Korean J. Math. **30** (2022), No. 3, pp. 533–538
http://dx.doi.org/10.11568/kjm.2022.30.3.533

CRYPTOGRAPHIC ALGORITHM INVOLVING THE MATRIX Q^{p*}

J. Kannan*, M. Mahalakshmi, and A. Deepshika

Abstract. Cryptography is one of the most essential developing areas, which deals with the secure transfer of messages. In recent days, there are more number of algorithms have been evolved to provide better security. This work is also such an attempt. In this paper, an algorithm is presented for encryption and decryption which employs the matrix Q^{p*} and the well- known equation $x^2 - py^2 = 1$ where p is a prime.

1. Introduction

The concept of sharing the messages via a secret medium is an essential one even for common people. This may be seen in our society merely from the evolution of message sharing. The major drawback in the concept of sharing a message is the medium through which we share. So maintaing a strong secret medium is an unavoidable one for not only an individual but also a country. This leads to the development of the area Cryptography [10]. In recent days, researchers developed so many algorithms for encryption and decryption. [3–5, 8] are some examples of encryption and decryption algorithms. Likewise, here is an attempt to encrypt and decrypt messages using the solutions of Pell' s equations.

The Fibonacci relation is given as $F_{n+1} = F_n + F_{n-1}$, $F_0 = 0$ and $F_1 = 1$. With the help of this the Fibonacci Q- matrix was defined as

$$Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

[2]. This matrix has a property that,

$$Q^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

[7]. That is, the n^{th} power of the Fibonacci Q- matrix can be easily found from the terms in Fibonacci relation. There is also some other recurrence relation, for which we can find a matrix like Fibonacci Q- matrix, such that whose power can be easily found from the relation itself [1]. In [4], one such relation is given and the corresponding matrix Q^{3*} is defined using the solution of the Pell equation $x^2 - 3y^2 = 1$. This paper

Received May 13, 2022. Revised September 6, 2022. Accepted September 7, 2022.
2010 Mathematics Subject Classification: 11B37, 11C20, 11D09, 11T71.
Key words and phrases: Cryptography, Q^{p*}, Encryption ,Decryption, Pell's Equation.
* Corresponding author.

is an analog work of [4, 8]. Here we use the Pell equation $x^2 - py^2 = 1$ where p is a prime and the matrix Q^{p*}. In [1, 9] the solutions (x_k, y_k) of the equation $x^2 - py^2 = 1$ are given as

$$x_{k+1} = x_1 x_k + p y_1 y_k$$
$$y_{k+1} = y_1 x_k + x_1 y_k$$

where (x_1, y_1) is the minimal solution. Corresponding these relations the matrix Q^{p*} is defined as

$$Q^{p*} = \begin{pmatrix} x_1 & py_1 \\ y_1 & x_1 \end{pmatrix}$$

Then its k^{th} power is

$$(Q^{p*})^k = \begin{pmatrix} x_k & py_k \\ y_k & x_k \end{pmatrix}$$

[1, 6].

In this paper, we try to encrypt and decrypt the message to be sent using the matrix Q^{p*}. Here the alphabets take their position as in the below mentioned table. The message to be sent is converted into an even order matrix. Then that matrix is divided into blocks of order 2. Using the determinants of each block and their entries, we encrpt the given message as a matrix. Based on the number of blocks the prime p is determined. For the decryption process, we make use of the matrix Q^{p*} and the encrypted matrix.

In this paper, initially encryption and decryption algorithms are displayed along with its own examples. Later, a common example is provided for the entire process.

Notations and Choices

- B - an even order matrix formed by the given message.
- B_j - j^{th} block of B whose size is 2.
- b - number of blocks of B.
- Choose $k = \begin{cases} b \ if \ b \leq p \\ p \ if \ b > p \end{cases}$
- p can be chosen as $\begin{cases} 2 \text{ if } b \text{ is 1 or even} \\ \text{smallest prime which divides } b \text{ if } b \text{ is odd other than 1} \end{cases}$
- d_j - determinant of B_j
- The elements of B_j are given by $\begin{pmatrix} b_{j1} & b_{j2} \\ b_{j3} & b_{j4} \end{pmatrix}$
- E is an encrypted matrix given by, $E = [\ d_j, b_{jk}]\ _{k=1,2,4}$
- The elements of $(Q^{p^*})^k$ are given by $\begin{pmatrix} q_1 & q_2 \\ q_3 & q_4 \end{pmatrix}$
- θ - notation for space

Position of Characters

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

2. Encryption Algorithm

1. First we have to construct the matrix B of even order for the given message.
2. Next divide the matrix into blocks B_j of size 2 and find b.
3. Choose k using b and p.
4. For finding p, we have two cases as given above.
5. Find the elements of B_j using the assigned member instead of characters.
6. Find the determinants d_j.
7. Finally, we construct E.

Example

Here we discuss example for $b = 1$

Consider the word ZOO which is to be encrypted.

- Here $B = \begin{pmatrix} Z & O \\ O & \theta \end{pmatrix}$. Since there is only one block, $b = 1$
- And $p = 2 > b \implies$ choose $k = b(\ 1) \implies k = 1$
- Hence $B = \begin{pmatrix} 26 & 15 \\ 15 & 0 \end{pmatrix}$
- The determinant is $d_1 = \begin{vmatrix} 26 & 15 \\ 15 & 0 \end{vmatrix} = -225$
- The encrypted matrix is obtained as $E = (\ -225\ 26\ 15\ 0)$

3. Decryption Algorithm

1. Using encrypted matrix, find B.
2. Find the matrix $(Q^{p^*})^k$
3. We have the elements of $(Q^{p^*})^k$ as $q_j^{'}s$.
4. Find $e_{j1} = q_1 b_{j1} + q_3 b_{j2}$ and $e_{j2} = q_2 b_{j1} + q_4 b_{j2}$
5. Solve $d_j = e_{j1}(\ q_2 t_j + q_4 b_{j4}) - e_{j2}(\ q_1 t_j + q_3 b_{j4})$ for t_j.
6. Next substitute b_{j3} instead of t_j.
7. Finally, we construct B_j and B.

Example

- For $p = 2$ and $k = 1$, we have $(\ Q^{2*})^1 = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$. Here $q_1 = 3, q_2 = 4, q_3 = 2, q_4 = 3$

- Putting $j = 1$, we get $e_{11} = q_1 b_{11} + q_3 b_{12} = 3(\ 26) + 2(\ 15) = 108$
- Putting $j = 2$, we get $e_{12} = q_2 b_{11} + q_4 b_{12} = 4(\ 26) + 3(\ 18) = 149$
- Solving the equation $d_1 = e_{11}(\ q_2 t_1 + q_4 b_{14}) - e_{12}(\ q_1 t_1 + q_3 b_{14})$, we obtain $d_1 = -225 \implies t_1 = 15$
- Hence $B_1 = \begin{pmatrix} 26 & 15 \\ 15 & 0 \end{pmatrix}$
- Thus $B = \begin{pmatrix} z & o \\ o & \theta \end{pmatrix}$

4. An Another Illustration

Here we discuss example for $b = 4$
Word : **TOPOLOGY**
Encryption:

- Here $B = \begin{pmatrix} T & O & P & O \\ L & O & G & Y \\ \theta & \theta & \theta & \theta \\ \theta & \theta & \theta & \theta \end{pmatrix}$. Since there is 4 blocks, $b = 4$
- And $p = 2 < b \implies$ choose $k = 2$
- $B_1 = \begin{pmatrix} 23 & 18 \\ 15 & 18 \end{pmatrix}$, $B_2 = \begin{pmatrix} 19 & 18 \\ 10 & 28 \end{pmatrix}$, $B_3 = \begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix}$, $B_1 = \begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix}$
- The determinants are $d_1 = 144, d_2 = 352, d_3 = 0, d_4 = 0$
- The encrypted matrix is obtained as $E = \begin{pmatrix} 144 & 23 & 18 & 18 \\ 352 & 19 & 18 & 28 \\ 0 & 3 & 3 & 3 \\ 0 & 3 & 3 & 3 \end{pmatrix}$.

Decryption:

- Using the Q^{p*} matrix, we have $(\ Q^{2*})^2 = \begin{pmatrix} 17 & 24 \\ 12 & 17 \end{pmatrix}$. Here $q_1 = 17, q_2 = 24, q_3 = 12, q_4 = 17$
- By simple calculation, we obtain $e_{11} = 607, e_{21} = 539, e_{31} = 87, e_{41} = 87, e_{12} = 858, e_{22} = 762, e_{32} = 123$ and $e_{42} = 123$
- As in the above example, here we have $t_1 = 15, t_2 = 10, t_3 = 3$ and $t_4 = 3$
- Hence $B_1 = \begin{pmatrix} 23 & 18 \\ 15 & 18 \end{pmatrix}$, $B_2 = \begin{pmatrix} 19 & 18 \\ 10 & 28 \end{pmatrix}$, $B_3 = \begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix}$ and $B_4 = \begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix}$

- Thus $B = \begin{pmatrix} T & O & P & O \\ L & O & G & Y \\ \theta & \theta & \theta & \theta \\ \theta & \theta & \theta & \theta \end{pmatrix}$.

5. Conclusion

In this paper, using the solutions of the Pell equation $x^2 - py^2 = 1$, the matrix Q^{p*} is defined. With this matrix, we develop decryption algorithm. Here a text is converted into a matrix of even order and then divide that into blocks of size 2. Value of p increases if the message to be sent is large. If so, the entries of Q^{p*} becomes larger. One may consider some other recurrence relations which leads to some matrix like Q^{p*}, for the further development of this work.

References

[1] Andreescu, T., Andrica, D., and Cucurezeanu, I, *An Introduction to Diophantine Equations a Problem- Based Approach*, Birkhauser Boston, 2010.

[2] Gould, H. W, *A history of the Fibonacci Q-matrix and a higher-dimensional problem*, Fibonacci Quart, **19**(3) (1981), 250–257.

[3] J. Kannan, Manju Somanath, M. Mahalakshmi and K. Raja, *Remodeled RSA Algorithm for Messages of Length Two Employing G- Primes*, International Journal of Mathematics and Computer Research, **10**(2)(2022), 2555–2558.

[4] J. Kannan, Manju Somanath, M. Mahalakshmi and K. Raja, *Encryption Decryption Algorithm Using Solutions of Pell Equation*, International Journal of Mathematics and its Applications, **10**(1) (2022), 1–8.

[5] M. Mahalakshmi, J. Kannan, Manju Somanath, K. Raja, and K. Kaleeswari,*Cryptographic Algorithm Based on Prime Assignment*, International Journal for Research in Applied Science & Engineering Technology, **10**(1) (2022),1744–1751, DOI: 10.22214/ijraset.2022.40138.

[6] Manju Somanath, K. Raja, J. Kannan and M. Mahalakshmi,*On a Class of Solutions for a Quadratic Diophantine Equation*, Advances and Applications in Mathematical Sciences, **19**(11) (2020),1097–1103.

[7] Sumeyra, U. C. A. R., Nihal, T. A. S., & Ozgur, N. Y,*A new application to coding theory via Fibonacci and Lucas numbers*, Mathematical Sciences and Applications E-Notes, **7**(1) (2019), 62–70.

[8] Tas, N., Ucar, S., Ozgur, N. Y., & Kaymak, O. O, *A new coding/decoding algorithm using Fibonacci numbers*, Discrete Mathematics, Algorithms and Applications, **10**(02) (2018), 1850028.

[9] Tekcan, A, *Continued fractions expansion of*$\sqrt{D}$ *and Pell equation* $x^2 - Dy^2 = 1$. Mathematica Moravica, **15**(2)(2011), 19–27.

[10] Trappe, W., & Washington, L. C, *Introduction to Cryptography*. Prentice Hall, 2006.

J. Kannan
Assistant Professor
Department of Mathematics, Ayya Nadar Janaki Ammal College
(Autonomous, affiliated to Madurai Kamaraj University, Madurai)
Sivakasi - 626 124, Tamil Nadu, Inida
E-mail: jayram.kannan@gmail.com

M. Mahalakshmi
Full Time Ph.D. Research Scholar
Department of Mathematics, Ayya Nadar Janaki Ammal College
(Autonomous, affiliated to Madurai Kamaraj University, Madurai)
Sivakasi - 626 124, Tamil Nadu, Inida
E-mail: maha1607laksmi@gmail.com

A. Deepshika
Post Graduate Student
Department of Mathematics, Ayya Nadar Janaki Ammal College
(Autonomous, affiliated to Madurai Kamaraj University, Madurai)
Sivakasi - 626 124, Tamil Nadu, Inida
E-mail: deepshi20mar@gmail.com