International Journal of Interdisciplinary Research in Arts and Humanities (IJIRAH)
Impact Factor: 5.225, ISSN (Online): 2456 - 3145
(www.dvpublication.com) Volume 5, Issue 2, 2020

MUSICAL CIPHER SYSTEMS: AN ISOLATED BUT CHALLENGING RESEARCH DOMAIN

Prashant Pranav*, Sandip Dutta* & Soubhik Chakraborty**
* Department of Computer Science and Engineering, Birla Institute of Technology, Mesra, Ranchi-835215, Jharkhand, India
** Department of Mathematics, Birla Institute of Technology, Mesra, Ranchi-835215, Jharkhand, India

Cite This Article: Prashant Pranav, Sandip Dutta & Soubhik Chakraborty, "Musical Cipher Systems: An Isolated but Challenging Research Domain", International Journal of Interdisciplinary Research in Arts and Humanities, Volume 5, Issue 2, Page Number 36-37, 2020.

Abstract:
The field of Musical Cryptography has been long overdue for a proper focus by the research community despite the benefits of using music as a cipher system. This short communication places on recordthe latest research in this fascinating field including some of our own contributions**.**

Key Words: Cryptography; Musical Cryptography; Encryption; Decryption; Music Ciphers

1. Introduction:

Do you think expanded security stretches out solace to excessively dubious creatures? Or then again does security goes about as an umbrella to bestow insurances that we accept that we neednot bother about? Given that the web has made the world a worldwide town by granting fundamental correspondence among billions of individuals and is utilized from multiple points of view, for example, devices for trade, social communication and the trading of individual data, so starting here, today security has become a fantastically critical subject for each client to participate in. There are a few angles to security and a few executions shifting from secure trade, instalments made to private correspondences and ensuring medical services data. One of the most noteworthy parts of secure correspondences is cryptography. While cryptography is significant for secure interchanges yet it is not adequate in itself.

Cryptographic calculations are the premise of joyful exchanges over the web today. Secret data of a legislature or private organization or division is made sure about using Cryptography. From doing tie down correspondence to moving data of public significance, Cryptographic calculations assume the sole part secluded from everything the privacy. Cryptography is essentially a numerical model utilized for concealing private data. With the headway in web advancements and dependence of pretty much everybody on the utilization of web in everyday life, it has happened to most extreme significance to shroud the classified data shared over the web in a structure that cannot be perused by a gatecrasher. Cryptography is the craft of composing something covertly; the principal remarkable utilization of Cryptography recorded as a hard copy goes back to around 1900 B.C. at the point when an Egyptian recorder utilized non-standard pictographs in an engraving. In information and broadcast communications, the utilization of Cryptographic calculations is absolutely critical when imparting over any untrusted medium, for example, the web. The goals accomplished by Cryptography are:

Confidentiality:

It infers nobody aside from the planned recipient can peruse the message. The sole correspondence must be done between the two included imparting parties and no busybody.

Authentication:

It keeps the aggressor from imitating as an imparting party. It is the way toward demonstrating one's character.

Integrity:

It guarantees the collector that the conveyed message has not been changed from the first on its way to the recipient. It keeps any outsider from altering the message without being taken note.

Non-repudiation:

It legitimizes the beneficiary that the sender has truly sent the message and not any other person.

Key Exchange:

The component by which Crypto keys are shared between the senders and the beneficiaries. It is essentially significant for asymmetric key cryptography.

2. Musical Cryptography:

Though in picture through centuries, *Musical Cryptography* have never gained the required research momentum so as to attract more researchers. It is a complete new genre (as far as the research is concerned) wherein the confidential information exchanged over any untrusted medium is done by the use of *musical notes*. Messages are encrypted using the note sequences of any possible composition. For increasing the security further, these messages are sent in the form of a musical signal. This defies the intruder of guessing with precision that any communication is being held between two parties or a group of parties. The use of note sequences to encrypt the messages is much secure in itself as every new composition encompasses a new sequence. It is the composer of the sequence, who is in the sole authority of his/ her composition (following a fixed raga structure).

The use of music for encryption has been well shown in a popular TV show Outlander a TV drama from Scotland and in one mystery novel named Secrets of the White Rose.Some mathematicians and cryptologists from the early 17th and 18th century such as John Wilkins and Philips Thicknesses believed that using music for the purpose of secrecy was the perfect camouflage arguing that the intruder will never suspect musical notes as the carriers of messages. Eric Sams [1] has given a much explained usage of musical ciphers and how these surpass the use of traditional ciphers in terms of randomness of the generated cipher text.

3. Our Contribution:

In [2], we have proposed a very novel and fascinating way of encrypting messages using Hindustani (North Indian) music. In Hindustani music, seven notes are used also called as *Swara* in an octave. The note to note correspondence of the seven notes with that of western music is

C	D	E	F	G	A	B
Sa	*Re*	*Ga*	*Ma*	*Pa*	*Dha*	*Ni*

The scales known as *thaat* in Hindustani music must contain all the seven notes in any form. The form here refers to *natural* (Hindustani correspondence as *Shudh*), *flat* (Hindustani correspondence as *Komal*) and *sharp* (Hindustani correspondence as *Tivra*). Note *Sa* and *Pa* must always be in their natural form, note *Re*, *Ga*, *Dha* and *Ni* can either be natural or flat and note *Ma* can be natural or sharp. The frequency at which note *Sa* is to be played is not fixed. If *Sa* is fixed as *C* sharp by some composer, say, then it means that the *C sharp* scale is being used.

A musical composition constitutes of two parts:

- *What to Play*: This part signifies the sequences of notes that are to be used for composing music.
- *How to Play*: This part shows how the selected sequences of the what part are to be played or sung.

With the advancement of computers in almost every possible field, music has also not remained untouched from being composed with the help of computers. But we argue that for selecting the what part of a musical composition, computers can be very good tool, but for the how part, it is the singer or the composer who is in the sole authority of the composition and the piece he/her generates is far more soothing than that composed with the help of computer.

If both, *what to play* and *how to play*, are decided by a composer, then the musical composition is called *natural composition*. If both, *what to play* and *how to play*, areselected by a computer, the composition is called *artificial composition*. But, if the *what to play* is selected by the computer and *how to play* is decided by a composer, then the composition is called semi-natural composition.

In our research work in [2], we used a method of semi-natural composition [3] for securing the messages. We selected raga *Yaman Kalyan* for generating the what part and subsequently, the how part was generated using Chebyshev's inequality to gather the duration and frequency of each note in raga *Yaman Klayan*. The proposed research uses a two level encryption algorithm. Some of the interesting results of our proposed methods are:

- The generated Cipher Texts using raga *Yaman Kalyan* and run through the Semi-natural composition algorithm are musicalif rendered and for the same messages run several times, we get a new sequence of notes.
- The encryption and decryption time of the proposed approach is very less compared with the standard AES-128 because of the less complex inner working structure of our algorithm.
- Out of the five goals of any Cryptographic algorithm, two of the goals, *Confidentiality* and *Authentication*are achieved with the proposed approach.

4. Future Research Directions:

Although isolated yet musical cryptography we feel has tremendous usage in the future especially if it can be extended to be employed in low-power usage or *lightweight devices*. Lightweight devices need very less energy consuming security mechanism. Traditional algorithms run on several rounds which increases their overall time complexity and so these are not fit to be used in low-power consumption scenarios such as IoT, edge computing, mobile phones, etc. Our proposed algorithm can be tried to be used in these structures. Further, the composed music using the Semi-natural composition algorithm and Chebyshev's inequality can be implemented with more musical attributes to sound more like a musical composition. We hope there will be many hands to take up the challenge.

5. References:

1. Sams, E. (1979), Muiscal Cryptography, Cryptologia vol. 3, n. 4, Oct.
2. Pranav P, Chakraborty S, Dutta S (2019), A new cipher system using semi natural composition in Indian raga, Soft Comput (2020), 24:1529–1537 https://doi.org/10.1007/s00500-019-03983-8(0123456789
3. Chakraborty S, Mazzola G, Tewari S, Patra M (2014) Computational Musicology in Hindustani music, Springer

.