

# A New Application to Coding Theory via Fibonacci and Lucas Numbers

Sümeyra Uçar\*, Nihal Taş and Nihal Yılmaz Özgür

## Abstract

Coding/decoding algorithms are of great importance to help in improving information security since information security is a more significant problem in recent years. In this paper we introduce two new coding/decoding algorithms using Fibonacci  $Q$ -matrices and  $R$ -matrices. Our models are based on the blocked message matrices and the encryption of each message matrix with different keys. These new algorithms will not only increase the security of information but also has high correct ability.

*Keywords:* coding/decoding algorithm; Fibonacci  $Q$ -matrix;  $R$ -matrix; minesweeper.

*AMS Subject Classification (2010):* Primary: 68P30 ; Secondary: 11B39, 11B37.

\*Corresponding author

## 1. Introduction

It is well known that the sequences of Fibonacci and Lucas numbers are defined by

$$F_{n+1} = F_n + F_{n-1}, \quad (1.1)$$

$$L_{n+1} = L_n + L_{n-1}$$

with the initial terms  $F_0 = 0, F_1 = 1$  and  $L_0 = 2, L_1 = 1$ , respectively (see [5] for more details). The Fibonacci  $Q$ -matrix is defined in [3] and [4] as follows:

$$Q = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

From [9] and [11], we known that the  $n$ .th power of the Fibonacci  $Q$ -matrix is of the following form:

$$Q^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}.$$

In [2], Buggles and Hoggat introduced the  $R$ -matrix as follows:

$$R = \begin{bmatrix} 1 & 2 \\ 2 & -1 \end{bmatrix}$$

Using the Fibonacci  $Q$ -matrix and  $R$ -matrix, it was obtained the matrix  $R_n$  of the following form:

$$R_n = RQ^n = \begin{bmatrix} 1 & 2 \\ 2 & -1 \end{bmatrix} \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} = \begin{bmatrix} L_{n+1} & L_n \\ L_n & L_{n-1} \end{bmatrix}.$$

Determinants of the Fibonacci  $Q$ -matrix and the  $R$ -matrix are as follows:

$$\text{Det}(Q^n) = F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$

and

$$Det(R_n) = L_{n+1}L_{n-1} - L_n^2 = 5(-1)^{n+1}.$$

Fibonacci coding theory was studied by different ways. For example, in [7] a new approach for secure information transmission over communication channel was obtained with key variability concept in symmetric key algorithms using Fibonacci  $Q$ -matrix. In [11], a new coding theory was introduced using the generalization of the Cassini formula for Fibonacci  $p$ -numbers and  $Q_p$ -matrices. In [14], it was constructed an application of mobile phone encryption based on Fibonacci structure of chaos using Fibonacci series. In [8], Prasad developed a new coding and decoding method using Lucas  $p$  numbers given in [6]. Recently, a new cryptography algorithm has been introduced by blocking matrices and Fibonacci numbers in [13]. Also there are more studies in the literature (see [1], [10], [12] and the references therein for more details).

In this study we introduce two new coding/decoding algorithms using Fibonacci  $Q$ -matrices and  $R$ -matrices. The basic idea of our method depends on dividing the message matrix into the block matrices of size  $2 \times 2$ . Because of using mixed type algorithm and different numbered alphabet for each message, we have a more safely coding/decoding method. The alphabet is determined by the number of block matrices of the message matrix. Our method will not only increase the security of information but also has high correct ability for data transfer over communication channel.

## 2. A New Coding/Decoding Method using $R$ -Matrix

In this section we introduce a new coding/decoding algorithm using Lucas numbers. We put our message in a matrix of even size adding zero between two words and end of the message until we obtain the size of the message matrix is even. Dividing the message square matrix  $M$  of size  $2m$  into the block matrices, named  $B_i$  ( $1 \leq i \leq m^2$ ) of size  $2 \times 2$ , from left to right, we construct a new coding method.

Now we explain the symbols of our coding method. Assume that matrices  $B_i, E_i, Q^n$  and  $R_n$  are of the following forms:

$$B_i = \begin{bmatrix} b_1^i & b_2^i \\ b_3^i & b_4^i \end{bmatrix}, E_i = \begin{bmatrix} e_1^i & e_2^i \\ e_3^i & e_4^i \end{bmatrix}, Q^n = \begin{bmatrix} q_1 & q_2 \\ q_3 & q_4 \end{bmatrix} \text{ and } R_n = \begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix}.$$

The number of the block matrices  $B_i$  is denoted by  $b$ . According to  $b$ , we choose the number  $n$  as follows:

$$n = \begin{cases} b & , b \leq 3 \\ \lceil \frac{b}{2} \rceil & , b > 3 \end{cases}.$$

Using the chosen  $n$ , we write the following character table according to  $mod30$  (this table can be extended according to the used characters in the message matrix). We begin the “ $n$ ” for the first character.

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

Now we explain the following new coding and decoding algorithms.

### Lucas Blocking Algorithm

#### Coding Algorithm

**Step 1.** Divide the matrix  $M$  into blocks  $B_i$  ( $1 \leq i \leq m^2$ ).

**Step 2.** Choose  $n$ .

**Step 3.** Determine  $b_j^i$  ( $1 \leq j \leq 4$ ).

**Step 4.** Compute  $\det(B_i) \rightarrow d_i$ .

**Step 5.** Construct  $F = [d_i, b_k^i]_{k \in \{1,2,4\}}$ .

**Step 6.** End of algorithm.

#### Decoding Algorithm

**Step 1.** Compute  $R_n$ .

**Step 2.** Determine  $r_j$  ( $1 \leq j \leq 4$ ).

**Step 3.** Compute  $r_1 b_1^i + r_3 b_2^i \rightarrow e_1^i$  ( $1 \leq i \leq m^2$ ).

**Step 4.** Compute  $r_2 b_1^i + r_4 b_2^i \rightarrow e_2^i$ .

**Step 5.** Solve  $5 \times (-1)^{n+1} \times d_i = e_1^i(r_2x_i + r_4b_4^i) - e_2^i(r_1x_i + r_3b_4^i)$ .

**Step 6.** Substitute for  $x_i = b_3^i$ .

**Step 7.** Construct  $B_i$ .

**Step 8.** Construct  $M$ .

**Step 9.** End of algorithm.

The above method is similar to the method obtained by Fibonacci numbers given in [13].

In the following example we give an application of the above algorithm for  $b > 3$ .

**Example 2.1.** Let us consider the message matrix for the following message text:

“HI! HOW ARE YOU?”

Using the message text, we get the following message matrix  $M$  :

$$M = \begin{bmatrix} H & I & ! & 0 \\ H & O & W & 0 \\ A & R & E & 0 \\ Y & O & U & ? \end{bmatrix}_{4 \times 4}.$$

**Coding Algorithm:**

**Step 1.** We can divide the message matrix  $M$  of size  $4 \times 4$  into the matrices, named  $B_i$  ( $1 \leq i \leq 4$ ), from left to right, each of size is  $2 \times 2$  :

$$B_1 = \begin{bmatrix} H & I \\ H & O \end{bmatrix}, B_2 = \begin{bmatrix} ! & 0 \\ W & 0 \end{bmatrix}, B_3 = \begin{bmatrix} A & R \\ Y & O \end{bmatrix} \text{ and } B_4 = \begin{bmatrix} E & 0 \\ U & ? \end{bmatrix}.$$

**Step 2.** Since  $b = 4 \geq 3$ , we calculate  $n = \lceil \frac{b}{2} \rceil = 2$ . For  $n = 2$ , we use the following “character table” for the message matrix  $M$  :

$H$	$I$	$!$	$0$	$H$	$O$	$W$	$0$
9	10	29	28	9	16	24	28
$A$	$R$	$E$	$0$	$Y$	$O$	$U$	$?$
2	19	6	28	26	16	22	0

**Step 3.** We have the elements of the blocks  $B_i$  ( $1 \leq i \leq 4$ ) as follows:

$b_1^1 = 9$	$b_2^1 = 10$	$b_3^1 = 9$	$b_4^1 = 16$
$b_1^2 = 29$	$b_2^2 = 28$	$b_3^2 = 24$	$b_4^2 = 28$
$b_1^3 = 2$	$b_2^3 = 19$	$b_3^3 = 26$	$b_4^3 = 16$
$b_1^4 = 6$	$b_2^4 = 28$	$b_3^4 = 22$	$b_4^4 = 0$

**Step 4.** Now we calculate the determinants  $d_i$  of the blocks  $B_i$  :

$d_1 = \det(B_1) = 54$
$d_2 = \det(B_2) = 140$
$d_3 = \det(B_3) = -462$
$d_4 = \det(B_4) = -616$

**Step 5.** Using Step 3 and Step 4 we obtain the following matrix  $F$  :

$$F = \begin{bmatrix} 54 & 9 & 10 & 16 \\ 140 & 29 & 28 & 28 \\ -462 & 2 & 19 & 16 \\ -616 & 6 & 28 & 0 \end{bmatrix}.$$

**Step 6.** End of algorithm.

**Decoding algorithm:**

**Step 1.** It is known that

$$R_2 = RQ^2 = \begin{bmatrix} 4 & 3 \\ 3 & 1 \end{bmatrix}.$$

**Step 2.** The elements of  $R_2$  are denoted by

$$r_1 = 4, r_2 = 3, r_3 = 3 \text{ and } r_4 = 1.$$

**Step 3.** We compute the elements  $e_1^i$  to construct the matrix  $E_i$  :

$$e_1^1 = 66, e_1^2 = 200, e_1^3 = 65 \text{ and } e_1^4 = 108.$$

**Step 4.** We compute the elements  $e_2^i$  to construct the matrix  $E_i$  :

$$e_2^1 = 37, e_2^2 = 115, e_2^3 = 25 \text{ and } e_2^4 = 46.$$

**Step 5.** We calculate the elements  $x_i$  :

$$\begin{aligned} 5(-1)^3(54) &= 66(3x_1 + 16) - 37(4x_1 + 48) \\ \Rightarrow x_1 &= 9. \end{aligned}$$

$$\begin{aligned} 5(-1)^3(140) &= 200(3x_2 + 28) - 115(4x_2 + 84) \\ \Rightarrow x_2 &= 24. \end{aligned}$$

$$\begin{aligned} 5(-1)^3(-462) &= 65(3x_3 + 16) - 25(4x_3 + 48) \\ \Rightarrow x_3 &= 26. \end{aligned}$$

$$\begin{aligned} 5(-1)^4(-616) &= 108(3x_4 + 0) - 46(4x_4 + 0) \\ \Rightarrow x_4 &= 22. \end{aligned}$$

**Step 6.** We rename  $x_i$  as follows:

$$x_1 = b_3^1 = 9, x_2 = b_3^2 = 24, x_3 = b_3^3 = 26 \text{ and } x_4 = b_3^4 = 22.$$

**Step 7.** We construct the block matrices  $B_i$  :

$$B_1 = \begin{bmatrix} 9 & 10 \\ 9 & 16 \end{bmatrix}, B_2 = \begin{bmatrix} 29 & 28 \\ 24 & 28 \end{bmatrix}, B_3 = \begin{bmatrix} 2 & 19 \\ 26 & 16 \end{bmatrix} \text{ and } B_4 = \begin{bmatrix} 6 & 28 \\ 22 & 0 \end{bmatrix}.$$

**Step 8.** We obtain the message matrix  $M$  :

$$M = \begin{bmatrix} 9 & 10 & 29 & 28 \\ 9 & 16 & 24 & 28 \\ 2 & 19 & 6 & 28 \\ 26 & 16 & 22 & 0 \end{bmatrix} = \begin{bmatrix} H & I & ! & 0 \\ H & O & W & 0 \\ A & R & E & 0 \\ Y & O & U & ? \end{bmatrix}.$$

**Step 9.** End of algorithm.

### 3. A Mixed Model: Minesweeper Model

In this section we present a new approach to coding/decoding algorithm method called as ‘‘Minesweeper Model’’ using Fibonacci  $Q^n$ -matrices and  $R$ -matrices. The main idea of this model is to decode blocks of the message matrix using Fibonacci and Lucas numbers randomly. In the following model is constructed by decoding the blocks with odd indices  $i$  using Fibonacci  $Q^n$ -matrices and decoding the blocks with even indices  $i$  using  $R$ -matrices.

#### Minesweeper Algorithm

##### Coding Algorithm

**Step 1.** Divide the matrix  $M$  into blocks  $B_i$  ( $1 \leq i \leq m^2$ ).

**Step 2.** Choose  $n$ .

**Step 3.** Determine  $b_j^i$  ( $1 \leq j \leq 4$ ).

**Step 4.** Compute  $\det(B_i) \rightarrow d_i$ .

**Step 5.** Construct  $F = [d_i, b_k^i]_{k \in \{1,2,3\}}$ .

**Step 6.** End of algorithm.

### Decoding Algorithm

**Step 1.** Compute  $Q^n$ .

**Step 2.** Compute  $R^n$ .

**Step 3.** Compute  $q_1 b_1^i + q_3 b_2^i \rightarrow e_1^i, i = 2l + 1$  for  $0 \leq l \leq 2m$ .

**Step 4.** Compute  $r_1 b_1^i + r_3 b_2^i \rightarrow e_1^i, i = 2l$  for  $1 \leq l \leq 2m$ .

**Step 5.** Compute  $q_2 b_1^i + q_4 b_2^i \rightarrow e_2^i, i = 2l + 1$  for  $0 \leq l \leq 2m$ .

**Step 6.** Compute  $r_2 b_1^i + r_4 b_2^i \rightarrow e_2^i, i = 2l$  for  $1 \leq l \leq 2m$ .

**Step 7.** Solve  $(-1)^n \times d_i = e_1^i(q_2 b_3^i + q_4 x_i) - e_2^i(q_1 b_3^i + q_3 x_i), i = 2l + 1$  for  $0 \leq l \leq 2m$ .

**Step 8.** Solve  $5 \times (-1)^{n+1} \times d_i = e_1^i(r_2 b_3^i + r_4 x_i) - e_2^i(r_1 b_3^i + r_3 x_i), i = 2l$  for  $0 \leq l \leq 2m$ .

**Step 9.** Substitute for  $x_i = b_4^i$ .

**Step 10.** Construct  $B_i$ .

**Step 11.** Construct  $M$ .

**Step 12.** End of algorithm.

Now, we give an application of the above algorithm for  $b > 3$ .

**Example 3.1.** Let us consider the message matrix for the following message text:

"MIXED MODELLING FOR CRYPTOGRAPHY"

Using the message text, we get the following message matrix  $M$  :

$$M = \begin{bmatrix} M & I & X & E & D & 0 \\ M & O & D & E & L & L \\ I & N & G & 0 & F & O \\ R & 0 & C & R & Y & P \\ T & O & G & R & A & P \\ H & Y & 0 & 0 & 0 & 0 \end{bmatrix}_{6 \times 6}.$$

### Coding Algorithm:

**Step 1.** We can divide the message matrix  $M$  of size  $6 \times 6$  into the matrices, named  $B_i$  ( $1 \leq i \leq 9$ ), from left to right, each of size is  $2 \times 2$  :

$$\begin{aligned} B_1 &= \begin{bmatrix} M & I \\ M & 0 \end{bmatrix}, B_2 = \begin{bmatrix} X & E \\ D & E \end{bmatrix}, B_3 = \begin{bmatrix} D & 0 \\ L & L \end{bmatrix}, \\ B_4 &= \begin{bmatrix} I & N \\ R & 0 \end{bmatrix}, B_5 = \begin{bmatrix} G & 0 \\ C & R \end{bmatrix}, B_6 = \begin{bmatrix} F & O \\ Y & P \end{bmatrix}, \\ B_7 &= \begin{bmatrix} T & O \\ H & Y \end{bmatrix}, B_8 = \begin{bmatrix} G & R \\ 0 & 0 \end{bmatrix}, B_9 = \begin{bmatrix} A & P \\ 0 & 0 \end{bmatrix}. \end{aligned}$$

**Step 2.** Due to  $b = 9 > 3$ , we calculate  $n = \lceil \frac{b}{2} \rceil = 4$ . For  $n = 4$ , we use the following "character table" for the message matrix  $M$  :

$M$	$I$	$X$	$E$	$D$	$0$	$M$	$O$	$D$	$E$	$L$	$L$
16	12	27	8	7	0	16	18	7	8	15	15
$I$	$N$	$G$	$0$	$F$	$O$	$R$	$0$	$C$	$R$	$Y$	$P$
12	17	10	0	9	18	21	0	6	21	28	19
$T$	$O$	$G$	$R$	$A$	$P$	$H$	$Y$	$0$	$0$	$0$	$0$
23	18	10	21	4	19	11	28	0	0	0	0

**Step 3.** We have the elements of the blocks  $B_i$  ( $1 \leq i \leq 9$ ) as follows:

$b_1^1 = 16$	$b_2^1 = 12$	$b_3^1 = 16$	$b_4^1 = 18$
$b_1^2 = 27$	$b_2^2 = 8$	$b_3^2 = 7$	$b_4^2 = 8$
$b_1^3 = 7$	$b_2^3 = 0$	$b_3^3 = 15$	$b_4^3 = 15$
$b_1^4 = 12$	$b_2^4 = 17$	$b_3^4 = 21$	$b_4^4 = 0$
$b_1^5 = 10$	$b_2^5 = 0$	$b_3^5 = 6$	$b_4^5 = 21$
$b_1^6 = 9$	$b_2^6 = 18$	$b_3^6 = 28$	$b_4^6 = 19$
$b_1^7 = 23$	$b_2^7 = 18$	$b_3^7 = 11$	$b_4^7 = 28$
$b_1^8 = 10$	$b_2^8 = 21$	$b_3^8 = 0$	$b_4^8 = 0$
$b_1^9 = 4$	$b_2^9 = 19$	$b_3^9 = 0$	$b_4^9 = 0$

**Step 4.** Now we calculate the determinants  $d_i$  of the blocks  $B_i$  :

$d_1 = \det(B_1) = 96$
$d_2 = \det(B_2) = 160$
$d_3 = \det(B_3) = 105$
$d_4 = \det(B_4) = -357$
$d_5 = \det(B_5) = 210$
$d_6 = \det(B_6) = -333$
$d_7 = \det(B_7) = 446$
$d_8 = \det(B_8) = 0$
$d_9 = \det(B_9) = 0$

**Step 5.** Using Step 3 and Step 4 we obtain the following matrix  $F$  :

$$F = \begin{bmatrix} 96 & 16 & 12 & 16 \\ 160 & 27 & 8 & 7 \\ 105 & 7 & 0 & 15 \\ -357 & 12 & 17 & 21 \\ 210 & 10 & 0 & 6 \\ -333 & 9 & 18 & 28 \\ 446 & 23 & 18 & 11 \\ 0 & 10 & 21 & 0 \\ 0 & 4 & 19 & 0 \end{bmatrix}.$$

**Step 6.** End of algorithm.

**Decoding algorithm:**

**Step 1.** It is known that

$$Q^4 = \begin{bmatrix} F_5 & F_4 \\ F_4 & F_3 \end{bmatrix} = \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix}.$$

**Step 2.** It is known that

$$R_4 = RQ^4 = \begin{bmatrix} L_5 & L_4 \\ L_4 & L_3 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 2 & -1 \end{bmatrix} \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 11 & 7 \\ 7 & 4 \end{bmatrix}.$$

**Step 3.** If  $i$  is an odd number, we use the Fibonacci  $Q$ -matrix. Now we compute the elements  $e_1^i$ , for  $i = 1, 3, 5, 7, 9$ , in order to construct the matrix  $E_i$  :

$$e_1^1 = 116, e_1^3 = 35, e_1^5 = 50, e_1^7 = 169 \text{ and } e_1^9 = 47.$$

**Step 4.** If  $i$  is an even number, we use the  $R$ -matrix. Now we compute the elements  $e_1^i$ , for  $i = 2, 4, 6, 8$  in order to construct the matrix  $E_i$  :

$$e_1^2 = 353, e_1^4 = 251, e_1^6 = 225 \text{ and } e_1^8 = 257.$$

**Step 5.** If  $i$  is an odd number, we use the Fibonacci  $Q$ -matrix. Now we compute the elements  $e_2^i$ , for  $i = 1, 3, 5, 7, 9$ , in order to construct the matrix  $E_i$  :

$$e_2^1 = 72, e_2^3 = 21, e_2^5 = 30, e_2^7 = 105 \text{ and } e_2^9 = 30.$$

**Step 6.** If  $i$  is an even number, we use the  $R$ -matrix. Now we compute the elements  $e_2^i$ , for  $i = 2, 4, 6, 8$ , in order to construct the matrix  $E_i$  :

$$e_2^2 = 221, e_2^4 = 152, e_2^6 = 135, \text{ and } e_2^8 = 154.$$

**Step 7.** If  $i$  is an odd number, we use the Fibonacci  $Q$ -matrix. Now, we calculate the elements  $x_i$  for  $i = 1, 3, 5, 7, 9$ .

$$\begin{aligned} (-1)^4 96 &= 116(48 + 2x_1) - 72(80 + 3x_1) \\ \Rightarrow x_1 &= 18. \end{aligned}$$

$$\begin{aligned} (-1)^4 105 &= 35(45 + 2x_3) - 21(75 + 3x_3) \\ \Rightarrow x_3 &= 15. \end{aligned}$$

$$\begin{aligned} (-1)^4 210 &= 50(18 + 2x_5) - 30(30 + 3x_5) \\ \Rightarrow x_5 &= 21. \end{aligned}$$

$$\begin{aligned} (-1)^4 446 &= 169(33 + 2x_7) - 105(55 + 3x_7) \\ \Rightarrow x_7 &= 28. \end{aligned}$$

$$\begin{aligned} (-1)^4 0 &= 47(0 + 2x_9) - 30(0 + 3x_9) \\ \Rightarrow x_9 &= 0. \end{aligned}$$

**Step 8.** If  $i$  is an even number, we use the  $R$ -matrix. Now, we calculate the elements  $x_i$  for  $i = 2, 4, 6, 8$ .

$$\begin{aligned} 5(-1)^5 160 &= 353(49 + 4x_2) - 221(77 + 7x_2) \\ \Rightarrow x_2 &= 8. \end{aligned}$$

$$\begin{aligned} 5(-1)^5 (-357) &= 251(147 + 4x_4) - 152(231 + 3x_4) \\ \Rightarrow x_4 &= 0. \end{aligned}$$

$$\begin{aligned} 5(-1)^5 (-333) &= 225(196 + 4x_6) - 135(308 + 7x_6) \\ \Rightarrow x_6 &= 19. \end{aligned}$$

$$\begin{aligned} 5(-1)^5 0 &= 257(0 + 4x_8) - 154(0 + 7x_8) \\ \Rightarrow x_8 &= 0. \end{aligned}$$

**Step 9.** We rename  $x_i$  as follows:

$$\begin{aligned} x_1 &= b_4^1 = 18, x_2 = b_4^2 = 8, x_3 = b_4^3 = 15, x_4 = b_4^4 = 0, x_5 = b_4^5 = 21, \\ x_6 &= b_4^6 = 19, x_7 = b_4^7 = 28, x_8 = b_4^8 = 0 \text{ and } x_9 = b_4^9 = 0. \end{aligned}$$

**Step 10.** We construct the block matrices  $B_i$  :

$$\begin{aligned} B_1 &= \begin{bmatrix} 16 & 12 \\ 16 & 18 \end{bmatrix}, B_2 = \begin{bmatrix} 27 & 8 \\ 7 & 8 \end{bmatrix}, B_3 = \begin{bmatrix} 7 & 0 \\ 15 & 15 \end{bmatrix}, \\ B_4 &= \begin{bmatrix} 12 & 17 \\ 4 & 0 \end{bmatrix}, B_5 = \begin{bmatrix} 10 & 0 \\ 6 & 21 \end{bmatrix}, B_6 = \begin{bmatrix} 9 & 18 \\ 28 & 19 \end{bmatrix}, \\ B_7 &= \begin{bmatrix} 23 & 18 \\ 11 & 28 \end{bmatrix}, B_8 = \begin{bmatrix} 10 & 21 \\ 0 & 0 \end{bmatrix}, B_9 = \begin{bmatrix} 4 & 9 \\ 0 & 0 \end{bmatrix}. \end{aligned}$$

**Step 11.** We obtain the following message matrix  $M$  :

$$M = \begin{bmatrix} 16 & 12 & 27 & 8 & 7 & 0 \\ 16 & 18 & 7 & 8 & 15 & 15 \\ 12 & 17 & 10 & 0 & 9 & 18 \\ 4 & 0 & 6 & 21 & 28 & 19 \\ 23 & 18 & 10 & 21 & 4 & 9 \\ 11 & 28 & 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} M & I & X & E & D & 0 \\ M & O & D & E & L & L \\ I & N & G & 0 & F & O \\ R & 0 & C & R & Y & P \\ T & O & G & R & A & P \\ H & Y & 0 & 0 & 0 & 0 \end{bmatrix}.$$

**Step 9.** End of algorithm.

#### 4. Comparisons and Conclusion

In this section we give the differences between the method given in [13] and the above methods. At first, in [13], the number  $n$  is defined by

$$n = \begin{cases} 3 & , \quad b \leq 3 \\ b & , \quad b > 3 \end{cases} .$$

On the other hand, in our methods the number  $n$  has been given in different ways as we have explained in Section 2. Because of the selection method of  $n$ , we are studying more smaller numbers to calculate the matrices  $Q^n$ ,  $R_n$  and to form the character table. Hence we obtain more easier methods than the method given in [13]. Furthermore if we use the minesweeper model, then the security has been increased according to Lucas Blocking Model given in Section 2 and Fibonacci Blocking Model given in [13]. Especially to increase the security it can be changed the decoding method of blocks using Fibonacci and Lucas numbers randomly.

#### References

- [1] Basu, M. and Prasad, B., The generalized relations among the code elements for Fibonacci coding theory. *Chaos Solitons Fractals* 41 (2009), no. 5, 2517-2525.
- [2] Bruggles I. D. and Jr Hoggatt, V. E., A Primer for the Fibonacci numbers-Part IV. *Fibonacci Q.* 1 (1963), no.4, 65-71.
- [3] Gould, H. W., A history of the Fibonacci  $Q$ -matrix and a higher-dimensional problem. *Fibonacci Quart.* 19 (1981), no. 3, 250-257.
- [4] Hoggatt, V. E., Fibonacci and Lucas Numbers. Houghton-Mifflin. Palo Alto, 1969.
- [5] Koshy, T., Fibonacci and Lucas numbers with applications. New York, NY: JohnWiley and Sons, 2001.
- [6] Kuhapatanakul, K., The Lucas  $p$ -matrix. *Internat. J. Math. Ed. Sci. Techn.* (2015). <http://dx.doi.org/10.1080/0020739X.2015.1026612>
- [7] Prajapat, S., Jain, A. and Thakur, R. S., A novel approach for information security with automatic variable key using Fibonacci  $Q$ -matrix. *IJCCT* 3 (2012), no. 3, 54-57.
- [8] Prasad, B., Coding theory on Lucas  $p$ -numbers. *Discrete Math. Algorithms Appl.* 8 (2016), no.4, 17 pages.
- [9] Stakhov, A. P., A generalization of the Fibonacci  $Q$ -matrix. *Rep. Natl. Acad. Sci. Ukraine* 9 (1999), 46-49.
- [10] Stakhov, A., Massingue, V. and Sluchenkov, A., Introduction into Fibonacci coding and cryptography. Osnova, Kharkov, 1999.
- [11] Stakhov, A. P., Fibonacci matrices, a generalization of the Cassini formula and a new coding theory. *Chaos Solitons Fractals* 30 (2006), no. 1, 56-66.
- [12] Tarle, B. S. and Prajapati, G. L., On the information security using Fibonacci series. International Conference and Workshop on Emerging Trends in Technology (ICWET 2011)-TCET, Mumbai, India.
- [13] Taş, N., Uçar, S., Özgür, N. Y. and Kaymak, Ö. Ö., A new coding/decoding algorithm using Finonacci numbers. *Discrete Math. Algorithms Appl.* 10 (2018), no. 02, 1850028.
- [14] Wang, F., Ding, J., Dai, Z. and Peng, Y., An application of mobile phone encryption based on Fibonacci structure of chaos. 2010 Second WRI World Congress on Software Engineering.



## Affiliations

SÜMEYRA UÇAR

**ADDRESS:** Balıkesir University, Dept. of Mathematics, 10145, Balıkesir-Turkey.

**E-MAIL:** sumeyraucar@balikesir.edu.tr

**ORCID ID:** 0000-0002-6628-526X

NIHAL TAŞ

**ADDRESS:** Balıkesir University, Dept. of Mathematics, 10145, Balıkesir-Turkey.

**E-MAIL:** nihaltas@balikesir.edu.tr

**ORCID ID:** 0000-0002-8152-1830

NIHAL YILMAZ ÖZGÜR

**ADDRESS:** Balıkesir University, Dept. of Mathematics, 10145, Balıkesir-Turkey.

**E-MAIL:** nihal@balikesir.edu.tr

**ORCID ID:** 0000-0002-4535-4019