Research Article GU J Sci 38(3): 1404-1418 (2025) DOI: 10.35378/gujs.1602943

Gazi University

Journal of Science

http://dergipark.org.tr/gujs

On Encryption by Stirling Polynomial Matrices

Serpil HALICI, Hatice KAYHAN*

Pamukkale University, Faculty of Science, Department of Mathematics, Denizli, Türkiye

Highlights

- Stirling polynomials were defined and examined.
- AES type encryption algorithm was performed using the special case of Stirling polynomials.
- The study was supported by giving a clear example.

Article Info

Received: 17 Dec 2024
Accepted: 10 Jun 2025

Keywords

Stirling polynomials
Galois field
Coding- decoding

Abstract

In this article, by examining Stirling numbers, a new matrix type containing these numbers is defined and this matrix is called Stirling matrix. Based on the fact that the use of matrices is very common and convenient in the field of encryption, we used the newly defined Stirling matrix to perform AES type encryption. Inspired by the properties of integer sequences, a new recurrence relation that gives Stirling polynomials is defined. The Stirling polynomials used in our study are associated with k-order generalized matrices. LU decomposition of this generalized matrix is performed and examined. The L matrix obtained with the help of this decomposition is used in AES-like encryption methods. In our study, the examination and verification of this algorithm are given with an application.

1. INTRODUCTION

Stirling numbers of the first type are defined by the recurrence relation

$$s(n,k) = s(n-1,k-1) + (n-1)s(n-1,k)$$

where n is greater than k and initial values are

$$s(n,0) = s(0,k) = 0, s(0,0) = 1.$$

These numbers have been studied by many authors. A large number of generalized finite sums involving Stirling numbers can be seen in Section 6.1 of Concrete Mathematics [1]. Some of these studies are worth recalling. These numbers are called after J. Stirling (1692-1770) and were first put forward in his book "Methodus differentialis" in 1730 [2]. However, Abraham de Moivre (1667-1754) was the mathematician who first worked on Stirling numbers. De Moivre used these numbers in permutations and combinatorics [3]. Later, James Stirling (1692-1770) examined and analyzed these numbers, known as Stirling numbers, in more detail [4]. Stirling's works have an important place, especially in asymptotic analysis. Abel, Norwegian mathematician, worked on Stirling numbers, polynomials [5]. Abel's work contributed to the understanding of Stirling numbers in a broader mathematical context. Jacobi (1804-1851) worked on Stirling numbers and determinant theories. Jacobi's work revealed the relationship of these numbers to matrix theory and linear algebra [6].

*Corresponding author, e-mail: haticekayhan.000@gmail.com

Modern Studies (20th and 21st century), Stirling numbers have found wide application in combinatorics, numerical analysis and computer science today. Modern mathematicians have further developed these numbers by using them in various algorithms and theories. In the study conducted by Aziza, H.A (2016), generating functions and combinatoric sums and their related applications were studied [7].

The first type of Stirling matrix is defined as

$S_n(1) = [s_{ij}]_{n\times n}$,

where i, j are the positive numbers and i is greater than j and "0" in the other cases. Details of the studies done with Stirling matrix can be seen in the references [8-10]. The studies done with the first type of Stirling polynomials can be seen in the references [11-17]. However, for this study, the first type of Stirling polynomials, similar to Fibonacci, was used. These polynomials were created using the row sums of the first type Stirling number table. These polynomials are defined by the same recursive relation as for the first type Stirling numbers,

$s_{n+1}(x) = xs_n(x) + (nx + n^2 - n)s_{n-1}(x)$

and give the first type Stirling numbers with special values. We now construct the Stirling polynomials and derive the general form of the Stirling polynomial matrix. In [18], for $k > 0$ and $n \geq k$, first and second type Stirling polynomials are defined by

$s_{n,k}(x) = x\, s(n-1, k-1) + (n-1)s(n-1, k)$

and

$S_{n,k}(x) = x\, s(n-1, k-1) + k\, s(n-1, k)$,

respectively, where $s_{0,0}(x) = S_{0,0}(x) = 1$ and $s_{0,k}(x) = s_{n,0}(x) = S_{0,k}(x) = S_{n,0}(x) = 0$.

Noticed that when $x = 1$, above last equations give the first and second type Stirling numbers, respectively. Some terms of the first sequence are

$s_{1,1}(x) = x$, $s_{2,1}(x) = x$, $s_{2,2}(x) = x^2$, $s_{3,1}(x) = 2x$, $s_{3,2}(x) = 3x^2$, … .

Table 1. *First and second type Stirling polynomials*

$s_{n,k}(x)$	1	2	3	4	5	6	⋯
1	x						
2	x	x^2					
3	$2x$	$3x^2$	x^3				
4	$6x$	$11x^2$	$6x^3$	x^4			
5	$24x$	$50x^2$	$35x^3$	$10x^4$	x^5		
6	$120x$	$274x^2$	$225x^3$	$85x^4$	$15x^5$	x^6	
⋮							

In the Table 1, if we take $x = 2$ we obtain the sequence (A125553) included in the OEIS and it's $T(n,k)$.

$$T(n,k) = 2^k s(n,k)$$

$$\{2, 2, 4, 4, 12, 8, 12, 44, 48, 16, 48, 200, \dots\}.$$

2. MATERIALS AND METHODS

2.1. Stirling Polynomials

In this section, Stirling polynomials are studied in detail and some new identities are given. In the following theorem, a recurrence relation is given that gives the row sums for Stirling polynomials.

Theorem 2.1.1. For $n > 0$, we have

$$s_{n+1}(x) = (n + x)s_n(x)$$

and

$$s_{n+1}(x) = xs_n(x) + (nx + n^2 - n)s_{n-1}(x). \quad (1)$$

Proof. The proof can be done by using the row sums of Table 1.

$s_0(x) = 1$, for $n = 0, 1$ and $m - 1$ the polynomials $s_{n+1}(x)$ are $s_1(x) = x$, $s_2(x) = x + x^2$ and $s_m(x) = (m-1)\, s_{m-1}(x) + x\, s_{m-1}(x)$, respectively.

For $n = m$, the Equality (1) is true. So,

$$s_{m+1}(x) = m\, s_m(x) + x\, s_m(x)$$

$$s_{m+1}(x) = m[(m-1)s_{m-1}(x) + xs_{m-1}(x)] + x[(m-1)s_{m-1}(x) + xs_{m-1}(x)]$$

$$s_{m+1}(x) = (m + x)(m - 1 + x)s_{m-1}(x).$$

Consequently, we can write

$$s_{m+1}(x) = (m^2 - m + 2mx - x + x^2)\, s_{m-1}(x).$$

Thus, we have

$$s_{n+1}(x) = (n + x)s_n(x)$$

which is the desired result.

Moreover, we have the following identities.

i. If $n - 1$ is written instead of n in the above Equation (1), then we get

$$s_n(x) = (n + x - 1)s_{n-1}(x).$$

ii. The sum of consecutive polynomials, is

$$s_{n+1}(x) = (n + x - 1)\big(s_n(x) + s_{n-1}(x)\big).$$

iii. The difference of consecutive polynomials is

$$s_{n+1}(x) = (n + x - 1)\big(s_n(x) - s_{n-1}(x)\big) + 2\, s_n(x).$$

Now, we can give the sums of the Stirling polynomials.

Theorem 2.1.2. For the polynomials $s_n(x)$, we have

$$i)\ \sum_{n=0}^{\infty} s_n(x) = 1 + \sum_{n=1}^{\infty} (n + x - 1)\, s_{n-1}(x).$$

$$ii)\ \sum_{n=0}^{\infty} s_{2n}(x) = 1 + \sum_{n=1}^{\infty} (2n + x - 1)\, s_{2n-1}(x).$$

$$iii)\ \sum_{n=0}^{\infty} s_{2n+1}(x) = (2n + x) \sum_{n=0}^{\infty} s_{2n}(x).$$

Proof. Here, only the proof of $i)$ will be given. Let's do it by induction over finite numbers k.

$\sum_{n=0}^{0} s_n(x) = 1$ is true. Assume that

$$\sum_{n=0}^{k+1} s_n(x) = \sum_{n=0}^{k} s_n(x) + s_{k+1}(x).$$

If we substitute the following equality a into the assumption,

$\sum_{n=0}^{k} s_n(x) = s_0(x) + \sum_{n=1}^{k} (n + x - 1)\, s_{n-1}(x)$ then, we write

$\sum_{n=0}^{k+1} s_n(x) = s_0(x) + \sum_{n=1}^{k} (n + x - 1)\, s_{n-1}(x) + s_{k+1}(x)$

Using the equation $s_{k+1}(x) = (k + x)s_k(x)$, we get

$$\sum_{n=0}^{k+1} s_n(x) = s_0(x) + \sum_{n=1}^{k+1} (n + x - 1)\, s_{n-1}(x).$$

Thus, the proof is completed.

In this study, the matrix $Q_k^n(x)$ is defined to be used in encryption and LU decomposition of this matrix was performed. AES type encryption was performed by using LU.

Definition 2.1.3. Let's define a new matrix, we call the Stirling polynomial matrix, denoted by $Q_k^n(x)$

$$Q_k^n(x) = \begin{bmatrix} s_0(x) & s_1(x) & s_2(x) & \cdots & s_k(x) \\ s_1(x) & s_2(x) & s_3(x) & \cdots & s_{k+1}(x) \\ s_2(x) & s_3(x) & s_4(x) & \cdots & s_{k+2}(x) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{n-1}(x) & s_n(x) & s_{n+1}(x) & \cdots & s_{n+k-1}(x) \end{bmatrix}.$$

Now, let us give two different decompositions of this matrix without proof.

Lemma 2.1.4. The LU decomposition of the matrix $Q_k^n(x)$ is

$$Q_k^n(x) = L_n U_n.$$

where $L_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ x & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ s_{n-1}(x) & \frac{s_n(x)}{x} - s_{n-1}(x) & \cdots & 1 \end{bmatrix}$ and $U_n = \begin{bmatrix} 1 & x & \cdots & s_k(x) \\ 0 & x & \cdots & s_{k+1}(x) - x s_k(x) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & s_{k+n-1}(x) - \sum_{i=1}^{k-1} L_{ki} U_{ik} \end{bmatrix}$.

In our current study, the L_n matrix of the LU decomposition given in the above lemma is used.

The AES method is known to be a classic method for encryption. This method is widely used both for encrypting the message to be transmitted and for decrypting the message. In this method, both keys used for encryption and decryption are the same. AES supports 128, 192 and 256 bit keys. The cycle for the method used is given in Figure 1. For more detailed information about AES, you can refer to references [19- 21].

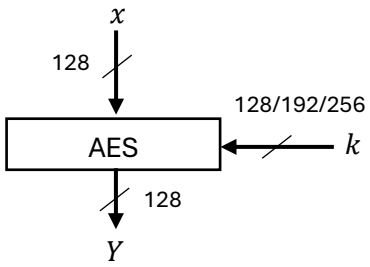


Figure 1. *Cycle AES [23]*

The Galois field is an algebraic structure that commonly includes matrix operations and provides ease of operation. Detailed information about this structure can be found in [22- 24]. The elements of $GF(2^m)$ can be integers as well as matrices and polynomials. In the situtation the elements of $GF(2^m)$ are polynomials, the degree of these polynomials is at most $m - 1$. The number of elements of the Galois field used in AES type encryption is 2^8.

A polynomial $A(x)$, is written as $A(x) = a_7x^7 + \ldots + a_1x + a_0, a_i \in GF(2) = \{0,1\}$.

Coding algorithms play an important role in ensuring information security and various number sequences are widely used in the cryption area.

In a study conducted in 2020, the authors used some special integer sequences to encrypt with AES type [25]. We also used matrix representations of Stirling polynomials to obtain the targeted algorithm, especially as a motivation from this study.

In the following section, we give an encryption algorithm using the first type Stirling polynomials, which we denote with the symbol $Q_k^n(x)$ and used the following key matrices.

$$1.Key = \begin{bmatrix} C & O & D \\ B & B & B \\ C & Ç & B \end{bmatrix},\ 2.Key = \begin{bmatrix} B & A \\ D & D \end{bmatrix}.$$

3. CODING AND DECODING WITH STIRLING POLYNOMIAL MATRICES

In this section, we examined the AES type encoding and decoding method using the matrix $Q_k^n(x)$.

Throughout the study, we redefined the elements of Stirling polynomials of order k using irreducible polynomials to be able to perform AES type coding. Since it is advantageous to use algebraic structures with finite elements, the Galois field containing 128 elements was used in this study.

Let the polynomials $A(x),\ B(x)$ in $GF(2^m)$ and for the irreducible polynomial p_i modulo. And $P(x) \equiv \sum_{i=0}^{m} p_i x_i$, $C(x) = A(x)B(x)$. As the polynomial, we use $P(x) = x^7 + x + 1$. Let's match each polynomial $s_i(x)$ used with a letter in the alphabet.

In the Table 2, the polynomials are defined on the Galois field and the alphabetical comparison are given.

Table 2. *Polynomials and their letter equivalents*

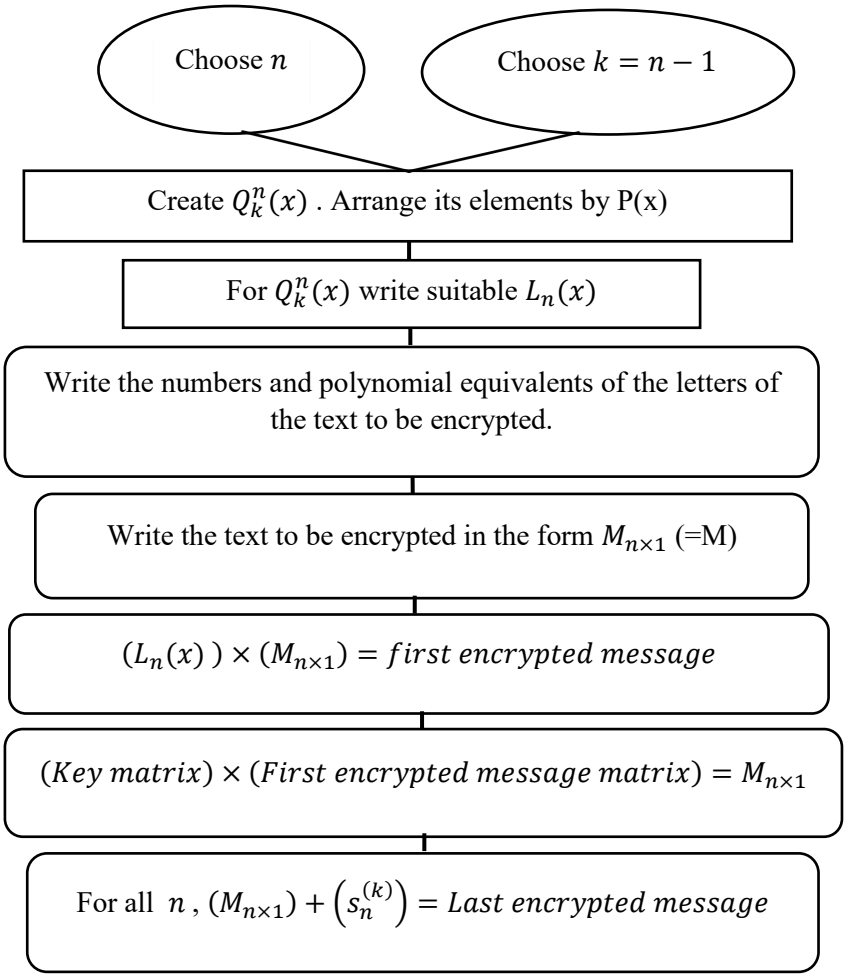
No	**Bit**	**Polynomials**	**Letter equivalents**
0	0000000	0	A
1	0000001	1	B
2	0000010	x	C
3	0000011	$x+1$	Ç
4	0000100	x^2	D
5	0000101	x^2+1	E
6	0000110	x^2+x	F
7	0000111	x^2+x+1	G
8	0001000	x^3	Ğ
9	0001001	x^3+1	H
10	0001010	x^3+x	I
11	0001011	x^3+x+1	İ
12	0001100	x^3+x^2	J
13	0001101	x^3+x^2+1	K
14	0001110	x^3+x^2+x	L
15	0001111	x^3+x^2+x+1	M
16	0010000	x^4	N
17	0010001	x^4+1	O
18	0010010	x^4+x	Ö
19	0010011	x^4+x+1	P
20	0010100	x^4+x^2	R
21	0010101	x^4+x^2+1	S
22	0010110	x^4+x^2+x	Ş
23	0010111	x^4+x^2+x+1	T
24	0011000	x^4+x^3	U
25	0011001	x^4+x^3+1	Ü
26	0011010	x^4+x^3+x	V

27	0011011	x^4+x^3+x+1	W
28	0011100	$x^4+x^3+x^2$	X
29	0011101	$x^4+x^3+x^2+1$	Y
30	0011110	$x^4+x^3+x^2+x$	Z
31	0011111	$x^4+x^3+x^2+x+1$	Q
32	0100000	x^5	A_1
33	0100001	x^5+1	B_1
34	0100010	x^5+x	C_1
35	0100011	x^5+x+1	$Ç_1$
36	0100100	x^5+x^2	D_1
37	0100101	x^5+x^2+1	E_1
38	0100110	x^5+x^2+x	F_1
39	0100111	x^5+x^2+x+1	G_1
40	0101000	x^5+x^3	$Ğ_1$
41	0101001	x^5+x^3+1	H_1
42	0101010	x^5+x^3+x	I_1
43	0101011	x^5+x^3+x+1	$İ_1$
44	0101100	$x^5+x^3+x^2$	J_1
45	0101101	$x^5+x^3+x^2+1$	K_1
46	0101110	$x^5+x^3+x^2+x$	L_1
47	0101111	$x^5+x^3+x^2+x+1$	M_1
48	0110000	x^5+x^4	N_1
49	0110001	x^5+x^4+1	O_1
50	0110010	x^5+x^4+x	$Ö_1$
51	0110011	x^5+x^4+x+1	P_1
52	0110100	$x^5+x^4+x^2$	R_1
53	0110101	$x^5+x^4+x^2+1$	S_1
54	0110110	$x^5+x^4+x^2+x$	$Ş_1$
55	0110111	$x^5+x^4+x^2+x+1$	T_1
56	0111000	$x^5+x^4+x^3$	U_1
57	0111001	$x^5+x^4+x^3+1$	$Ü_1$
58	0111010	$x^5+x^4+x^3+x$	V_1
59	0111011	$x^5+x^4+x^3+x+1$	W_1
60	0111100	$x^5+x^4+x^3+x^2$	X_1
61	0111101	$x^5+x^4+x^3+x^2+1$	Y_1
62	0111110	$x^5+x^4+x^3+x^2+x$	Z_1
63	0111111	$x^5+x^4+x^3+x^2+x+1$	Q_1
64	1000000	x^6	A_2
65	1000001	x^6+1	B_2
66	1000010	x^6+x	C_2
67	1000011	x^6+x+1	$Ç_2$
68	1000100	x^6+x^2	D_2
69	1000101	x^6+x^2+1	E_2
70	1000110	x^6+x^2+x	F_2
71	1000111	x^6+x^2+x+1	G_2
72	1001000	x^6+x^3	$Ğ_2$
73	1001001	x^6+x^3+1	H_2
74	1001010	x^6+x^3+x	I_2
75	1001011	x^6+x^3+x+1	$İ_2$
76	1001100	$x^6+x^3+x^2$	J_2

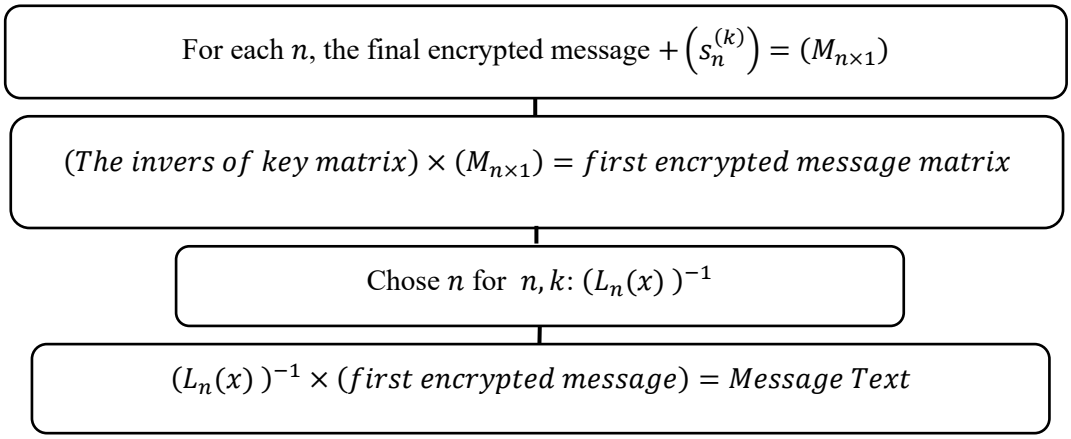
77	1001101	$x^6+x^3+x^2+1$	K_2
78	1001110	$x^6+x^3+x^2+x$	L_2
79	1001111	$x^6+x^3+x^2+x+1$	M_2
80	1010000	x^6+x^4	N_2
81	1010001	x^6+x^4+1	O_2
82	1010010	x^6+x^4+x	$\ddot{O}_2$
83	1010011	x^6+x^4+x+1	P_2
84	1010100	$x^6+x^4+x^2$	R_2
85	1010101	$x^6+x^4+x^2+1$	S_2
86	1010110	$x^6+x^4+x^2+x$	$\c{S}_2$
87	1010111	$x^6+x^4+x^2+x+1$	T_2
88	1011000	$x^6+x^4+x^3$	U_2
89	1011001	$x^6+x^4+x^3+1$	$\ddot{U}_2$
90	1011010	$x^6+x^4+x^3+x$	V_2
91	1011011	$x^6+x^4+x^3+x+1$	W_2
92	1011100	$x^6+x^4+x^3+x^2$	X_2
93	1011101	$x^6+x^4+x^3+x^2+1$	Y_2
94	1011110	$x^6+x^4+x^3+x^2+x$	Z_2
95	1011111	$x^6+x^4+x^3+x^2+x+1$	Q_2
96	1100000	x^6+x^5	A_3
97	1100001	x^6+x^5+1	B_3
98	1100010	x^6+x^5+x	C_3
99	1100011	x^6+x^5+x+1	$\c{C}_3$
100	1100100	$x^6+x^5+x^2$	D_3
101	1100101	$x^6+x^5+x^2+1$	E_3
102	1100110	$x^6+x^5+x^2+x$	F_3
103	1100111	$x^6+x^5+x^2+x+1$	G_3
104	1101000	$x^6+x^5+x^3$	$\breve{G}_3$
105	1101001	$x^6+x^5+x^3+1$	H_3
106	1101010	$x^6+x^5+x^3+x$	I_3
107	1101011	$x^6+x^5+x^3+x+1$	$\dot{I}_3$
108	1101100	$x^6+x^5+x^3+x^2$	J_3
109	1101101	$x^6+x^5+x^3+x^2+1$	K_3
110	1101110	$x^6+x^5+x^3+x^2+x$	L_3
111	1101111	$x^6+x^5+x^3+x^2+x+1$	M_3
112	1110000	$x^6+x^5+x^4$	N_3
113	1110001	$x^6+x^5+x^4+1$	O_3
114	1110010	$x^6+x^5+x^4+x$	$\ddot{O}_3$
115	1110011	$x^6+x^5+x^4+x+1$	P_3
116	1110100	$x^6+x^5+x^4+x^2$	R_3
117	1110101	$x^6+x^5+x^4+x^2+1$	S_3
118	1110110	$x^6+x^5+x^4+x^2+x$	$\c{S}_3$
119	1110111	$x^6+x^5+x^4+x^2+x+1$	T_3
120	1111000	$x^6+x^5+x^4+x^3$	U_3
121	1111001	$x^6+x^5+x^4+x^3+1$	$\ddot{U}_3$
122	1111010	$x^6+x^5+x^4+x^3+x$	V_3
123	1111011	$x^6+x^5+x^4+x^3+x+1$	W_3
124	1111100	$x^6+x^5+x^4+x^3+x^2$	X_3
125	1111101	$x^6+x^5+x^4+x^3+x^2+1$	Y_3
126	1111110	$x^6+x^5+x^4+x^3+x^2+x$	Z_3

127	1111111	$x^6+x^5+x^4+x^3+x^2+x+1$	Q_3

Now, let's give the encryption algorithm we want to apply.



Utilizing the above algorithm, the decoding algorithm becomes as follows.



Since the number of elements in Table 1 is very high, it is clear that the encryptions to be obtained will be more secure. A detailed application is given below to see this situation.

Let's assume that the message text to be sent is "PELİN GO BACK".

Step 1. The message text is 11 letters. According to the given coding algorithm, n can be chosen arbitrarily. Let's continue the coding algorithm by choosing $\mathrm{n} = 3$.

Step 2. The matrix $L_3(x)$ is created from the LU decomposition of the matrix $Q_k^n(x)$ using the polynomial $P(x)$, the matrix elements $L_3(x)$ are reduced.

$$L_3(x) = \begin{bmatrix} 1 & 0 & 0 \\ x & 1 & 0 \\ x^2 + x & 1 & 1 \end{bmatrix}.$$

For $n = 2$, we use the matrix $L_2(x) = \begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix}$.

Step 3. The numbers and polynomial equivalents corresponding to the text to be encrypted are written.

$19 = (0010011) = x^4 + x + 1 = \boldsymbol{P}$

$5 = (0000101) = \boldsymbol{E}$

$14 = (0001110) = \boldsymbol{L}$

$11 = (0001011) = \text{İ}$

$16 = (0010000) = \boldsymbol{N}$

$7 = (0000111) = \boldsymbol{G}$

$17 = (0010001) = \boldsymbol{O}$

$1 = (0000001) = \boldsymbol{B}$

$0 = (0000000) = \boldsymbol{A}$

$2 = (0000010) = \boldsymbol{C}$

$13 = (0001101) = \boldsymbol{K}.$

For the message text divided into block matrices 3×1 and 2×1. The matrices $L_n(x)$ are multiplied by the block matrices, respectively.

$$L_3(x)\begin{bmatrix} P \\ E \\ L \end{bmatrix} = \begin{bmatrix} x^4 + x + 1 \\ x^5 + x + 1 \\ x^6 + x^5 + 1 \end{bmatrix} = \begin{bmatrix} P \\ Ç_1 \\ B_3 \end{bmatrix},$$

$$L_3(x)\begin{bmatrix} \text{İ} \\ N \\ G \end{bmatrix} = \begin{bmatrix} \text{İ} \\ F \\ K_1 \end{bmatrix},$$

$$L_3(x)\begin{bmatrix} O \\ B \\ A \end{bmatrix} = \begin{bmatrix} O \\ Ç_1 \\ G_3 \end{bmatrix},$$

$$L_2(x)\begin{bmatrix} C \\ K \end{bmatrix} = \begin{bmatrix} C \\ H \end{bmatrix}.$$

Thus, according to the above operations, the first encrypted text is

$$P\ Ç_1\ B_3\ İ\ F\ K_1\ O\ Ç_1\ G_3\ C\ H.$$

Step 4. Let's multiply the message matrix obtained in Step 3 by the $1st$ key, respectively.

$$\begin{bmatrix} C & O & D \\ B & B & B \\ C & Ç & B \end{bmatrix}\begin{bmatrix} P \\ Ç_1 \\ B_3 \end{bmatrix} = \begin{bmatrix} U_1 \\ O_2 \\ C_1 \end{bmatrix}.$$

Since the block matrix obtained using the other six letters is of type 3×1, it is multiplied by the first key in order.

$$\begin{bmatrix} C & O & D \\ B & B & B \\ C & Ç & B \end{bmatrix}\begin{bmatrix} İ \\ F \\ K_1 \end{bmatrix} = \begin{bmatrix} G_2 \\ A_1 \\ O_1 \end{bmatrix}.$$

$$\begin{bmatrix} C & O & D \\ B & B & B \\ C & Ç & B \end{bmatrix}\begin{bmatrix} O \\ Ç_1 \\ G_3 \end{bmatrix} = \begin{bmatrix} D_1 \\ S_2 \\ A_1 \end{bmatrix}.$$

Since the block matrix to be created for the remaining two letters is of type 2×1, it is multiplied by the second key.

$$\begin{bmatrix} B & A \\ D & D \end{bmatrix}\begin{bmatrix} C \\ H \end{bmatrix} = \begin{bmatrix} C \\ R \end{bmatrix}.$$

Thus, the second encrypted message is as follows.

$$U_1\ O_2\ C_1\ G_2\ A_1\ O_1\ D_1\ S_2\ A_1\ C\ R.$$

Step 5. The resulting encrypted message is added to the kth powers of the Stirling polynomials $s_k(x)$ to obtain a new encrypted message.

$$U_1 + s_1^{(3)}(x) = x^5 + x^4 = \mathbf{N_1}$$

$$O_2 + s_2^{(3)}(x) = \mathbf{H_1}$$

$$C_1 + s_3^{(3)}(x) = \mathbf{İ_3}$$

$$G_2 + s_4^{(3)}(x) = \mathbf{Ü_3}$$

$$A_1 + s_5^{(3)}(x) = \boldsymbol{S_2}$$

$O_1 + s_6^{(3)}(x) = \boldsymbol{Y_2}$

$D_1 + s_7^{(3)}(x) = \boldsymbol{L_2}$

$S_2 + s_8^{(3)}(x) = \boldsymbol{Q}$

$A_1 + s_9^{(3)}(x) = \boldsymbol{X_3}$

$C + s_{10}^{(3)}(x) = \boldsymbol{X_3}$

$R + s_{11}^{(3)}(x) = \boldsymbol{K_3}$.

As a result, the encrypted text sent to the recipient of the message is as follows

$N_1\ H_1\ \dot{I}_3\ \ddot{U}_3\ S_2\ Y_2\ L_2\ Q\ X_3\ X_3\ K_3$.

Backward solving algorithm.

In order to obtain the initial state of the encrypted message obtained in the last operation of the encrypted algorithm, the following steps are followed in order.

Step 1. The letters of the encrypted message obtained in the last process of the encryption algorithm are summed, respectively, by the kth power of the Stirling polynomials.

$N_1 + s_1^{(3)}(x) = x^5 + x^4 + x^3 = \boldsymbol{U_1}$

$H_1 + s_2^{(3)}(x) = \boldsymbol{O_2}$

$\dot{I}_3 + s_3^{(3)}(x) = \boldsymbol{C_1}$

$\ddot{U}_3 + s_4^{(3)}(x) = \boldsymbol{G_2}$

$S_2 + s_5^{(3)}(x) = \boldsymbol{A_1}$

$Y_2 + s_6^{(3)}(x) = \boldsymbol{O_1}$

$L_2 + s_7^{(3)}(x) = \boldsymbol{D_1}$

$Q + s_8^{(3)}(x) = \boldsymbol{S_2}$

$X_3 + s_9^{(3)}(x) = \boldsymbol{A_1}$

$X_3 + s_{10}^{(3)}(x) = \boldsymbol{C}$

$K_3 + s_{11}^{(3)}(x) = \boldsymbol{R}$.

So, we can get

$U_1\ O_2\ C_1\ G_2\ A_1\ O_1\ D_1\ S_2\ A_1\ C\ R.$

Step 2. Let's multiply the resulting message matrix by the inverse of the key matrices, respectively

$$\begin{bmatrix} Z & \dot{I}_2 & E_2 \\ O_3 & V_2 & C_3 \\ O_3 & X_2 & B_3 \end{bmatrix}\begin{bmatrix} U_1 \\ O_2 \\ C_1 \end{bmatrix} = \begin{bmatrix} P \\ Ç_1 \\ B_3 \end{bmatrix}.$$

Since the block matrix to be used for the other six letters in the sequence is of order 3×1.

$$\begin{bmatrix} Z & \dot{I}_2 & E_2 \\ O_3 & V_2 & C_3 \\ O_3 & X_2 & B_3 \end{bmatrix}\begin{bmatrix} G_2 \\ A_1 \\ O_1 \end{bmatrix} = \begin{bmatrix} \dot{I} \\ F \\ K_1 \end{bmatrix},$$

$$\begin{bmatrix} Z & \dot{I}_2 & E_2 \\ O_3 & V_2 & C_3 \\ O_3 & X_2 & B_3 \end{bmatrix}\begin{bmatrix} D_1 \\ S_2 \\ A_1 \end{bmatrix} = \begin{bmatrix} D_1 \\ S_2 \\ A_1 \end{bmatrix}.$$

Since the block matrix required for the last two letters is of type 2×1.

$$\begin{bmatrix} B & A \\ Y_2 & K_3 \end{bmatrix}\begin{bmatrix} C \\ R \end{bmatrix} = \begin{bmatrix} C \\ H \end{bmatrix}.$$

Thus, we obtain the encrypted decryption message as follows

$P\ Ç_1\ B_3\ \dot{I}\ F\ K_1\ O\ Ç_1\ G_3\ C\ H.$

Step 3. Considering the polynomial $P(x)$, the matrix $(L_3(x))^{-1}$ is as follows

$$(L_3(x))^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ -x & 1 & 0 \\ -x^2 & -1 & 1 \end{bmatrix}.$$

Step 4. The ciphertext obtained in Step 2 should be multiplied by the matrices $(L_3(x))^{-1}$ in Step 3

$$(L_3(x))^{-1}\begin{bmatrix} P \\ Ç_1 \\ B_3 \end{bmatrix} = \begin{bmatrix} P \\ E \\ L \end{bmatrix},$$

$$(L_3(x))^{-1}\begin{bmatrix} \dot{I} \\ F \\ K_1 \end{bmatrix} = \begin{bmatrix} \dot{I} \\ N \\ G \end{bmatrix},$$

$$(L_3(x))^{-1}\begin{bmatrix} D_1 \\ S_2 \\ A_1 \end{bmatrix} = \begin{bmatrix} O \\ B \\ A \end{bmatrix} \text{ and } (L_2(x))^{-1}\begin{bmatrix} C \\ H \end{bmatrix} = \begin{bmatrix} C \\ K \end{bmatrix}.$$

When all these steps are followed, the text to be sent will be found as PELİN GO BACK.

4. CONCLUSION

In this study, Stirling numbers were examined and Stirling polynomials were defined with the help of these numbers. Using these newly defined polynomials, the AES type encryption algorithm, which is widely used in the literature, was examined and an application was given to perform encryption as an application of this algorithm. This given algorithm can be used in other studies to be done in the field of encryption.

CONFLICTS OF INTEREST

No conflict of interest was declared by the authors.

REFERENCES

[1] Graham, R.L., Knuth, D.E., Patashnik, O., "Concrete Math: A Foundation for Computer Science", Second Edition, Addison-Wesley, Massachusetts, 257-267, (1994).

[2] Stirling, J., Methodus Differentialis sive Tractatus de Summatione et Interpolatione Serierum Infinitarum, G. Strahan, London, 8-11, (1730).

[3] Pearson, K., "Historical note on the origin of the normal curve of errors", Biometrika, 16(3/4): 402-404, (1924). DOI: https://doi.org/10.2307/2331714

[4] Dominici, D., Variations on a theme by James Stirling, arXiv preprint math/0603007, (2006).

[5] Abel, N.H., "Mémoire Sur Les Équations Algeébriques Où on Démontre L'impssibilité de la Résolution de L'equation Générale Du Cinquième Dégré", Christiania, Groendahl, University of Olso, (1824).

[6] Mongelli, P., "Total positivity properties of Jacobi–Stirling numbers", Advances in Applied Mathematics, 48(2): 354-364, (2012). DOI: https://doi.org/10.1016/j.aam.2011.06.008

[7] Aziza, H.A., "Combinatoric sums and their applications in probability and statistics", Master's Thesis, Akdeniz University, Antalya, (2016).

[8] Cheon, G.S., Kim, J.S., "Stirling matrix via Pascal matrix", Linear Algebra and its Applications, 329(1/3): 49-59, (2001). DOI: https://doi.org/10.1016/S0024-3795(01)00234-8

[9] Lee, G.Y., Kim, J.S., Cho, S.H., "Some combinatorial identities via Fibonacci numbers", Discrete Applied Mathematics, 130(3): 527-534, (2003). DOI: https://doi.org/10.1016/S0166-218X(03)00331-7

[10] He, T.X., "Use Impulse Response Sequences in the Construction of Number Sequence Identities", arXiv preprint arXiv:1303.7466, (2013).

[11] Boyadzhiev, K.N., "Close encounters with the Stirling numbers of the second kind", Mathematics Magazine, 85(4): 252-266, (2012). DOI: https://doi.org/10.4169/math.mag.85.4.252

[12] Butzer, P.L., Markett, C., Schmidt, M., "Stirling numbers, central factorial numbers, and representations of the Riemann zeta function", Results in Mathematics, 19(3): 257-274, (1991). DOI: https://doi.org/10.1007/BF03323285

[13] Dere, R., "Generating Functions and Applications of Some Special Polynomials on Umbral Algebra", Master's Thesis, Akdeniz University, Antalya, (2011).

[14] Yıldız, Y., "Stirling Polynomial Families", Master's Thesis, Akdeniz University, Antalya, (2022).

[15] Nesin, A., "Stirling Sayıları", Sayma-Kombinasyon Hesapları (6. Baskı), Nesin Yayıncılık, İstanbul, 155-166, (2019).

[16] Hetyei, G., "The Stirling Polynomial of a Simplicial Complex", Discrete & Computational Geometry, 35(3): 437-455, (2006). DOI: https://doi.org/10.1007/s00454-005-1190-2

[17] Massey, J.L., Costello, D.J., Justesen, J., "Polynomial weights and code constructions", IEEE Transactions on Information Theory, 19(1): 101-110, (1973). DOI: 10.1109/TIT.1973.1054936

[18] Başar, Ü., "Merkezi Faktöriyel Sayılarının Üreteç Fonksiyonları ve Uygulamaları", Master's Thesis, Akdeniz University, Antalya, (2016).

[19] Halıcı, S., Koca, N., "On Excellent Safe Primary Numbers and Encryption", In Conference Proceedings of Science and Technology, 3(2): 247-251, (2020).

[20] Klima, R. E., Sigmon, N. P., "Cryptology: Classical and modern with maplets", Second Edition, New York: Chapman and Hall/CRC, (2012).

[21] Avaroglu, E., Koyuncu, I., Ozer, A.B., Turk, M., "Hybrid pseudo-random number generator for cryptographic systems", Nonlinear Dynamics, 82(1/2): 239-248, (2015). DOI: https://doi.org/10.1007/s11071-015-2152-8

[22] Kadıoğlu, E., "Cisim Genişlemeleri ve Galois Grupları", Master's Thesis, Atatürk University, Erzurum, (1986).

[23] Paar, C., Pelzl, J., "Understanding cryptography: A textbook for students and practitioners", London: Springer Science, Business Media, Berlin, Heidelberg, (2009).

[24] Pehlivan, M.K., Duru, N., Sakallı, M.T., "Sonlu Cisimler Teorisine Dayalı Gri Seviye Görüntü Şifreleme", Bilecik Şeyh Edebali University Journal of Science, 3(2): 10-17, (2016).

[25] Diskaya, O., Avaroglu, E., Menken, H., "The classical AES-like cryptology via the Fibonacci polynomial matrix", Turkish Journal of Engineering, 4(3): 123-128, (2020). DOI: 10.31127/tuje.646926