How to Encrypt Bytes with Rhythmic Figures?

Josué Alexis Lugos Abarca

How to Encrypt Bytes with Rhythmic Figures?

Josué Alexis Lugos Abarca

https://orcid.org/0000-0001-8980-7748

josuealexis22@gmail.com

Abstract

This paper seeks to propose a method of encryption for bytes by means of rhythmic figures. The consequences of the axiomatization of rhythmic figures and musical silences in number and set theory (Lugos Abarca, 2023) are used. It is determined as a private key the combination of the rhythmic figures t in a set $\psi^{\dagger}$. On the contrary, the form of the encrypted byte is expressed with the value of the sets: $\psi^{\dagger}$ and of the musical silences $\widetilde{t_i}$. Hence, a byte encryption method that appears to be functional has been defined. Alternatively, it must be tested to verify its efficiency in this task.

Keywords: rhythmic figures, encryption, bytes, axioms, sets

1. INTRODUCTION

Cryptography consists of protecting information through the use of encrypted algorithms (Fernandez, 2004; Díaz, 1995), and may also be defined as a set of techniques designed for the purpose of providing security to information at rest, in transit or in use (Maiorano, 2009). As a result, this mathematical tool is one of the best ways to guarantee the properties of confidentiality, integrity and availability of a system's resources (Paredes, 2006; Marrero Travieso, 2003).

On the contrary, it is well known that music has a great versatility, as its parameters are able to express emotions and feelings (Kaygusuz & Zuluaga, 2018; Panda et al., 2020; Ramos et al., 2011; Jimenez et al., 2020; Madgazin, 2009; Fernández Sotos, 2017), is used in medicine as a therapeutic tool (Bernardi et al., 2009; Siritunga et al., 2013; Kirk et al., 2022; Susanto et al., 2019; Baccarani et al., 2023; Liu et al., 2009), and as a language (Brandt et al., 2012; Masataka, 2007; Higgins, 2019).

It is this last feature that, perhaps has inspired to employ music within cryptography (Kumar et al., 2015; Sams, 1979; Dutta et al., 2013), specifically musical notes are used to encrypt messages in melodies (Kundu, 2020; Kumar et al., 2015; Krishnan et al., 2021; De Luca & Haines, 2017) so, melodic cryptograms are constructed. However, music coupled with cryptography is a little studied area (Kundu, 2020), therefore, to expand this field, this paper presents an encryption method for bytes using rhythmic figures instead of musical notes, which generates a different methodology than what has been proposed.

The reason for using rhythmic figures is due to the discoveries obtained in a previous research (Lugos Abarca, 2023), whose mathematical consequences make it possible to elaborate an encryption method for bits and bytes that could be efficient in this task.

2. PRELIMINARY

This research will be based on the axioms that in a previous article (Lugos Abarca, 2023) were proposed, such axioms were built by means of the rhythmic figures whose consequences in mathematics are used to develop a byte encryption method. For this reason, in this section these axioms will be reviewed and the concept of bit and byte will be introduced.

The four axioms are:

Axiom No. 1:

Any rhythmic figure could be expressed in terms of time t with the equation:

$$t = \frac{\beta}{T} \tag{2.1}$$

Such that T is the tempo of the song and β is the pulse of a rhythmic figure.

Let be t_0 is the quarter note, t_1 is the half note, t_2 is the half note with augmented dot, t_3 is the whole note, t_2^1 is the 8th note, t_3^1 is the triplet note, t_4^1 is the 16th note and t_5^1 is the quintuplet note.

$$t_0 = \frac{1}{T},\ \ t_1 = \frac{2}{T},\ \ t_2 = \frac{3}{T},\ \ t_3 = \frac{4}{T} \tag{2.2}$$

$$t_2^1 = \frac{1}{T2},\ \ t_3^1 = \frac{1}{T3},\ \ t_4^1 = \frac{1}{T4},\ \ t_5^1 = \frac{1}{T5}$$

Axiom No. 2:

Let $\psi^{\dagger}$ be the set representing a musical measure, it is determined that its elements will be only rhythmic figures t, whose result of summing these figures will be equal to the value of the time signature of the set $\psi^{\dagger}$.

$$If\ \dagger \in \psi^{\dagger} = n \longrightarrow \sum t \in \psi^{\dagger} = n \tag{2.3}$$

Let be $\psi^{\dagger}$ a musical measure whose time signature is $\frac{1}{4}$, ψ^2 is a musical measure whose time signature is $\frac{2}{4}$, ψ^3 is a musical measure whose time signature is $\frac{3}{4}$ and ψ^4 is a musical measure whose time signature is $\frac{4}{4}$.

Axiom No. 3:

Given two sets: $\psi^{\dagger}$ whose elements are the same figures t, but different from each other and with different order it is established that by musical property the sum of both sets does not commute.

$$t_2^1 + t_{4-0}^1 + t_{4-1}^1 \neq t_{4-0}^1 + t_2^1 + t_{4-1}^1 \tag{2.4}$$

Axiom No. 4:

All musical silences are defined with $\widetilde{t_\iota} \,/\, \beta = 0\ b$, however, although all silences are worth $\widetilde{t_\iota} = 0\ min$ by musical property none are equal to each other.

$$\widetilde{t_\iota} \neq \widetilde{t_\jmath} \,/\, \widetilde{t_\iota}, \widetilde{t_\jmath} = 0 \tag{2.5}$$

Let be $\widetilde{t_1}$ quarter note rest, $\widetilde{t_2}$ half note rest, $\widetilde{t_3}$ dotted half note rest, $\widetilde{t_4}$ whole note rest, $\widetilde{t_2^1}$ eighth note rest, $\widetilde{t_3^1}$ eighth note triplet rest, $\widetilde{t_4^1}$ sixteenth note rest.

A bit is defined as the basic unit of information whose value is binary, i.e., it uses zeros and ones (Prieto et al.,1989). In addition, it represents the occurrence of an event of two possibilities such as: on or off (Valdivia, 2020; White, 1993). Yet, a byte is another unit of information made up of a group of 8 bits (Bottaro, 2005; Tanenbaum, 2000) that, define data storage units (Pfaffenberger, 1990; Salazar, 2018) and also, function to encode characters for the purpose of sending messages (Prieto, 2017; del Carmen Delgado Venzalá, 2021: Long & Long, 1999).

3. ENCRYPTING BYTES WITH A TIME SIGNATURE

First, similar to what Arranz proposes in his book when defining a packed byte (Arranz, 1994), the byte is to be divided into two groups of four bits:

$$\text{Byte} \left\{ \underbrace{0010}_{\text{Group1}}, \underbrace{0010}_{\text{Group 2}} \right. \tag{3.1}$$

Thus, starts with the formation of four sets ψ^1, such that the sum of their elements is equal to: 1. This with the purpose of respecting the binary value of the bit (Martínez, 2008).

Let $T = 1$, the following sets are formed:

$$\psi_0^1 = (t_2^1 + t_2^1) = \left[\frac{1}{T2} + \frac{1}{T2}\right] = 1 \tag{3.2}$$

$$\psi_1^1 = (t_2^1 + t_4^1 + t_4^1) = \left[\frac{1}{T2} + \frac{1}{T4} + \frac{1}{T4}\right] = 1$$

$$\psi_2^1 = (t_4^1 + t_2^1 + t_4^1) = \left[\frac{1}{T4} + \frac{1}{T2} + \frac{1}{T4}\right] = 1$$

$$\psi_3^1 = (t_4^1 + t_4^1 + t_2^1) = \left[\frac{1}{T4} + \frac{1}{T4} + \frac{1}{T2}\right] = 1$$

Due to axiom no. 3, it follows that:

$$\psi_0^1 \neq \psi_1^1 \neq \psi_2^1 \neq \psi_3^1 \tag{3.3}$$

As a result:

$$1 \neq 1 \neq 1 \neq 1 \tag{3.4}$$

Because of this characteristic, the combinatorics of the rhythmic figures in 3.2 can be defined as the private keys to decrypt the first group of the byte (Plata Cheje, 2009; Celi Mendez, 2012). Therefore, each private key is assigned a bit (Yugcha Panimbosa, 1999), which make up the true byte. To the set ψ_0^1 corresponds 1, ψ_1^1 is 0, ψ_2^1 is 1 and ψ_3^1 is 0.

First, the first group of the encrypted byte would look like this:

$$1111 \tag{3.5}$$

Since, to represent the first group of the byte, in its encrypted form, the numerical value of each set ψ^1 is used, which, at the rate of $T = 1$; is equivalent to: 1. However, as indicated, 3.5 does not correspond to the first group of the byte; to know it the private key assigned by the issuer must be used for decryption.

Which is:

$$\psi_3^1\psi_1^1\psi_0^1\psi_3^1 \tag{3.6}$$

That according to the bits assigned to each set, the first decrypted byte group would be:

$$0010 \tag{3.7}$$

For 1111 encryption there are different combinations (Grimaldi, 1998). For instance, another way to encrypt 3.5 would be with the following private key:

$$\psi_0^1\psi_2^1\psi_1^1\psi_0^1 \tag{3.8}$$

What corresponds to:

$$1101 \tag{3.9}$$

Thus, the encrypted form of 3.7 and 3.9 is: 1111, it could be said that:

$$1111 \neq 1111 \tag{3.10}$$

Because both private keys give different combinations:

$$\psi_3^1\psi_1^1\psi_0^1\psi_3^1 \neq \psi_0^1\psi_2^1\psi_1^1\psi_0^1 \tag{3.11}$$

$$0010 \neq 1101$$

With this method, 1111 may encrypt the first group of any byte in different ways.

4. MUSICAL SILENCES

Given the above, the first two groups of the encrypted byte use the number: 1, to involve the zero, musical silences must be considered, i.e. apply axiom no. 4. In this case, it is not necessary to construct sets, it is enough to define the silences. The following is used:

$$\widetilde{t_1},\ \widetilde{t_2},\ \widetilde{t_3},\ \widetilde{t_4} \tag{4.1}$$

The actual bits that make up the first group of the byte are assigned:

$$\widetilde{t_1} = 1,\ \widetilde{t_2} = 1,\ \widetilde{t_3} = 0,\ \widetilde{t_4} = 0 \tag{4.2}$$

Thus, the first group of an encrypted byte could be:

$$0001 \tag{4.3}$$

Where one of your possible private keys would be:

$$\widetilde{t_1}\widetilde{t_2}\widetilde{t_1}\psi_0^1 \tag{4.4}$$

Since, the first byte group according to 4.4 would be:

$$1111 \tag{4.5}$$

5. ENCRYPTING BYTES WITH VARIOUS TIMES SIGNATURES

So far, the first group of the byte has been encrypted using only the set: ψ^1 , which corresponds to the $\frac{1}{4}$ time signature, however, other sets could be used and combined, which provides another encryption method. To the sets: ψ_0^1, ψ_1^1, ψ_2^1 and ψ_3^1; described in 3.2, the following are added:

Let $T = 1$:

$$\psi_0^2 = (t_0 + t_2^1 + t_4^1 + t_4^1) \tag{5.1}$$

$$\psi_1^2 = (t_0 + t_4^1 + t_2^1 + t_4^1)$$

$$\psi_2^2 = (t_0 + t_4^1 + t_4^1 + t_2^1)$$

These assemblies represent a time signature of $\frac{2}{4}$.

One bit is assigned to each of them:

$$\psi_0^2 = 0,\ \ \psi_1^2 = 1,\ \ \psi_2^2 = 1 \tag{5.2}$$

Musically, the sets: ψ_0^1 and ψ_0^2 represent times signatures, however, as seen in axiom no. 2, due to their duration they could be reinterpreted as quarter and half notes, respectively.

$$\psi_0^1 = t_0 \tag{5.3}$$

$$\psi_0^2 = t_1$$

This axiom allows to extend axiom no. 3 to the sets: ψ_0^1 y ψ_0^2.

Thus, with this new interpretation, the combinations in 3.2 are equivalent since they represent a quarter note. This interpretation does not conflict with the above since the sets were now studied individually and not by means of their elements (Yerly, 1969; Muñoz, 2012).

Then, the following set is equivalent:

$$\psi_3^1\psi_1^1\psi_0^1\psi_3^1 = \psi_0^1\psi_2^1\psi_1^1\psi_0^1 \tag{5.4}$$

Since, from this new perspective; 5.4 corresponds to write:

$$t_0t_0t_0t_0 = t_0t_0t_0t_0 \tag{5.5}$$

But if the 5.1 sets are combined, the equality is broken:

$$\psi_0^2\psi_0^1\psi_1^1\psi_2^1 \neq \psi_0^1\psi_0^2\psi_1^1\psi_2^1 \tag{5.6}$$

Because, 5.6 is equivalent to write:

$$t_1t_0t_0t_0 \neq t_0t_1t_0t_0 \tag{5.7}$$

Therefore, they could be used to encrypt the first group of one byte (Bohórquez, 2017). Let propose the following combinations:

$$\psi_0^2\psi_0^1\psi_1^1\widetilde{t_1} \tag{5.8}$$

$$\psi_0^1\psi_0^2\psi_1^1\widetilde{t_1}$$

$$\psi_0^1\psi_1^1\psi_0^2\widetilde{t_1}$$

$$\psi_0^1\psi_1^1\widetilde{t_1}\psi_0^2$$

One bit is assigned to each combination in 5.8 which, in turn, make up the real byte.

$$(\psi_0^2\psi_0^1\psi_1^1\widetilde{t_1}) = 0,\ \ (\psi_0^1\psi_0^2\psi_1^1\widetilde{t_1}) = 1,\ \ (\psi_0^1\psi_1^1\psi_0^2\widetilde{t_1}) = 1,\ \ (\psi_0^1\psi_1^1\widetilde{t_1}\psi_0^2) = 0 \tag{5.9}$$

Then, the encrypted byte would no longer have four digits, but sixteen:

$$1110\ 1110\ 1101\ 1110 \tag{5.10}$$

To decrypt 5.10, the following steps are followed: first, each group of four digits is decrypted independently using the process studied above:

$$\underset{\psi_0^2\psi_0^1\psi_1^1\widetilde{t_1}}{1110} \quad \underset{\psi_0^1\psi_0^2\psi_1^1\widetilde{t_1}}{1110} \quad \underset{\psi_0^1\psi_1^1\widetilde{t_1}\psi_0^2}{1101} \quad \underset{\psi_0^2\psi_0^1\psi_1^1\widetilde{t_1}}{1110} \tag{5.11}$$

Knowing the private keys of each group, which in this context function as sub-private keys, the private keys defined in 5.9 are now used to decrypt the first byte set:

$$0100 \tag{5.12}$$

Therefore, involving different sets such as: ψ^1 and ψ^2, causes this method to require a double decryption.

Put 5.10 and 3.5 together and you have full single-byte encryption:

$$1110\ 1110\ 1101\ 1110\ 1111 \tag{5.13}$$

With the private keys and the already known method, the following byte is obtained:

$$0100\ \ 0010 \tag{5.14}$$

6. CONCLUSION

In this paper, a method for encrypting bytes by means of the axiomatization of rhythmic figures and musical silences (Lugos Abarca, 2023) has been proposed, which, theoretically, turns out to be practical. This method is innovative for two reasons: first, in the context of cryptography and music, rhythmic figures are used instead of melodies, an aspect that had not been investigated before and that generates a new perspective of study in this area. Secondly, this method is based on axioms that cause the non-commutativity between some sums, which causes that these two groups of bits: 1111 and 1111 are different between them, and therefore, they could encrypt different groups of a byte; increasing even more the difficulty of decryption for a receiver who does not know the private key.

However, this encryption method should be tested to verify and improve its use as a security tool.

7. REFERENCES

Arranz, A. (1994). *Administración de Datos y Archivos Por Computadora*. Editorial Limusa.

Baccarani, A., Donnadieu, S., Pellissier, S., & Brochard, R. (2023). Relaxing effects of music and odors on physiological recovery after cognitive stress and unexpected absence of multisensory benefit. *Psychophysiology*, 60(7), e14251.

Bernardi, L., Porta, C., Casucci, G., Balsamo, R., Bernardi, N. F., Fogari, R., & Sleight, P. (2009). Dynamic interactions between musical, cardiovascular, and cerebral rhythms in humans. *Circulation*, 119(25), 3171-3180.

Bohórquez, L. E. M. (2017). *Algoritmo Para La Encriptación Y Desencriptación Entre Archivos Digitales De Audio E Imagen* (Doctoral dissertation, Tesis para optar el Título profesional, Facultad de Ingeniería, Universidad de San Buenaventura, Bogotá).

Bottaro, J. (2005). Manual de competencias básicas en informática. *Programa de Certificación de Competencias Laborales*.

Brandt, A., Gebrian, M., & Slevc, L. R. (2012). Music and early language acquisition. *Frontiers in psychology*, 3, 327.

Celi Mendez, J. A. (2012). *Implementación hardware del estandar de encriptación avanzado (AES) en una FPGA* (Bachelor's thesis, Espol).

De Luca, E., & Haines, J. (2017). Medieval Musical Notes as Cryptography. *A Material History of Medieval and Early Modern Ciphers: Cryptography and the History of Literacy*, 30.

del Carmen Delgado Venzalá, M. (2021). *Desarrollo firmware de un driver de control para el módulo Sigfox AX-SF10 ANT21-868*. Universidad de Sevilla.

Díaz, J. C. G. (1995). *Criptografía: historia de la escritura cifrada*. Editorial Complutense.

Dutta, S., Kumar, C., & Chakraborty, S. (2013). A symmetric key algorithm for cryptography using music. International Journal of Engineering and Technology, 5(3), 3109-3115.

Fernández Sotos, A. (2017). *Percepción de emociones en la música: un estudio de la influencia del parámetro musical" Duración".* (Doctoral dissertation, Universidad de Castilla-La Mancha).

Fernandez, S. (2004). La criptografía clásica. *Sigma*, 24(24), 119-141.

Grimaldi, R. P. (1998). *Matemáticas discretas y combinatoria: una introducción con aplicaciones*. Pearson Educación.

Higgins, K. M. (2019). *The music between us: Is music a universal language?*. University of Chicago Press.

Jimenez, I., Kuusi, T., & Doll, C. (2020). Common chord progressions and feelings of remembering. *Music & Science*, 3, (pp. 1-16).

Kaygusuz, C., & Zuluaga, J. (2018). Impact of Intervals on the Emotional Effect in Western Music. *arXiv preprint* arXiv:1812.04723.

Kirk, U., Ngnoumen, C., Clausel, A., & Purvis, C. K. (2022). Effects of Three Genres of Focus Music on Heart Rate Variability and Sustained Attention. *Journal of Cognitive Enhancement*, 6(2), 143-158.

Krishnan, R., Thomas, R., Akshay, D. S., Krishna, V. S., & Divya, R. S. (2021). An intelligent text encryption system using musical notes. In *Innovative Data Communication Technologies and Application: Proceedings of ICIDCA 2020* (pp. 449-459). Springer Singapore.

Kumar, C., Dutta, S., & Chakraborty, S. (2015). A hybrid polybius-playfair music cipher. *International Journal of Multimedia and Ubiquitous Engineering*, 10(8), 187-198.

Kumar, C., Dutta, S., & Chakraborty, S. (2015). Hiding messages using musical notes: A fuzzy logic approach. *International Journal of Security and Its Applications*, 9(1), 237-248.

Kundu, A. S. T. (2020). An Approach to Musical Cryptography. In *International Web Conference On Smart Engineering Technologies-2020*.

Liu, H., Hu, J., & Rauterberg, M. (2009, November). Music playlist recommendation based on user heartbeat and music preference. In *2009 International Conference on Computer Technology and Development* (Vol. 1, pp. 545-549). IEEE.

Long, L., & Long, N. (1999). *Introducción a las computadoras y a los sistemas de información*. México. Prentice Hall

Lugos Abarca, J. A. (2023). Four Axioms for a Theory of Rhythmic Sets and their Implications. *Online Journal Of Music Sciences*, *8*(1), 226-237. https://doi.org/10.31811/ojomus.1361656

Madgazin, V. R. (2009). The information theory of emotions of musical chords. *arXiv preprint* arXiv:0909.3976.

Maiorano, A. (2009). *Criptografía: técnicas de desarrollo para profesionales*. Alpha Editorial.

Marrero Travieso, Y. (2003). La Criptografía como elemento de la seguridad informática. *Acimed*, 11(6), 0-0.

Martínez, H. A. V. (2008). *Representación de números en binario*. Technical report, Universidad de Sonora, Hermosillo, Sonora.

Masataka, N. (2007). Music, evolution and language. *Developmental science*, *10*(1), 35-39.

Muñoz, J. (2012). *Introducción a la teoría de conjuntos*. Universidad Nacional.

Panda, R., Malheiro, R. M., & Paiva, R. P. (2020). Audio features for music emotion recognition: a survey. *IEEE Transactions on Affective Computing*. (01), 1-1.

Paredes, G. G. (2006). Introducción a la criptografía. *Revista Digital Universitaria*, 7(7).

Pfaffenberger, B. (1990). *Que's computer user's dictionary*. Carmel Indiana. Que

Plata Cheje, R. W. (2009). Des/Encriptacion en la Informatica Forense. *Revista de Información, Tecnología y Sociedad*, 35.

Prieto, A., Lloris, A., & Torres, J. C. (1989). *Introducción a la Informática* (Vol. 20). McGraw-Hill.

Prieto, V. S. (2017). *Migración del software de control de un vehículo a un computador dedicado*. Universidad Politécnica de Madrid.

Ramos, D., Bueno, J. L. O., & Bigand, E. (2011). Manipulating Greek musical modes and tempo affects perceived musical emotion in musicians and nonmusicians. *Brazilian Journal of Medical and Biological Research*, 44(2), (pp. 165-172).

Salazar, L. D. (2018). Tecnologías de Almacenamiento en Centro de Datos. *Tecnología Vital*, 2(4).

Sams, E. (1979). Musical cryptography. *Cryptologia*, 3(4), 193-201.

Siritunga, S. , Wijewardena, K. , Ekanayaka, R. and Mudunkotuwa, P. (2013) Effect of music on blood pressure, pulse rate and respiratory rate of asymptomatic individuals: A randomized controlled trial. *Health*, 5, 59-64.

Susanto, H., Merawati, D., & Andiana, O. (2019, April). The effect of tempo of musical treatment and acute exercise on vascular tension and cardiovascular performance: A case study on trained non-athletes. In *IOP Conference Series: Materials Science and Engineering* (Vol. 515, No. 1, p. 012033). IOP Publishing.

Tanenbaum, A. (2000). *Organización de computadoras un enfoque estructurado*. México. Pearson Educación.

Valdivia, C. (2020). *Sistemas informáticos y redes locales 2. ª edición 2020*. Ediciones Paraninfo, SA.

White, R. (1993). *How software works*. United States. ZD Press.

Yerly, H. (1969). Conjuntos y funciones. *Boletín de matemáticas*, 3(1), 22-32.

Yugcha Panimbosa, W. G. (1999). *Implementación de un algoritmo de clave única para la encriptación de información* (Bachelor's thesis, QUITO/EPN/1999).