Using congruence in encoding musical partituras

Besim Shala¹, Besiana Mehmedi², Shkodran Tolaj³, Azir Jusufi ¹,⁴
¹University for Business and Technology
²State University in Tetovo
³University of Audio and Visual Arts “Esra”
⁴State University of Tetovo
besimi_77@yahoo.com, besiana.mehmedi@unite.edu.mk, shkodran.tolaj@hotmail.com,
azir.jusufi@unite.edu.mk

Abstract. Along with theoretical review of partituras and encryption systems, we have tried to conduct encryption of sheets by encoding all of its elements such as: encoding musical notes, encoding values of notes and intermissions, encoding accords, encoding tonalities and encoding rhythm whereby the original musical piece is transformed into an irregular and meaningless sheet. Information technology today has allowed for easier copying of authorial pieces; therefore, it is necessary to know encryption which allows protection of pieces from any misuse. Cryptology including knowledge of congruence deals with resolution of these insecurities. The significance of this paper lies in intertwining knowledge from music, math and computer sciences thus rendering our paper into an interdisciplinary paper and we believe this will increase curiosity and the interest as well. In order to make our work more concrete, we have included encoding and decoding of a well-known melody from Shkodra “A’SAMAN TRËNDAFILI ÇELËS”, whereby as encryption key we used a two-tact fragment from the song “O VENDI IM”

Keywords: pentagram, cryptosystem, encryption, decryption, music note, congruence.

1 Knowledge on congruence and cryptosystems

Definition 1: Let’s have: \( m \in \mathbb{N} \). \( \forall a, b \in \mathbb{Z} \); Whereby \( a \) is congruent with \( b \) based on module \( m \) then and only if \( m \mid (a - b) \). We note: \( a \equiv b \pmod{m} \).

or

\[
a = b(\text{mod} \, m) \iff \exists k \in \mathbb{Z} \mid a - b = km
\]

(1)

The congruency relation is the relation of equivalence; therefore, the meaning of congruence is closely related with the meaning of residual classes.

Definition 2: Let’s have: \( m \in \mathbb{N} \). Classes of equivalence defined with the relation “ \( \equiv \) ” based on module \( m (or \ as \ they \ are \ called \ in \ the \ theory \ of \ residual \ class \ numbers \ based \ on \ module \ m) \), they represent the union of all the numbers, which when divided with \( m \) give the same residual value. Symbolically, residual classes based on module \( m \) are noted as in following:

\[
K_m(a) = \{x \in \mathbb{Z} | x \equiv a(\text{mod}m)\} \subset \mathbb{Z}
\]

(2)

Every residual class based on module \( m \) is not empty since always \( \exists a \in K_m(a) \) whereby \( a \equiv a(\text{mod}m) \).

Note 1: In our paper we use smallest non-negative representatives of the equivalence class.

The following serves as reminder of some congruency features:
**Theorem 1** ([1], p.52): If \(a, b, c \in \mathbb{Z}\) and \(m \in \mathbb{N}\), where by \(a \equiv b \pmod{m}\), then:

1. \(a + c \equiv b + c \pmod{m}\)
2. \(a - c \equiv b - c \pmod{m}\)
3. \(ac \equiv bc \pmod{m}\).

**Theorem 2** ([1], p.52): If \(a, b, c, d \in \mathbb{Z}\) and \(m \in \mathbb{N}\), whereby \(a \equiv b \pmod{m}\) and \(c \equiv d \pmod{m}\), then:

1. \(a + c \equiv b + d \pmod{m}\)
2. \(a - c \equiv b - d \pmod{m}\)
3. \(ac \equiv bd \pmod{m}\).

With the use of cryptography or cryptographic systems (also cryptosystem, code), we will understand the transformation of a message called open text through encoding function (or simply encoding) whereby only one authorized receiver can return the transformed message in the initial condition.

**Definition 3**: Cryptosystem is called a five \((P, C, K, E, D)\) if it meets the criteria:

- \(P\), is the final family of open texts
- \(C\), is the final family of encoded texts;
- \(K\), space of keys, is a final family of potential keys;
- Elements \(E\) and \(D\) are reflections respectively \(P\) into \(C\), of \(C\) into \(P\) whereby every \(k \in K\), has an encoding rule \(e_k \in E\) and a decoding rule \(d_k \in D\) for \(\forall x \in P\) applies \(d_k(e_k(x)) = x\).

**2 Encryption of music sheets**

Taken in consider paper [2], [3], [4] and [5], we came to the following results:

![Fig. 1 Piano's keyboard](image)

2.1 **Encryption of notes in three octaves**

(Keys in the small octave in the bass key, in the first and second octave in the violin key)
In order to encrypt notes into three octaves, we need another musical fragment, e.g. Elise Note 2.

Instead of this fragment, we can use any other musical fragment. Encryption is as in following: \(N_p + N_c = N_k \pmod{37}\) (3)

\(N_p\) means notes of the sheet we wish to encrypt; \(N_c\) means the notes of the key sheet (in our case, Elise [8]), while \(N_k\) means encrypted notes e.g. we encrypt the second octave with the help of key Elise

The second octave encrypted with the key Elise

**Note 3.** Decryption is done with

\(N_k - N_c = N_p \pmod{37}\) (4)

### 2.2 Value of notes and intermissions

(Apart from encryption of notes, values of notes and intermissions must also be encrypted)

- **00A Full note = 4**
- **01B Half note = 2**
- **02G Four note = 1**
- **03D Eight note = 1/2**
- **04E Sixteen note = 1/4**
- **05F Full note with dot = 6**
- **06G Half note with dot = 3**
- **07H Four note with dot = 1.5**
- **08I Eight note with dot**
- **09L Full intermission = 4**
- **10K Full intermission with dot = 2**
- **11L Four intermission = 1**
12M Eight intermission=1/2 3N Full intermission with dot=6 14O Half intermission with dot=2

15P Four intermission with dot = 1.5 16Q Sixteen intermission with dot = 0.75

**Note 4:** Dots extend the values of notes and intermissions by half their value.
Encryption of values is done based on module 17, e.g. one tact from Elise [8]

\[ V_p + V_c = V_k \pmod{17} \]  \hspace{1cm} (5)

**Piano**

\[ \frac{1}{4} \]

**Note 5:** Decryption of values will be done with

\[ V_k - V_c = V_p \pmod{17} \]  \hspace{1cm} (6)

Music partituras sheet, apart from notes, intermissions and their values that create the rhythm, it has the tonality, accords, the tact and a series of other composition elements. The following with introduce musical tonalities in order to encrypt the tonality. Musical tonality is the musical scale wherein the entire musical piece is developed. Tonalities are divided into Dur-Majeure or major or mol-minor or minor (with diezis and bemol) which differ greatly in sounds.

The musical tonalities are the following:

```
C-Dur  G-Dur  D-Dur  A-Dur  E-Dur  H-Dur  Fis-Dur
a-mol  e-mol  h-mol  fis-mol  cis-mol  gis-mol  dis-mol
b-F-Dur  B-Dur  Es-Dur  As-Dur  Des-Dur  Ges-Dur  Ces-Dur
d-mol  g-mol  c-mol  f-mol  b-mol  es-mol  as-mol
```

Encryption of the tonality

\[ T_p + T_c = T_k \pmod{28} \]  \hspace{1cm} (7)

while decryption with

\[ T_k - T_c = T_p \pmod{28} \]  \hspace{1cm} (8)
2.3 Accords

Main accords in a musical piece are into three grades: first grade: tonics that represents the conclusion of the musical piece; fourth grade: sub-dominant, which represents the development of the musical piece and the fifth grade – dominant, which represents the culmination of the musical piece. We will stop at the main accords which are also divided into mol and dur, major and minor. Musical sheets contain a variety of accords such as quint accord 3/5 with rotations, sextaccord 6/3 and second accord, nonarord 9. Apart from these, it is important to emphasize the musical partitions sheet and intervals. Nevertheless, we will stop only at the main quint-accords.

Encryption of accords follows

\[ Ap + Ac = Ak \pmod{21} \]  

while decryption is done with

\[ Ap - Ac = Ak \pmod{21} \]

**Note 6:** Quint accord is a simultaneous sound of three sounds.

Example:

A`SAMAN TRËNDAFILI ÇELËS  
(Melody from Shkodra [7], [9], [10])
Since the musical sheet contains the tonality and the key, the encryption is simple. Main sheet is in a-mol (03) while the key in d-mol (21). Tonality encryption is done with module 28.

03 + 21 = 24 (mod 21)

The encrypted tonality is f-mol.

**Rhythm**

The same method applies with rhythm as well since the entire musical sheet is in one rhythm. Main rhythms are: 2/4 (00), 3/4 (01), 4/4 (02), 5/8 (03), 6/8 (04), 7/8 (05), 9/8 (06), 12/8 (07)

Rhythm “A’saman trendafil çelles” 02
Rhythm “O vendi im”

\[ 02 + 01 = 03 \pmod{8} \]

Encrypted rhythm is \((03) = 5/8\).

### Encryption musical note done with the help of the formula (1)

\[
\begin{align*}
Rhythm & \quad \text{01} \\
02 + 01 & = 03 \pmod{8} \\
\text{Encrypted rhythm is } (03) & = 5/8.
\end{align*}
\]

### Encryption of values and breaks done with the help of the formula (5)
Encryption of accord done with the help of the formula (9)

\[
\begin{array}{cccccccccccccccc}
A & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 \\
\hline
08 & 08 & 08 & 08 & 08 & 08 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 \\
+02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 \\
13 & 13 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 \\
+02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 & 02 \\
15 & 15 & 15 & 15 & 14 & 14 & 00 & 00 & 00 & 00 & 10 & 15 & 15 & 15 & 15 & 15 & 15 \\
08 & 08 & 08 & 13 \\
+12 & 13 & 13 & 13 \\
10 & 00 & 00 & 05
\end{array}
\]

Encrypted partituras is an irregular combination and in fact it does not represent anything.

Encrypted Partituras
After having received the irregular sheet, the receiver deals with the following decoding whereby again as decoding key utilizing the two-tact fragment from the song "O VENDI IM"

**Decryption musical notated done with the help of the formula (4)**

\[ \begin{align*}
08 & 05 01 03 35 00 00 00 01 33 34 33 08 08 04 02 35 \\
- & 17 16 14 17 14 14 17 14 17 17 17 17 16 14 \ldots \\
28 & 26 24 23 21 20 23 21 21 19 17 16 28 26 24 23 21 \ldots
\end{align*} \]

**Decryption of values done with the help of the formula (6)**

\[ \begin{align*}
V_k: & 08 06 06 04 14 06 04 06 05 04 05 09 05 05 04 08 04 06 04 \\
V_c & 01 03 01 03 01 12 08 01 08 03 01 12 03 02 02 02 02 \ldots \\
V_p & 07 03 03 03 02 03 03 03 03 02 07 03 03 03 03 03 03 03 03 03 03 01
\end{align*} \]

**Decryption of accord done with the help of the formula (10)**

\[ \begin{align*}
15 & 15 15 10 10 10 15 15 15 15 20 20 04 \ldots \\
02 & 02 02 02 02 02 02 02 02 02 02 02 02 02 02 12 12 \ldots \\
13 & 13 13 13 08 08 08 08 13 13 13 08 08 08 \ldots
\end{align*} \]
Decrypted rhythm is $03 - 01 = 02 \pmod{8}$, (02) is 4/4.

Decrypted element placing in the partitures and we receive Shkodran melody “A’SAMAN TRËNDAFILI ÇELEŠ”,