



APPLICATION OF CHELDHIYA SEQUENCE IN CRYPTOGRAPHY

V. Pandichelvi^{1*}, S. Saranya²

Abstract:

In this paper, the application of the Cheldhiya sequence in cryptography is invented by coding and decoding matrices with the help of American Standard Code for information interchange, the way of finding errors and the procedures for rectifying the errors are presented. Furthermore, blocking methods are discussed.

Key words: The Cheldhiya sequence, Cryptography, ASCII, Coding theory, Decoding theory.

^{1*}Assistant Professor, PG & Research Department of Mathematics, Urumu Dhanalakshmi College, Trichy. (Affiliated to Bharathidasan University). E-mail: mvpmahesh2017@gmail.com

² Research Scholar, PG & Research Department of Mathematics, Urumu Dhanalakshmi College, Trichy. (Affiliated to Bharathidasan University). E-mail: srsaranya1995@gmail.com

***Corresponding Author:** - V. Pandichelvi

*Assistant Professor, PG & Research Department of Mathematics, Urumu Dhanalakshmi College, Trichy. (Affiliated to Bharathidasan University). E-mail: mvpmahesh2017@gmail.com

DOI: 10.53555/ecb/2023.12.Si13.194

1. Introduction:

Brief notes on cryptography and some practise are shown in [1]. In [2,3], the authors displayed the Golden Matrix used in cryptography. The message can be converted into matrix style and used with elliptical curve cryptography in [4]. Coding and decoding the message with Pell and Pell-Lucas numbers are dealt with in [5,-7]. In [8], the author introduced a new Cheldhiya sequence, the Cheldhiya companion sequence and discovered some properties among the members of both sequences.

In this paper, the application of the Cheldhiya sequence in cryptography is developed by coding and decoding matrices, the method of finding errors and the techniques for remedying the errors are offered. Additionally, blocking methods are deliberated.

2. Process of coding and decoding in cryptography:

In this section, the process of coding and decoding in cryptography concerning the Cheldhiya numbers are exhibited.

The Cheldhiya sequence is formed from the solution to the Diophantine equation $x^2 - dy^2 = 1$, where $d = k^2 + 1$ is a square free positive integer.

The recurrence relation of the Cheldhiya sequence is $C_{n,k} = 2(k^2 + 1)C_{n-1,k} - C_{n-2,k}$ where $k \in N$ with $C_{0,k} = 0, C_{1,k} = k$.

The Cheldhiya sequence for $k = 1$ is given by

$$C_{n,1} = 0, 1, 4, 15, 56, \dots$$

The Cheldhiya S matrix of order two is taken as $S = \begin{pmatrix} 4 & -1 \\ 1 & 0 \end{pmatrix}$ and is monitored by mathematical induction on n by

$$S^n = \begin{pmatrix} C_{n+1,1} & -C_{n,1} \\ C_{n,1} & -C_{n+2,1} \end{pmatrix} \text{ for all } n \in N \quad (2.1)$$

Note that $Det(S^n) = C_{n,1}^2 - C_{n+1,1} C_{n+2,1}$.

Choose the message matrix as $R = \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix}$ where $r_1, r_2, r_3, r_4 \in Z^+$.

Let $n = 1$ be the order to construct the code matrix

$$S^1 = \begin{pmatrix} C_{2,1} & -C_{1,1} \\ C_{1,1} & -C_{0,1} \end{pmatrix} = \begin{pmatrix} 4 & -1 \\ 1 & 0 \end{pmatrix}$$

Initiate the Cheldhiya coding and decoding matrices M and R respectively by the successive transformations

$$M = R \times S^n \text{ and } R = M \times (S^n)^{-1}. \text{ Then, the code matrix } M = \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} \times \begin{pmatrix} C_{2,1} & -C_{1,1} \\ C_{1,1} & -C_{0,1} \end{pmatrix}$$

$$M = \begin{pmatrix} r_1 C_{2,1} + r_2 C_{1,1} & -r_1 C_{1,1} - r_2 C_{0,1} \\ r_3 C_{2,1} + r_4 C_{1,1} & -r_3 C_{1,1} - r_4 C_{0,1} \end{pmatrix} = \begin{pmatrix} l_1 & l_2 \\ l_3 & l_4 \end{pmatrix}$$

Now, the code matrix is transferred to the receiver. He will get the message matrix R by decoding as follows.

$$R = \begin{pmatrix} l_1 & l_2 \\ l_3 & l_4 \end{pmatrix} \times \begin{pmatrix} -C_{0,1} & C_{1,1} \\ -C_{1,1} & C_{2,1} \end{pmatrix} = \begin{pmatrix} -l_1 C_{0,1} - l_2 C_{1,1} & l_1 C_{1,1} - l_2 C_{2,1} \\ -l_3 C_{0,1} - l_4 C_{1,1} & l_3 C_{1,1} - l_4 C_{2,1} \end{pmatrix}$$

It is well known that the relation between the coding matrix M and the decoding matrix R is

$$Det(M) = Det(R \times S^1) = Det(R) \times Det(S^1) = 1$$

Also,

$$r_1 = -l_1 C_{0,1} - l_2 C_{1,1} > 0 \quad (2.2)$$

$$r_2 = l_1 C_{1,1} + l_2 C_{2,1} > 0 \quad (2.3)$$

$$r_3 = -l_3 C_{0,1} - l_4 C_{1,1} > 0 \quad (2.4)$$

$$r_4 = l_3 C_{1,1} + l_4 C_{2,1} > 0 \quad (2.5)$$

In the vision of (2.2) and (2.3), it is noticed that

$$\frac{C_{2,1}}{C_{1,1}} < \frac{l_1}{l_2} < \frac{C_{1,1}}{C_{0,1}} \quad (2.6)$$

In a similar way, from equation (2.4) and (2.5), it is obtained as

$$\frac{C_{2,1}}{C_{1,1}} < \frac{l_3}{l_4} < \frac{C_{1,1}}{C_{0,1}} \quad (2.7)$$

By compiling (2.6) and (2.7), it is perceived that

$$\frac{l_1}{l_2} = \frac{l_3}{l_4} = \alpha \text{ (say)} \quad (2.8)$$

Illustration of the process:

Assume that the message to be transferred is "area".

The corresponding message text is $R = \begin{pmatrix} a & r \\ e & a \end{pmatrix}$

Now, the coding and decoding processes are described below.

Using ASCII (American Standard Code for Information Interchange) for the corresponding letter, the message matrix becomes

$$R = \begin{pmatrix} 97 & 114 \\ 101 & 97 \end{pmatrix} \text{ and the coding matrix for } n = 1 \text{ is represented by}$$

$$M = R \times S^1 = \begin{pmatrix} 97 & 114 \\ 101 & 97 \end{pmatrix} \times \begin{pmatrix} 4 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 502 & -97 \\ 501 & -101 \end{pmatrix}$$

The decoding matrix for $n = 1$ is exemplified by

$$R = M \times (S^1)^{-1}$$

$$R = \begin{pmatrix} 502 & -97 \\ 501 & -101 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ -1 & 4 \end{pmatrix} = \begin{pmatrix} 97 & 114 \\ 101 & 97 \end{pmatrix}$$

Finally, the ASCII code helps to treasure the correct word "area".

3. Error detection and correction for coding and decoding method:

Some error may happen in the code matrix *M* for various reasons in the process.

If *n* = 1, then the 2 × 2 message matrix is $R = \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix}$ and $Det(R) = r_1r_4 - r_2r_3$. Also, the code matrix $M = R \times S^1$ and $Det(M) = Det(R)$.

The basic concept of this method depends on calculating the determinants of *M* and *R*. By comparing the determinants obtained from the sender, the receiver can decide whether the code message *M* is correct or not.

It is not possible to decide which element of the code message is wrong. The error may be a single error, double error, triple error etc. First, let us clear up the single error in the code matrix *M*. There are the following four ways to make the error.

- a) $\begin{pmatrix} e_1 & l_2 \\ l_3 & l_4 \end{pmatrix}$
- b) $\begin{pmatrix} l_1 & e_2 \\ l_3 & l_4 \end{pmatrix}$
- c) $\begin{pmatrix} l_1 & l_2 \\ e_3 & l_4 \end{pmatrix}$
- d) $\begin{pmatrix} l_1 & l_2 \\ l_3 & e_4 \end{pmatrix}$

where *e_i*, 1 ≤ *i* ≤ 4 are error elements. To rectify the error in the above four different cases, let us use the following relations

$$e_1l_4 - l_2l_3 = Det(R) \quad (3.1)$$

$$l_1l_4 - e_2l_3 = Det(R) \quad (3.2)$$

$$l_1l_4 - l_2e_3 = Det(R) \quad (3.3)$$

$$l_1e_4 - l_2l_3 = Det(R) \quad (3.4)$$

Then, the possible error values are noted by

$$e_1 = \frac{Det(R)+l_2l_3}{l_4} \quad (3.5)$$

$$e_2 = \frac{-Det(R)+l_1l_4}{l_3} \quad (3.6)$$

$$e_3 = \frac{-Det(R)+l_1l_4}{l_2} \quad (3.7)$$

$$e_4 = \frac{Det(R)+l_2l_3}{l_1} \quad (3.8)$$

It is concluded that if any one of the values of *e_i*, 1 ≤ *i* ≤ 4 is an integer, then it is the damaged element otherwise (all are not integer values) single error is incorrect or an error can be occurred in the element *Det(R)*. If *Det(R)* is incorrect, the relation given in (2.8) is used to rectify the error in the code matrix *M*.

For example, the message "area" is coded by $M = \begin{pmatrix} 502 & -97 \\ 501 & -101 \end{pmatrix}$. Due to some disturbance if

the code matrix is assumed by $\begin{pmatrix} 502 & -98 \\ 501 & -101 \end{pmatrix}$, then it can be decoded by $\begin{pmatrix} 98 & 110 \\ 101 & 97 \end{pmatrix}$ and the

corresponding ASCII code is "bnea". The receiver can identify some error occurs in the coding process in such a way that the message is incorrect. So, the receiver asked the sender to send the determinant value of the message. Then sender contributes that $Det(R) = -2105$.

Now, the receiver try to find whether any single error exists in the code matrix *M*. There are the following four possibilities for the same.

- a) $\begin{pmatrix} e_1 & -98 \\ 501 & -101 \end{pmatrix}$
- b) $\begin{pmatrix} 502 & e_2 \\ 501 & -101 \end{pmatrix}$
- c) $\begin{pmatrix} 502 & -98 \\ e_3 & -101 \end{pmatrix}$
- d) $\begin{pmatrix} 502 & -98 \\ 501 & e_4 \end{pmatrix}$

Then, (3.1) to (3.4) can be modified as follows.

$$-101e_1 + 49098 = -2105$$

$$-50702 - 501e_2 = -2105$$

$$-50702 + 98e_3 = -2105$$

$$502e_4 + 49098 = -2105$$

Solving the above equations, the values of *e_i*, 1 ≤ *i* ≤ 4 are obtained as *e₁* = 506.9, *e₂* = -97, *e₃* = 495.8, *e₄* = -101.9. Since, the value of *e₂* is an integer, it is decided that the error is *e₂*. Replace the corresponding value of *e₂*, the exact code matrix is found to be

$$M = \begin{pmatrix} 502 & -97 \\ 501 & -101 \end{pmatrix}.$$

Similarly, one can clear double errors in the code matrix *M*. There are six opportunities to occur double errors in *M* which are presented below.

- a) $\begin{pmatrix} e_1 & e_2 \\ l_3 & l_4 \end{pmatrix}$
- b) $\begin{pmatrix} e_1 & l_2 \\ e_3 & l_4 \end{pmatrix}$
- c) $\begin{pmatrix} e_1 & l_2 \\ l_3 & e_4 \end{pmatrix}$
- d) $\begin{pmatrix} l_1 & e_2 \\ e_3 & l_4 \end{pmatrix}$
- e) $\begin{pmatrix} l_1 & e_2 \\ l_3 & e_4 \end{pmatrix}$
- f) $\begin{pmatrix} l_1 & l_2 \\ e_3 & e_4 \end{pmatrix}$

Since $Det(M) = Det(R)$, the equivalent forms of (3.1), (3.2), (3.3) and (3.4) are written as

$$e_1l_4 - e_2l_3 = Det(R) \quad (3.9)$$

$$e_1l_4 - l_2e_3 = Det(R) \quad (3.10)$$

$$e_1e_4 - l_2l_3 = Det(R) \quad (3.11)$$

$$l_1l_4 - e_2e_3 = Det(R) \quad (3.12)$$

$$l_1e_4 - e_2l_3 = Det(R) \quad (3.13)$$

$$l_1e_4 - l_2e_3 = Det(R) \quad (3.14)$$

Since $l_1l_4 = l_2l_3$, it is clear that the the equation (3.9) to (3.14) are Diophantine equations. By selecting the values l_1, l_2, l_3 and l_4 satisfying the above relation, the errors can be altered. In this manner, one can modify errors more than two in the code matrix.

4. Blocking methods:

In this section, new coding and decoding algorithms by using the Cheldhiya sequence are introduced. Put our message in a matrix of even order. Dividing the message matrix R of order $2r$ into the block matrices named as B_j , ($1 \leq j \leq r^2$) of order 2 from left to right. Assume that matrices B_j and K_j are of the following forms

$$B_j = \begin{pmatrix} b_1^j & b_2^j \\ b_3^j & b_4^j \end{pmatrix}$$

$$K_j = \begin{pmatrix} k_1^j & k_2^j \\ k_3^j & k_4^j \end{pmatrix}$$

Rewrite the elements in the matrix S^n as given in (2.1) by $S^n = \begin{pmatrix} s_1 & s_2 \\ s_3 & s_4 \end{pmatrix}$.

Define $n = \begin{cases} 3, & \text{if } b \leq 3 \\ \lfloor \frac{b}{2} \rfloor, & \text{if } b > 3 \end{cases}$

where b is the number of the block matrices B_j .

Coding process:

1. Divide the matrix R into block matrix B_j , ($1 \leq j \leq r^2$).
2. Choose n .
3. Find b_x^j , ($1 \leq x \leq 4$).
4. $Det(B_j) = y_j$.
5. coding matrix $M = [y_j, b_x^j]_{x \in \{1,3,4\}}$

Decoding process:

1. Calculate S^n .
2. Determine s_j , ($1 \leq j \leq 4$).
3. Find $s_1b_3^j + s_3b_4^j = k_3^j$, ($1 \leq j \leq m^2$).
4. Evaluate $s_2b_3^j + s_4b_4^j = k_4^j$, ($1 \leq j \leq m^2$).
5. Find $y_j = k_4^j(s_1b_1^j - s_3z_j) - k_3^j(s_2b_1^j - s_4z_j)$.
6. Replace $z_j = b_2^j$.
7. Construct B_j .
8. Finally determine the decoding matrix R .

Example:

Let us consider the message matrix for the message text

“**Number theory is quite interesting**” as

$$R = \begin{pmatrix} N & u & m & b & e & r \\ t & h & e & o & r & y \\ * & \# & i & s & + & ! \\ q & u & i & t & e & * \\ (& i & n & t & e & r \\ e & s & t & i & n & g \end{pmatrix}$$

Coding procedure:

1. Divide the message matrix R of order 6×6 into the matrices of order 2 named as B_j , ($1 \leq j \leq 9$) from left to right.

$$B_1 = \begin{pmatrix} N & u \\ t & h \end{pmatrix}, B_2 = \begin{pmatrix} m & b \\ e & o \end{pmatrix}, B_3 = \begin{pmatrix} e & r \\ r & y \end{pmatrix},$$

$$B_4 = \begin{pmatrix} * & \# \\ q & u \end{pmatrix}, B_5 = \begin{pmatrix} i & s \\ i & t \end{pmatrix}, B_6 = \begin{pmatrix} + & ! \\ e & * \end{pmatrix},$$

$$B_7 = \begin{pmatrix} (& i \\ e & s \end{pmatrix}, B_8 = \begin{pmatrix} n & t \\ t & i \end{pmatrix}, B_9 = \begin{pmatrix} e & r \\ n & g \end{pmatrix}.$$

2. Here $b = 9 > 3$, so $n = 4$. Consider the ASCII code for the elements in the matrix M as given in table 4.1.

Table 4.1

N	u	m	b	e	r	t	h	e
78	117	109	98	101	114	116	104	101
o	r	y	*	#	i	s	+	!
111	114	121	42	35	105	115	43	33
q	u	i	t	e	*	(i	n
113	117	105	116	101	42	40	105	110
t	e	r	e	s	t	i	n	g
116	101	114	101	115	116	105	110	103

3. Illustrate the elements of the blocks B_j , ($1 \leq j \leq 9$) as presented in table 4.2.

Table 4.2

$b_1^1 = 78$	$b_2^1 = 117$	$b_3^1 = 116$	$b_4^1 = 104$
$b_1^2 = 109$	$b_2^2 = 98$	$b_3^2 = 101$	$b_4^2 = 111$
$b_1^3 = 101$	$b_2^3 = 114$	$b_3^3 = 114$	$b_4^3 = 121$
$b_1^4 = 42$	$b_2^4 = 35$	$b_3^4 = 113$	$b_4^4 = 117$
$b_1^5 = 105$	$b_2^5 = 115$	$b_3^5 = 105$	$b_4^5 = 116$
$b_1^6 = 43$	$b_2^6 = 33$	$b_3^6 = 101$	$b_4^6 = 42$
$b_1^7 = 40$	$b_2^7 = 105$	$b_3^7 = 101$	$b_4^7 = 115$
$b_1^8 = 110$	$b_2^8 = 116$	$b_3^8 = 116$	$b_4^8 = 105$
$b_1^9 = 101$	$b_2^9 = 114$	$b_3^9 = 110$	$b_4^9 = 103$

4. Calculate the determinants y_j of the block B_j , $1 \leq j \leq 9$ which are listed in table 4.3.

Table 4.3

$y_1 = \det(B_1) = -5460$
$y_2 = \det(B_2) = 2201$
$y_3 = \det(B_3) = -775$
$y_4 = \det(B_4) = 959$
$y_5 = \det(B_5) = 105$
$y_6 = \det(B_6) = -1527$
$y_7 = \det(B_7) = -6005$
$y_8 = \det(B_8) = -1906$
$y_9 = \det(B_9) = -2137$

5. Determine the matrix M by applying step 3 and step 4.

$$M = \begin{pmatrix} -5460 & 78 & 116 & 104 \\ 2201 & 109 & 101 & 111 \\ -775 & 101 & 114 & 121 \\ 959 & 42 & 113 & 117 \\ 105 & 105 & 105 & 116 \\ -1527 & 43 & 101 & 42 \\ -6005 & 40 & 101 & 115 \\ -1906 & 110 & 116 & 105 \\ -2137 & 101 & 110 & 103 \end{pmatrix}$$

Decoding procedure:

- From equation (2.1), the 4th power of the S is attained by $S^4 = \begin{pmatrix} 209 & -56 \\ 56 & -15 \end{pmatrix}$.
- The elements of S^4 are denoted by $s_1 = 209, s_2 = -56, s_3 = 56$ and $s_4 = -15$.
- Evaluate the elements k_3^j to build the matrix K_j by using the relation $s_1 b_3^j + s_3 b_4^j = k_3^j, 1 \leq j \leq 9$
Therefore, $k_3^1 = 30068, k_3^2 = 27325,$
 $k_3^3 = 30602, k_3^4 = 30169, k_3^5 = 28441,$
 $k_3^6 = 23461, k_3^7 = 27549,$
 $k_3^8 = 30124, k_3^9 = 28758.$
- Find the elements k_4^j to form the matrix K_j with the help of the identity $s_2 b_3^j + s_4 b_4^j = k_4^j, 1 \leq j \leq 9$.
Thus, $k_4^1 = -8056,$
 $k_4^2 = -7321, k_4^3 = -8199,$
 $k_4^4 = -8083, k_4^5 = -7620,$
 $k_4^6 = -6286, k_4^7 = -7381,$
 $k_4^8 = -8071, k_4^9 = -7705.$
- Compute the elements z_j by the relation $y_j = k_4^j(s_1 b_1^j - s_3 z_j) - k_3^j(s_2 b_1^j - s_4 z_j), 1 \leq j \leq 9$. Then, $z_1 = 117, z_2 = 98, z_3 = 114,$
 $z_4 = 35, z_5 = 115, z_6 = 33, z_7 = 105,$
 $z_8 = 116, z_9 = 114.$

6. Rename $z_j = b_2^j, 1 \leq j \leq 9$ as mentioned in table 4.4.

Table 4.4

$z_1 = b_2^1 = 117$	$z_2 = b_2^2 = 98$	$z_3 = b_2^3 = 114$
$z_4 = b_2^4 = 35$	$z_5 = b_2^5 = 115$	$z_6 = b_2^6 = 33$
$z_7 = b_2^7 = 105$	$z_8 = b_2^8 = 116$	$z_9 = b_2^9 = 114$

7. construct the block matrices $B_j, 1 \leq j \leq 9$.

$$B_1 = \begin{pmatrix} 78 & 117 \\ 116 & 104 \end{pmatrix}, B_2 = \begin{pmatrix} 109 & 98 \\ 101 & 111 \end{pmatrix},$$

$$B_3 = \begin{pmatrix} 101 & 114 \\ 114 & 121 \end{pmatrix}, B_4 = \begin{pmatrix} 42 & 35 \\ 113 & 117 \end{pmatrix},$$

$$B_5 = \begin{pmatrix} 105 & 115 \\ 105 & 116 \end{pmatrix}, B_6 = \begin{pmatrix} 43 & 33 \\ 101 & 42 \end{pmatrix},$$

$$B_7 = \begin{pmatrix} 40 & 105 \\ 101 & 115 \end{pmatrix}, B_8 = \begin{pmatrix} 110 & 116 \\ 116 & 105 \end{pmatrix},$$

$$B_9 = \begin{pmatrix} 101 & 114 \\ 110 & 103 \end{pmatrix}.$$

8. Finally, the decoding matrix is assembled by

$$R = \begin{pmatrix} 78 & 117 & 109 & 98 & 101 & 114 \\ 116 & 104 & 101 & 111 & 114 & 121 \\ 42 & 35 & 105 & 115 & 43 & 33 \\ 113 & 117 & 105 & 116 & 101 & 42 \\ 40 & 105 & 110 & 116 & 101 & 114 \\ 101 & 115 & 116 & 105 & 110 & 103 \end{pmatrix}$$

Consequently, the ASCII code for the corresponding number matrix is of the form

$$R = \begin{pmatrix} N & u & m & b & e & r \\ t & h & e & o & r & y \\ * & \# & i & s & + & ! \\ q & u & i & t & e & * \\ (& i & n & t & e & r \\ e & s & t & i & n & g \end{pmatrix}$$

Conclusion:

This article is mainly focused on how the Cheldhiya sequence is applied in cryptography. The ASCII code is used to analyse the concepts. In this manner one can scrutinize the application of any other sequences in cryptography by supposing specific secret codes for letters in message text.

References:

[1]Stinson, Douglas R. Cryptography: theory and practice. Chapman and Hall/CRC, 2005.
[2]Del Rey, Ángel Martín, and Gerardo Rodríguez Sánchez, "On the Security of "Golden Cryptography" International Journal of Network Security, Volume 7, Number 3, 2008, 448450.
[3]Tahghighi. M., et al, "The cryptanalysis and extension of the generalized golden cryptography" 2011 IEEE Conference on Open Systems. IEEE, 2011, 65-68.

- [4]Kamalakaran. V. and Tamilselvan. S, "Security enhancement of text message based on matrix approach using elliptical curve cryptosystem" *Procedia Materials Science* 10, 2015, 489-496.
- [5]Taş, Nihal, Sümevra Uçar and Nihal Yılmaz Özgür. "Pell coding and pell decoding methods with some applications" *arXiv preprint arXiv: 1706.04377v1 [math.NT]* Junr 2017.
- [6]Sundarayya. P. and MG Vara Prasad. "Coding theory on Pell-Lucas p numbers" *Journal of Physics: Conference Series*.1344. IOP Publishing, 2019.
- [7]Zerrouh. M., A. Chillali and Abdelkarim Boua. "Cryptography based on the matrices" *Boletim da Sociedade Paranaense de Matematica* Volume 37, Issue 3, 2019, 75-83.
- [8]Sandhya, P. and V. Pandichelvi. "Invention of four novel sequences and their properties" *Journal of Xi'an Shiyou University, Natural Science Edition*, Volume 17, Issue 06, 2021,59-68.