# Cryptographic Defence with Embedded Audio File Based on Bernoulli Numbers

Muharrem Tuncay Gençoğlu*‡

*Fırat University Vocational School of Technical Sciences, Elazığ, TÜRKİYE, mt.gencoglu@firat.edu.tr

‡ Corresponding Author; mt.gencoglu@firat.edu.tr

*Received: 25.07.2019 Accepted:27.12.2019*

**Abstract-** As a result of the digitalizing world, the importance of communication security continues to increase. Encryption, which is one of the most important elements of communication security, has become a powerful tool for information security in many applications. In this study, the applications of Bernoulli numbers in the field of influence have been examined and an encryption method based on this has been suggested. Then, the message was encrypted with the proposed method, embedded in an audio file, the application was performed and then the performance of the method was analyzed.

**Keywords** Cryptography, Bernoulli Numbers, Cryptographic Defense, Embedded Audio

## 1. Introduction

Security in the cyber environment has become an indispensable element of vital importance. Even, cyber intelligence activities are carried out over social media data by infiltrating the smartphones used by the people with the social media platforms introduced to the market. It is therefore proposed encrypted messaging and encryption.

Cypher is an algorithm used to perform encryption and decryption encrypted message covers whole the data of the plain text message but is not in a human or computer-readable format, which does not have a suitable mechanism for decrypting it.

Ciphers are usually parameterized by ancillary knowledge called a key. The encryption process depends on the key that alteration the comprehensive operation of the algorithm [1-4].

Bernoulli numbers are useful in certain counting problems. Bernoulli numbers are associated with recursive algorithms. For the series "recursive relationship" is an equation that is associated with the terms. There are some studies about the Bernoulli number and its application to cryptography [5-10].

In the second part of this study, the definition of Bernoulli numbers will be given and then the B^n Bernoulli matrix will be written. In the third chapter, the cryptographic application will be explained and an example will be given. In the fourth section, the performance of the proposed method will be tested and the encryption and decryption steps will be given. In the fifth section, experimental results will be given and in the last section results and interpretations will be given.

## 2. Bernoulli Numbers

The Bernoulli numbers are described by

$$\frac{x}{e^{x-1}} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}, \quad |x| < 2\pi \tag{1}$$

Bernoulli is

$$B_n = \sum_{k=0}^{n} \binom{n}{k} B_k \;\; for\; n \geq 2 \tag{2}$$

Taking

$$B_0 = 1\,, B_1 = -\frac{1}{2}$$

which successively produces the values

$$B_2 = \frac{1}{6}\,, B_4 = -\frac{1}{30}\,, B_6 = \frac{1}{42}, B_8 = -\frac{1}{30}\,, B_{10} = \frac{5}{66}\,, B_{12} = -\frac{691}{2730}, \ldots$$

$$B_{2k+1} = 0\,, (\,k = 1,2,\ldots\,)$$

Furthermore, the Bernoulli numbers $B_{2k}$ alternate in sign, and re-associated with Riemann zeta function $\zeta(2k)$ as follows:

$$\zeta(2k) = (-1)^{k+1} \frac{(2\pi)^{2k} B_{2k}}{2(2k)!} \tag{3}$$

The suggested matrix using Bernoulli is

$$B^{n} = \begin{bmatrix} B_{n-1} & B_n \\ B_n & B_{n+1} \end{bmatrix} \tag{4}$$

$$\Rightarrow B_1 = \begin{bmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{6} \end{bmatrix} \equiv \begin{bmatrix} 1 & 14 \\ 14 & 5 \end{bmatrix} (mod\ 29)$$

The widening of the above matrix is as follows

$$\Rightarrow B_2 = \begin{bmatrix} 1 & -\frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{6} & 0 \\ 0 & 0 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 14 & 0 \\ 14 & 5 & 0 \\ 0 & 0 & 1 \end{bmatrix} (mod\ 29) \tag{5}$$

$$B_2^{-1} = \begin{bmatrix} -2 & -6 & 0 \\ -6 & -12 & 0 \\ 0 & 0 & 1 \end{bmatrix} \equiv \begin{bmatrix} 27 & 23 & 0 \\ 23 & 17 & 0 \\ 0 & 0 & 1 \end{bmatrix} (mod\ 29) \tag{6}$$

For any variable x

$$B_2^{-1} = \begin{bmatrix} -2 & -6 & 0 \\ -6 & -12 & 0 \\ 0 & 0 & 1 \end{bmatrix} \equiv \begin{bmatrix} 27 & 23 & 0 \\ 23 & 17 & 0 \\ 0 & 0 & 1 \end{bmatrix} (mod\ 29) \tag{7}$$

The other forms of $B^n$ can be obtained similarly.

## 3. Application Cryptography

In this section will be examined a practice with a new size in the matrix of the substitution method and mode 29 for the Türkish alphabet will be used for digital transformation. Table 1 gives the Türkish alphabet substitution.scientific process.

**Table 1.** Turkish alphabet substitution

| A | B | C | Ç | D | E | F | G | Ğ | H | I | İ | J | K | L | M | N | O | Ö | P | R | S | Ş | T | U | Ü | V | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |

Let the primary message be a signal whit a real numbers sequence like $a_1, a_2, a_3, \dots, a_9, \dots$

$$A = \begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{bmatrix} \tag{8}$$

Here 9! different matrix can be obtained. If $P_i$ is permutation, the matrix selected is the encryption matrix and the inverse of this matrix is the decryption matrix. The variable x is selected as an encryption key. The K key take place of P permutation, x variable and R Bernoulli number

$$K = \{P, x, R\} \tag{9}$$

Let $C(x)$ be encrypted text matrix then encryption algorithm is[11]

```
If $R = Bern$ then
$[C] \leftarrow [A][B_2{}^x];$
$[A] \leftarrow [C][B_2{}^{-x}];$
Endif
```

### 3.1. Example

Let "PEYGAMBER" plain text to be transmitted

$$A = \begin{bmatrix} 18 & 4 & 26 \\ 6 & 0 & 14 \\ 1 & 4 & 19 \end{bmatrix}$$

$x = 1$, Bernoulli $B_2{}^n$ for $n = 2$ is

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

The first stage is to form $C(x)$. For this purpose, instead of the word PEYGAMBER 18 4 26 6 0 14 1 4 19 numerical values are written.

$$C(x) = \begin{bmatrix} 18 & 4 & 26 \\ 6 & 0 & 14 \\ 1 & 4 & 19 \end{bmatrix} x \begin{bmatrix} 1 & 14 & 0 \\ 14 & 5 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 16 & 11 & 26 \\ 6 & 26 & 14 \\ 27 & 5 & 19 \end{bmatrix}$$

Thus "PEYGAMBER" plain text converts "OJYGYMZFR".

The second stage is the computation of A from

$C(x)$

$$A = \begin{bmatrix} 16 & 11 & 26 \\ 6 & 26 & 14 \\ 27 & 5 & 19 \end{bmatrix} x \begin{bmatrix} 27 & 23 & 0 \\ 23 & 17 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 18 & 4 & 26 \\ 6 & 0 & 14 \\ 1 & 4 & 19 \end{bmatrix}$$

Then; instead of OJYGYMZFR is written 17 12 27 7 27 15 28 6 20 numerical values. From here; The chipper text “OJYGYMZFR” turns into "PEYGAMBER".

## 4. The efficiency of The Suggested Technique

It is feasible to rise encrypted conservation by using more than one encryption and decryption [11]. The first step of encryption is to adopt incidental $P$ and $x$. Let the first value of permutation be $P_i$ and variable $x_1$. Therefore, the first encryption key will be

$$K_1 = \{P_i, x_1, R\}$$

This value is owing to the encryption matrix

$$C_1 = C(P_i, x_1, R)$$

The second encryption key will be

$$K_2 = \{P_j, x_2, R\}$$

The new matrix created by this encryption key is

$$C_2 = C_1(P_i, x_1, R; P_j, x_2, R)$$

However, this procedure may be recapped n times and the $C = C(K)$ matrix is taken for the n value of the variable.

That is

$$K = \{P_i, x_1, R; P_j, x_2, R \ldots P_k, x_n, R.\} \qquad (10)$$

Consequently this more than one encryption; For the decryption algorithm, When we use the inverse encryption key, $K^{-1}$due to the closeness feature is equal to

$$K^{-1} = \{P_k, x_n, R; P_r, x_{n-1}, R; \ldots\ldots\ldots.P_i, x_1, R\} \qquad (11)$$

### 4.1. Encryption

The steps of the suggested encryption technic are as follows;

Step1. $[B^n]$ Bernoulli matrix is assigned.

Step2. The real numbers corresponding to the letters of the plain text are assigned.

Step3. From these numbers, the matrix A of the same type as the $B^n$ Bernoulli matrix is determined.

Step4. $[C(x)] = [A]x[B^n]$ is written to the encryption matrix.

Step5. The elements of the matrix$[C(x)]$ are hidden in any text by a special method.

Step6. This hidden text is embedded in the stego file.

Step7. The embedded audio file is sent to the recipient.

Flow Diagram of Encryption is shown in Fig.1.

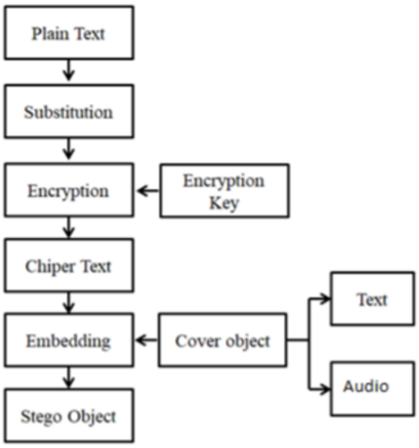


Fig.1. Flow Diagram of Encryption

### 4.2. Decryption

The steps of the suggested decryption technic are as follows;

Step1. The hidden text from the incoming audio file opens.

Step2. By decoding the hidden text, the matrix. $[C(x)]$ is obtained.

Step3. $[A] = [C(x)].[B^{-n}]$ decryption matrix is written.

Step4. The letters corresponding to the elements of [A] matrix are written.

Step5. Plain text is obtained.

Flow Diagram of Decryption is shown in Fig.2.

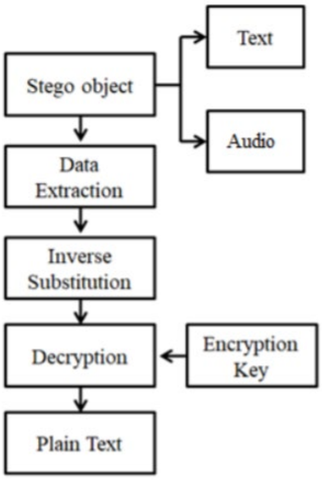


Fig.2. Flow Diagram of Decryption

## 5. Empirical Conclusion

In this part, audio files are used as data hiding environment [12,13]. The main audio window is shown in Fig.3. Data encryption and embedding window are shown in Fig.4. Matlab window for audio is shown in Fig. 5.

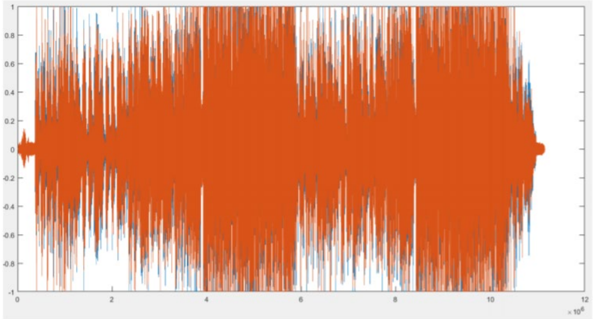


Fig. 3. The main window for audio.

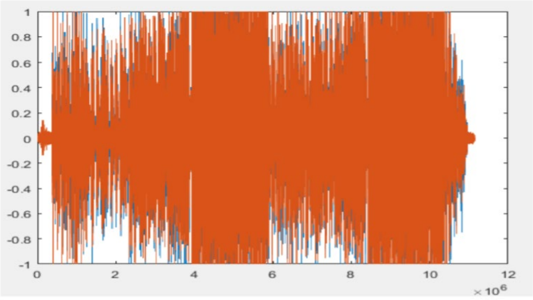
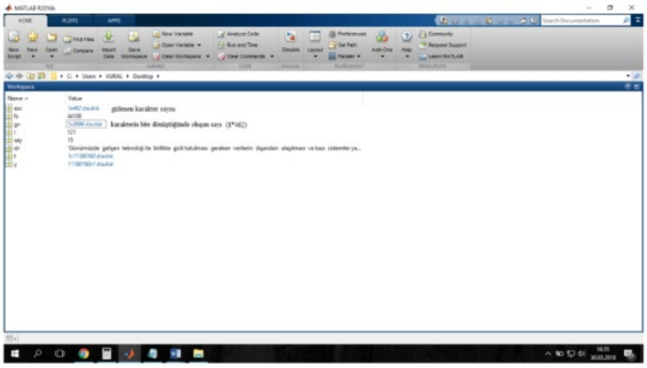


Fig. 4. Data encryption and embedding window for audio.



| Name | Value |
|---|---|
| asc | 1x462 double gizlenen karakter sayısı |
| fs | 44100 |
| gv | 1x3696 double karakterin bite dönüştüğünde oluşan sayı (8*462) |
| i | 121 |
| say | 15 |
| str | 'Günümüzde gelişen teknoloji ile birlikte gizli tutulması gereken verilerin dışardan ulaşılması ve bazı sistemler ya... |
| t | 1x11180160 double |
| y | 11180160x1 double |

Fig. 5.Matlab window for audio

## 6. Conclusions

The above method means symmetric cryptography. The security level is more because it contains three parameters, such as permutation, the strength of the matrix, the use of Bernoulli. In addition, the password conservation of the signals can be advanced by using more than one encryption and decryption. Also, by resing the size of the matrix, more knowledge can be send off safely. The security level can be increased by supporting with steganography techniques. As a result, the security of the proposed method is increased by data encryption and embedding audio.

In this study, it has been proved that security problem which is one of the most important problems for cryptography can be solved by using recursive mathematical functions such as Bernoulli numbers. In addition, the proposed method can be developed using other recursive expressions, Lucas and Fibonacci numbers. The most important contribution of this study to the literature; mathematics will be vital in encryption systems and cyber security.

## References

[1] Ç.K. Koç, Cryptographic Engineering, Springer. PP 125-128, 2009.

[2] C. Paar, C. and J. Pelzl, Understanding Cryptography, Springer 2010.

[3] K. M. Martin, Everyday Cryptography Fundamental Principles and Applications, Oxford University Press 2012.

[4] H. Delfs, and H. Knebl, Introduction to Cryptography Principles and Applications, Springer 2007.

[5] Z. Tianping, M. Yuankui, "On Generalized Fibonacci Polynomials and Bernoulli Numbers" Journal of Integer Sequences, Vol. 8 (2005), pp1-6

[6] M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, New York, 1976.

[7] V. Hoggat, "Fibonacci and Lucas numbers". Palo Alto, CA: Houghton-Mifflin; 1969.

[8] D. Tony, Noe, Jonathan Vos Post "Primes in Fibonacci n-step and Lucas n-step Sequences" Journal of Integer Sequences, Vol. 8 (2005), Article 05.4.4, pp1-12

[9] T. Koshy, Fibonacci and Lucas Numbers with Applications, John Wile y and Sons, NY, 2001

[10] R. A. Mollin, An Introduction to Cryptography, Chapman, 2007.

[11] K. R. Sudha, A. C. Sekhar, P. Reddy, Cryptography Protection of Digital Signals using Some Recurrence Relations, Ijcsns, 7(5) (2007), pp.203-207.

[12] M. Vural, M. T. Gençoğlu, Embedded Audıo Codıng Usıng Laplace Transform For Turkısh Letters, Journal of the Technical University - Sofia Plovdiv branch, Bulgaria "Fundamental Sciences and Applications", Vol. 24 (2018), pp.109-116.

[13] M. T. Gençoğlu, Embedded Image Codıng Usıng Laplace Transform For Turkısh Letters, Multimedia Tools and Applications, Volume 78, Issue 13 (2019), pp 17521–17534.systems, The Institute of Electrical and Electronics Engineers, 1993. (Standards and Reports)