JSSE
JOURNAL OF SCIENCE & SCIENCE EDUCATION
Faculty of Science, Ubon Ratchathani University
Vol. 7 No. 7 (Jul. – Dec. 2024): 295 - 304
http://doi.org/10.14456/jsse.2024.23

Research Article in Science

Encoding and Decoding by Using Pell and modify Pell Matrices

Supunnee Sompong[1], Phongphan Mukwachi[1], Sa-at Muangchan[1] and Jirawat Kantalo[1,*]

[1]Department of Mathematics and Statistics, Faculty of Science and Technology,
Sakon Nakhon Rajabhat University, Sakon Nakhon
**Email: jirawat@snru.ac.th*

Received <26 April 2024>; Revised <17 July 2024>; Accepted <26 July 2024 >

Abstract

In this paper, we study the Pell, modify Pell sequences, and the matrices whose entries are related to Pell and modify Pell sequences. Moreover, we apply these matrices to present a new algorithm for encoding, which transforms plain text into cipher text for secure transmission, and decoding, which involves decrypting the received cipher text back into its original message.

Keywords: Cryptography, Sequences, Matrices

บทความวิจัยทางวิทยาศาสตร์

การเข้ารหัสและถอดรหัสโดยการใช้เมทริกซ์เพลล์และเพลล์ที่ปรับปรุงแล้ว

สุพรรณี สมพงษ์[1] พงษ์พันธ์ มุขวะชิ[1] สอาด ม่วงจันทร์[1] และ จิรวัฒน์ กันทะโล[1,*]

[1]สาขาวิชาคณิตศาสตร์และสถิติ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏสกลนคร จังหวัดสกลนคร

**Email: jirawat@snru.ac.th*

รับบทความ: 26 เมษายน 2567 แก้ไขบทความ: 17 กรกฎาคม 2567 ยอมรับตีพิมพ์: 26 กรกฎาคม 2567

บทคัดย่อ

บทความวิจัยนี้ คณะผู้วิจัยได้ศึกษาเมทริกซ์เพลล์และเพลล์ที่ปรับปรุงแล้วที่สมาชิกในเมทริกซ์เกี่ยวข้องกับลำดับเพลล์และลำดับเพลล์ที่ปรับปรุงแล้ว นอกจากนี้ คณะผู้วิจัยได้นำเมทริกซ์ดังกล่าวมาใช้ในการนำเสนอขั้นตอนวิธีการใหม่สำหรับการเข้ารหัสซึ่งแปลงข้อความธรรมดาเป็นข้อความที่ได้รับการเข้ารหัสเพื่อความปลอดภัยในการส่งข้อมูลและการถอดรหัสเป็นขั้นตอนในการแปลรหัสข้อความที่ได้รับการเข้ารหัสเพื่อให้ได้ข้อความเดิม

คำสำคัญ: วิทยาการเข้ารหัสลับ ลำดับ เมทริกซ์

Introduction

Several sequences of real numbers are important in mathematics and have been widely studied for their properties and applications such as the Fibonacci and Lucas sequences. In this paper, we have studied the Pell and modify Pell sequences which are among the well-known sequences. The Pell sequences (Halici and Daşdemir, 2010) is defined by

$$p_n = 2p_{n-1} + p_{n-2}, \tag{1}$$

for positive integer $n \geq 2$ with initial condition $p_0 = 0$ and $p_1 = 1$. The modify Pell sequences (Halici and Daşdemir, 2010) is defined by

$$q_n = 2q_{n-1} + q_{n-2}, \tag{2}$$

for positive integer $n \geq 2$ with initial condition $q_0 = 1$ and $q_1 = 1$.

At present, there are many research studies related to the study of the properties and applications of sequences of real numbers, particularly in the application of cryptography theory. For example, in 2018, (Taş, *et al.*, 2018) proposed a new method for encryption and decryption using the Fibonacci sequence. In 2019, (Sümeyra *et al.*, 2019) have introduced new algorithms by using $Q-$ matrix and $R-$matrix which are respectively defined by

$$Q = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } R = \begin{bmatrix} 1 & 2 \\ 2 & -1 \end{bmatrix}. \tag{3}$$

Then

$$Q^n = \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix} \text{ and } R^n = \begin{bmatrix} l_{n+1} & l_n \\ l_n & l_{n-1} \end{bmatrix}, \tag{4}$$

where f_n is Fibonacci sequences and l_n is Lucas sequences. See more examples in (Stakhov, 1999; Hoggatt and Ruggles, 1963; Shtayat and Al-Kateeb, 2019; Flaut, 2019; Sundarayya and Vara Prasad,2019; Shtayat and Al-Kateeb, 2022).

In this paper, we will present a new method for encryption and decryption using a matrix whose entries are related to the power of matrix associated with the modified Pell sequence, and we will provide an illustrative example of this method.

Preliminary

In this section, we will introduce and study the following definitions and lemmas of the Pell and modify Pell as defined in (1) and (2).

Lemma 1. (Horadam, 1994) Let p_n be the Pell sequences and q_n be the modify Pell sequences. Then, for every positive integer n,

1. $q_n = p_{n+1} - p_n$
2. $q_{n+1} = p_{n+1} + p_n$
3. $p_{n+1} = \dfrac{q_{n+1} + q_n}{2}$.

Lemma 2. (Ercolano, 2010) Let P be a matrix, is defined by

$$P=\begin{bmatrix}2 & 1\\ 1 & 0\end{bmatrix} \text{ then } P^n=\begin{bmatrix}p_{n+1} & p_n\\ p_n & p_{n-1}\end{bmatrix} \tag{5}$$

and $\det\left(P^n\right)=(-1)^n$ for n is positive integer.

Now, we will present new definitions and lemma that are useful in our research.

Definition 1. Let Z_k be a matrix for $k\in\{1,2,3,4\}$, is defined by

$$Z_1=\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix},\ Z_2=\begin{bmatrix}1 & 1\\ -1 & 1\end{bmatrix},\ Z_3=\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix},\ Z_4=\begin{bmatrix}-1 & 1\\ 1 & 1\end{bmatrix}. \tag{6}$$

Definition 2. Let T_{n_k} be a matrix, is defined by

$$T_{n_k}=Z_kP^n \tag{7}$$

for positive integer n and $k\in\{1,2,3,4\}$.

Lemma 3. Let T_{n_k} be defined as in equation (7). Then we have

1. $T_{n_1}=\begin{bmatrix}q_n & q_{n-1}\\ q_{n+1} & q_n\end{bmatrix}$
2. $T_{n_2}=\begin{bmatrix}q_{n+1} & q_n\\ -q_n & -q_{n-1}\end{bmatrix}$
3. $T_{n_3}=\begin{bmatrix}q_{n+1} & q_n\\ q_n & q_{n-1}\end{bmatrix}$
4. $T_{n_4}=\begin{bmatrix}-q_n & -q_{n-1}\\ q_{n+1} & q_n\end{bmatrix}$.

Proof. We will prove 1. From (5), (6) and (7), we have

$$\begin{aligned}T_{n_1}&=Z_1P^n\\ &=\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix}\begin{bmatrix}p_{n+1} & p_n\\ p_n & p_{n-1}\end{bmatrix}\\ &=\begin{bmatrix}p_{n+1}-p_n & p_n-p_{n-1}\\ p_{n+1}+p_n & p_n+p_{n-1}\end{bmatrix}\\ &=\begin{bmatrix}q_n & q_{n-1}\\ q_{n+1} & q_n\end{bmatrix}.\end{aligned}$$

For 2-4, the proof is similar to the proof of 1.

Note that: From the definition 2 and the determinant of product Z_k and P^n, we have

$$\det\left(T_{n_k}\right)=\begin{cases}2(-1)^n & ;\ k\in\{1,2\}\\ 2(-1)^{n+1} & ;\ k\in\{3,4\}\end{cases}. \tag{8}$$

Main Results

In the main results, we present two sections. The first section introduces a new algorithm for encryption and decryption, as shown in Figure 1. In the second section, we will demonstrate an example of using the encryption and decryption algorithms.

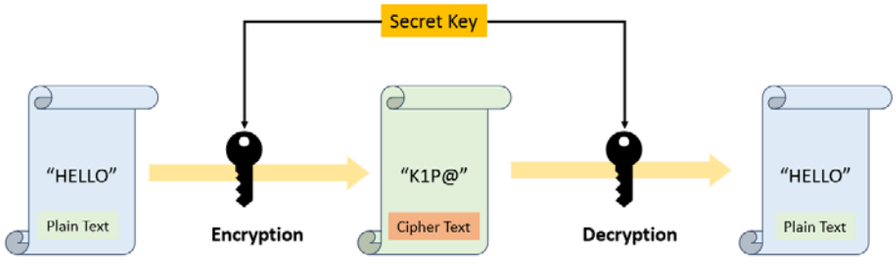

Figure 1 Diagram of flow of work

New algorithm for encryption and decryption

Firstly, we will introduce the notations used in the new algorithm.

1. Let M be a $2m\times 2m$ plain text square matrix. If entries of M has a spaced between words, we will add zeros. Moreover, if M does not satisfy the given size requirement, we will also add zeros until it is complete.
2. Let B_i be a 2×2 blocked matrix divided from M from left to right.
3. Let E_i be any 2×2 matrix.
4. Let T_{n_k} be a 2×2 matrix, defined as in equation (7).
5. Let l be the number of matrices B_i.
6. Let n be positive integer, defined by

$$n=\begin{cases}3 & ;\ l\le 3\\ \left\lfloor\frac{l}{2}\right\rfloor & ;\ l>3\end{cases},$$

where $\left\lfloor\frac{l}{2}\right\rfloor$ is the largest integer less than or equal to $\frac{l}{2}$.

So, we have

$$B_i=\begin{bmatrix}b_1^i & b_2^i\\ b_3^i & b_4^i\end{bmatrix},\ E_i=\begin{bmatrix}e_1^i & e_2^i\\ e_3^i & e_4^i\end{bmatrix}\text{ and }T_n=\begin{bmatrix}t_1 & t_2\\ t_3 & t_4\end{bmatrix}, \tag{9}$$

where $1\le i\le m^2$.

Then, we assign values based on modular 29 for the following character Table 1.

Table 1. The values based on modular 29 for the following characters.

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

Encryption and decryption algorithms are as follows:

Encryption algorithm

Step 1: Divide matrix M into matrices B_i for $1 \le i \le m^2$.

Step 2: Choose n.

Step 3: Define b_j^i for $1 \le i, j \le 4$.

Step 4: Calculate d_i such that $d_i = \det(B_i)$.

Step 5: Construct key matrix K such that $K = \begin{bmatrix} d_i & b_k^i \end{bmatrix}$ for $k \in \{1,3,4\}$.

Finally, we will send matrix K and n to recipient for decoding the cipher text.

Decryption algorithm

Step 1: Choose Z_k for $k \in \{1,2,3,4\}$.

Step 2: Calculate T_{n_k}.

Step 3: Define t_j for $1 \le j \le 4$.

Step 4: Calculate e_3^i such that $e_3^i = t_1 b_3^i + t_3 b_4^i$.

Step 5: Calculate e_4^i such that $e_4^i = t_2 b_3^i + t_4 b_4^i$.

Step 6: Find solutions x_i for $1 \le i \le m^2$.

If we choose Z_1 or Z_2, we find the solution x_i from

$$2(-1)^n d_i = e_4^i(t_3 x_i + t_1 b_1^i) - e_3^i(t_4 x_i + t_2 b_1^i).$$

If we choose Z_3 or Z_4, we find the solution x_i from

$$2(-1)^{n+1} d_i = e_4^i(t_3 x_i + t_1 b_1^i) - e_3^i(t_4 x_i + t_2 b_1^i).$$

Step 7: Let $x_i = b_2^i$.

Step 8: Construct matrix B_i.

Step 9: Construct matrix M.

Numerical Example

Example 1. We suppose that the plain text is “HAPPY NEW YEAR”. Then, M defined in equation (10) is plain text square matrix with size of 4×4 (in the case $m = 2$):

$$M = \begin{bmatrix} H & A & P & P \\ Y & 0 & N & E \\ W & 0 & Y & E \\ A & R & 0 & 0 \end{bmatrix}. \tag{10}$$

Encryption algorithm

In the encryption algorithm, M defined in equation (10) has B_i for $1 \le i \le 4$ in step 2, which are

$$B_1 = \begin{bmatrix} H & A \\ Y & 0 \end{bmatrix} \quad B_2 = \begin{bmatrix} P & P \\ N & E \end{bmatrix} \quad B_3 = \begin{bmatrix} W & 0 \\ A & R \end{bmatrix} \quad B_4 = \begin{bmatrix} Y & E \\ 0 & 0 \end{bmatrix}. \tag{11}$$

Since $l = 4$, $n = \left\lfloor \frac{4}{2} \right\rfloor = 2$. Then, we get the numeric as characters based on modular 29 from Table 1:

H	A	P	P	Y	0	N	E
23	1	15	15	6	4	17	26
W	0	Y	E	A	R	0	0
8	4	6	26	1	13	4	4

We get the entries b_j^i in matrices B_i for $1 \le i, j \le 4$ which are following in table:

$b_1^1 = 23$	$b_2^1 = 1$	$b_3^1 = 6$	$b_4^1 = 4$
$b_1^2 = 15$	$b_2^2 = 15$	$b_3^2 = 17$	$b_4^2 = 26$
$b_1^3 = 8$	$b_2^3 = 4$	$b_3^3 = 1$	$b_4^3 = 13$
$b_1^4 = 6$	$b_2^4 = 26$	$b_3^4 = 4$	$b_4^4 = 4$

After that, we calculate d_i such that $d_i = \det(B_i)$. We have

$$d_1 = \det(B_1) = \det\left(\begin{bmatrix} 23 & 1 \\ 6 & 4 \end{bmatrix}\right) = 86, \tag{12}$$

$$d_2 = \det(B_2) = \det\left(\begin{bmatrix} 15 & 15 \\ 17 & 26 \end{bmatrix}\right) = 135, \tag{13}$$

$$d_3 = \det(B_3) = \det\left(\begin{bmatrix} 8 & 4 \\ 1 & 13 \end{bmatrix}\right) = 100, \tag{14}$$

$$d_4 = \det(B_4) = \det\left(\begin{bmatrix} 6 & 26 \\ 4 & 4 \end{bmatrix}\right) = -80. \tag{15}$$

Finally, we have obtained the key matrix K, which is

$$K = \begin{bmatrix} 86 & 23 & 6 & 4 \\ 135 & 15 & 17 & 26 \\ 100 & 8 & 1 & 13 \\ -80 & 6 & 4 & 4 \end{bmatrix} \tag{16}$$

and send K and n to recipient for decoding.

Decryption algorithm

In the decryption algorithm, the recipient will receive matrix K for using in decoding, with the following steps.

Firstly, we choose Z_k for $k \in \{1,2,3,4\}$. In this paper, we choose $Z_1 = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$. Then, we calculate T_{2_1} from lemma 3., we get $T_{2_1} = \begin{bmatrix} 3 & 1 \\ 7 & 3 \end{bmatrix}$. So, we have $t_1 = 3,\ t_2 = 1,\ t_3 = 7$, and $t_4 = 3$.

We calculate $e_3^i = t_1 b_3^i + t_3 b_4^i$ and $e_4^i = t_2 b_3^i + t_4 b_4^i$ for $1 \le i \le 4$ to construct matrix E. So, we have

$$
\begin{aligned}
e_3^1 &= (3\times 6) + (7\times 4) = 46, \\
e_3^2 &= (3\times 17) + (7\times 26) = 233, \\
e_3^3 &= (3\times 1) + (7\times 13) = 94, \\
e_3^4 &= (3\times 4) + (7\times 4) = 40, \\
e_4^1 &= (1\times 6) + (3\times 4) = 18, \\
e_4^2 &= (1\times 17) + (3\times 26) = 95, \\
e_4^3 &= (1\times 1) + (3\times 13) = 40, \\
e_4^4 &= (1\times 4) + (3\times 4) = 16.
\end{aligned}
$$

In the next step, we will find all solutions x_i for $1 \le i \le 4$.

To find solution x_1, we observe the following equations:

$$
\begin{aligned}
2(-1)^2 d_1 &= e_4^1(t_3 x_1 + t_1 b_1^1) - e_3^1(t_4 x_1 + t_2 b_1^1), \\
2(-1)^2 (86) &= 18(7x_1 + (3\times 23)) - 46(3x_1 + (1\times 23)), \\
x_1 &= \frac{184 - 172}{12}, \\
x_1 &= 1.
\end{aligned}
$$

To find solution x_2, we observe the following equations:

$$
\begin{aligned}
2(-1)^2 d_2 &= e_4^2(t_3 x_2 + t_1 b_1^2) - e_3^2(t_4 x_2 + t_2 b_1^2), \\
2(-1)^2 (135) &= 95(7x_2 + (3\times 15)) - 233(3x_2 + (1\times 15)), \\
x_2 &= \frac{780 - 270}{34}, \\
x_2 &= 15.
\end{aligned}
$$

To find solution x_3, we observe the following equations:

$$
\begin{aligned}
2(-1)^2 d_3 &= e_4^3(t_3 x_3 + t_1 b_1^3) - e_3^3(t_4 x_3 + t_2 b_1^3), \\
2(-1)^2 (100) &= 40(7x_3 + (3\times 8)) - 94(3x_3 + (1\times 8)), \\
x_3 &= \frac{208 - 200}{2}, \\
x_3 &= 4.
\end{aligned}
$$

To find solution x_4, we observe the following equations:

$$\begin{aligned} 2(-1)^2 d_4 &= e_4^4(t_3x_4 + t_1b_1^4) - e_3^4(t_4x_4 + t_2b_1^4), \\ 2(-1)^2(-80) &= 16(7x_4 + (3\times 6)) - 40(3x_4 + (1\times 6)), \\ x_4 &= \frac{208+48}{8}, \\ x_4 &= 26. \end{aligned}$$

Hence, we have obtained $b_2^1 = x_1 = 1,\ b_2^2 = x_2 = 15,\ b_2^3 = x_3 = 4$ and $b_2^4 = x_4 = 26.$

So, the matrices B_i for $1 \le i \le 4$ which are

$$B_1 = \begin{bmatrix} b_1^1 & b_2^1 \\ b_3^1 & b_4^1 \end{bmatrix} = \begin{bmatrix} 23 & 1 \\ 6 & 4 \end{bmatrix},\ B_2 = \begin{bmatrix} b_1^2 & b_2^2 \\ b_3^2 & b_4^2 \end{bmatrix} = \begin{bmatrix} 15 & 15 \\ 17 & 26 \end{bmatrix},$$
$$B_3 = \begin{bmatrix} b_1^3 & b_2^3 \\ b_3^3 & b_4^3 \end{bmatrix} = \begin{bmatrix} 8 & 4 \\ 1 & 13 \end{bmatrix},\ B_4 = \begin{bmatrix} b_1^4 & b_2^4 \\ b_3^4 & b_4^4 \end{bmatrix} = \begin{bmatrix} 6 & 26 \\ 4 & 4 \end{bmatrix}.$$

Finally, the matrix M is

$$M = \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix} = \begin{bmatrix} 23 & 1 & 15 & 15 \\ 6 & 4 & 17 & 26 \\ 8 & 4 & 6 & 26 \\ 1 & 13 & 4 & 4 \end{bmatrix} = \begin{bmatrix} H & A & P & P \\ Y & 0 & N & E \\ W & 0 & Y & E \\ A & R & 0 & 0 \end{bmatrix}.$$

The message after decoding will be “HAPPY NEW YEAR”.

Conclusions

In this paper, we present a new algorithm for encryption and decryption of messages. This algorithm, involves dividing the message matrix into size of $2m$ and applying properties from the n^{th} power matrix related to modify Pell sequences for decryption. Additionally, we provided an example demonstrating the steps of encryption and decryption using the new algorithm.

Acknowledgements

We would like to sincerely appreciate the reviewers for reading and providing feedback on the manuscript, as well as to Sakon Nakhon Rajabhat University for supporting the research facilities used in this study.

References

Ercolano, J. (1979). Matrix generators of Pell sequences. **Fibonacci Quart**, 17(1), 71-77.

Flaut, C. (2019). Some application of difference equations in Cryptography and Coding Theory. **Journal of Difference Equations and Applications**, 25(7), 905-920.

Halici, S. and Daşdemir, A. (2010). On some relationships among Pell, Pell-Lucas and modified Pell sequences. **Sakarya University Journal of Science**, 14(2), 141-145.

Hoggatt Jr, V. E. and Ruggles, I. D. (1963). A Primer for the Fibonacci Numbers-Part IV. **The Fibonacci Quarterly**, 1(4), 39-45.

Horadam, A. F. (1994). Applications of modified Pell numbers to representations. **Ulam Quarterly**, 3(1),34-53.

Shtayat, J. and Al-Kateeb, A. (2019). An Encoding-Decoding algorithm based on Padovan numbers. **arXiv preprint arXiv**, 1907.02007.

Shtayat, J. and Al-Kateeb, A. (2022). The Perrin R-matrix and more properties with an application. **Journal of Discrete Mathematical Sciences and Cryptography**, 25(1), 41-52.

Stakhov, A. P. (1999). A generalization of the Fibonacci Q-matrix. **Reports of the National Academy of Sciences of Ukraine**, 9, 46-49.

Sundarayya, P. and Vara Prasad, G. (2019). A public key cryptosystem using Affine Hill Cipher under modulation of prime number. **Journal of Information and Optimization Sciences**, 40(4), 919-930.

Sümeyra, U. Ç. A. R., Nihal, T. A. Ş. and Özgür, N. Y. (2019). A new application to coding theory via Fibonacci and Lucas numbers. **Mathematical Sciences and Applications E-Notes**, 7(1), 62-70.

Taş, N., Uçar, S., Özgür, N. Y. and Kaymak, Ö. Ö. (2018). A new coding/decoding algorithm using Fibonacci numbers. **Discrete Mathematics, Algorithms and Applications**, 10(02), 1850028.