International Journal of Applied Mathematics

Volume 38 No. 2 2025, 227–252
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
doi: http://dx.doi.org/10.12732/ijam.v38i2.5

# AN RSA CRYPTOSYSTEM BASED ON NEW SEQUENCES FROM THE GENERALIZED JACOBSTHAL NUMBERS AND GENERALIZED PELL NUMBERS

**Elahe Mehraban [1,2,3], T. Aaron Gulliver [4], Evren Hinçal [1,2,3]**

[1] Mathematics Research Center

Near East University

TRNC, Mersin 10, 99138 Nicosia, TURKEY

[2] Department of Mathematics

Near East University

TRNC, Mersin 10, 99138 Nicosia, TURKEY

[3] Faculty of Art and Science

University of Kyrenia

TRNC, Mersin 10, 99320 Kyrenia, TURKEY

emails: e.mehraban.math@gmail.com, evren.hincal@neu.edu.tr

[4] Department of Electrical and Computer Engineering

University of Victoria

Victoria, BC, V8W 2Y2, CANADA

e-mail: agullive@uvic.ca

Received: 2 February 2025 

.

**Abstract**

In this paper, we define two new sequences using the generalized Jacobsthal numbers and generalized Pell $(p,i)-$ numbers. First, sequences are obtained from the characteristic polynomials of these numbers and then sequences are derived from the Hadamard-type product of these polynomials. The determinants and combinatorial and exponential representations of these new sequences are given. As an application, they are used in an RSA cryptosystem.

**Math. Subject Classification:** Primary: 11C20, 11K31, 68P25 Secondary: 68R01, 68P30, 15A15

**Key Words and Phrases:** Jacobsthal numbers, Pell numbers, cryptography, matrix, RSA cryptosystem

## 1. Introduction

The Pell numbers denoted by $\{P_n\}_0^\infty$ are defined as

$$P_n = 2P_{n-1} + P_{n-2}, \quad n \geq 0,$$

with initial conditions $P_0 = 0$ and $P_1 = 1$. The Pell sequence can be generated in different ways. One is via the generalized Pell $(p,i)-$numbers that are defined as follows.

Definition 1.1 ([19]). For $p \in \mathbb{N}$ and $0 \leq i \leq p$, the generalized Pell $(p,i)-$numbers are

$$P_n^i(p) = 2P_{n-1}^i(p) + P_{n-p-1}^i(p), \quad n > p+1,$$

with initial conditions $P_0^i(p) = P_1^i(p) = \cdots = P_i^i(p) = 0$ and $P_{(i+1)}^i(p) = \cdots = P_p^i(p) = 1$.

For example, if $i = 2$ and $p = 3$, we have

$$P_n^2(3) = 2P_{n-1}^2(3) + P_{n-4}^2(3), \quad n > 4,$$

so the sequence is $\{P_n^2(3)\}_0^\infty = \{0, 0, 0, 1, 2, 4, 8, 17, 36, 76, 160, \cdots\}$.

The $k-$step generalized Pell sequence was introduced in [7] and its properties modulo $m$ were investigated. The quaternion-Pell sequence was defined in [8] and some useful results were obtained. The generalized order 2$-$Pell sequences of some classes of groups were investigated in [12].

In [13], the Fibonacci length and generalized order of $k$-Pell sequences of the 2-generator $p-$groups of nilpotency class 2 were obtained.

The Jacobsthal numbers $J_n$ are another important sequence which is defined as, [15],

$$J_n = J_{n-1} + 2J_{n-2}, \quad n \geq 0,$$

with initial conditions $J_0 = 0$ and $J_1 = 1$. The Jacobsthal numbers have many generalizations [9, 27], one of which is as follows.

DEFINITION 1.2. For $k \geqslant 2$, the generalized Jacobsthal numbers, $J_{n,k}$, are [3]

$$J_{n,k} = (k-1)J_{n-1,k} + kJ_{n-2,k}, \quad n \geq 2,$$

with initial conditions $J_{0,k} = 0$ and $J_{1,k} = 1$.

For example, if $k = 2$ we have $J_{n,2} = J_{n-1,2} + 2J_{n-2,2}$ so the sequence is $\{J_{n,2}\}_0^\infty = \{0, 1, 2, 6, 16, \cdots\}$. The characteristic polynomials of the generalized Pell $(p, i)-$numbers and generalized Jacobsthal numbers are $x^{p+1} - 2x^p - 1$ and $x^2 - (k-1)x - k$, respectively.

The Hadamard-type product of polynomials $f$ and $g$ is defined as follows, [2].

DEFINITION 1.3. The Hadamard-type product of polynomials $f$ and $g$ is $f * g = \sum_{i=0}^{\infty}(a_i * b_i)x^i$, where

$$a_i * b_i = \begin{cases} a_i b_i, & \text{if } a_i b_i \neq 0, \\ a_i + b_i, & \text{if } a_i b_i = 0, \end{cases}$$

and $f(x) = a_m x^m + \cdots + a_1 x + a_0$ and $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$.

An important application of sequences is in cryptography. In [22], the Fibonacci sequence was used for image encryption. The Fibonacci sequence was employed in [1] to secure data for transmission. In [23], Fibonacci matrices were used to construct an Affine-Hill cipher. Here, an RSA algorithm using sequences is proposed.

The RSA algorithm [26] is

$$M^e \equiv C \pmod{n},$$
$$C^d \equiv M \pmod{n},$$

where $M$ and $C$ are the plaintext and ciphertext, respectively, $n$ is a prime number, $e$ is the public key, and $d$ is the secret key. It is an

important public key cryptosystem that has been studied extensively [16, 17, 18]. In [4], an attack on a short secret exponent $d_q$ modulo a larger RSA prime $q$ was presented. A multi-signature RSA algorithm which has both fixed length and verification time was given in [11]. In [6], fixed points of the RSA algorithm were obtained to provide estimates for the randomly chosen parameters. The weaknesses of this algorithm with multiple encryption and decryption exponents were studied in [25].

Motivated by the above results, we introduce two new sequences from generalized Pell $(p,i)-$numbers and the generalized Jacobsthal numbers and examine their properties. These sequences are used to obtain new RSA cryptosystems and their security is studied. This is one of the first applications of sequences in cryptography.

The remainder of this paper is organized as follows. In Sections 2 and 3, we present the generalized Jacobsthal-Pell $(k,p)-$sequences and Hadamard-type generalized Jacobsthal-Pell $(k,p)-$sequences, respectively. Then the generalized Jacobsthal-Pell $(k,p)-$sequence matrix and generalized Jacobsthal-Pell $(k,p)-$sequence matrix are used to develop two RSA algorithms.

## 2. The generalized Jacobsthal-Pell $(k,p)-$sequences

In this section, we introduce new sequences from the characteristic polynomials of the generalized Pell $(p,i)-$numbers and generalized Jacobsthal numbers. Then, some results are obtained that will be useful in subsequent sections.

The generalized Jacobsthal-Pell $(p,k)-$sequences, $p$ an integer, are defined as follows.

Definition 2.1. For $k \geq 2$ and $p$ an integer, $p \geq 3$, the generalized Jacobsthal-Pell $(k,p)-$sequences, $\{JP_n(k,p)\}_0^\infty$, are

$$\begin{aligned} &JP_{n+p+3}(k,p) = (k+1)JP_{n+p+2}(k,p) - (k-2)JP_{n+p+1}(k,p) \\ &- 2kJP_{n+p}(k,p) + JP_{n+2}(k,p) - (k-1)JP_{n+1}(k,p) - kJP_n(k,p), \\ &n \geq 0, \end{aligned} \tag{1}$$

where $JP_0(k,p) = JP_1(k,p) = \cdots = JP_{p+1}(k,p) = 0$ and $JP_{p+2}(k,p) = 1$.

EXAMPLE 2.1. For $k = 3$ and $p = 3$ we have

$$JP_{n+6}(3,3) = 4JP_{n+5}(3,3) - 1JP_{n+4}(3,3) - 6JP_{n+3}(3,3)$$

$$+ JP_{n+2}(3,3) - 2JP_{n+1}(3,3) - 3JP_n(3,3), \quad n \geq 0,$$

so the sequence is

$$\{JP_n(3,3)\}_0^\infty = \{0,0,0,0,0,1,4,15,50,162,510,\cdots\}.$$

From (1),

$$\begin{bmatrix} JP_{n+p+3}(k,p) \\ JP_{n+p+2}(k,p) \\ \vdots \\ JP_{n+2}(k,p) \\ JP_{n+1}(k,p) \end{bmatrix}$$

$$= \begin{bmatrix} k+1 & -(k-2) & -2k & 0 & \cdots & 0 & 1 & -(k-1) & -k \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\times \begin{bmatrix} JP_{n+p+2}(k,p) \\ JP_{n+p+1}(k,p) \\ \vdots \\ JP_{n+1}(k,p) \\ JP_n(k,p) \end{bmatrix}.$$

LEMMA 2.1. *For $p = 3$, $k = 3$, and $n \geq 6$ we have*

$$(\Gamma_3(3))^n = \begin{bmatrix} JP_{n+5}(3,3) & -(6JP_{n+3}(3,3) + JP_{n+4}(3,3)) + P_n(3) \\ JP_{n+4}(3,3) & -(6JP_{n+2}(3,3) + JP_{n+3}(3,3)) + P_{n-1}(3) \\ JP_{n+3}(3,3) & -(6JP_{n+1}(3,3) + JP_{n+2}(3,3)) + P_{n-2}(3) \\ JP_{n+2}(3,3) & -(6JP_n(3,3) + JP_{n+1}(3,3)) + P_{n-3}(3) \\ JP_{n+1}(3,3) & -(6JP_{n-1}(3,3) + JP_n(3,3)) + P_{n-4}(3) \\ JP_n(3,3) & -(6JP_{n-2}(3,3) + JP_{n-1}(3,3)) + P_{n-5}(3) \end{bmatrix}$$

$$\begin{matrix} -6JP_{n+4}(3,3) + P_{n+1}(3) & P_{n+2}(3) \\ -6JP_{n+3}(3,3) + P_n(3) & P_{n+1}(3) \\ -6JP_{n+2}(3,3) + P_{n-1}(3) & P_n(3) \\ -6JP_{n+1}(3,3) + P_{n-2}(3) & P_{n-1}(3) \\ -6JP_n(3,3) + P_{n-3}(3) & P_{n-2}(3) \\ -6JP_{n-1}(3,3) + P_{n-4}(3) & P_{n-3}(3) \end{matrix}$$

$$\begin{matrix} -(3JP_{n+3}(3,3) + 2JP_{n+4}(3,3)) & -3JP_{n+4}(3,3) \\ -(3JP_{n+2}(3,3) + 2JP_{n+3}(3,3)) & -3JP_{n+3}(3,3) \\ -(3JP_{n+1}(3,3) + 2JP_{n+2}(3,3)) & -3JP_{n+2}(3,3) \\ -(3JP_n(3,3) + 2JP_{n+1}(3,3)) & -3JP_{n+1}(3,3) \\ -(3JP_{n-1}(3,3) + 2JP_n(3,3)) & -3JP_n(3,3) \\ -(3JP_{n-2}(3,3) + 2JP_{n-1}(3,3)) & -3JP_{n-1}(3,3) \end{matrix} \Bigg] := (A_3(3))^n,$$

*where*

$$\Gamma_3(3) = \begin{bmatrix} 4 & -1 & -6 & 1 & -2 & -3 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \tag{2}$$

*and $P_n(3) := P_n^2(3)$.*

P r o o f. The proof is by induction on $n$.

For $p = 3$, $k = 3$, and $n = 6$ we have

$$(\Gamma_3(3))^6 = \begin{bmatrix} 1582 & -1474 & -3043 & 36 & -1506 & -1530 \\ 510 & -458 & -964 & 17 & -474 & -486 \\ 162 & -138 & -296 & 8 & -145 & -150 \\ 50 & -38 & -88 & 4 & -42 & -45 \\ 15 & -10 & -23 & 2 & -11 & -12 \\ 4 & -1 & -6 & 1 & -2 & -3 \end{bmatrix}$$

$$= \begin{bmatrix} JP_{11}(3,3) & -(6JP_9(3,3) + JP_{10}(3,3)) + P_6(3) \\ JP_{10}(3,3) & -(6JP_8(3,3) + JP_9(3,3)) + P_5(3) \\ JP_9(3,3) & -(6JP_7(3,3) + JP_8(3,3)) + P_4(3) \\ JP_8(3,3) & -(6JP_6(3,3) + JP_7(3,3)) + P_3(3) \\ JP_7(3,3) & -(6JP_5(3,3) + JP_6(3,3)) + P_2(3) \\ JP_6(3,3) & -(6JP_3(3,3) + JP_5(3,3)) + P_1(3) \end{bmatrix}$$

$$\begin{matrix} -6JP_{10}(3,3) + P_7(3) & P_8(3) \\ -6JP_9(3,3) + P_6(3) & P_7(3) \\ -6JP_8(3,3) + P_5(3) & P_6(3) \\ -6JP_7(3,3) + P_4(3) & P_5(3) \\ -6JP_6(3,3) + P_3(3) & P_4(3) \\ -6JP_5(3,3) + P_2(3) & P_3(3) \end{matrix}$$

$$\begin{matrix} -(3JP_9(3,3) + 2JP_{10}(3,3)) & -3JP_{10}(3,3) \\ -(3JP_8(3,3) + 2JP_9(3,3)) & -3JP_9(3,3) \\ -(3JP_7(3,3) + 2JP_8(3,3)) & -3JP_8(3,3) \\ -(3JP_6(3,3) + 2JP_7(3,3)) & -3JP_7(3,3) \\ -(3JP_5(3,3) + 2JP_6(3,3)) & -3JP_6(3,3) \\ -(3JP_4(3,3) + 2JP_5(3,3)) & -3JP_5(3,3) \end{matrix} \Bigg].$$

Now, assume that the statement holds for $n = s$. Then, for $n = s + 1$

$$(\Gamma_3(3))^{s+1} = \begin{bmatrix} 4 & -1 & -6 & 1 & -2 & -3 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\times \begin{bmatrix} JP_{s+5}(3,3) & -(6JP_{s+3}(3,3) + JP_{s+4}(3,3)) + P_s(3) \\ JP_{s+4}(3,3) & -(6JP_{s+2}(3,3) + JP_{s+3}(3,3)) + P_{s-1}(3) \\ JP_{s+3}(3,3) & -(6JP_{s+1}(3,3) + JP_{s+2}(3,3)) + P_{s-2}(3) \\ JP_{s+2}(3,3) & -(6JP_s(3,3) + JP_{s+1}(3,3)) + P_{s-3}(3) \\ JP_{s+1}(3,3) & -(6JP_{s-1}(3,3) + JP_s(3,3)) + P_{s-4}(3) \\ JP_s(3,3) & -(6JP_{s-2}(3,3) + JP_{s-1}(3,3)) + P_{s-5}(3) \end{bmatrix}$$

$$\begin{matrix} -6JP_{s+4}(3,3) + P_{s+1}(3) & P_{s+2}(3) \\ -6JP_{s+3}(3,3) + P_s(3) & P_{s+1}(3) \\ -6JP_{s+2}(3,3) + P_{s-1}(3) & P_s(3) \\ -6JP_{s+1}(3,3) + P_{s-2}(3) & P_{s-1}(3) \\ -6JP_s(3,3) + P_{s-3}(3) & P_{s-2}(3) \\ -6JP_{s-1}(3,3) + P_{s-4}(3) & P_{s-3}(3) \end{matrix}$$

$$\begin{bmatrix} -(3JP_{s+3}(3,3) + 2JP_{s+4}(3,3)) & -3JP_{s+4}(3,3) \\ -(3JP_{s+2}(3,3) + 2JP_{s+3}(3,3)) & -3JP_{s+3}(3,3) \\ -(3JP_{s+1}(3,3) + 2JP_{s+2}(3,3)) & -3JP_{s+2}(3,3) \\ -(3JP_s(3,3) + 2JP_{s+1}(3,3)) & -3JP_{s+1}(3,3) \\ -(3JP_{s-1}(3,3) + 2JP_s(3,3)) & -3JP_s(3,3) \\ -(3JP_{s-2}(3,3) + 2JP_{s-1}(3,3)) & -3JP_{s-1}(3,3) \end{bmatrix}$$

$$= (A_3(3))^{s+1}.$$

□

Using (2), we have $\Gamma_3(3) = -2$, so the determinant of $(\Gamma_3(3))^n$ is equal to $(-2)^n$.

Let $\Gamma_p(3) = [m_{i,j}]_{(p+3)\times(p+3)}$ be the companion matrix for the generalized Jacobsthal-Pell $(3,p)-$sequences. It can readily be established by

induction $n$ that for $p \geq 4$ and $n \geq p+3$:

$$(\Gamma_p(3))^n =$$

$$\begin{bmatrix} JP_{n+p+2}(3,p) & -(6JP_{n+p}(3,p) + JP_{n+p+1}(3,p)) + P_n(p) \\ JP_{n+p+1}(3,p) & -(6JP_{n+p-1}(3,p) + JP_{n+p}(3,p)) + P_{n-1}(p) \\ \vdots & \vdots \\ JP_{n+1}(3,p) & -(6JP_{n-1}(3,p) + JP_n(3,p)) + P_{n-p-1}(p) \\ JP_n(3,p) & -(6JP_{n-2}(3,p) + JP_{n-1}(3,p)) + P_{n-p-2}(p) \end{bmatrix}$$

$$\begin{matrix} -6JP_{n+p+1}(3,3) + P_{n+1}(3) & P_{n+2}(3) & \cdots & P_{n+p-1}(p) \\ -6JP_{n+p}(3,3) + P_n(p) & P_{n+1}(p) & \cdots & P_{n+p-2}(p) \\ \vdots & \vdots & \ddots & \vdots \\ -6JP_n(3,3) + P_{n-p}(p) & P_{n-p+1}(p) & \cdots & P_{n-2}(p) \\ -6JP_{n-1}(3,3) + P_{n-p-1}(p) & P_{n-p}(p) & \cdots & P_{n-3}(p) \end{matrix}$$

$$\begin{bmatrix} -(3JP_{n+p}(3,p) + 2JP_{n+p+1}(3,p)) & -3JP_{n+p+1}(3,p) \\ -(3JP_{n+p-1}(3,p) + 2JP_{n+p}(3,p)) & -3JP_{n+p}(3,p) \\ \vdots & \vdots \\ -(3JP_{n-1}(3,p) + 2JP_n(3,p)) & -3JP_n(3,p) \\ -(3JP_{n-2}(3,p) + 2JP_{n-1}(3,p)) & -3JP_{n-1}(3,p) \end{bmatrix},$$

where $P_n(p) := P_n^{p-1}(p)$.

LEMMA 2.2. *The characteristic equation of the generalized Jacobsthal-Pell $(k,p)-$sequences*

$$x^{p+3} - (k+1)x^{p+2} + (k-2)x^{p+1} + 2kx^p - x^2 + (k-1)x + k = 0,$$

*does not have multiple roots for $p \geq 3$ and $k \geq 2$ .*

P r o o f. It is clear that $x^{p+3} - (k+1)x^{p+2} + (k-2)x^{p+1} + 2kx^p - x^2 + (k-1)x + k = (x^{p+1} - 2x^p - 1)(x^2 - (k-1)x - k)$. We show that for $p > 3, x^{p+1} - 2x^p - 1 = 0$ has distinct roots. Suppose $\beta$ is a root of $f(x) = 0$ where $f(x) = x^{p+1} - 2x^p - 1 = 0$ so that $\beta \notin \{0,1\}$. If $\beta$ is a multiple root, then $f(\beta) = f'(\beta) = 0$. Now, $f'(\beta) = 0$ and $\beta \neq 0$ give $\beta = \dfrac{2p}{p+1}$ while $f(\beta) = 0$ means that $\beta^p(\beta - 2) - 1 = 0$. Then $(\dfrac{2p}{p+1})^p(-\dfrac{2}{p+1}) = 1$, which is impossible since the left hand side is less than 1 for $p \geq 3$. On the other hand, the roots of $x^2 - (k-1)x - k = 0$ are $-1$ and $k$. Since $(-1)^{p+1} - 2(-1)^p - 1 \neq 0$ and $(k)^{p+1} - 2(k)^p - 1 \neq 0$, the result follows. □

For the generalized Jacobsthal-Pell $(k,p)-$sequences, $\{JP_n(k,p)\}$, we have

$$D_p = \begin{bmatrix} k+1 & -(k-2) & -2k & 0 & \cdots & 0 & 1 & -(k-1) & -k \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Let $\beta_1, \beta_2, \cdots, \beta_{p+3}$ be the roots of $x^{p+3} - (k+1)x^{p+2} + (k-2)x^{p+1} + 2kx^p - x^2 + (k-1)x + k = 0$ and $U_p$ be the following $(p+3) \times (p+3)$ Vandermonde matrix

$$U_p = \begin{bmatrix} (\beta_1)^{p+2} & (\beta_2)^{p+2} & \cdots & (\beta_{p+3})^{p+2} \\ (\beta_1)^{p+1} & (\beta_2)^{p+1} & \cdots & (\beta_{p+3})^{p+1} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1 & \beta_2 & \cdots & \beta_{p+3} \\ 1 & 1 & \cdots & 1 \end{bmatrix}.$$

Now let $U_p(i,j)$ be a $(p+3)\times(p+3)$ matrix obtained from $U_p$ by replacing the $j$th column of $U_p$ by $V_P(i)$ where $V_P(i)$ is the following $(p+3) \times 1$ matrix

$$V_p(i) = \begin{bmatrix} (\beta_1)^{n+p+3-i} \\ (\beta_2)^{n+p+3-i} \\ \vdots \\ (\beta_{p+3})^{n+p+3-i} \end{bmatrix}.$$

THEOREM 2.1. *For $p \geq 3, k \geq 3$, and $(D_p)^n = [f_{i,j}^{(p,n)}]$, we have*

$$f_{i,j}^{(p,n)} = \frac{\det U_p(i,j)}{\det U_p}.$$

P r o o f. For $p \geq 3$ and $k \geq 3$, the matrix $D_p(k)$ can be diagonalized since the eigenvalues are distinct. Let $B_p = \operatorname{diag}(\beta_1, \beta_2, \cdots, \beta_{p+3})$, so

that $D_pU_p = U_pB_p$. Since $U_p$ is invertible, we have

$$\begin{cases} f_{i,1}^{(p,n)}(\beta_1)^{p+2} + f_{i,2}^{(p,n)}(\beta_1)^{p+1} + \cdots + f_{i,p+3}^{(p,n)} = (\beta_1)^{n+p+3-i}, \\ f_{i,1}^{(p,n)}(\beta_2)^{p+2} + f_{i,2}^{(p,n)}(\beta_2)^{p+1} + \cdots + f_{i,p+3}^{(p,n)} = (\beta_2)^{n+p+3-i}, \\ \vdots \\ f_{i,1}^{(p,n)}(\beta_{p+2})^{p+2} + f_{i,2}^{(p,n)}(\beta_{p+2})^{p+1} + \cdots + f_{i,p+3}^{(p,n)} = (\beta_{p+2})^{n+p+3-i}. \\ f_{i,1}^{(p,n)}(\beta_{p+3})^{p+2} + f_{i,2}^{(p,n)}(\beta_{p+3})^{p+1} + \cdots + f_{i,p+3}^{(p,n)} = (\beta_{p+3})^{n+p+3-i}. \end{cases}$$

Then it can be concluded that

$$f_{i,j}^{(p,n)} = \frac{\det U_p(i,j)}{\det U_p},$$

for $1 \le i, j \le p+3$. □

LEMMA 2.3. *Let $t(x)$ be a generation function for the generalized Jacobsthal-Pell $(k,p)-$sequences. Then*

$$t(x) = \frac{x^{p+2}}{1-(k+1)x+(k-2)x^2+2kx^3-x^{(p+1)}+(k-1)x^{p+2}+kx^{p+3}}. \tag{3}$$

P r o o f. We have

$$\begin{aligned} &t(x) = \textstyle\sum_{n=1}^{\infty} JP_n(k,p)x^n \\ &= (k+1)JP_{n+p+2}(k,p) - (k-2)JP_{n+p+1}(k,p) - 2kJP_{n+p}(k,p) \\ &\ +JP_{n+2}(k,p) - (k-1)JP_{n+1}(k,p) - kJP_n(k,p) \\ &= x^{p+2} + \textstyle\sum_{n=p+3}^{\infty}[(k+1)JP_{n+p+2}(k,p) - (k-2)JP_{n+p+1}(k,p) \\ &\ -2kJP_{n+p}(k,p) + JP_{n+2}(k,p) - (k-1)JP_{n+1}(k,p) - kJP_n(k,p)]x^n \\ &= x^{p+2} + \textstyle\sum_{n=p+3}^{\infty}(k+1)JP_{n+p+2}(k,p)x^n + \sum_{n=p+3}^{\infty} -(k-2)JP_{n+p+1}(k,p)x^n \\ &\ + \textstyle\sum_{n=p+3}^{\infty} -2kJP_{n+p}(k,p)x^n + \sum_{n=p+3}^{\infty} JP_{n+2}(k,p)x^n \\ &\ + \textstyle\sum_{n=p+3}^{\infty} -(k-1)JP_{n+1}(k,p)x^n - k\sum_{n=p+3}^{\infty} JP_n(k,p)x^n \\ &= x^{p+2} + (k+1)\textstyle\sum_{n=1}^{\infty} JP_{n+p+2}(k,p)x^n - (k-2)\sum_{n=1}^{\infty} JP_{n+p+1}(k,p)x^n \\ &\ -2k\textstyle\sum_{n=1}^{\infty} JP_{n+p}(k,p)x^n + \sum_{n=1}^{\infty} JP_{n+2}(k,p)x^n \\ &\ -(k-1)\textstyle\sum_{n=1}^{\infty} JP_{n+1}(k,p)x^n - k\sum_{n=1}^{\infty} JP_n(k,p)x^n \\ &= x^{p+2} + (k+1)xt(x) - (k-2)x^2t(x) - 2kx^3t(x) + 1x^{p+1}t(x) \\ &\ -(k-1)x^{p+2}t(x) - kx^{p+3}t(x). \end{aligned}$$

□

THEOREM 2.2. *The generalized Jacobsthal-Pell $(k,p)-$sequences $\{JP_n(k,p)\}$ have the following exponential representation*

$$t(x)=x^{p+2}\exp\sum_{i=1}^{\infty}\frac{(x)^i}{i}((k+1)-(k-2)x-2kx^2+x^p-(k-1)x^{p+1}-kx^{p+2})^i,$$

*where $p\geq 3$.*

P r o o f. Using (2), we have

$$\ln t(x)=\ln x^{p+2}-\ln(1-(k+1)x+(k-2)x^2+2kx^3-x^{(p+1)}+(k-1)x^{p+2}+kx^{p+3}),$$

and since

$$\begin{aligned}&-\ln 1-(k+1)x+(k-2)x^2+2kx^3-x^{(p+1)}+(k-1)x^{p+2}+kx^{p+3}\\&=-[-x((k+1)-(k-2)x-2kx^2+x^p-(k-1)x^{p+1}-kx^{p+2})\\&-\frac{1}{2}x^2((k+1)-(k-2)x-2kx^2+x^p-(k-1)x^{p+1}-kx^{p+2})^2\\&-\cdots-\frac{1}{i}x^i((k+1)-(k-2)x-2kx^2+x^p-(k-1)x^{p+1}-kx^{p+2})^i-\cdots],\end{aligned}$$

the result follows. □

THEOREM 2.3. *For $r,p\in\mathbb{N}$ and $n\geq p+3$, we have*

$$(\Gamma_p(3))^n(\Gamma_p(3))^r=(\Gamma_p(3))^r(\Gamma_p(3))^n=(\Gamma_p(3))^{n+r}.$$

P r o o f. The proof is straightforward by induction on $r$. □

## 3. The Hadamard-type generalized Jacobsthal-Pell $(k,p)-$sequences

In this section, we define new sequences using the Hadamard type of the generalized Jacobsthal and Pell $(p,i)-$numbers.

DEFINITION 3.1. For $k\geq 2$ and $p$ an integer, $p\geq 3$, the Hadamard-type sequence, denoted $\{HJ_n(k,p)\}_0^{\infty}$, is

$$\begin{aligned}HJ_{n+p+1}(k,p) &= 2HJ_{n+p}(k,p)-HJ_{n+2}(k,p)+(k-1)HJ_{n+1}(k,p)\\&\quad -kHJ_n(k,p), n\geq 0,\end{aligned}\tag{4}$$

with initial conditions $HJ_0(k,p)=HJ_1(k,p)=\cdots=HJ_{p-1}(k,p)=0$ and $HJ_p(k,p)=1$.

EXAMPLE 3.1. For $p = 3$ and $k = 2$ we have

$$HJ_{n+4}(2,3) =$$

$$2HJ_{n+3}(2,3) - HJ_{n+2}(2,3) + HJ_{n+1}(2,3) - 2HJ_n(2,3), \quad n \geq 0, \quad (5)$$

so the sequence is

$$\{HJ_{n+4}(2,3)\}_0^\infty = \{0,0,0,1,2,3,5,7,8,8,5,-4,-21,\cdots\}.$$

From (4),

$$\begin{bmatrix} HJ_{n+p+1}(k,p) \\ HJ_{n+p}(k,p) \\ \vdots \\ HJ_{n+2}(k,p) \\ HJ_{n+1}(k,p) \end{bmatrix} = \begin{bmatrix} 2 & 0 & \cdots & 0 & -1 & k+1 & -k \\ 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} HJ_{n+p}(k,p) \\ HJ_{n+p-1}(k,p) \\ \vdots \\ HJ_{n+1}(k,p) \\ HJ_n(k,p) \end{bmatrix}.$$

LEMMA 3.1. *For $p = 3$, $k = 2$, and $n \geq 4$ we have*

$$(\omega_3(2))^n = \begin{bmatrix} HJ_{n+3}(2,3) & -2HJ_{n+3}(2,3) + HJ_{n+4}(2,3) \\ HJ_{n+2}(2,3) & -2HJ_{n+2}(2,3) + HJ_{n+3}(2,3) \\ HJ_{n+1}(2,3) & -2HJ_{n+1}(2,3) + HJ_{n+2}(2,3) \\ HJ_n(2,3) & -2HJ_n(2,3) + HJ_{n+1}(2,3) \end{bmatrix}$$

$$\begin{bmatrix} -2HJ_{n+1}(2,3) + HJ_{n+2}(2,3) & -2HJ_{n+2}(2,3) \\ -2HJ_n(2,3) + HJ_{n+1}(2,3) & -2HJ_{n+1}(2,3) \\ -2HJ_{n-1}(2,3) + HJ_n(2,3) & -2HJ_n(2,3) \\ -2HJ_{n-2}(2,3) + HJ_{n-1}(2,3) & -2HJ_{n-1}(2,3) \end{bmatrix}$$

*where*

$$\omega_3(2) = \begin{bmatrix} 2 & -1 & 1 & -2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \quad (6)$$

P r o o f. The proof is by induction on $n$. For $p = 3$, $k = 2$, and $n = 4$ we have

$$(\omega_3(2))^4 = \begin{bmatrix} 7 & -6 & -1 & -10 \\ 5 & -3 & -1 & -6 \\ 3 & -1 & 0 & -4 \\ 2 & -1 & 1 & -2 \end{bmatrix}$$

$$= \begin{bmatrix} HJ_7(2,3) & -2HJ_7(2,3) + HJ_8(2,3) \\ HJ_6(2,3) & -2HJ_6(2,3) + HJ_7(2,3) \\ HJ_5(2,3) & -2HJ_5(2,3) + HJ_6(2,3) \\ HJ_4(2,3) & -2HJ_4(2,3) + HJ_5(2,3) \end{bmatrix}$$

$$\begin{bmatrix} -2HJ_5(2,3) + HJ_6(2,3) & -2HJ_6(2,3) \\ -2HJ_4(2,3) + HJ_5(2,3) & -2HJ_5(2,3) \\ -2HJ_3(2,3) + HJ_4(2,3) & -2HJ_4(2,3) \\ -2HJ_2(2,3) + HJ_3(2,3) & -2HJ_3(2,3) \end{bmatrix}.$$

Assume the statement holds for $n = t$. Then for $n = t + 1$

$$(\omega_3(2))^{t+1} = \begin{bmatrix} 2 & -1 & 1 & -2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\times \begin{bmatrix} HJ_{t+3}(2,3) & -2HJ_{t+3}(2,3) + HJ_{t+4}(2,3) \\ HJ_{t+2}(2,3) & -2HJ_{t+2}(2,3) + HJ_{t+3}(2,3)) \\ HJ_{t+1}(2,3) & -2HJ_{t+1}(2,3) + HJ_{t+2}(2,3) \\ HJ_t(2,3) & -2HJ_t(2,3) + HJ_{t+1}(2,3) \end{bmatrix}$$

$$\begin{bmatrix} -2HJ_{t+1}(2,3) + HJ_{t+2}(2,3) & -2HJ_{t+2}(2,3) \\ -2HJ_t(2,3) + HJ_{t+1}(2,3) & -2HJ_{t+1}(2,3) \\ -2HJ_{t-1}(2,3) + HJ_t(2,3) & -2HJ_t(2,3) \\ -2HJ_{t-2}(2,3) + HJ_{t-1}(2,3) & -2HJ_{t-1}(2,3) \end{bmatrix}$$

$$= \begin{bmatrix} HJ_{t+4}(2,3) & -2HJ_{t+4}(2,3) + HJ_{t+5}(2,3) \\ HJ_{t+3}(2,3) & -2HJ_{t+3}(2,3) + HJ_{t+4}(2,3)) \\ HJ_{t+2}(2,3) & -2HJ_{t+2}(2,3) + HJ_{t+3}(2,3) \\ HJ_{t+1}(2,3) & -2HJ_{t+1}(2,3) + HJ_{t+2}(2,3) \end{bmatrix}$$

$$\begin{bmatrix} -2HJ_{t+2}(2,3) + HJ_{t+3}(2,3) & -2HJ_{t+3}(2,3) \\ -2HJ_{t+1}(2,3) + HJ_{t+2}(2,3) & -2HJ_{t+2}(2,3) \\ -2HJ_t(2,3) + HJ_{t+1}(2,3) & -2HJ_{t+1}(2,3) \\ -2HJ_{t-1}(2,3) + HJ_t(2,3) & -2HJ_t(2,3) \end{bmatrix}.$$

□

Using (6), we have $\omega_3(2) = -2$, so the determinant of $(\omega_3(2))^n$ is equal to $(-2)^n$. Let $\omega_p(2) = [m_{i,j}]_{(p+1)\times(p+1)}$ be the companion matrix for the Hadamard-type generalized Jacobsthal-Pell $(2,p)-$sequences. It can be readily established by induction on $n$ that for $p \geq 4$ and $n \geq p+1$

$$(\omega_p(2))^n = \begin{bmatrix} HJ_{n+p}(2,p) & -2HJ_{n+p}(2,p) + HJ_{n+p+1}(2,p) \\ HJ_{n+p-1}(2,p) & -2HJ_{n+p-1}(2,p) + HJ_{n+p}(2,p) \\ \vdots & \vdots \\ HJ_{n+1}(2,p) & -2HJ_{n+1}(2,p) + HJ_{n+2}(2,p) \\ HJ_n(2,p) & -2HJ_n(2,p) + HJ_{n+1}(2,p) \end{bmatrix}$$

$$\begin{matrix} -2HJ_{n+p+1}(2,p) + HJ_{n+p+2}(2,p) & \cdots \\ -2HJ_{n+p}(2,p) + HJ_{n+p+1}(2,p) & \cdots \\ \vdots & \ddots \\ -2HJ_{n+2}(2,p) + HJ_{n+3}(2,p) & \cdots \\ -2HJ_{n+1}(2,p) + HJ_{n+2}(2,p) & \cdots \end{matrix}$$

$$\begin{matrix} -2HJ_{2n+p-4}(2,p) + HJ_{2n+p-3}(2,p) \\ -2HJ_{2n+p-5}(2,p) + HJ_{2n+p-4}(2,p) \\ \vdots \\ -2HJ_{n+p-2}(2,p) + HJ_{n+p-1}(2,p) \\ -2HJ_{n+p-3}(2,p) + HJ_{n+p-2}(2,p) \end{matrix}$$

$$\begin{matrix} -2HJ_{n+p-2}(2,p) + HJ_{n+p-1}(2,p) & -2HJ_{n+p-1}(2,p) \\ -2HJ_{n+p-3}(2,p) + HJ_{n+p-2}(2,p) & -2HJ_{n+p-2}(2,p) \\ \vdots & \vdots \\ -2HJ_{n-1}(2,p) + HJ_n(2,p) & -2HJ_n(2,p) \\ -2HJ_{n-2}(2,p) + HJ_{n-1}(2,p) & -2HJ_{n-1}(2,p) \end{matrix} \Bigg] .$$

LEMMA 3.2. *Let $g(x)$ be the generating function of the Hadamard-type generalized Jacobsthal-Pell $(2,p)-$sequences. Then*

$$g(x) = \frac{x^p}{1 - 2x + x^{p-1} - (k-1)x^p + kx^{p+1}} . \tag{7}$$

P r o o f. We have

$$
\begin{aligned}
g(x) &= \sum_{n=1}^{\infty} HJ_{n+p+1}(k,p)x^n \\
&= 2HJ_{n+p}(k,p) - HJ_{n+2}(k,p) + (k-1)HJ_{n+1}(k,p) - kHJ_n(k,p) \\
&= x^p + \sum_{n=p+1}^{\infty} 2HJ_{n+p}(k,p) - HJ_{n+2}(k,p) + (k-1)HJ_{n+1}(k,p) - kHJ_n(k,p)x^n \\
&= x^p + \sum_{n=p+1}^{\infty} 2HJ_{n+p}(k,p) - \sum_{n=p+1}^{\infty} HJ_{n+2}(k,p) + \sum_{n=p+1}^{\infty} (k-1)HJ_{n+1}(k,p) \\
&\quad - \sum_{n=p+1}^{\infty} kHJ_n(k,p)x^n \\
&= x^p + 2x\sum_{n=1}^{\infty} HJ_{n+p}(k,p) - x^{p-1}\sum_{n=1}^{\infty} HJ_{n+2}(k,p) + (k-1)x^p\sum_{n=1}^{\infty} HJ_{n+1}(k,p) \\
&\quad - kx^{p+1}\sum_{n=1}^{\infty} HJ_n(k,p)x^n \\
&= x^p + 2xg(x) - x^{p-1}g(x) + (k-1)x^p g(x) - kx^{p+1}g(x).
\end{aligned}
$$

□

Theorem 3.1. *The Hadamard-type generalized Jacobsthal-Pell $(2,p)-$sequences $\{HJ_n(k,p)\}$ have the following exponential representation*

$$g(x) = x^p \exp\sum_{i=1}^{\infty} \frac{(x)^i}{i}(2 - x^{p-2} + (k-1)x^{p-1} - kx^p)^i,$$

*where $p \geq 5$.*

P r o o f. Using (6), we have

$$\ln g(x) = \ln x^p - \ln(1 - 2x + x^{p-1} - (k-1)x^p + kx^{p+1}),$$

and since

$$\begin{aligned}
&-\ln\left(1-2x+x^{p-1}-(k-1)x^p+kx^{p+1}\right)\\
&=-[-x(2-x^{p-2}+(k-1)x^{p-1}-kx^p)\\
&-\frac{1}{2}x^2(2-x^{p-2}+(k-1)x^{p-1}-kx^p)^2\\
&-\cdots-\frac{1}{i}x^i(2-x^{p-2}+(k-1)x^{p-1}-kx^p)^i-\cdots]\\
&=\sum_{i=1}^{\infty}\frac{(x)^i}{i}(2-x^{p-2}+(k-1)x^{p-1}-kx^p)^i,
\end{aligned}$$

the result follows. □

The following lemma can easily be proven by induction on $s$.

LEMMA 3.3. *For $s, p \in \mathbb{N}$, and $n \geq p+1$ we have*

$$(\omega_p(3))^n(\omega_p(3))^s = (\omega_p(3))^{n+s}(= \omega_p(3))^s(\omega_p(3))^n.$$

## 4. An RSA cryptosystem using the generalized Jacobsthal sequences and generalized Pell numbers

In this section, we introduce two RSA algorithms using the generalized Jacobsthal-Pell $(k,p)-$sequences and Hadamard-type generalized Jacobsthal-Pell $(k,p)-$sequences. Then the security of these algorithms is examined.

First, for $p \geq 3$ and $m \geq 2$ we give an RSA algorithm using the generalized Jacobsthal-Pell $(3,p)-$sequences. Alice and Bob agree on a public key $((\Gamma_p(3)), m)$ and a secret key $d := (\Gamma_p(3))^{-n}$, $n$ a positive integer. Alice chooses $(\Gamma_p(3))^n$ and computes $C = M \times (\Gamma_p(3))^n \equiv C \pmod{m}$ where $M = (\Gamma_p(3))^i$, $i \geq 3$, is the plaintext, and sends this to Bob. He uses the secret key $d$ to obtain $C \times (\Gamma_p(3))^{-n} \equiv M \pmod{m}$. The algorithm steps are given below and illustrated in Fig. 1.

**Algorithm 1**

(1) Alice and Bob agree on a public key $((\Gamma_p(3)), m)$ and secret key $d := (\Gamma_p(3))^{-n}$, $n$ a positive integer.

(2) Using $(\Gamma_p(3))^n$ with the plaintext $M = (\Gamma_p(3))^i \pmod m$, Alice calculates $C = M \times (\Gamma_p(3))^n \equiv C \pmod m$ and sends this to Bob.

(3) Bob uses the secret key $d$ to obtain $C \times (\Gamma_p(3))^{-n} \equiv M \pmod m$.

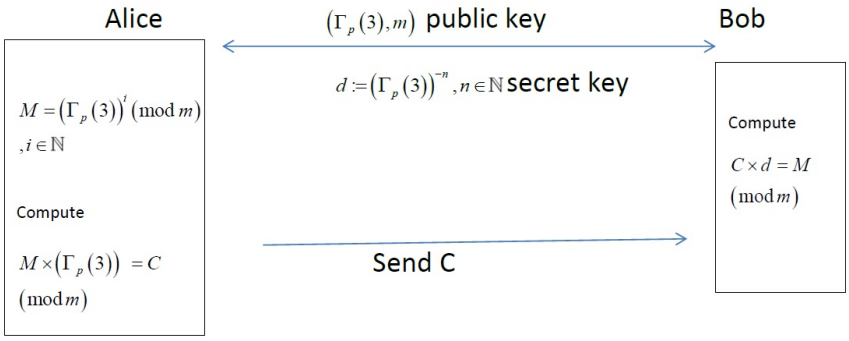


FIGURE 1. Algorithm 1

LEMMA 4.1. *The message $M$ is obtained by Bob after decrypting the ciphertext $C$.*

P r o o f. We have that $C \times d \equiv M \pmod m$ so

$$C \equiv M \times (\Gamma_p(3))^n \pmod m.$$

From Theorem 11

$$C \times (\Gamma_p(3))^{-n} = (\Gamma_p(3))^{i+n} \times (\Gamma_p(3))^{-n} = (\Gamma_p(3))^i \pmod m.$$

□

EXAMPLE 4.1. Alice and Bob agree on a public key $((\Gamma_3(3)), 5)$ and a secret key $d := (\Gamma_3(3))^{-6}$. Using $(\Gamma_3(3))^n$ with the plaintext

$$M = (\Gamma_3(3))^8 = \begin{bmatrix} 1471 & -14310 & -29048 & 160 & -14454 & -14562 \\ 4854 & -4625 & -9456 & 76 & -4694 & -4746 \\ 1582 & -1474 & -3043 & 36 & -1506 & -1530 \\ 510 & -458 & -964 & 17 & -474 & -486 \\ 162 & -138 & -296 & 8 & -145 & -150 \\ 50 & -38 & -88 & 4 & -42 & -45 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 2 & 0 & 1 & 3 \\ 4 & 0 & 4 & 1 & 1 & 4 \\ 2 & 1 & 2 & 1 & 4 & 0 \\ 0 & 2 & 1 & 2 & 4 & 4 \\ 2 & 2 & 4 & 3 & 0 & 0 \\ 0 & 2 & 2 & 4 & 3 & 0 \end{bmatrix} \pmod 5,$$

Alice calculates

$$C = (\Gamma_3(3))^8 \times (\Gamma_3(3))^6$$

$$= \begin{bmatrix} 1 & 0 & 2 & 0 & 1 & 3 \\ 4 & 0 & 4 & 1 & 1 & 4 \\ 2 & 1 & 2 & 1 & 4 & 0 \\ 0 & 2 & 1 & 2 & 4 & 4 \\ 2 & 2 & 4 & 3 & 0 & 0 \\ 0 & 2 & 2 & 4 & 3 & 0 \end{bmatrix} \times \begin{bmatrix} 1582 & -1474 & -3043 & 36 & -1506 & -1530 \\ 510 & -458 & -964 & 17 & -474 & -486 \\ 162 & -138 & -296 & 8 & -145 & -150 \\ 50 & -38 & -88 & 4 & -42 & -45 \\ 15 & -10 & -23 & 2 & -11 & -12 \\ 4 & -1 & -6 & 1 & -2 & -3 \end{bmatrix}$$

$$= \begin{bmatrix} 3 & 2 & 4 & 2 & 2 & 4 \\ 2 & 0 & 4 & 1 & 0 & 1 \\ 3 & 0 & 3 & 2 & 2 & 1 \\ 3 & 1 & 3 & 1 & 4 & 4 \\ 2 & 0 & 3 & 0 & 4 & 3 \\ 4 & 4 & 4 & 2 & 1 & 2 \end{bmatrix} \pmod 5,$$

and sends this to Bob. Bob uses the secret key $d$ to obtain

$$C \times d = \begin{bmatrix} 3 & 2 & 4 & 2 & 2 & 4 \\ 2 & 0 & 4 & 1 & 0 & 1 \\ 3 & 0 & 3 & 2 & 2 & 1 \\ 3 & 1 & 3 & 1 & 4 & 4 \\ 2 & 0 & 3 & 0 & 4 & 3 \\ 4 & 4 & 4 & 2 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} 1582 & -1474 & -3043 & 36 & -1506 & -1530 \\ 510 & -458 & -964 & 17 & -474 & -486 \\ 162 & -138 & -296 & 8 & -145 & -150 \\ 50 & -38 & -88 & 4 & -42 & -45 \\ 15 & -10 & -23 & 2 & -11 & -12 \\ 4 & -1 & -6 & 1 & -2 & -3 \end{bmatrix}^{-6}$$

$$= \begin{bmatrix} 1 & 0 & 2 & 0 & 1 & 3 \\ 4 & 0 & 4 & 1 & 1 & 4 \\ 2 & 1 & 2 & 1 & 4 & 0 \\ 0 & 2 & 1 & 2 & 4 & 4 \\ 2 & 2 & 4 & 3 & 0 & 0 \\ 0 & 2 & 2 & 4 & 3 & 0 \end{bmatrix} \pmod 5.$$

The Hadamard-type generalized Jacobsthal-Pell $(2,p)-$sequences are now used in an RSA algorithm. Alice and Bob agree on a public key $((\omega_p(2)), m)$ and a secret key $d := (\omega_p(2))^{-n}$, $n$ a positive integer. Alice chooses $(\omega_p(2))^n$ and computes $C = M \times (\omega_p(2))^n \equiv C \pmod m$ where $M = (\omega_p(2))^i$, $i \geq 3$, is the plaintext, and sends this to Bob. He uses the secret key $d$ to obtain $C \times (\omega_p(2))^{-n} \equiv M \pmod m$. The algorithm steps are given below and illustrated in Fig. 2.

**Algorithm 2**

(1) Alice and Bob agree on a public key $((\omega_p(2)), m)$ and secret key $d := (\omega_p(2))^{-n}$, $n$ a positive integer.
(2) Using $(\omega_p(2))^n$ with the plaintext $M = (\omega_p(2))^i \pmod m$, Alice calculates $C = M \times (\omega_p(2))^n \equiv C \pmod m$ and sends this to Bob.
(3) Bob uses the secret key $d$ to obtain $C \times (\omega_p(2))^{-n} \equiv M \pmod m$.

LEMMA 4.2. *In Algorithm 2, the message $M$ is obtained by Bob after decrypting the ciphertext $C$.*

P r o o f. The proof is similar to that of Lemma 4.1 and so is omitted. □

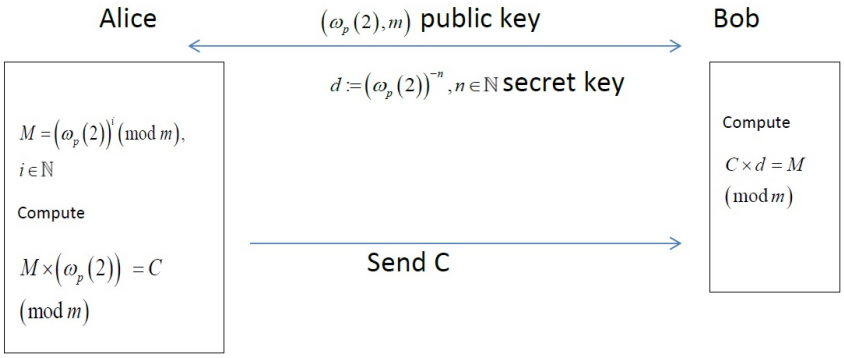


FIGURE 2. Algorithm 2

EXAMPLE 4.2. Alice and Bob agree on a public key $((\omega_3(2), 5)$ and a secret key $d := ((\omega_3(2))^{-7}$. Using $((\omega_3(2))^7$ and the plaintext $M$

$$M = ((\omega_3(2))^3 = \begin{bmatrix} 5 & -3 & -1 & -6 \\ 3 & -1 & 0 & -4 \\ 2 & -1 & 1 & -2 \\ 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 2 & 4 & 4 \\ 3 & 4 & 0 & 1 \\ 2 & 4 & 1 & 3 \\ 1 & 0 & 0 & 0 \end{bmatrix} \pmod 5,$$

Alice calculates

$$C = (\omega_3(2)^3 \times (\omega_3(2)^7 = \begin{bmatrix} 0 & 2 & 4 & 4 \\ 3 & 4 & 0 & 1 \\ 2 & 4 & 1 & 3 \\ 1 & 0 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 4 & -14 & -8 & -16 \\ 8 & -11 & -6 & -16 \\ 8 & -8 & -3 & -14 \\ 7 & -6 & -1 & -10 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 7 & 2 & 2 \\ 4 & 2 & 1 & 3 \\ 1 & 2 & 4 & 0 \\ 0 & 1 & 2 & 4 \end{bmatrix} \pmod 5,$$

and sends this to Bob. Bob uses the secret key $d$ to obtain

$$C \times d = \begin{bmatrix} 1 & 7 & 2 & 2 \\ 4 & 2 & 1 & 3 \\ 1 & 2 & 4 & 0 \\ 0 & 1 & 2 & 4 \end{bmatrix} \times \begin{bmatrix} 4 & -14 & -8 & -16 \\ 8 & -11 & -6 & -16 \\ 8 & -8 & -3 & -14 \\ 7 & -6 & -1 & -10 \end{bmatrix}^{-7}$$

$$= \begin{bmatrix} 0 & 2 & 4 & 4 \\ 3 & 4 & 0 & 1 \\ 2 & 4 & 1 & 3 \\ 1 & 0 & 0 & 0 \end{bmatrix} \pmod 5.$$

4.1. **Security analysis.** We now consider attacks on the proposed cryptosystem and compare it with the original RSA algorithm. Attacks on the RSA algorithm include:

(1) known plaintext attacks
(2) chosen ciphertext attacks
(3) factorization attacks
(4) encryption key attacks
(5) decryption key attacks.

Since Algorithms 1 and 2 use large matrices, a brute force attack is considered as in [5, 24]. In this attack, all possible matrices should be considered. In Algorithms 1 and 2, $(\Gamma_p(2))$ and $(\omega_p(3))$ are employed, respectively. The general linear group $GL_\lambda(F_q)$, $q$ prime, consists of all invertible matrices of order $\lambda \times \lambda$ over $F_q$ [10]. Since the matrices used to create the keys are invertible, the number of keys is equal to the order of the general linear group

$$\mid GL_\lambda(F_q) \mid = (q^\lambda - q^{\lambda-1})(q^\lambda - q^{\lambda-2}) \cdots (q^\lambda - 1).$$

For $\lambda$ a large number and $q$ a very large prime, the number of keys is extremely large.

Example 4.3. Consider $(\Gamma_p(2))$. Since $(\Gamma_p(2))$ is a $(p+3) \times (p+3)$ matrix, there are

$$\mid GL_{p+3}(F_m) \mid = (m^{p+3} - m^{p+2})(m^{p+3} - m^{p+1}) \cdots (m^{p+3} - m)(m^{p+3} - 1), \tag{8}$$

matrices.

(i) If $p = 3$ and $m = 5$, the number of keys is

$$| GL_3(F_5) | = (5^6-5^5)(5^6-5^4)(5^6-5^3)(5^6-5^2)(5^6-5)(5^6-1) = 2.26\times10^{17}.$$

(ii) If $p = 47$ and $m = 37$, the number of keys is

$$| GL_{50}(F_{37}) | = (37^{50}-37^{49})(37^{50}-37^{48})\cdots(37^{50}-37)(37^{50}-1) = 3.1\times10^{3920}.$$

EXAMPLE 4.4. For Algorithm 2, the number of keys using $(\omega_p(3))$ is

$$| GL_{p+1}(F_m) | = (m^{p+1}-m^p)(m^{p+1}-m^{p-1})\cdots(m^{p+1}-m)(m^{p+1}-1). \quad (9)$$

(i) If $p = 2$ and $m = 3$, we have

$$| GL_3(F_3) | = (3^3 - 3^2)(3^3 - 3)(3^3 - 1) = 11232.$$

(ii) if $p = 49$ and $m = 37$, we have

$$| GL_{50}(F_{37}) | = (37^{50}-37^{49})(37^{50}-37^{48})\cdots(37^{50}-37)(37^{50}-1) = 3.1\times10^{3920}.$$

If $m$ is a very large prime number and $p$ is a large integer, the number of keys makes it intractable for an attacker to consider all possible keys. Thus, this algorithm has higher security compared to the original RSA algorithm.

Consider the following attacks.

1. Side channel attack: In a side channel attack, the cryptographic system is broken using information that is accidentally leaked or maliciously obtained. In the proposed algorithm, the public key is a matrix with very large size and $m$ is a very large prime number. Thus, it would be very time consuming and unlikely to provide complete information, and so is not feasible.
2. Timing attack: This is a type of side channel attack in which the attacker tries to compromise the cryptographic system by analyzing the time taken to execute the algorithm. Because the keys in the proposed algorithm are in the form of a matrix and multiplication is employed, accessing the system and obtaining the required information will be very time-consuming and prone to errors, so this is not a useful attack.
3. Chosen ciphertext attack: A chosen ciphertext attack is an attack where the attacker gathers information by obtaining decryptions of chosen encryptions. As with the others, this attack will be very time consuming as significant data is required, thus it is infeasible.

4. Fault attack: In this approach, the attacker intentionally introduces faults or errors into the cryptographic system to exploit vulnerabilities and extract information. Considering that the keys are very large, the calculations will likely be done on very powerful computer systems. Thus, accessing and damaging these systems is not viable.

## 5. Conclusion

We introduced two new sequences from the generalized Pell $(p, i)-$numbers and generalized Jacobsthal numbers. Matrices were obtained from these sequences and they were used to develop RSA algorithms. This is the first application of these sequences in a cryptosystem. The RSA algorithms were explained with examples, and they were shown to have high security. These algorithms can be implemented with other sequences such as Fibonacci and Pell like sequences and their generalizations that have simple periodicity [14, 20, 21].

## References

[1] A. Agarwal, S. Agarwal, B. K. Singh, Algorithm for data encryption & decryption using Fibonacci prime, *J. Math. Control Sci. Appl.*, **6**, No 1 (2020), 63-71.

[2] Y. Aküzüm, Ö. Deveci, The Hadamard-type $k$-step Fibonacci sequences in groups, *Commun. Algebra*, **48**, No 7 (2020), 2844-2856.

[3] D. Brod, A. Michalski, On generalized Jacobsthal and Jacobsthal-Lucas numbers, *Ann. Math. Sil.*, **36**, No 2 (2022), 115-128.

[4] C. Y. Chen, C. Y. Ku, D. C. Yen, Cryptanalysis of short secret exponents modulo RSA primes, *Inf. Sci.*, **160**, (2004), 225-233.

[5] J. S. Cho, S. S. Yeo, S. K. Kim, Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value, *Comput. Commun.*, **34**, No 3 (2011), 391-397.

[6] A. Chmielowiec, Fixed points of the RSA encryption algorithm, *Theor. Comput. Sci.*, **411**, No 1 (2010), 288-292.

[7] Ö. Deveci, E. Karaduman, The Pell sequences in finite groups, *Util. Math.*, **96** (2015), 263-279.

[8] Ö. Deveci, A. Shannon, The quaternion-Pell sequence, *Commun. Algebra*, **46**, No 12 (2018), 5403-5409

[9] S. Falcon, On the $k-$Jacobsthal numbers, *Amer. Rev. Math. Stat.*, **2**, No 1 (2014), 67-77.

[10] P. A. Grillet, *Abstract Algebra*, 2nd Ed., Graduate Texts in Mathematics, **242**, (2007), Springer, Berlin.
[11] L. Harn, J. Renb, Efficient identity-based RSA multisignatures, *Comput. Secur.*, **27**, No 1-2 (2008), 12-15.
[12] M. Hashemi, E. Mehraban, On the generalized order 2-Pell sequence of some classes of groups, *Commun. Algebra*, **46**, No 9 (2018), 4104-4119.
[13] M. Hashemi, E. Mehraban, Fibonacci length and the generalized order $k-$Pell sequences of the 2-generator $p-$groups of nilpotency class 2, *J. Algebra Appl.*, **22**, No 3 (2023), 2350061.
[14] M. Hashemi, E. Mehraban, Some new codes on the $k-$Fibonacci sequence, *Math. Probl. Eng.*, **2021** (2021), 7660902.
[15] A. F. Horadam, Jacobsthal and Pell curves, *Fibonacci Q.*, **26**, No 1 (1988), 79-83.
[16] E. Jochemsz, Cryptanalysis of RSA variants using small roots of polynomials, *Ph.D. Thesis*, Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, Eindhoven, The Netherlands (2007).
[17] E. Jochemsz, A. May, A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants, in: X. Lai and K. Chen (Eds.), *Advances in Cryptology - Asiacrypt 2006*, Lecture Notes in Computer Science, **4284**, (2006), 267-282, Springer, Berlin.
[18] M. Kaminaga, T. Watanabe, T. Endo, T. Okochi, Power analysis and countermeasure of RSA cryptosystem, *Electron. Commun. Jpn. 3*, **89**, No 8, (2006), 10-20.
[19] E. Kiliç, The generalized Pell $(p, i)-$numbers and their Binet formulas, combinatorial representations, sums, *Chaos Solit. Fractals*, **40**, No 4 (2009), 2047-2063.
[20] E. Mehraban, M. Hashemi, Coding theory on the generalized balancing sequence, *Notes Numb. Thy. Disc. Math.*, **29**, No 3 (2023), 503-524.
[21] E. Mehraban, T. A. Gulliver, S. M. Boulaaras, K. Hosseini, E. Hinçal, New sequences from the generalized Pell $p-$numbers and Mersenne numbers and their application in cryptography, *AIMS Math.*, **9**, No 5 (2024), 13537-13552.
[22] M. Mishra, A. R. Routray, S. Kumar, High security image steganography with modified Arnold's cat map, *Int. J. Comput. Appl.*, **37**, No 9 (2012), 16-20.

[23] K. Prasad, H. Mahato, Cryptography using generalized Fibonacci matrices with Affine-Hill cipher, *J. Disc. Math. Sci. Cryptogr.*, **25**, No 8 (2022), 2341-2352.

[24] S. Yu, K. Ren, W. Lou, A privacy-preserving lightweight authentication protocol for low-cost RFID tags, in: *Proc. IEEE MILCOM*, Orlando, FL (2007).

[25] R. L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Commun. ACM*, **21**, No 2 (1978), 120-126.

[26] K. Satake, M. Kasahara, Fast RSA-type cryptosystem with public data of small size, *Electron. Commun. Jpn. 3*, **80**, No 2 (1997), 24-34.

[27] Ş. Uygun, H. Eldogan, Properties of $k-$Jacobsthal and $k-$Jacobsthal Lucas sequences, *Gen. Math. Notes*, **36**, No 1 (2016), 34-47.