theory of natural selection with an inventive finesse of nature. The genetic algorithm consists of mainly three operators: selection, crossover, and mutation. The selection operators select the appropriate data satisfied with our constraints. After that the crossover and mutation process performed. The pairing operation is crossover and substitution operation is mutation.

Genetic algorithm starts with an initial population. The initial population holds the chromosomes, where each chromosome represents a possible solution. Each chromosome is associated with a fitness value, which represents the quality of the solution. Then chromosomes from the initial population are selected for crossover and mutation. After the crossover and mutation new chromosomes are generated which are now subjected to a fitness function. If the newly generated chromosomes pass the fitness test the chromosomes are added to the population and the old chromosomes are discarded. After every generation the number of chromosomes in the population remains same, to accomplish this chromosomes least fitness value are killed. The stopping criteria of Genetic Algorithm are generally either the maximum no of iterations reached or the satisfactory fitness value is reached. The chromosome with the maximum fitness value from the population is taken as the best solution.



Consider the message "HELLO"

The Candidate notes for the character be:

H= {Sa3.7, Re2.4, Ni3.2, pa3.1}

E= {Ni4.2, Re4.1, Ma4.1}

L= {Da4.1, Ma4.2, Re4.3}

L= {Ma7.4, Ni7.3}

O= {Ma2.2, Ni5.1}

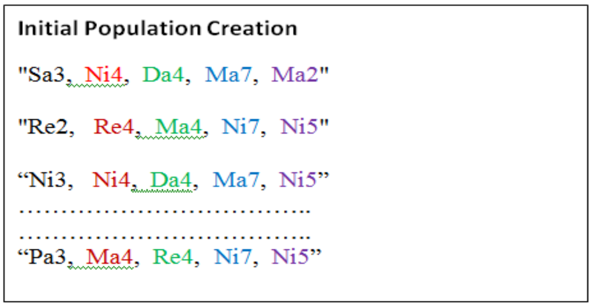
Where the notes are followed with the octave and channel number.

Fig-5: Candidate Note Selection

In this paper, the initial populations are generated by selecting the candidate notes from the transition table. After that taking the cross product of the selected candidate notes. Finally we gave huge set of candidate notes, which are the initial population of our genetic algorithm. All these cross products are same as our encrypted message i.e, music. So we want to select the best music fro the population. So, we performed the crossover and mutation process. Finally we will get the filtered music. That is the best encrypted music. Which are to be decrypted by the help of transition table. Finally we get the corresponding plain text. The fitness functions are generated by using the equation:

$$\Sigma_{i=1}^{n} x_i \leq n$$

$$S_x \leq n$$



Initial Population Creation

"Sa3, Ni4, Da4, Ma7, Ma2"

"Re2, Re4, Ma4, Ni7, Ni5"

"Ni3, Ni4, Da4, Ma7, Ni5"

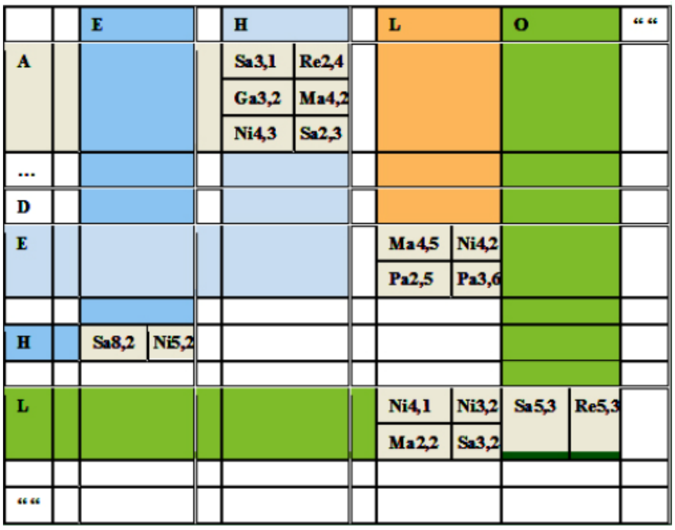
…………………………………..

…………………………………..

"Pa3, Ma4, Re4, Ni7, Ni5"

Fig-6: Creation of Initial Population

The Message HELLO is encrypted and corresponding Transition table generated from the raga rendering table of Raga Sankarabharanam. These transition table is the key matrix for both sender and receiver and also a seed value is generated which is generated by using a pseudo random generator. The seed value is different for each transmission of data.



		E		H		L	O	" "
A				Sa3,1 Re2,4 Ga3,2 Ma4,2 Ni4,3 Sa2,3				
...								
D								
E						Ma4,5 Ni4,2 Pa2,5 Pa3,6		
H		Sa8,2 Ni5,2						
L						Ni4,1 Ni3,2 Ma2,2 Sa3,2	Sa5,3 Re5,3	
" "								

Fig -6: Transition Table of Encrypted message

3.7. Working of Genetic Algorithm for Selection of Best Music

ALGORITHM: INPUT (plain text message, transition Table/ key matrix **OUTPUT** (Musical Sequence)

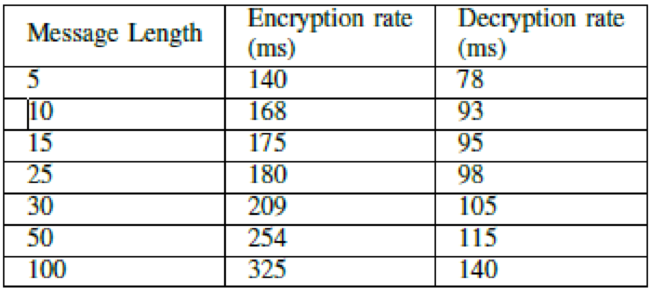
```
Step 1:  Generate the transition matrix.
Step 2:  Determine the candidate notes for each character of plain text and initialize the population for GA
Step 3:  For each window do following:
         1) Generate a total of n number of musical sequence as initial population for the window frame, where n is the total population size.

         2) Do the following until the termination criteria reached:
                  a) Select multi chromosomes from the Population.

                  b) Apply crossover operator on selected population

                  c) Perform mutation operator on the features velocity, duration and tempo

                  d) Calculate fitness value of successor Population

                  e) If fitness (Parental Chromosome) less than or equal to fitness (Child Chromosome), then add child chromosome else add parental Chromosome into the population.
.
                  f) If (maximum iteration reached), then select the fittest multi-chromosome and add it at the end of final musical sequence else, iteration=iteration+1.

Step 4: Obtain the final musical sequence as encrypted message.
```

4. EXPERIMENT RESULTS AND ANALYSIS

The proposed work was implemented in JAVA Net beans. At first the transition table was generated. A genesis rule was provided depending on the transitional probabilities of notes. Candidate musical notes were used to generate the initial population for the genetic algorithm. Depending on the transition of characters the candidate notes were provided to the genetic algorithm for proper synthesis and sequencing. The genetic algorithm has to do the proper selection, mutation, crossover and sequencing of the musical notes. The runtime of the algorithm basically depended on the complexity of the selection, mutation and crossover of the chromosomes. The no of iterations and the fitness function had an important role to play. It was found that greater the no. of iterations threshold value for the fitness function the generated musical piece was more realistic. The proposed work is more efficient than existing work, because the different permutations of raga are to be generated at each instant of data transferring. So, intruders cannot detect or guesses the data.

The time complexity of an algorithm represents the amount of time taken by an algorithm to run as a function of the length of the string representing the input. The time complexity of an algorithm is commonly expressed using big O notation, which excludes coefficients and lower order terms. Here, the encryption and decryption rate is measured on the basis of length of the message to be encrypted. As the length of message increases, the encryption and decryption rate also increases.

Table- 1: Performance Analysis of Time Complexity



Message Length	Encryption rate (ms)	Decryption rate (ms)
5	140	78
10	168	93
15	175	95
25	180	98
30	209	105
50	254	115
100	325	140

Cryptanalysis is the study of ciphers, cipher text, or crypto systems or secret code systems with a view to finding weaknesses in them that will permit retrieval of the plain text from the cipher text, without necessarily knowing the key or the algorithm. This is known as breaking the cipher, cipher text, or crypto system. There are numerous techniques for performing cryptanalysis, depending on what access the cryptanalyst has to the plain text, cipher text, or other aspects of the crypto system. Below are some of the most common types of attacks:

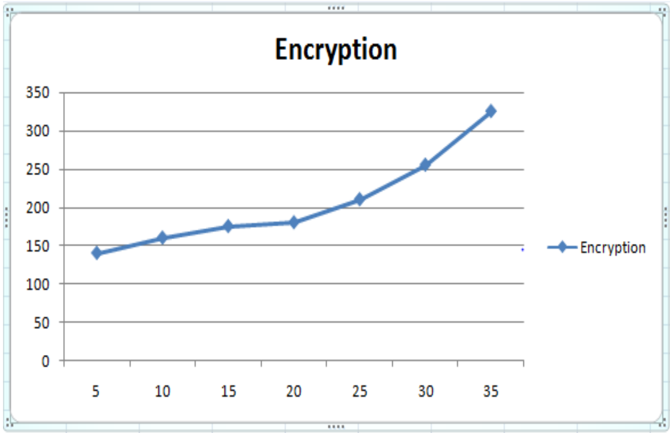


Fig -7: Encryption Rate

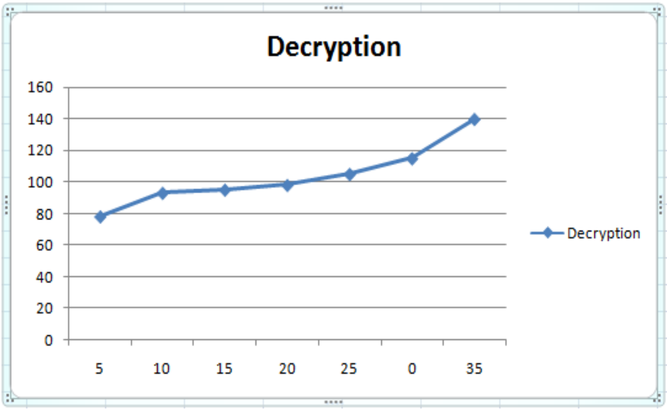


Fig -8: Decryption Rate

4.1. Brute force Attack

Brute force also known as brute force cracking is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort using brute force rather than employing intellectual strategies. Here the total 32 characters are used for the encryption process. So we get total of 32 permutations of characters or combinations. Therefore the whole combination of characters:

The factorial of 32 is 2.631386×10^{35} it will be divided by with 3600 seconds and again divided by this value with 24 hours and finally this will be divided with 365 days and finally we get whole combination. Therefore the brute force attack is not possible here.

4.2. Man in Middle Attack

In computer security, a man in the middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. We need a key exchange algorithm for transmission of seed value. Use any efficient key exchange algorithm for this purpose. The threat of man in middle attack depends on this key exchange algorithm. How strong is the key exchange our system will also secure from the man in middle attack. Even if the attack is happen the intruder can only attack on a particular cipher text because, seed value will exchange with each session. So, the man in middle attack is not possible in the proposed system.

5. CONCLUSIONS

In this paper we proposed a work such as security using music. Here a data is hide within the music and transmitted to the destination. Even though the musical piece doesn't sound natural and is guessed to have message encrypted in it, it is hard to get the message without the key used to decrypt the message. So using musical language it is possible to encrypt the message. The permutation and combinations required to decrypt the message makes it nearly impossible provided the intruder doesn't have the key.

ACKNOWLEDGEMENT

We would like to thank those who supported for the Completion of our work

REFERENCES

Khan,David," The Code Breakers: The Comprehensive histoty of Secret Communication From Ancient Times To The Internet ", 1996.

AbuTaha, M., Farajallah, M., Tahboub, R., Odeh," Survey Paper: Cryptography is the Science of Information Security" International Journal of Computer Science and Security (IJCSS), 1992 Vol.5.

Narayan Srinivasan," Hindustani Raga Represenatation and Identification: A Transition Probability based approach"(AAAI), 2012.

Davies. D, "A brief history of cryptography", Information Security Technical Report, Vol. 2, No. 2, 1997, pp.14-17, 2008.

Sams, Eric, "Musical Cryptography", CRYPTOLOGIA, Vol. 3, No.4, pp.193-201., 1979.

Dutta S, Chakraborty S, Mahanti N.C,"A Novel method of hiding messages using musical notes" International Journal of Computer applications, vol.1, No.16, 2010.

Dutta S, Chakraborty S, Mahanti N.C,"Using raga as a Cryptographic tool", Advances in Network Security and Applications, Communications in Computer and Information Science, Volume, 196,(Springer).,2011.

Dutta, Sandip, Chandan Kumar, and Soubhik Chakraborty,"A Symmetric Key Algorithm for Cryptography Using Music", International Journal of Engineering and technology, Vol.5, No.3, pp. 3109-3115., 2013.

M. Yamuna ,Sankar A., Ravichandran S., V. Harish, "Encryption of a Binary string using Music notes and Graph theory", International Journal of Engineering and Technology, Vol.5, No.3, pp. 2920-2925, 2013.

Yamamoto, Kotaro, and Munetoshi Iwakiri, "A Standered MIDI file steganography based on fluctuation of duration",International Conference on. IEEE, 2009.

Adli, Alexander, and Zensho Nakao,"Three Steganography alggorithms for MIDI files", Machine Learning and Cybernetics,IEEE,2005.

Gartland-Jones, Andrew, and Peter Copley," The suitability of genetic algorithms for musical composition", Contemporary Music Review, Vol.22, No.3, pp.43-55, 2003.

Fortier, Nathan, and Michele Van Dyne, "A Genetic Algorithm approach to Improve Automated Music Composition", International Journal Of Computers, Vol. 5, No. 4, pp.525-532., 2011.

Menezes, van Oorschot, and Vanstone"Applied Cryptography by Schneier" , Handbook of Applied Cryptography.

Sandip Dutta, Avijit Kar, N.C.Mahanti and B.N. Chatterji,"Network Security Using Biometric and Cryptography", Springer 2008

S. Chakraborty, K. Krishnapriya, Loveleen," Analyzing the Melodic Structure of a North Indian raga: A Statistical approach ",Electronic Musicological review ,2009.

Rhoads, Geoffrey B," Audio steganography", U.S. Patent No.6,330,335 11 Dec 2001.

Jacob, Bruce, ""Composing with genetic algorithms",1995

Fortier, Nathan, and Michele Van Dyne,"A Genetic algorithm approach to improve automated music composition", 2011

Dutta, Sandip, Chandan Kumar,"A Symmetric Key Algorithm for music cryptography", IJET,2102.