*Journal of Discrete Mathematical Sciences & Cryptography*
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
DOI : 10.47974/JDMSC-2233

# A new method for coding theory by third order jacobsthal sequence

Sukran Uygun *
Ersen Akinci †
*Department of Mathematics, Science and Art Faculty*
*Gaziantep University*
*Campus 27310*
*Gaziantep*
*Turkey*

**Abstract**

In this paper, we describe a coding/decoding algorithm by third order Jacobsthal and Jacobsthal-Lucas matrix sequences. In this method the blocked message matrices are based on. In this method it is used that the encryption of each message matrix use a different key. Therefore, the method is more secure. Of course, it is an important advantage using this method.

***Subject Classification:*** *68P30, 11B83, 11B39, 15B99, 11B50, 11B37, 14G50, 11T71.*

***Keywords:*** *Encoding-decoding algorithms, Third order Jacobsthal sequence.*

## 1. Introduction and Preliminaries

In [1], it is used that the generalized relations among the code matrix elements for all values of $p$ for Fibonacci coding theory. A new coding theory based on Tribonacci numbers was introduced in [2]. Basu and Das stated new coding theories based on Fibonacci $n$-step polynomials in [3]. In [4], a Fibonacci coding method using Fibonacci polynomials is presented. Prasad [6] developed a new coding procedure based on the a Lucas matrix in [6]. In [7], Shtayat and Al-Kateeb mentioned a matrix with the Perrin numbers for a coding method. Fibonacci coding and cryptography were studied in detail by the authors in [8,9]. In [10, 12, 13], the authors investigated new coding/decoding methods using Fibonacci and Lucas numbers, and their polynomials. In [11], the authors showed

* *ORCID-ID:* `0000-0002-7878-2175`
† *ORCID-ID:* `0000-0001-8517-3987`

* *E-mail:* `suygun@gantep.edu.tr (Corresponding Author)`
† *E-mail:* `ersenakinci33@gmail.com`

that a new cryptosystem, which is a modification of the Golden Cryptosystem, is secure against the attack on the chosen plaintext.

The goal of the paper is to express a new coding/decoding method by the third order Jacobsthal and Jacobsthal-Lucas matrices. We divide the message matrix into the block matrices of $3 \times 3$. We use a new numbered alphabet for each message, hence we have a more secure coding/decoding method. We determine the numbered alphabet with respsect to the number of block matrices of the message matrix. Our method will give more information security and high correct ability for data transmission.

**Definition 1:** The third order Jacobsthal $\{j_n\}_{n\in\mathbb{N}}$ number sequence is defined with starting points $j_0 = 0$, $j_1 = .1$, and $j_2 = 1$ *by* $j_{n+2} = j_{n+1} + j_n + 2j_{n-1}$. Similarly, third order Jacobsthal-Lucas $\{c_n\}_{n\in\mathbb{N}}$ number sequence is defined by $c_{n+2} = c_{n+1} + c_n + 2c_{n-1}$, with $c_0 = 2$, $c_1 = 1$, and $c_2 = 5$ where $n$ is any integer

**Definition 2:** [5] For $n \in \mathbb{N}$, the third order Jacobsthal matrix sequence $\{\hat{J}_n\}_{n\in\mathbb{N}}$ is denoted as

$$\hat{J}_{n+1} = \hat{J}_n + \hat{J}_{n-1} + 2\hat{J}_{n-2}$$

with the following initial conditions

$$\hat{J}_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \hat{J}_1 = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \text{ and } \hat{J}_2 = \begin{pmatrix} 1 & 3 & 2 \\ 1 & 1 & 2 \\ 1 & 0 & 0 \end{pmatrix}.$$

**Definition 3:** [5] For $n \in \mathbb{N}$, third order Jacobsthal-Lucas matrix sequence $\{C_n\}_{n\in\mathbb{N}}$ is denoted by the following

$$C_{n+1} = C_n + C_{n-1} + 2C_{n-2}$$

with the starting values

$$C_0 = \begin{pmatrix} 1 & 4 & 4 \\ 2 & -1 & 2 \\ 1 & 1 & -2 \end{pmatrix}, C_1 = \begin{pmatrix} 5 & 5 & 2 \\ 1 & 4 & 4 \\ 2 & -1 & 2 \end{pmatrix} \text{ and } C_2 = \begin{pmatrix} 10 & 7 & 10 \\ 5 & 5 & 2 \\ 1 & 4 & 4 \end{pmatrix}.$$

**Theorem 4:** *Assume that $n$ be any positive integer, the $n$th elements of the third order Jacobsthal and Jacobsthal-Lucas matrix sequences are demonstrated by*

$$\hat{J}_n = \begin{pmatrix} j_{n+1} & j_n + 2j_{n-1} & 2j_n \\ j_n & j_{n-1} + 2j_{n-2} & 2j_{n-1} \\ j_{n-1} & j_{n-2} + 2j_{n-3} & 2j_{n-2} \end{pmatrix},$$

and

$$C_n = \begin{pmatrix} c_{n+1} & c_n + 2c_{n-1} & 2c_n \\ c_n & c_{n-1} + 2c_{n-2} & 2c_{n-1} \\ c_{n-1} & c_{n-2} + 2c_{n-3} & 2c_{n-2} \end{pmatrix}.$$

**Theorem 5:** *Let $m, n$ be positive integers, the following identities are verified for the third order Jacobsthal and Jacobsthal-Lucas matrix sequences*

1. $\hat{J}_n = \hat{J}_1^n$
2. $\hat{J}_{m+n} = \hat{J}_m.\hat{J}_n$
3. $C_{n+1} = C_1\hat{J}_n = \hat{J}_n C_1$
4. $det(\hat{J}_n) = (-2)^n$
5. $det(C_n) = (-2)^{n-1}72$

***Proof:*** For the first proof, we use induction method. For $n = 0$, the assertion is verified. Let assume that it is satisfied by $k \leq n$. Then for the value of $k = n + 1$, it is proved that the validity of the assertion as

$$\begin{aligned}\hat{J}_1^{n+1} &= \hat{J}_1^n\hat{J}_1 = \begin{pmatrix} j_{n+1} & j_n + 2j_{n-1} & 2j_n \\ j_n & j_{n-1} + 2j_{n-2} & 2j_{n-1} \\ j_{n-1} & j_{n-2} + 2j_{n-3} & 2j_{n-2} \end{pmatrix}\begin{pmatrix} 1 & 1 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} j_{n+1} + j_n + 2j_{n-1} & j_{n+1} + 2j_n & 2j_{n+1} \\ j_n + j_{n-1} + 2j_{n-2} & j_n + 2j_{n-1} & 2j_n \\ j_{n-1} + j_{n-2} + 2j_{n-3} & j_{n-1} + 2j_{n-2} & 2j_{n-1} \end{pmatrix} = \hat{J}_{n+1}.\end{aligned}$$

The second proof can also be obtained by induction method.

For the third proof, we can again apply induction method. For $n = 0$, the statement is true. We assume that it holds for $k \leq n$. We want to show it is also true for $k = n + 1$. So, we get

$$\begin{aligned}\hat{J}_n C_1 &= \begin{pmatrix} j_{n+1} & j_n + 2j_{n-1} & 2j_n \\ j_n & j_{n-1} + 2j_{n-2} & 2j_{n-1} \\ j_{n-1} & j_{n-2} + 2j_{n-3} & 2j_{n-2} \end{pmatrix}\begin{pmatrix} 5 & 5 & 2 \\ 1 & 4 & 4 \\ 2 & -1 & 2 \end{pmatrix} \\ &= \begin{pmatrix} c_{n+2} & c_{n+1} + 2c_n & 2c_{n+1} \\ c_{n+1} & c_n + 2c_{n-1} & 2c_n \\ c_n & c_{n-1} + 2c_{n-2} & 2c_{n-1} \end{pmatrix} = C_{n+1}.\end{aligned}$$

1.1 *Coding/ Decoding Algorithm with third order Jacobsthal Sequence*

In this section, it is mentioned that a new coding/decoding algorithm by the third order Jacobsthal matrix sequence. We settle the message in a given third order matrix. Dividing the $3m \times 3m$ message matrix $M$ into $3 \times 3$ block matrices from left to right, $B_i$ for $i = 1, \ldots, m^2$, the new coding method is obtained.

The symbol matrices $B_i$, $E_i$, and $\hat{J}_n$ are demonstrated as:

$$B_i = \begin{pmatrix} b_1^i & b_2^i & b_3^i \\ b_4^i & b_5^i & b_6^i \\ b_7^i & b_8^i & b_9^i \end{pmatrix}, \qquad E_i = \begin{pmatrix} e_1^i & e_2^i & e_3^i \\ e_4^i & e_5^i & e_6^i \\ e_7^i & e_8^i & e_9^i \end{pmatrix}, \hat{J}_n = \begin{pmatrix} j_{11} & j_{12} & j_{13} \\ j_{21} & j_{22} & j_{23} \\ j_{31} & j_{32} & j_{33} \end{pmatrix}.$$

Let's now explain new coding and decoding algorithms in the following:

**Coding algorithm by third order Jacobsthal matrix sequences**

**1**. Divide the matrix $M$ into blocks $B_i$ $(1 \leq i \leq m^2)$. We can select the number $n$ as follows:

$$t = \begin{cases} 3, & m = 1 \\ 3m - 2, & \text{otherwise} \end{cases}$$

**2**. By $m$, we give the characters table according to $mod30$ (this table for the message can be exlarged according to the letters, numbers and so.). We begin " $t$" to the letter table.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ | $J$ |
| $t$ | $t+1$ | $t+2$ | $t+3$ | $t+4$ | $t+5$ | $t+6$ | $t+7$ | $t+8$ | $t+9$ |
| $K$ | $L$ | $M$ | $N$ | $O$ | $P$ | $R$ | $Q$ | $S$ | $T$ |
| $t+10$ | $t+11$ | $t+12$ | $t+13$ | $t+14$ | $t+15$ | $t+16$ | $t+17$ | $t+18$ | $t+19$ |
| $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ | $:$ | $.$ | $,$ | $0$ |
| $t+20$ | $t+21$ | $t+22$ | $t+23$ | $t+24$ | $t+25$ | $t+26$ | $t+27$ | $t+28$ | $t+29$ |

**3**. Determine $b_j^i$ $(1 \leq j \leq 9)$.

**4.** Find $det(B_i) = d_i$.

**5**. Evaluate the coding matrix as $F = [d_i,\ b_j^i,]$ $_{j \in \{1,2,3,4,6,7,8,9\}}$.

**Decoding Algorithm**

**1**. We know that $\det(\hat{J}_n B_i) = (-2)^n d_i$.

**2.** Evaluate

$$\begin{gathered}
j_{11}b_1^i + j_{12}b_4^i + j_{13}b_7^i \to e_1^i \\
j_{11}b_2^i + j_{12}b_5^i + j_{13}b_8^i \to e_2^i \\
j_{11}b_3^i + j_{12}b_6^i + j_{13}b_9^i \to e_3^i \\
j_{21}b_1^i + j_{22}b_4^i + j_{23}b_7^i \to e_4^i \\
j_{21}b_2^i + j_{22}b_5^i + j_{23}b_8^i \to e_5^i \\
j_{21}b_3^i + j_{22}b_6^i + j_{23}b_9^i \to e_6^i \\
j_{31}b_1^i + j_{32}b_4^i + j_{33}b_7^i \to e_7^i \\
j_{31}b_2^i + j_{32}b_5^i + j_{33}b_8^i \to e_8^i \\
j_{31}b_3^i + j_{32}b_6^i + j_{33}b_9^i \to e_9^i
\end{gathered}$$

**4.** Evaluate

$$(-2)^n d_i = -(j_{11}b_2^i + j_{12}x + j_{13}b_8^i)\begin{vmatrix} e_4^i & e_6^i \\ e_7^i & e_9^i \end{vmatrix}$$
$$+\left(j_{21}b_2^i + j_{22}x + j_{23}b_8^i\right)\begin{vmatrix} e_1^i & e_3^i \\ e_7^i & e_9^i \end{vmatrix} - \left(j_{31}b_2^i + j_{32}x + j_{33}b_8^i\right)\begin{vmatrix} e_1^i & e_3^i \\ e_4^i & e_6^i \end{vmatrix}$$

**5.** Substitute for $x_i = b_5^i$

**6.** Construct $Bi$ and $M$.

We can denote an application for the algorithm mentioned above by the following example.

**Example 6:** We give the message matrix as

$$\text{"}THIRD\ \ ORDER\ \ JACOBSTHAL\ \ SEQUENCES\text{"}$$

Hence, we construct the message matrix $M$ as follows

$$M = \begin{bmatrix} T & H & I & R & D & 0 \\ O & R & D & E & R & 0 \\ J & A & C & O & B & S \\ T & H & A & L & 0 & S \\ E & Q & U & E & N & C \\ E & S & . & 0 & 0 & 0 \end{bmatrix}$$

**1.** It is divided the message matrix $M$ of size $3 \times 3$ into the matrices, called $B_i$ $(1 \leq m \leq 2)$, as the following

$$B_1 = \begin{bmatrix} T & H & I \\ O & R & D \\ J & A & C \end{bmatrix} \quad B_2 = \begin{bmatrix} R & D & 0 \\ E & R & 0 \\ O & B & S \end{bmatrix}$$

$$B_3 = \begin{bmatrix} T & H & A \\ E & Q & U \\ E & S & . \end{bmatrix} \quad B_4 = \begin{bmatrix} L & 0 & S \\ E & N & C \\ 0 & 0 & 0 \end{bmatrix}$$

**2.** $n = 4 > 2$. For $n = 4$, by the "character table", we find the entries of the block matrices $B_i$ $(1 \leq i \leq 4)$. We compute the determinants $d_i$ of the blocks $B_i$:

$$B_1 = \begin{bmatrix} 23 & 11 & 12 \\ 18 & 20 & 7 \\ 13 & 4 & 6 \end{bmatrix} \text{ then } d_1 = \det(B_1) = -327$$

$$B_2 = \begin{bmatrix} 20 & 7 & 3 \\ 8 & 20 & 3 \\ 18 & 5 & 22 \end{bmatrix} \text{ then } d_2 = \det(B_2) = 6686$$

$$B_3 = \begin{bmatrix} 23 & 11 & 4 \\ 8 & 21 & 24 \\ 8 & 22 & 1 \end{bmatrix} \text{ then } d_3 = \det(B_3) = -9605$$

$$B_4 = \begin{bmatrix} 15 & 3 & 22 \\ 8 & 17 & 6 \\ 3 & 3 & 3 \end{bmatrix} \text{ then } d_4 = \det(B_4) = -117$$

**3.** We construct the $F$ matrix as:

$$F = \begin{bmatrix} -327 & 23 & 11 & 12 & 18 & 7 & 13 & 4 & 6 \\ 6686 & 20 & 7 & 3 & 8 & 3 & 18 & 5 & 22 \\ -9605 & 23 & 11 & 4 & 8 & 24 & 8 & 22 & 1 \\ -117 & 15 & 3 & 22 & 8 & 6 & 3 & 3 & 3 \end{bmatrix}$$

**Decoding Algorithm**

**1.** We choose, $n = 4$ and determine by the elements of matrix $\hat{J}_4$

$$j_{11} = 9 \quad j_{12} = 9 \quad j_{13} = 10$$
$$j_{21} = 5 \quad j_{22} = 4 \quad j_{23} = 4$$
$$j_{31} = 2 \quad j_{32} = 3 \quad j_{33} = 2$$

**2.** We evaluate $e_3^i$ to find the matrices $E_i$:

$e_1^1=499$ $e_2^1=319$ $e_3^1=231$ $e_4^1=239$ $e_5^1=151$ $e_6^1=112$ $e_7^1=126$ $e_8^1=90$ $e_9^1=57$
$e_1^2=432$ $e_2^2=293$ $e_3^2=274$ $e_4^2=204$ $e_5^2=135$ $e_6^2=115$ $e_7^2=100$ $e_8^2=84$ $e_9^2=59$
$e_1^3=359$ $e_2^3=508$ $e_3^3=262$ $e_4^3=179$ $e_5^3=227$ $e_6^3=120$ $e_7^3=86$ $e_8^3=129$ $e_9^3=82$
$e_1^4=237$ $e_2^4=210$ $e_3^4=282$ $e_4^4=119$ $e_5^4=95$ $e_6^4=146$ $e_7^4=60$ $e_8^4=63$ $e_9^4=68$

**3.** We calculate the elements $x_i$:

$$(-2)^4(-327)=-(9b_2^1+9x_1+10b_8^1)\begin{vmatrix} e_4^1 & e_6^1 \\ e_7^1 & e_9^1 \end{vmatrix}+(5b_2^1+4x_1+4b_8^1)\begin{vmatrix} e_1^1 & e_3^1 \\ e_7^1 & e_9^1 \end{vmatrix}$$
$$-(2b_2^1+3x_1+2b_8^1)\begin{vmatrix} e_1^1 & e_3^1 \\ e_4^1 & e_6^1 \end{vmatrix}$$

$$(-2)^4(-327)=-(9.11+9x_1+10.4)\begin{vmatrix} 239 & 231 \\ 126 & 57 \end{vmatrix}+(5.11+4x_1+4.4)\begin{vmatrix} 499 & 231 \\ 126 & 57 \end{vmatrix}$$
$$-(2.11+3x_1+2.4)\begin{vmatrix} 499 & 231 \\ 239 & 112 \end{vmatrix}$$

$$-5232=-(139+9x_1)(-489)+(71+4x_1)(-663)-(30+3x_1)679$$
$$x_1=20$$

$$(-2)^4(6686)=-(9b_2^2+9x_2+10b_8^2)\begin{vmatrix} e_4^2 & e_6^2 \\ e_7^2 & e_9^2 \end{vmatrix}+(5b_2^2+4x_2+4b_8^2)\begin{vmatrix} e_1^2 & e_3^2 \\ e_7^2 & e_9^2 \end{vmatrix}$$
$$-(2b_2^2+3x_2+2b_8^2)\begin{vmatrix} e_1^2 & e_3^2 \\ e_4^2 & e_6^2 \end{vmatrix}$$

$$(-2)^4(6686)=-(9.7+9x_2+10.5)\begin{vmatrix} 204 & 115 \\ 100 & 59 \end{vmatrix}+(5.7+4x_2+4.5)\begin{vmatrix} 432 & 274 \\ 100 & 59 \end{vmatrix}$$
$$-(2.7+3x_2+2.5)\begin{vmatrix} 432 & 274 \\ 204 & 115 \end{vmatrix}$$

$$106976=-(113+9x_2)536+(55+4x_2)(-1912)-(24+3x_2)(-6216)$$
$$x_2=20$$

$$(-2)^4(-9605)=-(9b_2^3+9x_3+10b_8^3)\begin{vmatrix} e_4^3 & e_6^3 \\ e_7^3 & e_9^3 \end{vmatrix}+(5b_2^3+4x_3+4b_8^3)\begin{vmatrix} e_1^3 & e_3^3 \\ e_7^3 & e_9^3 \end{vmatrix}$$
$$-(2b_2^3+3x_3+2b_8^3)\begin{vmatrix} e_1^3 & e_3^3 \\ e_4^3 & e_6^3 \end{vmatrix}$$

$$(-2)^4(-9605)=-(9.11+9x_3+10.22)\begin{vmatrix} 179 & 120 \\ 86 & 82 \end{vmatrix}+(5.11+4x_3+4.22)\begin{vmatrix} 359 & 262 \\ 86 & 82 \end{vmatrix}$$
$$-(2.11+3x_3+2.22)\begin{vmatrix} 359 & 262 \\ 179 & 120 \end{vmatrix}$$

$$-153680=-(319+9x_3)4358+(187+4x_3)(6906)-(66+3x_3)(-3818)$$
$$-153680+144x_3=-150656$$
$$x_3=21$$

$$(-2)^4(-117) = -(9b_2^4 + 9x_4 + 10b_8^4)\begin{vmatrix} e_4^4 & e_6^4 \\ e_7^4 & e_9^4 \end{vmatrix} + (5b_2^4 + 4x_4 + 4b_8^4)\begin{vmatrix} e_1^4 & e_3^4 \\ e_7^4 & e_9^4 \end{vmatrix}$$
$$-(2b_2^4 + 3x_4 + 2b_8^4)\begin{vmatrix} e_1^4 & e_3^4 \\ e_4^4 & e_6^4 \end{vmatrix}$$
$$(-2)^4(-117) = -(9.3 + 9x_4 + 10.3)\begin{vmatrix} 119 & 146 \\ 60 & 68 \end{vmatrix} + (5.3 + 4x_4 + 4.3)\begin{vmatrix} 237 & 282 \\ 60 & 68 \end{vmatrix}$$
$$-(2.3 + 3x_4 + 2.3)\begin{vmatrix} 237 & 282 \\ 119 & 146 \end{vmatrix}$$
$$-1872 = -(57 + 9x_4)(-668) + (27 + 4x_4)(-804) - (12 + 3x_4)(1044)$$
$$x_4 = 17$$

**4** We determine $x_i$

$$x_1 = b_5^1 = 20 x_2 = b_5^2 = 20 x_3 = b_5^3 = 21 x_4 = b_5^4 = 17$$

**5** We construct the block matrices $B_i$ and $M$:

$$F = \begin{bmatrix} -327 & 23 & 11 & 12 & 18 & 7 & 13 & 4 & 6 \\ 6686 & 20 & 7 & 3 & 8 & 3 & 18 & 5 & 22 \\ -9605 & 23 & 11 & 4 & 8 & 24 & 8 & 22 & 1 \\ -117 & 15 & 3 & 22 & 8 & 6 & 3 & 3 & 3 \end{bmatrix}$$

$$M = \begin{bmatrix} T & H & I & R & D & 0 \\ O & R & D & E & R & 0 \\ J & A & C & O & B & S \\ T & H & A & L & 0 & S \\ E & Q & U & E & N & C \\ E & S & . & 0 & 0 & 0 \end{bmatrix}$$

**Coding Algorithm by third order Jacobsthal-Lucas matrix**

**1**. First we split the message matrix $M$ $3b$ by $3b$ into blocks $B_i$ $(1 \le i \le b^2)$ of size $3 \times 3$. Assume that the symbol matrices of the coding method $B_i$, $E_i$ and $\hat{J}_n$ are given as:

$$B_i = \begin{pmatrix} b_1^i & b_2^i & b_3^i \\ b_4^i & b_5^i & b_6^i \\ b_7^i & b_8^i & b_9^i \end{pmatrix},\ E_i = \begin{pmatrix} e_1^i & e_2^i & e_3^i \\ e_4^i & e_5^i & e_6^i \\ e_7^i & e_8^i & e_9^i \end{pmatrix} = \begin{cases} \hat{J}_m B_i, & i \quad odd \\ C_n B_i, & i \quad even \end{cases},$$
$$\hat{J}_m = \begin{pmatrix} j_{11} & j_{12} & j_{13} \\ j_{21} & j_{22} & j_{23} \\ j_{31} & j_{32} & j_{33} \end{pmatrix},\quad C_n = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix}.$$

Notice that

$$det(E_i) = \begin{cases} (-2)^m, & i \quad odd \\ (-2)^n 72, & i \quad even \end{cases}.$$

We can choose $m, \quad n$ as $m = \begin{cases} 4, & b = 1 \\ b+2, & b \neq 1 \end{cases}$ and

$$n = \begin{cases} 5, & b = 1 \\ 2b-2, & b \neq 1 \end{cases}.$$

**2**. This table is used transforming characteristics to numbers $(mod 30)$

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ | $J$ |
| $p$ | $p+1$ | $p+2$ | $p+3$ | $p+4$ | $p+5$ | $p+6$ | $p+7$ | $p+8$ | $p+9$ |
| $K$ | $L$ | $M$ | $N$ | $O$ | $P$ | $R$ | $Q$ | $S$ | $T$ |
| $p+10$ | $p+11$ | $p+12$ | $p+13$ | $p+14$ | $p+15$ | $p+16$ | $p+17$ | $p+18$ | $p+19$ |
| $U$ | $V$ | $W$ | $X$ | $Y$ | $Z$ | $:$ | $.$ | $,$ | $0$ |
| $p+20$ | $p+21$ | $p+22$ | $p+23$ | $p+24$ | $p+25$ | $p+26$ | $p+27$ | $p+28$ | $p+29$ |

where $p = \begin{cases} m, & i \quad odd \\ n, & i \quad even \end{cases}.$

**3**. Determine $b_j^i, \quad (1 \leq j \leq 9)$

**4.** Compute $det(B_i) = d_i$.

**5**. Construct the coding matrix $F = [d_i, b_j^i,]_{j \in \{1,2,3,4,6,7,8,9\}}$.

**Decoding Algorithm**

**1**. For $i$ odd, the first column are used to evaluate, and for $i$ even, the second column are used to evaluate:

$$\begin{array}{ll}
j_{11}b_1^i + j_{12}b_4^i + j_{13}b_7^i \to e_1^i & c_{11}b_1^i + c_{12}b_4^i + c_{13}b_7^i \to e_1^i \\
j_{11}b_2^i + j_{12}b_5^i + j_{13}b_8^i \to e_2^i & c_{11}b_2^i + c_{12}b_5^i + c_{13}b_8^i \to e_2^i \\
j_{11}b_3^i + j_{12}b_6^i + j_{13}b_9^i \to e_3^i & c_{11}b_3^i + c_{12}b_6^i + c_{13}b_9^i \to e_3^i \\
j_{21}b_1^i + j_{22}b_4^i + j_{23}b_7^i \to e_4^i & c_{21}b_1^i + c_{22}b_4^i + c_{23}b_7^i \to e_4^i \\
j_{21}b_2^i + j_{22}b_5^i + j_{23}b_8^i \to e_5^i & c_{21}b_2^i + c_{22}b_5^i + c_{23}b_8^i \to e_5^i \\
j_{21}b_3^i + j_{22}b_6^i + j_{23}b_9^i \to e_6^i & c_{21}b_3^i + c_{22}b_6^i + c_{23}b_9^i \to e_6^i \\
j_{31}b_1^i + j_{32}b_4^i + j_{33}b_7^i \to e_7^i & c_{31}b_1^i + c_{32}b_4^i + c_{33}b_7^i \to e_7^i \\
j_{31}b_2^i + j_{32}b_5^i + j_{33}b_8^i \to e_8^i & c_{31}b_2^i + c_{32}b_5^i + c_{33}b_8^i \to e_8^i \\
j_{31}b_3^i + j_{32}b_6^i + j_{33}b_9^i \to e_9^i & c_{31}b_3^i + c_{32}b_6^i + c_{33}b_9^i \to e_9^i
\end{array}$$

**2.** So, we get

$$(-2)^n d_i = -(j_{11}b_2^i + j_{12}x + j_{13}b_8^i) \begin{vmatrix} e_4^i & e_6^i \\ e_7^i & e_9^i \end{vmatrix} + \left(j_{21}b_2^i + j_{22}x + j_{23}b_8^i\right) \begin{vmatrix} e_1^i & e_3^i \\ e_7^i & e_9^i \end{vmatrix} - \left(j_{31}b_2^i + j_{32}x + j_{33}b_8^i\right) \begin{vmatrix} e_1^i & e_3^i \\ e_4^i & e_6^i \end{vmatrix}, \quad i \quad \text{odd}$$

$$(-2)^n 72 d_i = -(c_{11}b_2^i + c_{12}x + c_{13}b_8^i) \begin{vmatrix} e_4^i & e_6^i \\ e_7^i & e_9^i \end{vmatrix} + \left(c_{21}b_2^i + c_{22}x + c_{23}b_8^i\right) \begin{vmatrix} e_1^i & e_3^i \\ e_7^i & e_9^i \end{vmatrix} - \left(c_{31}b_2^i + c_{32}x + c_{33}b_8^i\right) \begin{vmatrix} e_1^i & e_3^i \\ e_4^i & e_6^i \end{vmatrix}, \quad i \quad \text{even}$$

**3.** Substitute for $x_i = b_5^i$

**4.** Construct $Bi$ and $M$.

This example shows us an application of the above method.

**Example 7:** Assume that the message text is given as

$$"MATHEMATICS\ \ CRYPTOLOGY\ \ JACOBSTHAL"$$

The message matrix $M$ are obtained as follows:

$$M = \begin{bmatrix} M & A & T & H & E & M \\ A & T & I & C & S & 0 \\ C & R & Y & P & T & O \\ L & O & G & Y & 0 & J \\ A & C & O & B & S & T \\ H & A & L & 0 & 0 & 0 \end{bmatrix}.$$

We split the message matrix $M$ of size $3 \times 3$ into the matrices, $B_i$ $(1 \leq m \leq 2)$,

$$B_1 = \begin{bmatrix} M & A & T \\ A & T & I \\ C & R & Y \end{bmatrix}, B_2 = \begin{bmatrix} H & E & M \\ C & S & 0 \\ P & T & O \end{bmatrix}, B_3 = \begin{bmatrix} L & O & G \\ A & C & O \\ H & A & L \end{bmatrix}, B_4 = \begin{bmatrix} Y & 0 & J \\ B & S & T \\ 0 & 0 & 0 \end{bmatrix}$$

It is easily seen that $b = 2$. For $m = 4,\ n = 2,$ we use the "character table" for $M$ matrix. The elements of the blocks $B_i$ $(1 \leq i \leq 4)$ are obtained as: We evaluate the determinants $d_i$ of the blocks $B_i$:

$$B_1 = \begin{bmatrix} 16 & 4 & 23 \\ 4 & 23 & 12 \\ 6 & 20 & 28 \end{bmatrix} \text{ then we get } d_1 = \det(B_1) = 4970$$

$$B_2 = \begin{bmatrix} 9 & 6 & 14 \\ 4 & 20 & 31 \\ 17 & 21 & 16 \end{bmatrix} \text{ then we get } d_2 = \det(B_2) = -3785$$

$$B_3 = \begin{bmatrix} 15 & 18 & 10 \\ 4 & 6 & 18 \\ 11 & 4 & 5 \end{bmatrix} \text{ then we get } d_3 = \det(B_3) = 2254$$

$$B_4 = \begin{bmatrix} 26 & 31 & 11 \\ 3 & 20 & 21 \\ 31 & 31 & 31 \end{bmatrix} \text{ then we get } d_4 = \det(B_4) = 10695$$

We have the $F$ matrix as:

$$F = \begin{bmatrix} 4970 & 16 & 4 & 23 & 4 & 12 & 6 & 20 & 28 \\ -3785 & 9 & 6 & 14 & 4 & 31 & 17 & 21 & 16 \\ 2254 & 15 & 18 & 10 & 4 & 18 & 11 & 4 & 5 \\ 10695 & 26 & 31 & 11 & 3 & 21 & 31 & 31 & 31 \end{bmatrix}$$

**Decoding Algorithm**

We know $m = 4,\ n = 2,$ and determine

$$\begin{array}{lll} j_{11} = 9 & j_{12} = 9 & j_{13} = 10 \\ j_{21} = 5 & j_{22} = 4 & j_{23} = 4 \\ j_{31} = 2 & j_{32} = 3 & j_{33} = 2 \end{array}$$

and

$$c_{11}=10 \quad c_{12}=7 \quad c_{13}=10$$
$$c_{21}=5 \quad c_{22}=5 \quad c_{23}=2$$
$$c_{31}=2 \quad c_{32}=4 \quad c_{33}=4$$

We evaluate the elements of the matrix $E_i$ as:

$e_1^1=240$ $e_2^1=443$ $e_3^1=595$ $e_4^1=120$ $e_5^1=192$ $e_6^1=275$ $e_7^1=56$ $e_8^1=117$ $e_9^1=138$
$e_1^2=288$ $e_2^2=410$ $e_3^2=517$ $e_4^2=99$ $e_5^2=172$ $e_6^2=257$ $e_7^2=93$ $e_8^2=170$ $e_9^2=202$
$e_1^3=281$ $e_2^3=256$ $e_3^3=402$ $e_4^3=135$ $e_5^3=130$ $e_6^3=182$ $e_7^3=64$ $e_8^3=62$ $e_9^3=104$
$e_1^4=591$ $e_2^4=760$ $e_3^4=567$ $e_4^4=207$ $e_5^4=317$ $e_6^4=222$ $e_7^4=162$ $e_8^4=235$ $e_9^4=219.$

We calculate the elements

$$2^4(4970)=-(9b_2^1+9x_1+10b_8^1)\begin{vmatrix} e_4^1 & e_6^1 \\ e_7^1 & e_9^1 \end{vmatrix}+(5b_2^1+4x_1+4b_8^1)\begin{vmatrix} e_1^1 & e_3^1 \\ e_7^1 & e_9^1 \end{vmatrix}$$
$$-(2b_2^1+3x_1+2b_8^1)\begin{vmatrix} e_1^1 & e_3^1 \\ e_4^1 & e_6^1 \end{vmatrix}$$
$$2^4(4970)=-(9.4+9x_1+10.20)\begin{vmatrix} 120 & 275 \\ 56 & 138 \end{vmatrix}+(5.4+4x_1+4.20)\begin{vmatrix} 240 & 595 \\ 56 & 138 \end{vmatrix}$$
$$-(2.4+3x_1+2.20)\begin{vmatrix} 240 & 595 \\ 120 & 275 \end{vmatrix}$$
$$x_1=23$$

$$144(-3785)=-(10b_2^2+7x_2+10b_8^2)\begin{vmatrix} e_4^2 & e_6^2 \\ e_7^2 & e_9^2 \end{vmatrix}+(5b_2^2+5x_2+2b_8^2)\begin{vmatrix} e_1^2 & e_3^2 \\ e_7^2 & e_9^2 \end{vmatrix}$$
$$-(b_2^2+4x_2+4b_8^2)\begin{vmatrix} e_1^2 & e_3^2 \\ e_4^2 & e_6^2 \end{vmatrix}$$
$$2^2 72(-3785)=-(10.6+7x_2+10.21)\begin{vmatrix} 99 & 257 \\ 93 & 202 \end{vmatrix}+(5.6+5x_2+2.21)\begin{vmatrix} 288 & 517 \\ 93 & 202 \end{vmatrix}$$
$$-(1.6+4x_2+4.21)\begin{vmatrix} 288 & 517 \\ 99 & 257 \end{vmatrix}$$
$$x_2=20$$
$$2^4(2254)=-(9b_2^3+9x_3+10b_8^3)\begin{vmatrix} e_4^3 & e_6^3 \\ e_7^3 & e_9^3 \end{vmatrix}+(5b_2^3+4x_3+4b_8^3)\begin{vmatrix} e_1^3 & e_3^3 \\ e_7^3 & e_9^3 \end{vmatrix}$$
$$-(2b_2^3+3x_3+2b_8^3)\begin{vmatrix} e_1^3 & e_3^3 \\ e_4^3 & e_6^3 \end{vmatrix}$$
$$36064=-(9.18+9x_3+10.4)\begin{vmatrix} 135 & 182 \\ 64 & 104 \end{vmatrix}+(5.18+4x_3+4.4)\begin{vmatrix} 281 & 402 \\ 64 & 104 \end{vmatrix}$$

$$-(2.18+3x_3+2.4)\begin{vmatrix}281 & 402\\135 & 182\end{vmatrix}$$

$$x_3 = 6$$

$$144(10695) = -(10b_2^4+7x_4+10b_8^4)\begin{vmatrix}e_4^4 & e_6^4\\e_7^4 & e_9^4\end{vmatrix} + (5b_2^4+5x_4+2b_8^4)\begin{vmatrix}e_1^4 & e_3^4\\e_7^4 & e_9^4\end{vmatrix}$$

$$-(b_2^4+4x_4+4b_8^4)\begin{vmatrix}e_1^4 & e_3^4\\e_4^4 & e_6^4\end{vmatrix}$$

$$1540080 = -(10.31+7x_4+10.31)\begin{vmatrix}207 & 222\\162 & 219\end{vmatrix}(5.31+5x_4+2.31)\begin{vmatrix}591 & 567\\162 & 219\end{vmatrix}$$

$$-(1.31+4x_4+4.31)\begin{vmatrix}591 & 567\\207 & 222\end{vmatrix}$$

$$x_4 = -20$$

We determine $x_i$

$$x_1 = b_5^1 = 23 \quad x_2 = b_5^2 = 20 \quad x_3 = b_5^3 = 6 \quad x_4 = b_5^4 = 20$$

We construct the block matrices $B_i$ and $M$:

$$F = \begin{bmatrix}-327 & 23 & 11 & 12 & 18 & 7 & 13 & 4 & 6\\ 6686 & 20 & 7 & 3 & 8 & 3 & 18 & 5 & 22\\ -9605 & 23 & 11 & 4 & 8 & 24 & 8 & 22 & 1\\ -117 & 15 & 3 & 22 & 8 & 6 & 3 & 3 & 3\end{bmatrix}$$

$$M = \begin{bmatrix}T & H & I & R & D & 0\\ O & R & D & E & R & 0\\ J & A & C & O & B & S\\ T & H & A & L & 0 & S\\ E & Q & U & E & N & C\\ E & S & . & 0 & 0 & 0\end{bmatrix}$$

**Conclusion**

In this article, we developed new algorithms in coding theory with the help of $J$-matrix and $C$-matrix. In the algorithms, we divide the desired message into blocks and transform the message matrix into an encoded message matrix. In the decryption process, we converted the encrypted message matrix to the desired message matrix by using the $J$-matrix and $C$-matrix.

## References

[1] M. Basu and B. Prasad, "The generalized relations among the code elements for Fibonacci coding theory," *Chaos Solitons Fractals*, vol. 41, no. 5, pp. 2517–2525 (2009), doi: 10.1016/j.chaos.2008.09.030.

[2] M. Basu and M. Das, "Tribonacci matrices and a new coding theory," *Discrete Math. Algorithms Appl.,* vol. 6, no. 1, p. 1450008 (2014), doi: 10.1142/S1793830914500086.

[3] M. Basu and M. Das, "Coding theory on Fibonacci n-step numbers," *Discrete Math. Algorithms Appl.*, vol. 6, no. 2, p. 1450017 (2014), doi: 10.1142/S1793830914500177.

[4] M. Esmaeili and M. Esmaeili, "Fibonacci-polynomial based coding method with error detection and correction," *Comput. Math. Appl.*, vol. 60, no. 10, pp. 2738–2752 (2010).

[5] G. C. Morales, "On the third-order Jacobsthal and third-order Jacobsthal–Lucas sequences and their matrix representations," *Mediterr. J. Math.*, pp. 16–32 (2019), doi: 10.1007/s00009-019-1319-9.

[6] B. Prasad, "Coding theory on Lucas p-numbers," *Discrete Math. Algorithms Appl.,* vol. 8, no. 4, 17 pages (2016).

[7] J. Shtayat and A. Al-Kateeb, "The Perrin R-matrix and more properties with an application," *J. Discrete Math. Sci. Cryptogr.,* vol. 25, no. 1, pp. 41–52 (2022), doi: 10.1080/09720529.2020.1866299.

[8] A. P. Stakhov, "Fibonacci matrices, a generalization of the Cassini formula and a new coding theory," *Chaos Solitons Fractals*, vol. 30, no. 1, pp. 56–66 (2006).

[9] A. Stakhov, V. Massingue, and A. Sluchenkov, Introduction into Fibonacci Coding and Cryptography. Kharkov, Ukraine: Osnova (1999).

[10] N. Tas, S. Ucar, N. Y. Ozgur, and O. O. Kaymak, "A new coding/ decoding algorithm using Fibonacci numbers," *Discrete Math. Algorithms Appl.*, vol. 2, p. 1850028 (2018).

[11] M. Tahghighi, A. R. Jafaar, and A. R. Mahmod, "Generalization of Golden Cryptography based on k-Fibonacci numbers," presented at the Int. Conf. Information and Network Communication (ICINC) (2010).

[12] S. Uçar and N. Y. Ozgur, "Right circulant matrices with generalized Fibonacci and Lucas polynomials and coding theory," *J. BAUN Inst. Sci. Technol.*, vol. 21, no. 1, pp. 306–322 (2019).

[13] S. Uçar, N. Tas, and N. Y. Özgür, "A new application to coding theory via Fibonacci and Lucas numbers," *Math. Sci. Appl. e-Notes,* vol. 7, no. 1, pp. 62–70 (2019).

*Received May, 2024*