J. COMBIN. MATH. COMBIN. COMPUT. 124 (2025) 47–58

Journal of Combinatorial Mathematics
and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Combinatorial Press

Affine-Hill cipher key generation using self-invertible matrices from $k-$division $L-$Lehmer-Pell sequences

Elahe Mehraban[1,2,3,✉], T. Aaron Gulliver[4], Ömür Deveci[5], Evren Hincal[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*
[4] *Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC, V8W 2Y2, Canada*
[5] *Department of Mathematics, Faculty of Science and Letters Kafkas University, 36100, Turkey*

ABSTRACT

This paper presents a new sequence called the $k-$division sequence. The Pell and Lehmer sequences are then used to define new sequences called the $k-$division $L-$Lehmer-Pell sequences and some properties of these sequences are determined. Then the $k-$division $L-$Lehmer-Pell sequences and corresponding self-invertible matrices are used in a new Affine-Hill cipher algorithm. The security of this cipher is examined.

Keywords: Lehmer sequence, Pell sequence, Affine-Hill cipher, self-invertible matrix

1. Introduction

Definition 1.1. For integers L, M, and $LM \neq 0$, $L-4M \neq 0$, the Lehmer sequence $\{U_n(L,M)\}_{n=0}^{\infty}$ is

$$U_n(L,M) = \begin{cases} LU_{n-1}(L,M) - MU_{n-2}(L,M) & n \text{ odd}, \\ UF_{n-1}(L,M) - MU_{n-2}(L,M) & n \text{ even}, \end{cases}$$

where $U_0(L,M) = 0$ and $U_1(L,M) = 1$ [13].

The Lehmer sequence in finite groups was introduced in [3] and the period was studied. In [2], perfect powers in sequences were derived by shifting non-degenerate quadratic Lucas-Lehmer binary sequences by a fixed integer. The Lehmer sequences and Lehmer orbits of groups were considered in [17] to obtain a new RSA algorithm.

✉ Corresponding author.
E-mail address: e.mehraban.math@gmail.com (E. Mehraban).

Received 31 January 2025; Accepted 23 February 2025; Published Online 16 March 2025.

DOI: 10.61091/jcmcc124-03

The Pell sequence $\{P_n\}_{n=0}^{\infty}$ is defined as

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

with initial conditions $P_0 = 0$ and $P_1 = 1$. The Pell sequence and its generalizations have been investigated extensively [12, 6, 15, 4, 11]. In [9], the $k-$nacci sequences were introduced and the generalized order $k-$Pell sequences in the semi-direct product of finite cyclic groups were given. The generalized order 2-Pell sequences of some classes of groups were also presented. In [16], new sequences were obtained from the generalized Pell $p-$numbers and Mersenne numbers. They were used in algorithms for Diffie-Hellman key exchange.

The characteristic polynomials of the Pell and Lehmer sequences are $x^2 - 2x - 1$ and

$$\begin{cases} x^2 - Lx + M & n \text{ odd}, \\ x^2 - x + M & n \text{ even}, \end{cases}$$

respectively.

Definition 1.2. A matrix M is called self-invertible matrix if $M = M^{-1}$ [1].

The Hill cipher was introduced in [10] and the Affine cipher was defined in [21]. Public key cryptography using the Hill cipher was considered in [22]. In [19], a key matrix of order 3 that reflects a line $y = ax + b$ was used to overcome the noninvertible matrix problem in the Affine-Hill cipher modulo a prime number. The following encryption and decryption algorithms were also given. Encryption is

$$C_i \equiv P_i K + B \pmod{p},$$

and decryption is

$$P_i \equiv (C_i - B)K^{-1} \pmod{p},$$

where K is an $n \times n$ key matrix, and P_i, C_i, and B are $1 \times n$ matrices over Z_p, p a prime [18].

Here, the Pell and Lehmer sequences are used to define new sequences called the $k-$division $L-$Lehmer-Pell sequences. Some properties of these sequences are obtained. Then the $k-$division $L-$Lehmer-Pell sequences and corresponding self-invertible matrices are employed to propose a new Affine-Hill cipher algorithm. The security of this algorithm is also discussed.

The remainder of this paper is organized as follows. Section 2 introduces a new method for constructing sequences called $k-$division. Then the $k-$division $L-$Lehmer-Pell sequences are defined and some results are given. Section 3 presents a new Affine-Hill cipher algorithm and its security is examined. Finally, some concluding remarks are given in Section 4.

2. The $k-$division $L-$Lehmer-Pell sequences

In this section, we present a new method for constructing sequences called $k-$division. Then the $k-$division $L-$Lehmer-Pell sequences are defined.

Definition 2.1. Let $f(x)$ and $g(x)$ be the characteristic polynomials of two sequences of degree u and m, respectively, where $m \geq u$. For $k \in \mathbb{N}$, the $k-$division sequence, $\{h_n(k)\}_{n=0}^{\infty}$, is

$$h_n(k) = x^k(g(x)) + t(x), n \geq k + m. \tag{1}$$

where $t(x)$ is the remainder of $\dfrac{x^k(g(x))}{f(x)}$, and the initial conditions are $h_0(k) = h_1(k) = \cdots = h_{m+k-2}(k) = 0, h_{m+k-1}(k) = 1$.

Let

$$g(x) = \begin{cases} x^2 - Lx + M & n \text{ odd}, \\ x^2 - x + M & n \text{ even}, \end{cases}$$

and $f(x) = x^2 - 2x - 1$, and consider $M = -1$ in the remainder of the paper. By Definition 2.1, the following new sequences are obtained.

Definition 2.2. For $M = -1$, the $1-$division $3-$Lehmer-Pell sequences, denoted by $\{hL_n(k, L)\}_{n=0}^{\infty}$, are

$$hL_n(1,3) = \begin{cases} 3hL_{n-1}(1,3) + 3hL_{n-2}(1,3) + hL_{n-3}(1,3) & n \text{ odd}, \\ hL_{n-1}(1,3) + hL_{n-2}(1,3) + hL_{n-3}(1,3) & n \text{ even}, \end{cases}$$

where $hL_0(1,3) = hL_1(1,3) = 0$ and $hL_2(1,3) = 1$.

Thus, we have $\{hL_n(1,3)\}_{n=0}^{\infty} = \{0, 0, 1, 3, 2, 16, 11, 83, 56, 428, 2289, \cdots, \}$.
We have the following $k-$division $3-$Lehmer-Pell sequences.
(i) The $2-$division $3-$Lehmer-Pell sequence, denoted by $\{hL_n(2,3)\}_{n=0}^{\infty}$, is

$$hL_n(2,3) = \begin{cases} 3hL_{n-1}(2,3) + hL_{n-2}(2,3) + 5hL_{n-3}(2,3) + 2hL_{n-4}(2,3) & n \text{ odd}, \\ hL_{n-1}(2,3) + hL_{n-2}(2,3) - 5hL_{n-3}(2,3) - 2hL_{n-3}(2,3) & n \text{ even}, \end{cases}$$

with initial conditions $hL_0(2,3) = hL_1(2,3) = hL_2(2,3) = 0, hL_2(2,3) = 1$, so

$$\{hL_n(2,3)\}_{n=0}^{\infty} = \{0, 0, 0, 1, 1, 4, 0, 11, -11, -14, -80, -287, \cdots\}.$$

(ii) The $3-$division $3-$Lehmer-Pell sequence, denoted by $\{hL_n(3,3)\}_{n=0}^{\infty}$, is

$$hL_n(3,3) = \begin{cases} 3hL_{n-1}(3,3) + hL_{n-2}(3,3) + 12hL_{n-4}(3,3) + 5hL_{n-5}(3,3) & n \text{ odd}, \\ hL_{n-1}(3,3) + hL_{n-2}(3,3) - 12hL_{n-4}(3,3) - 5hL_{n-5}(3,3) & n \text{ even}, \end{cases}$$

with initial conditions $hL_0(3,3) = hL_1(3,3) = hL_2(3,3) = hL_3(3,3) = 0,\ hL_4(3,3) = 1$, so

$$\{hL_n(3,3)\}_{n=0}^{\infty} = \{0, 0, 0, 0, 1, 3, 4, 15, 7, 77, 21, 340, 202, 1905, 1407, \cdots\}.$$

(iii) The $4-$division $3-$Lehmer-Pell sequence, denoted by $\{hL_n(4,3)\}_{n=0}^{\infty}$, is

$$hL_n(4,3) = \begin{cases} 3hL_{n-1}(4,3) + hL_{n-2}(4,3) + 29hL_{n-5}(4,3) + 12hL_{n-6}(4,3) & n \text{ odd}, \\ hL_{n-1}(4,3) + hL_{n-2}(4,3) - 29hL_{n-5}(4,3) - 12hL_{n-6}(4,3) & n \text{ even}, \end{cases}$$

with initial conditions $hL_0(4,3) = hL_1(4,3) = hL_2(4,3) = hL_3(4,3) = hL_4(4,3) = 0, hL_5(4,3) = 1$, so

$$\{hL_n(4,3)\}_{n=0}^{\infty} = \{0, 0, 0, 0, 0, 1, 1, 4, 5, 19, -5, 45, -88, -26, -725, \cdots\}.$$

(iv) The $k-$division $3-$Lehmer-Pell sequences, denoted by $\{hL_n(k,3)\}_{n=0}^{\infty}$, are

$$hL_n(k,3) = \begin{cases} 3hL_{n-1}(k,3) + hL_{n-2}(k,3) + P_{k+1}hL_{n-k-1}(k,3) + P_khL_{n-k-2}(k,3) & n \text{ odd}, \\ hL_{n-1}(k,3) + hL_{n-2}(k,3) - P_{k+1}hL_{n-k-1}(k,3) - P_khL_{n-k-2}(k,3) & n \text{ even}, \end{cases}$$

with initial conditions $hL_0(k,3) = hL_1(k,3) = \cdots = hL_k(k,3) = 0, hL_{k+1}(k,3) = 1$.

Lemma 2.3. *For $k \geq 2$, let $g_{hL_n(k,3)}$ be the generating function of the $k-$division $3-$Lehmer-Pell sequences. Then*

$$g_{hL_n(k,3)} = \begin{cases} \dfrac{x^{k+1}}{1-3x-x^2-P_{k+1}x^{k+1}-P_kx^{k+2}} & n \text{ odd}, \\ \dfrac{x^{k+1}}{1-x-x^2+P_{k+1}x^{k+1}+P_kx^{k+2}} & n \text{ even}, \end{cases} \tag{2}$$

Proof. For $k \geq 2$, let $g_{hL_n(k,3)}$ be the generating function of the $k-$division $3-$Lehmer-Pell sequences. If n is odd, then

$$\begin{aligned} g_{hL_n(k,3)} &= \sum_{n=1}^{\infty} hL_n(k,3)x^n \\ &= hL_1(k,3)x + hL_2(k,3)x^2 + \cdots + hL_{k+1}(k,3)x^{k+1} + \sum_{n=k+2}^{\infty} hL_n(k,3)x^n \\ &= x^{k+1} + \sum_{n=k+2}^{\infty} (3hL_{n-1}(k,3) + hL_{n-2}(k,3) + P_{k+1}hL_{n-k-1}(k,3) + P_khL_{n-k-2}(k,3))x^n \\ &= x^{k+1} + 3\sum_{n=k+2}^{\infty} hL_{n-1}(k,3)x^n + \sum_{n=k+2}^{\infty} hL_{n-2}(k,3)x^n + P_{k+1}\sum_{n=k+2}^{\infty} hL_{n-k-1}(k,3)x^n \\ &\quad + P_k\sum_{n=k+2}^{\infty} h_{n-k-2}(k,3)x^n \\ &= x^{k+1} + 3x\sum_{n=1}^{\infty} hL_n(k,3)x^n + x^2\sum_{n=1}^{\infty} hL_n(k,3)x^n + P_{k+1}x^{k+1}\sum_{n=1}^{\infty} hL_n(k,3)x^n \\ &\quad + P_kx^{k+2}\sum_{n=1}^{\infty} hL_n(k,3)x^n \\ &= x^{k+1} + 3xg_{hL_n(k,3)} + x^2g_{hL_n(k,3)} + P_{k+1}x^{k+1}g_{hL_n(k,3)} + P_kx^{k+2}g_{hL_n(k,3)}, \end{aligned}$$

so

$$g_{hL_n(k,3)} = \frac{x^{k+1}}{1-3x-x^2-P_{k+1}x^{k+1}-P_kx^{k+2}}.$$

If n is even, then

$$\begin{aligned} g_{hL_n(k,3)} &= \sum_{n=1}^{\infty} hL_n(k,3)x^n \\ &= hL_1(k,3)x + hL_2(k,3)x^2 + \cdots + hL_{k+1}(k,3)x^{k+1} + \sum_{n=k+2}^{\infty} hL_n(k,3)x^n \\ &= x^{k+1} + \sum_{n=k+2}^{\infty} (hL_{n-1}(k,3) + hL_{n-2}(k,3) - P_{k+1}hL_{n-k-1}(k,3) - P_khL_{n-k-2}(k,3))x^n \\ &= x^{k+1} + \sum_{n=k+2}^{\infty} hL_{n-1}(k,3)x^n + \sum_{n=k+2}^{\infty} hL_{n-2}(k,3)x^n - P_{k+1}\sum_{n=k+2}^{\infty} hL_{n-k-1}(k,3)x^n \\ &\quad - P_k\sum_{n=k+2}^{\infty} h_{n-k-2}(k,3)x^n \end{aligned}$$

$$= x^{k+1} + x\sum_{n=1}^{\infty} hL_n(k,3)x^n + x^2\sum_{n=1}^{\infty} hL_n(k,3)x^n - P_{k+1}x^{k+1}\sum_{n=1}^{\infty} hL_n(k,3)x^n$$
$$- P_k x^{k+2}\sum_{n=1}^{\infty} hL_n(k,3)x^n$$
$$= x^{k+1} + xg_{hL_n(k,3)} + x^2 g_{hL_n(k,3)} - P_{k+1}x^{k+1}g_{hL_n(k,3)} - P_k x^{k+2}g_{hL_n(k,3)},$$

so

$$g_{hL_n(k,3)} = \frac{x^{k+1}}{1 - x - x^2 + P_{k+1}x^{k+1} + P_k x^{k+2}}.$$

□

Lemma 2.4. *For $k \geq 2$, the generating function of the $k-$division $3-$Lehmer-Pell sequences has exponential representation*

$$g_{hL_n(k,3)} = \begin{cases} x^{k+1}exp\sum_{i=1}^{\infty}\frac{x^i}{i}(3 + x + P_{k+1}x^k + P_k x^{k+1})^i & n \text{ odd}, \\ x^{k+1}exp\sum_{i=1}^{\infty}\frac{x^i}{i}(1 + x - P_{k+1}x^k - P_k x^{k+1})^i & n \text{ even}, \end{cases}$$

Proof. From Lemma 2.3, for n odd we have

$$\ln\frac{g_{hL_n(k,3)}}{x^{k+1}} = -\ln(1 - 3x - x^2 - P_{k+1}x^{k+1} - P_k x^{k+2}),$$

so then

$$-\ln(1 - 3x - x^2 - P_{k+1}x^{k+1} - P_k x^{k+2}) = -[-x(3 + x + P_{k+1}x^k + P_k x^{k+1})$$
$$-\frac{1}{2}x^2(3 + x + P_{k+1}x^k + P_k x^{k+1})^2 - \cdots - \frac{1}{i}x^i(3 + x + P_{k+1}x^k + P_k x^{k+1})^i - \cdots],$$

and for n even we have

$$\ln\frac{g_{hL_n(k,3)}}{x^{k+1}} = -\ln(1 - x - x^2 + P_{k+1}x^{k+1} + P_k x^{k+2}),$$

so then

$$-\ln(1 - x - x^2 + P_{k+1}x^{k+1} + P_k x^{k+2}) = -[-x(1 + x - P_{k+1}x^k - P_k x^{k+1})$$
$$-\frac{1}{2}x^2(1 + x - P_{k+1}x^k - P_k x^{k+1})^2 - \cdots - \frac{1}{i}x^i(1 + x - P_{k+1}x^k - P_k x^{k+1})^i - \cdots].$$

□

For $k \geq 2$, define the $k-$division $4-$Lehmer-Pell sequences as follows.
(i) The $2-$division $4-$Lehmer-Pell sequence, denoted by $\{hL_n(2,4)\}_{n=0}^{\infty}$, is

$$hL_n(2,4) = \begin{cases} 4hL_{n-1}(2,4) + hL_{n-2}(2,4) + 10hL_{n-3}(2,4) + 4hL_{n-4}(2,4) & n \text{ odd}, \\ hL_{n-1}(2,4) + hL_{n-2}(2,4) - 10hL_{n-3}(2,4) - 4hL_{n-3}(2,4) & n \text{ even}, \end{cases}$$

with initial conditions $hL_0(2,4) = hL_1(2,4) = hL_2(2,4) = 0, hL_2(2,4) = 1$, so

$$\{hL_n(2,4)\}_{n=0}^{\infty} = \{0,0,0,1,1,5,-4,3,-55,-237,-306,-1999,285,\cdots\}.$$

(ii) The 3−division 4−Lehmer-Pell sequence, denoted by $\{hL_n(3,4)\}_{n=0}^{\infty}$, is

$$hL_n(3,4) = \begin{cases} 4hL_{n-1}(3,4) + hL_{n-2}(3,4) + 24hL_{n-4}(3,4) + 10hL_{n-5}(3,4) & n \text{ odd}, \\ hL_{n-1}(3,4) + hL_{n-2}(3,4) - 24hL_{n-4}(3,4) - 10hL_{n-5}(3,4) & n \text{ even}, \end{cases}$$

with initial conditions $hL_0(3,4) = hL_1(3,4) = hL_2(3,4) = hL_3(3,4) = 0,\ hL_4(3,4) = 1$, so

$$\{hL_n(3,4)\}_{n=0}^{\infty} = \{0,0,0,0,1,4,5,24,5,150,-5,756,391,5970,4981,\cdots\}.$$

(iii) The 4−division 4−Lehmer-Pell sequence, denoted by $\{hL_n(4,4)\}_{n=0}^{\infty}$, is

$$hL_n(4,4) = \begin{cases} 4hL_{n-1}(4,4) + hL_{n-2}(4,4) + 58hL_{n-5}(4,4) + 24hL_{n-6}(4,4) & n \text{ odd}, \\ hL_{n-1}(4,4) + hL_{n-2}(4,4) - 58hL_{n-5}(4,4) - 24hL_{n-6}(4,4) & n \text{ even}, \end{cases}$$

with initial conditions $hL_0(4,4) = hL_1(4,4) = hL_2(4,4) = hL_3(4,4) = hL_4(4,4) = 0, hL_5(4,4) = 1$, so

$$\{hL_n(4,4)\}_{n=0}^{\infty} = \{0,0,0,0,0,1,1,5,6,29,-23,19,-318,\cdots\}.$$

(iv) The k−division 4−Lehmer-Pell sequences, denoted by $\{hL_n(k,4)\}_{n=0}^{\infty}$, are

$$hL_n(k,4) = \begin{cases} 4hL_{n-1}(k,4) + hL_{n-2}(k,4) + 2P_{k+1}hL_{n-k-1}(k,4) + 2P_khL_{n-k-2}(k,4) & n \text{ odd}, \\ hL_{n-1}(k,4) + hL_{n-2}(k,4) - 2P_{k+1}hL_{n-k-1}(k,4) - 2P_khL_{n-k-2}(k,4) & n \text{ even}, \end{cases}$$

with initial conditions $hL_0(k,4) = hL_1(k,4) = \cdots = hL_k(k,4) = 0, hL_{k+1}(k,4) = 1$.

For $k \geq 2$, define the k−division 5−Lehmer-Pell sequence as follows.

(i) The 2−division 5−Lehmer-Pell sequence, denoted by $\{hL_n(2,5)\}_{n=0}^{\infty}$, is

$$hL_n(2,5) = \begin{cases} 5hL_{n-1}(2,5) + hL_{n-2}(2,5) + 15hL_{n-3}(2,5) + 6hL_{n-4}(2,5) & n \text{ odd}, \\ hL_{n-1}(2,5) + hL_{n-2}(2,5) - 15hL_{n-3}(2,5) - 6hL_{n-3}(2,5) & n \text{ even}, \end{cases}$$

with initial conditions $hL_0(2,5) = hL_1(2,5) = hL_2(2,5) = 0, hL_2(2,5) = 1$, so

$$\{hL_n(2,5)\}_{n=0}^{\infty} = \{0,0,0,1,1,6,-8,-13,-117,-682,-556,-5295,5018,\cdots\}.$$

(ii) The 3−division 5−Lehmer-Pell sequence, denoted by $\{hL_n(3,5)\}_{n=0}^{\infty}$, is

$$hL_n(3,5) = \begin{cases} 5hL_{n-1}(3,5) + hL_{n-2}(3,5) + 36hL_{n-4}(3,5) + 15hL_{n-5}(3,5) & n \text{ odd}, \\ hL_{n-1}(3,5) + hL_{n-2}(3,5) - 36hL_{n-4}(3,5) - 15hL_{n-5}(3,5) & n \text{ even}, \end{cases}$$

with initial conditions $hL_0(3,5) = hL_1(3,5) = hL_2(3,5) = hL_3(3,5) = 0,\ hL_4(3,5) = 1$, so

$$\{hL_n(3,5)\}_{n=0}^{\infty} = \{0,0,0,0,1,5,6,35,5,255,-31,1450,714,\cdots\}.$$

(iii) The 4−division 5−Lehmer-Pell sequence, denoted by $\{hL_n(4,5)\}_{n=0}^{\infty}$, is

$$hL_n(4,5) = \begin{cases} 5hL_{n-1}(4,5) + hL_{n-2}(4,5) + 87hL_{n-5}(4,5) + 36hL_{n-6}(4,5) & n \text{ odd}, \\ hL_{n-1}(4,5) + hL_{n-2}(4,5) - 87hL_{n-5}(4,5) - 36hL_{n-6}(4,5) & n \text{ even}, \end{cases}$$

with initial conditions $hL_0(4,5) = hL_1(4,5) = hL_2(4,5) = hL_3(4,5) = hL_4(4,5) = 0, hL_5(4,5) = 1$, so

$$\{hL_n(4,5)\}_{n=0}^{\infty} = \{0,0,0,0,0,1,1,6,7,41,-39,-31,-628,-2346,-2346,\cdots\}.$$

(iv) The $k-$division 5$-$Lehmer-Pell sequence, denoted by $\{hL_n(k,5)\}_{n=0}^{\infty}$, is

$$hL_n(k,5)=\begin{cases}5hL_{n-1}(k,5)+hL_{n-2}(k,5)+3P_{k+1}hL_{n-k-1}(k,5)+3P_khL_{n-k-2}(k,5) & n \text{ odd},\\ hL_{n-1}(k,5)+hL_{n-2}(k,5)-3P_{k+1}hL_{n-k-1}(k,5)-3P_khL_{n-k-2}(k,5) & n \text{ even},\end{cases}$$

with initial conditions $hL_0(k,5)=hL_1(k,5)=\cdots=hL_k(k,5)=0, hL_{k+1}(k,5)=1$.

Thus, for $k\geq 2$, the $k-$division $L-$Lehmer-Pell sequences, denoted by $\{hL_n(k,L)\}_{n=0}^{\infty}$, are

$$hL_n(k,5)=\begin{cases}LhL_{n-1}(k,5)+hL_{n-2}(k,5)+(L-2)P_{k+1}hL_{n-k-1}(k,5)\\ \quad +(L-2)P_khL_{n-k-2}(k,5) & n \text{ odd},\\ hL_{n-1}(k,5)+hL_{n-2}(k,5)-(L-2)P_{k+1}hL_{n-k-1}(k,5)\\ \quad -(L-2)P_khL_{n-k-2}(k,5) & n \text{ even},\end{cases}$$

with initial conditions $hL_0(k,L)=hL_1(k,L)=\cdots=hL_k(k,L)=0, hL_{k+1}(k,L)=1$.

Lemma 2.5. *For $k\geq 2$, let $g_{hL_n(k,L)}$ be the generating function of the $k-$division $L-$Lehmer-Pell sequences. Then*

$$g_{hL_n(k,L)}=\begin{cases}\dfrac{x^{k+1}}{1-Lx-x^2-(L-2)P_{k+1}x^{k+1}-(L-2)P_kx^{k+2}} & n \text{ odd},\\ \dfrac{x^{k+1}}{1-x-x^2+(L-2)P_{k+1}x^{k+1}+(L-2)P_kx^{k+2}} & n \text{ even},\end{cases} \tag{3}$$

Proof. The proof is similar to that for Lemma 2.3 and so is omitted. □

Similar to Lemma 2.4, the following lemma is obtained.

Lemma 2.6. *For $k\geq 2$, the generating function of the $k-$division $L-$Lehmer-Pell sequences has exponential representation*

$$g_{hL_n(k,L)}=\begin{cases}x^{k+1}exp\sum_{i=1}^{\infty}\dfrac{x^i}{i}(L+x+(L-2)P_{k+1}x^k+(L-2)P_kx^{k+1})^i & n \text{ odd},\\ x^{k+1}exp\sum_{i=1}^{\infty}\dfrac{x^i}{i}(1+x-(L-2)P_{k+1}x^k-(L-2)P_kx^{k+1})^i & n \text{ even},\end{cases}$$

3. An Affine-Hill Cipher from the $k-$division $L-$Lehmer-Pell sequences

In this section, the $k-$division $L-$Lehmer-Pell sequences and corresponding self-invertible matrices are employed to obtain an Affine-Hill cipher algorithm. Let the public key be $(hL_n(k,L),p)$ where p is prime and $i\in\mathbb{N}$ is the secret key. The message m is first divided into matrices of size 1×4 modulo p denoted P_j, $1\leq j\leq n$. The secret key is used to compute

$$hL_i(k,L),\ hL_{i+1}(k,L), hL_{i+2}(k,L),\ hL_{i+3}(k,L).$$

Then, a self-invertible matrix K is obtained as follows

$$K=\begin{bmatrix}hL_i(k,L) & hL_{i+1}(k,L) & 1-hL_i(k,L) & -hL_{i+1}(k,L)\\ hL_{i+2}(k,L) & hL_{i+3}(k,L) & -hL_{i+2}(k,L) & 1-hL_{i+3}(k,L)\\ 1+hL_i(k,L) & hL_{i+1}(k,L) & -hL_i(k,L) & -hL_{i+1}(k,L)\\ hL_{i+2}(k,L) & 1+hL_{i+3}(k,L) & -hL_{i+2}(k,L) & -hL_{i+3}(k,L)\end{bmatrix} \pmod p,$$

as well as

$$B = \begin{bmatrix} hL_{p+i}(k,L) & hL_{p+i+1}(k,L) & hL_{p+i+2}(k,L) & hL_{p+i+3}(k,L) \end{bmatrix}.$$

The message is used to compute $C_j \equiv P_j K + B \pmod{p}$ and $C = C_j, 1 \leq j \leq n$ is sent. For decryption, the public key $(hL_n(k,L), p)$ and the secret key i are employed to compute K and B. Then K and B are used to obtain

$$P_j \equiv (C_j - B)K^{-1} \pmod{p}.$$

The proposed algorithm is given below.

Algorithm

Let $(hL_n(k,L), p)$ be the public key where p is prime and $i \in \mathbb{N}$ be the secret key.

- Encryption

  1. Divide the message into matrices of size 1×4 modulo p denoted P_j. Using the secret key, compute $hL_i(k,L), hL_{i+1}(k,L), hL_{i+2}(k,L), hL_{i+3}(k,L)$.

  2. Obtain a self-invertible matrix K as follows

$$K = \begin{bmatrix} hL_i(k,L) & hL_{i+1}(k,L) & 1 - hL_i(k,L) & -hL_{i+1}(k,L) \\ hL_{i+2}(k,L) & hL_{i+3}(k,L) & -hL_{i+2}(k,L) & 1 - hL_{i+3}(k,L) \\ 1 + hL_i(k,L) & hL_{i+1}(k,L) & -hL_i(k,L) & -hL_{i+1}(k,L) \\ hL_{i+2}(k,L) & 1 + hL_{i+3}(k,L) & -hL_{i+2}(k,L) & -hL_{i+3}(k,L) \end{bmatrix} \pmod{p}.$$

  3. Compute

$$B = \begin{bmatrix} hL_{p+i}(k,L) & hL_{p+i+1}(k,L) & hL_{p+i+2}(k,L) & hL_{p+i+3}(k,L) \end{bmatrix}.$$

  4. Using the message, compute $C_j \equiv P_j K + B \pmod{p}$.

  5. Send C.

- Decryption

  1. Using the public key $(hL_n(k,L), p)$ and secret key i, compute K and B.

  2. Using K and B, obtain $P_j \equiv (C_j - B)K^{-1} \pmod{p}$.

The proposed algorithm is illustrated in the following example.

Example 3.1. Let the public key be $(hL_n(1,3), 5)$ and the secret key be $i = 4$. The message is $12, 13, 2, 3, 3, 7, 9, 2380, 1, 3$.

- Encryption

  1. Divide a message into matrix size 1×4 modulo p denoted P_j, $1 \leq j \leq n$. We have

$$P_1 = \begin{bmatrix} 12 & 13 & 2 & 3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 2 & 3 \end{bmatrix} \pmod{5}.$$

$$P_2 = \begin{bmatrix} 3 & 7 & 9 & 2380 \end{bmatrix} = \begin{bmatrix} 3 & 2 & 4 & 0 \end{bmatrix} \pmod{5}.$$

$$P_3 = \begin{bmatrix} 1 & 3 & 0 & 0 \end{bmatrix} \pmod{5}.$$

  Using secret key, compute $hL_4(1,3) = 2, hL_5(1,3) = 16, hL_6(k,3) = 11, hL_7(k,3) = 83$.

2. Obtain a self-invertible matrix K as follows

$$\begin{aligned} K &= \begin{bmatrix} hL_4(1,3) & hL_5(1,3) & 1-hL_4(1,3) & -hL_5(1,3) \\ hL_6(1,3) & hL_7(1,3) & -hL_6(1,3) & 1-hL_7(1,3) \\ 1+hL_4(1,3) & hL_5(1,3) & -hL_4(1,3) & -hL_5(1,3) \\ hL_6(1,3) & 1+hL_7(1,3) & -hL_6(1,3) & -hL_7(1,3) \end{bmatrix} \\ &= \begin{bmatrix} 2 & 16 & -1 & -16 \\ 11 & 83 & -11 & -82 \\ 3 & 16 & -2 & -16 \\ 11 & 84 & -11 & -83 \end{bmatrix} \\ &= \begin{bmatrix} 2 & 1 & 4 & 4 \\ 1 & 3 & 4 & 3 \\ 3 & 1 & 3 & 4 \\ 1 & 4 & 4 & 2 \end{bmatrix} \pmod 5. \end{aligned}$$

3. Compute

$$\begin{aligned} B &= \begin{bmatrix} hL_9(1,3) & hL_{10}(1,3) & hL_{11}(1,3) & hL_{12}(1,3) \end{bmatrix} \\ &= \begin{bmatrix} 428 & 289 & 2207 & 1407 \end{bmatrix} \\ &\equiv \begin{bmatrix} 3 & 4 & 2 & 0 \end{bmatrix} \pmod 5. \end{aligned}$$

4. Using the message, compute $C_j \equiv P_jK + B \pmod p$ so then we have

$$C_1 \equiv P_1K + B = \begin{bmatrix} 2 & 3 & 2 & 3 \end{bmatrix} \begin{bmatrix} 2 & 1 & 4 & 4 \\ 1 & 3 & 4 & 3 \\ 3 & 1 & 3 & 4 \\ 1 & 4 & 4 & 2 \end{bmatrix} + \begin{bmatrix} 3 & 4 & 2 & 0 \end{bmatrix} \equiv \begin{bmatrix} 4 & 4 & 0 & 1 \end{bmatrix} \pmod 5.$$

$$C_2 \equiv P_2K + B = \begin{bmatrix} 3 & 2 & 4 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 & 4 & 4 \\ 1 & 3 & 4 & 3 \\ 3 & 1 & 3 & 4 \\ 1 & 4 & 4 & 2 \end{bmatrix} + \begin{bmatrix} 3 & 4 & 2 & 0 \end{bmatrix} \equiv \begin{bmatrix} 3 & 2 & 4 & 4 \end{bmatrix} \pmod 5.$$

$$C_3 \equiv P_3K + B = \begin{bmatrix} 1 & 3 & 0 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 & 4 & 4 \\ 1 & 3 & 4 & 3 \\ 3 & 1 & 3 & 4 \\ 1 & 4 & 4 & 2 \end{bmatrix} + \begin{bmatrix} 3 & 4 & 2 & 0 \end{bmatrix} \equiv \begin{bmatrix} 3 & 4 & 3 & 3 \end{bmatrix} \pmod 5.$$

5. Send $C = C_1C_2C_3 = 4, 4, 0, 1, 3, 2, 4, 4, 3, 4, 3, 3$.

- Decryption

1. Using the public key $(hL_n(1,3), 5)$ and secert key 4, compute K and B.
2. Using K and B, obtain $P_j \equiv (C_j - B)K^{-1} \pmod 5$.

$$P_1 \equiv (C_1 - B)K^{-1}$$

$$= \left(\begin{bmatrix}4 & 4 & 0 & 1\end{bmatrix} - \begin{bmatrix}3 & 4 & 0 & 1\end{bmatrix}\right) \times \begin{bmatrix}2 & 1 & 4 & 4\\ 1 & 3 & 4 & 3\\ 3 & 1 & 3 & 4\\ 1 & 4 & 4 & 2\end{bmatrix}^{-1}$$

$$\equiv \begin{bmatrix}2 & 3 & 2 & 3\end{bmatrix} \pmod 5,$$

$$P_2 \equiv (C_2 - B)K^{-1}$$

$$= \left(\begin{bmatrix}3 & 2 & 4 & 4\end{bmatrix} - \begin{bmatrix}3 & 4 & 0 & 1\end{bmatrix}\right) \times \begin{bmatrix}2 & 1 & 4 & 4\\ 1 & 3 & 4 & 3\\ 3 & 1 & 3 & 4\\ 1 & 4 & 4 & 2\end{bmatrix}^{-1}$$

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

$$P_3 \equiv (C_3 - B)K^{-1}$$

$$= \left(\begin{bmatrix}3 & 4 & 3 & 3\end{bmatrix} - \begin{bmatrix}3 & 4 & 0 & 1\end{bmatrix}\right) \times \begin{bmatrix}2 & 1 & 4 & 4\\ 1 & 3 & 4 & 3\\ 3 & 1 & 3 & 4\\ 1 & 4 & 4 & 2\end{bmatrix}^{-1}$$

$$\equiv \begin{bmatrix}1 & 3 & 0 & 0\end{bmatrix} \pmod 5.$$

For $s \geq 5$, the proposed algorithm can be generalized so that K is an $s \times s$ self-invertible matrix [1], B is an $l \times s$ matrix, and the message matrix divides an $l \times s$ matrix.

3.1. Security analysis

An important attack on the Affine-Hill cipher is the brute force attack [20]. In this method, all possible matrices must be tested. In the proposed algorithm, the keys are constructed using self-invertible matrices. Since these matrices are invertible, we must check the order of the group $GL_n(F_p)$. $GL_n(F_p)$, p prime, consists of all invertible matrices of order $n \times n$ over F_p [8]. This group has order

$$| GL_n(F_p) | = (p^n - p^{n-1})(p^n - p^{n-2}) \cdots (p^n - 1).$$

Since K is an invertible matrix of order 4×4, we have

$$| GL_4(F_p) | = (p^4 - p^3)(p^4 - p^2)(p^4 - p^1)(p^4 - 1).$$

For example

$$\text{if } p = 2, \text{ we have } | GL_4(F_2) | = (2^4 - 2^3)(2^4 - 2^2)(2^4 - 2^1)(2^4 - 1) = 20160,$$
$$\text{if } p = 3, \text{ we have } | GL_4(F_3) | = (3^4 - 3^3)(3^4 - 3^2)(3^4 - 3^1)(3^4 - 1) = 24261120,$$
$$\text{if } p = 5, \text{ we have } | GL_4(F_5) | = (5^4 - 5^3)(5^4 - 5^2)(5^4 - 5^1)(5^4 - 1) = 116064000000.$$

As p and n increase, $| GL_n(F_p) | \to \infty$. Therefore, the key space is very large so the probability of a successful attack is negligible.

Another attack is a 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 matrices 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 practical attack.

4. Conclusion

A new sequence called the $k-$division sequence was introduced. Then the Pell and Lehmer sequences were used to obtain new sequences called the $k-$division $L-$Lehmer-Pell sequences, and some properties of these sequences were determined. As an application, the $k-$division $L-$Lehmer-Pell sequences and corresponding self-invertible matrices were employed in a new Affine-Hill cipher algorithm, and the security was studied. Other sequences such as Mersenne, Fibonacci, and Jacobsthal sequences [5, 7, 14] can be used for this algorithm.

References

[1] B. Acharya, G. S. Rath, S. K. Patra, and S. K. Panigrahy. Novel methods of generating self-invertible matrix for hill cipher algorithm. *International Journal of Security*, 1(1), 2007.

[2] M. A. Bennett, V. Patel, and S. Siksek. Shifted powers in lucas–lehmer sequences. *Research in Number Theory*, 5:1–27, 2019. https://doi.org/10.1007/s40993-019-0153-2.

[3] Ö. Deveci and E. Karaduman. Lehmer sequences in finite groups. *Ukrains' kyi Matematychnyi Zhurnal*, 68(2):175–182, 2016.

[4] O. Deveci. The k-nacci sequences and the generalized order-k pell sequences in the semi-direct product of finite cyclic groups. *Chiang Mai Journal of Science*, 40(1):89–98, 2013.

[5] Ö. Deveci and G. Artun. On the adjacency-jacobsthal numbers. *Communications in Algebra*, 47(11):4520–4532, 2019. https://doi.org/10.1080/00927872.2018.1541464.

[6] Ö. Deveci and A. G. Shannon. The quaternion-pell sequence. *Communications in Algebra*, 46(12):5403–5409, 2018.

[7] M. Esmaeili, M. Moosavi, and T. A. Gulliver. A new class of fibonacci sequence based error correcting codes. *Cryptography and Communications*, 9:379–396, 2017. https://doi.org/10.1007/s12095-015-0178-x.

[8] P. A. Grillet. *Abstract algebra*, volume 242. Springer Science & Business Media, 2007.

[9] M. Hashemi and E. Mehraban. On the generalized order 2-pell sequence of some classes of groups. *Communications in Algebra*, 46(9):4104–4119, 2018. https://doi.org/10.1080/00927872.2018.1435793.

[10] L. S. Hill. Cryptography in an algebraic alphabet. *The American Mathematical Monthly*, 36(6):306–312, 1929.

[11] E. Kilic and D. Tasci. On the generalized fibonacci and pell sequences by hessenberg matrices. *Ars Combinatoria*, 94:161–174, 2010.

[12] E. Kiliç and D. Taşci. The generalized binet formula, representation and sums of the generalized order-k pell numbers. *Taiwanese Journal of Mathematics*, 10(6):1661–1670, 2006.

[13] D. H. Lehmer. An extended theory of lucas' functions. *Annals of Mathematics*, 31(3):419–448, 1930.

[14] E. Mehraban, O. Deveci, and E. Hincal. The generalized order (k, t)-mersenne sequences in groups. *AIMS Math*, 30(2):271–282, 2024. http://dx.doi.org/10.7546/nntdm.2024.30.2.271-282.

[15] E. Mehraban and M. Hashemi. Fibonacci length and the generalized order k-pell sequences of the 2-generator p-groups of nilpotency class 2. *Journal of Algebra and Its Applications*, 22(03):2350061, 2023. https://doi.org/10.1142/S0219498823500615.

[16] E. Mehraban, T. A. Gulliver, S. M. Boulaaras, K. Hosseini, and E. Hincal. New sequences from the generalized pell p- numbers and mersenne numbers and their application in cryptography. *AIMS Math*, 9(5):13537–13552, 2024. http://dx.doi.org/\%2010.3934/math.2024660.

[17] E. Mehraban, T. A. Gulliver, and E. Hincal. An rsa cryptosystem based on lehmer sequences in some classes of groups. *Advances in Mathematics of Communications*:inpress, 2024. http://dx.doi.org/10.3934/amc.2024039.

[18] K. Prasad and H. Mahato. Cryptography using generalized fibonacci matrices with affine-hill cipher. *Journal of Discrete Mathematical Sciences and Cryptography*, 25(8):2341–2352, 2022. https://doi.org/10.1080/09720529.2020.1838744.

[19] M. V. Prasad, P. P. P. Chari, and K. P. Satyam. Affine hill cipher key generation matrix of order 3 by using reflects in an arbitrary line y= a x+ b. *International Journal of Science Technology and Management*, 5(08), 2016.

[20] W. Stallings. *Cryptography and Network Security: Principles and Practice, 7th Ed.* Pearson, Harlow, UK, 2017.

[21] D. R. Stinson. *Cryptography: theory and practice*. Chapman and Hall/CRC, 2005.

[22] M. Viswanath and M. R. Kumar. A public key cryptosystem using hiil's cipher. *Journal of Discrete Mathematical Sciences and Cryptography*, 18(1-2):129–138, 2015. https://doi.org/10.1080/09720529.2014.962856.