Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 9s (2025)

Implementation of R in Cryptographic Algorithms: Integrating Symmetric Matrices and Positive Integer-Valued Functions

[1]K. Kaleeswari, [*2]J. Kannan, [3]M. Mahalakshmi, [4]A. Deepshika, [5]Manju Somanath and [6]V. Sangeetha

[1]Part Time Ph.D. Research Scholar, Department of Mathematics, Ayya Nadar Janaki Ammal College (Autonomous, affiliated to Madurai Kamaraj University), Sivakasi – 626124, Tamil Nadu, India.

[2]Assistant Professor, Department of Mathematics, Ayya Nadar Janaki Ammal College (Autonomous, affiliated to Madurai Kamaraj University), Sivakasi – 626124, Tamil Nadu, India.

[3, 4]Full Time Ph.D. Research Scholar, Department of Mathematics, Ayya Nadar Janaki Ammal College (Autonomous, affiliated to Madurai Kamaraj University), Sivakasi – 626124, Tamil Nadu, India.

[5]Associate Professor, PG and Research Department of Mathematics, National College (Autonomous, affiliated to Bharathidasan University), Trichy – 620 001, Tamil Nadu, India.

[6]Assistant Professor, PG and Research Department of Mathematics, National College (Autonomous, affiliated to Bharathidasan University), Trichy – 620 001, Tamil Nadu, India.

*Corresponding Author's E-mail ID.: jayram.kannan@gmail.com

Article History:

Received: 20-11-2024

Revised: 22-12-2024

Accepted: 15-01-2025

Abstract: In this paper, algorithms for encryption and decryption are displayed by means of functions $f, g: \mathbb{N} \to \mathbb{N}$ and a unique assignment for alphabets. In the process of encryption, a cyclic symmetric matrix is also employed. The algorithms are followed by a few exemplifications for both processes. In the end, separate R programs for encryption and decryption are provided with samples.

Keywords: Encryption, decryption, cyclic symmetric matrix, positive integer-valued function.

2010 MSC Subject Classification: 11A25,11T71, 94A60.

1. Introduction

The concept of encryption is the process of transmitting the original message in a different form, whereas decryption is the process of converting the encrypted message to its original form. There are a lot of algorithms for doing these processes effectively. This paper possesses such encryption and decryption algorithms.

In recent days, researchers have employed various unique terms in their own encryption and decryption algorithms. For example, (Dasdemir, 2011) and (Thiagarajan, 2018) used matrices in algorithms. Basic number theoretical concepts, Fibonacci and Lucas numbers are also used in the algorithms provided in (Taş, 2018) and (Uçar, 2019).

Apart from these, the Diophantine equation, an equation over $\mathbb{Z}$, whose solutions are to be found in $\mathbb{Z}$, is also considered for the conversion of messages into an alternative form. For instance,

(Dasdemir, 2011) and (Kannan, 2022) employ the well-known Pell equation and its solutions in recursive matrix form.

This study was also developed with the thought of encrypting and decrypting messages by using number theoretic components. (Thiagarajan, 2018) and (Zeriouh, 2019) were utilized as a precursor to its creation.

The main theme of this paper is to use positive integer-valued function and a cyclic symmetric matrix corresponding to the message taken. Let $f: \mathbb{N} \to \mathbb{N}$ be a function defined by

$$f(n) = \begin{cases} A\left(\frac{n+1}{2}\right), if\ n\ is\ odd \\ B\left(\frac{n}{2}\right), if\ n\ is\ even \end{cases}$$

where $A(n)$ is the n^{th} smallest element in the set $A = \{3k+1: k = 0,1,2,\cdots\}$ and $B(n)$ is the n^{th} smallest element in the set $B = \mathbb{N}\backslash A$. This is the positive integer-valued function used for the conversion of messages in this paper. Also, the alphabets are assigned uniquely.

This article comprises various components, such as sections and subsections. Notations and positions are the major requirements of this paper, and they follow the section "Introduction". The section "Procedures for Encryption and Decryption" displays the algorithms of encryption and decryption, along with examples in the subsection "Few Exemplifications". After that, the section "R Code for Encryption and Decryption" is placed. This section provides R programs for both processes with an illustration. Finally, there is a conclusion to this article.

1.1. Notations

The following are the basic notations used in this paper:

- W_i: i^{th} word in the message to be sent
- $n(W_i)$: number of letters in the word W_i
- $\mathbb{N}$: the set of all natural numbers
- A: the set of all natural numbers of the form $3k+1, k = 0,1,2,\cdots$
- B: the set of all natural numbers not in the set A
- $A(n)$: n^{th} smallest element in the set A
- $B(n)$: n^{th} smallest element in the set B
- f: a positive integer-valued function defined on $\mathbb{N}$ by

$$f(n) = \begin{cases} A\left(\frac{n+1}{2}\right), if\ n\ is\ odd \\ B\left(\frac{n}{2}\right), if\ n\ is\ even \end{cases}$$

- g: a positive integer-valued function defined on $\mathbb{N}$ by

$$g(n) = \begin{cases} \frac{n+1}{2}, if\ n\ is\ odd \\ \frac{n}{2}, if\ n\ is\ even \end{cases}$$

- M_i: cyclic symmetric matrix for W_i

- I_i: identity matrix of order i
- R_i: $g\left(n(W_i)\right)^{th}$ row of the cyclic matrix M_i
- $D(R_i)$: diagonal matrix with entries in R_i

1.2. Positions

The following is the table for position of alphabets:

A	B	C	D	E	F	G	H	I	J	K	L	M
7	13	21	31	43	57	73	91	111	133	157	183	211
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
241	273	307	343	381	421	463	507	553	601	651	703	757

Table 1: Numerical Assignments for Alphabets

2. Procedures for Encryption and Decryption

This section covers the steps for the processes of encryption and decryption for a given message.

2.1. Encryption

In this encryption process, each word has to be encrypted separately. First, split the message (assume it has n words) to be sent into $W_1, W_2, \cdots, W_n$ (omit spaces). Then do the same steps given below for each i (the following steps are provided for the word W_i)

(E1) Using the Table 1, find the position for each letter in the word W_i.

(E2) Apply the function f for each of these numerical positions.

(E3) Construct a cyclic symmetric matrix M_i of order $i \times i$ using the values obtained in $(E2)$.

(E4) Calculate $n(W_i)$.

(E5) Calculate $g\left(n(W_i)\right)$.

(E6) Construct the diagonal matrix $D(R_i)$.

(E7) Find $D(R_i) - n(W_i)I_{n(W_i)}$, which is the encrypted key.

This encrypted key is to be sent as $E_i = (e_{i1} \quad e_{i2} \quad \cdots \quad e_{ik_i})$ where $e_{ik_i}{}'s$ are the diagonal entries of $D(R_i) - n(W_i)I_{n(W_i)}$.

2.2. Decryption

For each i do the following steps for the decryption of the encrypted key E_i.

(D1) Calculate $C_i = (c_{i1} \quad c_{i2} \quad \cdots \quad c_{ik_i}) = D(E_i) + k_i I_{k_i}$.

(D2) Find $g(k_i)$.

(D3) Construct $S_i = (s_{i1} \quad s_{i2} \quad \cdots \quad s_{ik_i})$ where $s_{ig(k_i)}$ is $c_{i1}, s_{i(g(k_i)+1)}$ is c_{i2}, $\cdots$ (occurs in cyclic order).

(D4) For each $s_{ij} (1 \leq j \leq k_i)$, calculate $y\left(s_{ij}\right) = \frac{2(s_{ij}-1)}{3} + 1$.

(D5) Replacing $y(s_{ij})$ for all $1 \leq j \leq k_i$ by its corresponding alphabet, the required word is obtained.

2.3. Few Exemplifications

Here are two examples for the above given encryption and decryption processes.

Example 2.1. Encrypt and decrypt the message “PRIMES”.

Here we have only one word to process. So $W_1 = PRIMES$.

Encryption:

(E1)

P	R	I	M	E	S
307	381	111	211	43	421

(E2)

n	307	381	111	211	43	421
$f(n)$	460	571	166	316	64	631

(E3) $$M_1 = \begin{pmatrix} 460 & 571 & 166 & 316 & 64 & 631 \\ 571 & 166 & 316 & 64 & 631 & 460 \\ 166 & 316 & 64 & 631 & 460 & 571 \\ 316 & 64 & 631 & 460 & 571 & 166 \\ 64 & 631 & 460 & 571 & 166 & 316 \\ 631 & 460 & 571 & 166 & 316 & 64 \end{pmatrix}$$

(E4) $$n(W_1) = 6$$

(E5) $$g\big(n(W_1)\big) = 3$$

(E6) $$D(R_1) = \begin{pmatrix} 166 & 0 & 0 & 0 & 0 & 0 \\ 0 & 316 & 0 & 0 & 0 & 0 \\ 0 & 0 & 64 & 0 & 0 & 0 \\ 0 & 0 & 0 & 631 & 0 & 0 \\ 0 & 0 & 0 & 0 & 460 & 0 \\ 0 & 0 & 0 & 0 & 0 & 571 \end{pmatrix}$$

(E7) $$D(R_1) - n(W_1)I_{n(W_1)} = \begin{pmatrix} 166 & 0 & 0 & 0 & 0 & 0 \\ 0 & 316 & 0 & 0 & 0 & 0 \\ 0 & 0 & 64 & 0 & 0 & 0 \\ 0 & 0 & 0 & 631 & 0 & 0 \\ 0 & 0 & 0 & 0 & 460 & 0 \\ 0 & 0 & 0 & 0 & 0 & 571 \end{pmatrix} - \begin{pmatrix} 6 & 0 & 0 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 160 & 0 & 0 & 0 & 0 & 0 \\ 0 & 310 & 0 & 0 & 0 & 0 \\ 0 & 0 & 58 & 0 & 0 & 0 \\ 0 & 0 & 0 & 625 & 0 & 0 \\ 0 & 0 & 0 & 0 & 454 & 0 \\ 0 & 0 & 0 & 0 & 0 & 565 \end{pmatrix}$$

The encrypted key is $E_1 = (160 \quad 310 \quad 58 \quad 625 \quad 454 \quad 565)$

Decryption:

Here $k_1 = 6$.

(D1) $C_1 = D(E_1) + k_1 I_{k_1} = (166 \quad 316 \quad 64 \quad 631 \quad 460 \quad 571)$

(D2) $g(k_1) = 3$

(D3) $S_1 = (460 \quad 571 \quad 166 \quad 316 \quad 64 \quad 631)$

	s_{11}	s_{12}	s_{13}	s_{14}	s_{15}	s_{16}
s_{ij}	460	571	166	316	64	631
$y(s_{ij})$	307	381	111	211	43	421

(D4) The required word is “PRIMES”.

Example 2.2. Encrypt and decrypt the message “SHE DRIVES A CAR”.

Encryption: The following table presents the encryption process.

W_i	SHE	DRIVES	A	CAR
(E_1)	• $S = 421$ • $H = 91$ • $E = 43$	• $D = 31$ • $R = 381$ • $I = 111$ • $V = 553$ • $E = 43$ • $S = 421$	• $A = 7$	• $C = 21$ • $A = 7$ • $R = 381$
(E_2)	• $f(421) = 631$ • $f(91) = 136$ • $f(43) = 64$	• $f(31) = 46$ • $f(381) = 571$ • $f(111) = 166$ • $f(553) = 829$ • $f(43) = 64$ • $f(421) = 631$	• $f(7) = 10$	• $f(21) = 31$ • $f(7) = 10$ • $f(381) = 571$
(E_3)	$\begin{pmatrix} 631 & 136 & 64 \\ 136 & 64 & 631 \\ 64 & 631 & 136 \end{pmatrix}$	$\begin{pmatrix} 46 & 571 & 166 & 829 & 64 & 631 \\ 571 & 166 & 829 & 64 & 631 & 46 \\ 166 & 829 & 64 & 631 & 46 & 571 \\ 829 & 64 & 631 & 46 & 571 & 166 \\ 64 & 631 & 46 & 571 & 166 & 829 \\ 631 & 46 & 571 & 166 & 829 & 64 \end{pmatrix}$	(10)	$\begin{pmatrix} 31 & 10 & 571 \\ 10 & 571 & 31 \\ 571 & 31 & 10 \end{pmatrix}$
(E_4)	$n(W_1) = 3$	$n(W_2) = 6$	$n(W_3) = 1$	$n(W_4) = 3$
(E_5)	$g(n(W_1)) = 2$	$g(n(W_2)) = 3$	$g(n(W_3)) = 1$	$g(n(W_4)) = 2$

(E_6)	$\begin{pmatrix}136 & 0 & 0\\ 0 & 64 & 0\\ 0 & 0 & 631\end{pmatrix}$	$\begin{pmatrix}166 & 0 & 0 & 0 & 0 & 0\\ 0 & 829 & 0 & 0 & 0 & 0\\ 0 & 0 & 64 & 0 & 0 & 0\\ 0 & 0 & 0 & 631 & 0 & 0\\ 0 & 0 & 0 & 0 & 46 & 0\\ 0 & 0 & 0 & 0 & 0 & 571\end{pmatrix}$	(10)	$\begin{pmatrix}10 & 0 & 0\\ 0 & 571 & 0\\ 0 & 0 & 31\end{pmatrix}$
(E_7)	$\begin{pmatrix}133 & 0 & 0\\ 0 & 61 & 0\\ 0 & 0 & 628\end{pmatrix}$	$\begin{pmatrix}160 & 0 & 0 & 0 & 0 & 0\\ 0 & 823 & 0 & 0 & 0 & 0\\ 0 & 0 & 58 & 0 & 0 & 0\\ 0 & 0 & 0 & 625 & 0 & 0\\ 0 & 0 & 0 & 0 & 40 & 0\\ 0 & 0 & 0 & 0 & 0 & 565\end{pmatrix}$	(9)	$\begin{pmatrix}7 & 0 & 0\\ 0 & 568 & 0\\ 0 & 0 & 28\end{pmatrix}$
E_i	$(133 \quad 61 \quad 628)$	$(160 \quad 823 \quad 58 \quad 625 \quad 40 \quad 565)$	(9)	$(7 \quad 568 \quad 28)$

Table 2. Encryption for “SHE DRIVES A CAR”

Decryption: The following table presents the decryption process.

E_i	$(133 \quad 61 \quad 628)$	$(160 \quad 823 \quad 58 \quad 625 \quad 40 \quad 565)$	(9)	$(7 \quad 568 \quad 28)$
k_i	$k_1 = 3$	$k_2 = 6$	$k_3 = 1$	$k_4 = 3$
(D_1)	$(136 \quad 64 \quad 631)$	$(166 \quad 829 \quad 64 \quad 631 \quad 46 \quad 571)$	(10)	$(10 \quad 571 \quad 31)$
(D_2)	$g(k_1) = 2$	$g(k_2) = 3$	$g(k_3) = 1$	$g(k_4) = 2$
(D_3)	$(631 \quad 136 \quad 64)$	$(46 \quad 571 \quad 166 \quad 829 \quad 64 \quad 631)$	(10)	$(31 \quad 10 \quad 571)$

(D_4)

	s_{11}	s_{12}	s_{13}
s_{1j}	631	136	64
$y(s_{1j})$	421	91	43

	s_{21}	s_{22}	s_{23}	s_{24}	s_{25}	s_{26}
s_{2j}	46	571	166	829	64	631
$y(s_{2j})$	31	381	111	553	43	421

	s_{31}
s_{3j}	10
$y(s_{3j})$	7

	s_{41}	s_{42}	s_{43}
s_{4j}	31	10	571
$y(s_{4j})$	21	7	381

(D_5)	SHE	DRIVES	A	CAR

Table 3. Decryption for “SHE DRIVES A CAR”

3. R Code for Encryption and Decryption of Words with Four Letters

Code for Encryption

```
Me=readline(prompt="Enter the message:");
print(paste("The message to be encrypted is:", Me))
{
L1 = readline(prompt = "Enter usual position of first letter:");
L1 <- as.integer(L1)
L2 = readline(prompt = "Enter usual position of second letter:");
L2 <- as.integer(L2)
L3 = readline(prompt = "Enter usual position of third letter:");
L3 <- as.integer(L3)
L4 = readline(prompt = "Enter usual position of fourth letter:");
L4 <- as.integer(L4)
}
{
n11=(L1)**2+3*(L1)+3
n11 <- as.integer(n11)
n12=(L2)**2+3*(L2)+3
n12 <- as.integer(n12)
n13=(L3)**2+3*(L3)+3
n13 <- as.integer(n13)
n14=(L4)**2+3*(L4)+3
n14 <- as.integer(n14)
}
f <- function(n) {
if (n %% 2 == 1)
{
print(3*((n-1)/2)+1)
}
else
{
m=4
print(m)
```

Figure 1. Code for encryption

```
}
}
{
n<-c(n11,n12,n13,n14)
t1<-f(n11)
t2<-f(n12)
t3<-f(n13)
t4<-f(n14)
}
cat("The position of letters is \n")
print(n)
cat("After applying f the position becomes \n")
print(c(t1,t2,t3,t4))
cat("The cyclic symmetric matrix is\n")
M = matrix(
m<-c(c(t1,t2,t3,t4),c(t2,t3,t4,t1),c(t3,t4,t1,t2),c(t4,t1,t2,t3)),
nrow = 4,
ncol = 4,
byrow = TRUE
)
print(M)
E1=M[2, ]-4
cat("The encrypted key is:\n")
print(E1)
```

Figure 2. Continuation of figure 1

Sample Output for Encryption

```
[1] "The message to be encrypted is: ROCK"
[1] 571
[1] 409
[1] 31
[1] 235
The position of letters is
[1] 381 273  21 157
After applying f the position becomes
[1] 571 409  31 235
The cyclic symmetric matrix is
     [,1] [,2] [,3] [,4]
[1,]  571  409   31  235
[2,]  409   31  235  571
[3,]   31  235  571  409
[4,]  235  571  409   31
The encrypted key is:
[1] 405  27 231 567
```

Figure 3. Encryption of ROCK

Code for Decryption

```
{
e1 = readline(prompt = "Enter the first position of the encrypted key:");
e1 <- as.integer(e1)
e2 = readline(prompt = "Enter the second position of the encrypted key:");
e2 <- as.integer(e2)
e3 = readline(prompt = "Enter the third position of the encrypted key:");
e3 <- as.integer(e3)
e4 = readline(prompt = "Enter the fourth position of the encrypted key:");
e4 <- as.integer(e4)
}
E<-c(e1,e2,e3,e4)
cat("The encrypted key is\n")
print(E)
s2<-e1+4
s3<-e2+4
s4<-e3+4
s1<-e4+4
S1<-c(s1,s2,s3,s4)
cat("The values of S1 are\n")
print(S1)
y1=(2*(s1-1))/3+1
y2=(2*(s2-1))/3+1
y3=(2*(s3-1))/3+1
y4=(2*(s4-1))/3+1
cat("The values of y are\n")
print(c(y1,y2,y3,y4))
n1<-(sqrt((4*y1)-3)-3)/2
n2<-(sqrt((4*y2)-3)-3)/2
n3<-(sqrt((4*y3)-3)-3)/2
n4<-(sqrt((4*y4)-3)-3)/2
cat("The usual positions of alphabets are\n")
print(c(n1,n2,n3,n4))
#replace these numbers with letters
```

Figure 4. Code for decryption

Output for Decrypting "ROCK"

```
The encrypted key is
[1] 405  27 231 567
The values of S1 are
[1] 571 409  31 235
The values of y are
[1] 381 273  21 157
The usual positions of alphabets are
[1] 18 15  3 11
```

Figure 5. Decryption of ROCK

4. Conclusion

This paper presents encryption and decryption algorithms employing positive integer-valued functions and cyclic symmetric matrices. These algorithms are successfully verified by means of examples and R codes for words with four letters. One may extend those R codes for more than four lettered word. Also, this article paves the way to create new such algorithms by effectively changing the arithmetic functions given here.

References

[1] Dasdemir, A. (2011). On the Pell, Pell- Lucas and modified Pell numbers by matrix method. Applied Mathematical Sciences, 5(64), 3173-3181.

[2] Kannan, J., Mahalakshmi,M., & Deepshika, A. (2022). Cryptographic algorithm involving the matrix Q_p^*. Korean Journal of Mathematics, 30(3), 533-538.

[3] Kannan, J., Manju, S., Mahalakshmi, M., & Raja, K. (2022). Encryption decryption algorithm using solutions of Pell equation. International Journal of Mathematics and Its Applications, 10(1), 1-8.

[4] Taş, N., Uçar, S., Özgür, N.Y., & Kaymak, Ö. Ö. (2018). A new coding/decoding algorithm using Fibonacci numbers. Discrete Mathematics, Algorithms and Applications, 10(2), 1850028.

[5] Thiagarajan, K., Balasubramanian, P., Nagaraj, J., & Padmashree, J. (2018). Encryption and decryption algorithm using algebraic matrix approach. Journal of Physics: Conference series, 1000(1), 012148.

[6] Uçar, S., Taş, N., & Özgür, N.Y. (2019). A new application to coding theory via ibonacci and Lucas numbers. Mathematical Sciences and Applications E-notes, 7(1), 62-70.

[7] Zeriouh, M., Chillali, A., & Boua, A. (2019). Cryptography based on the matrices. Bol.Soc.Paran.Mat, 37(3), 75-83.