# MUSICYPHER:
# MUSIC FOR MESSAGE ENCRYPTION

**V. Jaime, A. Peinado**
Escuela Técnica Superior de Ingeniería de Telecomunicación, Universidad de Málaga
victorjm96@uma.es, apeinado@ic.uma.es

## ABSTRACT

An Android application has been developed to encrypt messages using musical notes that can be automatically played from the smartphone and/or stored in a midi file to be transmitted over any available connection. The app has been designed to recover the original message on-the-fly detecting the notes played by a different device. The main objective of this project is to make known the relationship between cryptography and music showing old systems (XVII century) implemented in modern devices, the smartphones, using the tools they provide us, such as the microphone, the speakers, and the internal storage.

## 1. INTRODUCTION

The encryption of information has always been a matter that the human being has been developing over the years [7], whether for war purposes or as in the present, for example, for privacy of sensitive data in the network [8]. One of the most used techniques since the first attempts to hide the information has been the substitution of the message's characters by other symbols, such as letters of the same or another language, numbers or symbols invented for the occasion.

One of the best treatises in Cryptography of all time, written by Lieutenant Carmona in 1894 [6], includes the cryptosystem proposed by Guyot, based on the idea of Gaspar Schott (1667), of using musical notes to encrypt messages. Although this is not the first cryptosystem using music as a vehicle to encrypt or hide the information, it can be considered as the most representative one.

Musicypher is an Android application that brings to the present this ancient cryptosystem with several objectives in mind: on the one hand, highlight the existing relationship between music and cryptography since many years; on the other hand, bring cryptography closer to the general public through the music, and conversely, promote the musical learning through games using (in this case) the message encryption.

Section 2 describes the Guyot cryptosystem with more detail. Section 3 presents the more relevant aspects of the software developed. Finally, several conclusions are provided in section 4.

## 2. THE GUYOT CRYPTOSYSTEM

There have been various types of encryption, some quite original such as Guyot in the seventeenth century, which uses music as a way to hide the original text. Using an artifact, a musical note or chord was assigned to each letter and, with this same device, the sender and receiver of the message could encrypt and decipher the information.

Guyot's device consists of two concentric circles. In one of them the 26 letters of the alphabet are represented, and in the other the note or musical chord with which it will be encrypted. With this device, the notes would be written in a score. Of course, the final result had no musical sense, but it went unnoticed among people without musical knowledge. When the recipient receives the score, the message could be obtained with the same device that was used to encrypt the original.

## 3. THE ANDROID APPLICATION

Musicypher is an application that consists of the implementation of the Guyot crypto-system adapted to current technology using a very common device: the Smartphone. The main objective is this adaptation, but not the improvement of its security.

Musicypher is a program for Android systems, developed in Java using the Android Studio programming environment, in which the encryption of a text string is carried out transforming it in a sequence of musical notes. Similarly, the corresponding deciphering is implemented.

The transmission of encrypted messages can be carried out in two ways: by means of sound, by playing a coded music message in order to be captured by the microphone of a receiver smartphone, and by means of an audio MIDI [1] file, without the need for reproduction. Therefore, the decryption has been implemented such that the message is recovered from the MIDI file, or detected in real-time while the sound is being played by the transmitter device.

### 3.1 Encryption of the message

In order to provide more options to the final user, before the musical part he will be offered different types of encryption systems to be applied to the text, basically based on substitution or transposition, which require of a key that the receiver must also know in order to decode the information. After this part the text-to-music conversion takes place in which, as in the Guyot system, musical notes are assigned to the alphabet.

Once the encrypted file is generated, it can be stored to be later shared with other users, and played, within the same application.

### 3.2 Decryption of the message

The deciphering of a text can be done through the microphone of the device. It starts to catch the melody and each time a note change occurs, deciphers the fundamental frequency [4] [5] and concatenates the corresponding letter to the unique text string. The process will end when a note that means the end is recorded.

After that, the encrypted text message is obtained and through the substitution or transposition method and the source key it is decrypted, and the original message is obtained.

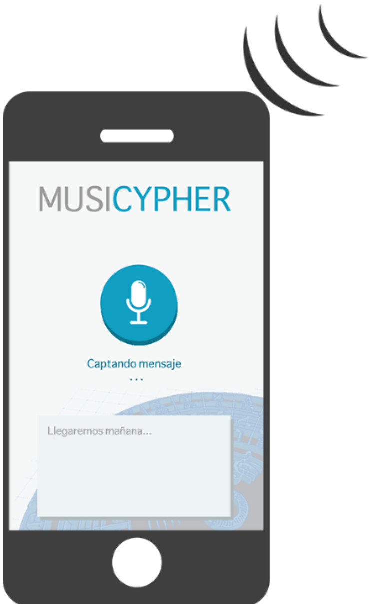

**Figure 1**. Real-time decoding of the musical message

### 3.3 Considerations

Text to music conversion is done using the MIDI standard, in which each musical note is identified by a number. Taking it into account, and assigning a duration time to each note, a ".MID" file is generated. This file can be reproduced by Musicypher or by any device that supports the standard.

In order to capture the sound, the technical limitations of mobile microphones [2] [3] have been taken into account, and we have chosen to use the frequency range of the telephone channel band (300Hz to 3kHz), since this is where the frequency response is flatter in most devices and, therefore, the capture is more reliable.

## 4. CONCLUSIONS

The Guyot [6] encryption system has been adapted to an Android application, using the current technology available at usual smartphones, in order to deploy a complete communication system (transmission, encryption, decryption, reception). The current prototype is focused on the musical part. Further developments will take into consideration the improvement of the security part, allowing us to provide a more robust app.

### Acknowledgments

This work was partially supported by the Universidad de Málaga, Andalucía Tech, and by the Ministerio de Economía, Industria y Competitividad (MINECO), Agencia Estatal de Investigación (AEI), and Fondo Europeo de Desarrollo Regional (FEDER, UE) under Grant TIN2017-84844-C2-1-R (COPCIS project).

## 5. REFERENCES

[1] J. Bartolomé. La especificación MIDI, 2013. URL: http://tolaemon.com/docs/midi1.htm

[2] B.B. Morson. “Hearing voices in the high frequencies: What your cell phone isn’t telling you”, in Proc 168th Acoustic Society of America (ASA) Meeting, Indianapolis, October, 2014. Available at https://acoustics.org/hearing-voices-in-the-high-frequencies-what-your-cell-phone-isnt-telling-you-brian-b-monson/

[3] Technical Direct. “Smartphone User Experience Analysis - Audio (II)”, 2016. URL; http://www.technical-direct.com/en/smartphone-user-experience-analysis-audio-ii/

[4] J. Six, O. Cornelis, M. Leman. TarsosDSP, a Real-Time Audio Processing Framework in JAVA. Univertisy College Ghent. 2014.

[5] A. de Cheveigne, H. Kawahara. “YIN, a fundamental frequency estimator for speech and music”, in J. Acoust. Soc. Am. 111 (4), 2002, pp. 1917-1930.

[6] J. García Carmona. Tratado de criptografía con aplicación especial al ejército. Madrid: Sucesores de Rivadeneyra. 1894. Re-edited by Ministerio de Defensa, 2011.

[7] D. Kahn, The codebreakers: the story of secret writing. New York: Macmillan. 1967

[8] A.J. Menezes, P.C. Oorschot, S.A. Vanstone. Handbook of applied cryptography. Boca Raton, FL, USA: CRC Press, 5th printing. 2001