Int. J. Math. And Appl., 10(1)(2022), 1–8
ISSN: 2347-1557
Available Online: http://ijmaa.in/

International Journal of *Mathematics And its Applications*

Encryption Decryption Algorithm Using Solutions of Pell Equation

J. Kannan[1,*], Manju Somanath[2], M. Mahalakshmi[1] and K. Raja[2]

1 Department of Mathematics, Ayya Nadar Janaki Ammal College (Autonomous, Affiliated to Madurai Kamaraj University, Madurai), Sivakasi, Tamil Nadu, India.

2 Department of Mathematics, National College (Autonomous, Affiliated to Bharathidasan University, Trichy), Trichy, Tamil Nadu, India.

Abstract: Cryptography is a concept of protecting information and conversations which are transmitted through a public source, so that the intended persons only read and process it. There are several encryption and decryption algorithm which involves mathematical concepts to provide more security to the text which has to be shared through a medium. In this paper, the algorithm is written on the basis of the Pell equation $x^2 - 3y^2 = 1$ whose solutions are given by the recurrence relations from which the matrix Q^{3*} is defined. The central theme is to convert the taken message into a matrix of even size which is later divided into blocks.

MSC: 11B37, 11C20, 11D09, 11T71.

Keywords: Pell equation, Encryption-decryption algorithm, Q^{3*} matrix, Cryptography.

1. Introduction

There are so many encryption and decryption algorithms using number theoretical concepts for increasing the security of the messages to be sent. Here is another such algorithm which uses recurrence relations for decryption. In [10, 11], the concept was built with the usage of Fibonacci Q-matrix which was defined in [3]. Employing this technique with new matrix (which is named as (Q^{3*})) this paper is processed. For that purpose, consider the Pell equation $x^2 - 3y^2 = 1$. The solutions of this equation are obtained in [1] which was motivated from [4]. There defined a recurrence relation for its solutions as

$$x_{n+1} = 2x_n + 3y_n$$

$$y_{n+1} = x_n + 2y_n$$

for $n \geq 1$, where $x_1 = 2,\ y_1 = 1$. It is noted that $(Q^{3*}) = \begin{pmatrix} x_k & 3y_k \\ y_k & x_k \end{pmatrix}$.

This paper displays an encryption and decryption algorithm and provide some examples regarding that. The main idea is converting the message into block matrices of order 2×2. Based on the number of blocks, the position of alphabets are to be defined. Then by using some terms, the encrypted matrix E is obtained.For decryption, (Q^{3*}) is used.

* *E-mail: jayram.kannan@gmail.com*

1.1. Notations

1. B – an even order matrix formed by the message to be sent.
2. B_i – i^{th}block of B whose size is 2.
3. b – No. of blocks B_i of B
4. $n = \begin{cases} 3 \ if \ b \leq 3 \\ b \ if \ b > 3 \end{cases}$
5. d_i – determinant of B_i
6. The elements ofB_i are defined as $\begin{pmatrix} b_{i1} & b_{i2} \\ b_{i3} & b_{i4} \end{pmatrix}$
7. E – encrypted matrix defined by $E = [d_i, b_{\text{ik}}]_{k\in\{1,2,4\}}$
8. The elements of $\left(Q^{3*}\right)^n$are defined as $\begin{pmatrix} q_1 & q_2 \\ q_3 & q_4 \end{pmatrix}$
9. θ – notation for space

1.2. Position of characters

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

1.3. Encryption Algorithm

1. Construct the matrix $B$of even order for the given text.
2. Divide it into blocks $B_i$of size 2 and find b.
3. Choose n using b.
4. Identify the elements of B_i by replacing letters with assigned numbers.
5. Find d_i.
6. Construct E.

1.4. Decryption Algorithm

Using E, one have to find B. The idea is to find b_{i3} as Econtains b_{i1}, b_{i2}, b_{i4}.

1. Find $\left(Q^{3*}\right)^n$

2. Identify its elements as $q_j's$.

3. Find $e_{i1} = q_1 b_{i1} + q_3 b_{i2}$

4. Find $e_{i2} = q_2 b_{i1} + q_4 b_{i2}$

5. Solve $d_i = e_{i1}\left(q_2 t_i + q_4 b_{i4}\right) - e_{i2}\left(q_1 t_i + q_3 b_{i4}\right)$ for t_i

6. Substitute $t_i = b_{i3}$

7. Construct B_i

8. Construct B

2. Encryption Decryption Algorithm Using (x, y) such that $x^2 - 3y^2 = 1$

Now, let us see some examples for the cases $b = 1, 4, 9$.

Some solutions of the Pell equation $\mathbf{x^2 - 3y^2 = 1}$ are given as below:

k	1	2	3	4	5	6	7	8	9
x_k	2	7	26	97	362	1351	5042	18817	70226
y_k	1	4	15	56	209	780	2911	10864	40545

Example 2.1. *The message to be encrypted is " TAKE "*

Encryption:

1. $B = \begin{pmatrix} T & A \\ K & E \end{pmatrix}$

2. *Here there is only one block. So* $B_1 = \begin{pmatrix} T & A \\ K & E \end{pmatrix}$ *and* $b = 1$

3. *Choose* $n = 3$

4. *Thus* $B_1 = \begin{pmatrix} 22 & 3 \\ 13 & 7 \end{pmatrix}$ *and so* $b_{11} = 22, b_{12} = 3, b_{13} = 13,\ b_{14} = 7$

5. $d_1 = \begin{vmatrix} 22 & 3 \\ 13 & 7 \end{vmatrix} = 115$

6. $E = \begin{pmatrix} 115 & 22 & 3 & 7 \end{pmatrix}$

Decryption:

1. $\left(Q^{3*}\right)^3 = \begin{pmatrix} x_3 & 3y_3 \\ y_3 & x_3 \end{pmatrix} = \begin{pmatrix} 26 & 45 \\ 15 & 26 \end{pmatrix}$

2. $q_1 = 26, q_2 = 45, q_3 = 15, q_4 = 26$

3. $e_{11} = q_1 b_{11} + q_3 b_{12} = 26\,(22) + 15\,(3) = 617$

4. $e_{12} = q_2 b_{11} + q_4 b_{12} = 45\,(22) + 26\,(3) = 1068$

5. $d_1 = e_{11}(q_2 t_1 + q_4 b_{14}) - e_{12}(q_1 t_1 + q_3 b_{14})$

   $115 = 617(45t_1 + 182) - 1068(26t_1 + 105)$

   $t_1 = 13$

6. $b_{13} = t_1 = 13$

7. *Thus* $B_1 = \begin{pmatrix} 22 & 3 \\ 13 & 7 \end{pmatrix}$ *from* E.

8. *Hence* $B = \begin{pmatrix} T & A \\ K & E \end{pmatrix}$

Example 2.2. *The message to be encrypted is " HAVE A NICE DAY "*

Encryption:

1. $B = \begin{pmatrix} H & A & V & E \\ \theta & A & \theta & N \\ I & C & E & \theta \\ D & A & Y & \theta \end{pmatrix}$

2. *Here there are four blocks. So* $B_1 = \begin{pmatrix} H & A \\ \theta & A \end{pmatrix}$, $B_2 = \begin{pmatrix} V & E \\ \theta & N \end{pmatrix}$, $B_3 = \begin{pmatrix} I & C \\ D & A \end{pmatrix}$, $B_4 = \begin{pmatrix} E & \theta \\ Y & \theta \end{pmatrix}$ *and* $b = 4$

3. *Choose* $n = 4$

4. *Thus* $B_1 = \begin{pmatrix} 11 & 4 \\ 3 & 4 \end{pmatrix}$, $B_2 = \begin{pmatrix} 25 & 8 \\ 3 & 17 \end{pmatrix}$, $B_3 = \begin{pmatrix} 12 & 6 \\ 7 & 4 \end{pmatrix}$, $B_4 = \begin{pmatrix} 8 & 3 \\ 28 & 3 \end{pmatrix}$ *and so*

$i=1$	$\mathbf{b_{11}}$	$\mathbf{b_{12}}$	$\mathbf{b_{13}}$	$\mathbf{b_{14}}$
$i=1$	*11*	*4*	*3*	*4*
$i=2$	$\mathbf{b_{21}}$	$\mathbf{b_{22}}$	$\mathbf{b_{23}}$	$\mathbf{b_{24}}$
$i=2$	*25*	*8*	*3*	*17*
$i=3$	$\mathbf{b_{31}}$	$\mathbf{b_{32}}$	$\mathbf{b_{33}}$	$\mathbf{b_{34}}$
$i=3$	*12*	*6*	*7*	*4*
$i=4$	$\mathbf{b_{41}}$	$\mathbf{b_{42}}$	$\mathbf{b_{43}}$	$\mathbf{b_{44}}$
$i=4$	*8*	*3*	*28*	*3*

5. *Values of* d_i

i	*1*	*2*	*3*	*4*
$\mathbf{d_i}$	*32*	*401*	*6*	*-60*

6. $E = \begin{pmatrix} 32 & 11 & 4 & 4 \\ 401 & 25 & 8 & 17 \\ 6 & 12 & 6 & 4 \\ -60 & 8 & 3 & 3 \end{pmatrix}$

Decryption:

1. $\left(Q^{3*}\right)^4 = \begin{pmatrix} x_4 & 3y_4 \\ y_4 & x_4 \end{pmatrix} = \begin{pmatrix} 97 & 168 \\ 56 & 97 \end{pmatrix}$

2. $q_1 = 97, q_2 = 168, q_3 = 56, q_4 = 97$

3. *Value of* $e_{11}, e_{21}, e_{31}, e_{41}$

e_{11}	*1291*
e_{21}	*2873*
e_{31}	*1500*
e_{41}	*944*

4. $e_{12} = 2236, e_{22} = 4976, e_{32} = 2598, e_{42} = 1635$

e_{12}	*2236*
e_{22}	*4976*
e_{32}	*2598*
e_{42}	*1635*

5. *Solving the equations* $d_i = e_{i1}\left(q_2 t_i + q_4 b_{i4}\right) - e_{i2}\left(q_1 t_i + q_3 b_{i4}\right)$*, one can get*

$$t_1 = 3, t_2 = 3, t_3 = 7, t_4 = 28$$

6. $b_{13} = t_1 = 3,\ b_{23} = t_2 = 3,\ b_{33} = t_3 = 7,\ b_{43} = t_4 = 28.$

7. *Thus* $B_1 = \begin{pmatrix} 11 & 4 \\ 3 & 4 \end{pmatrix}, B_2 = \begin{pmatrix} 25 & 8 \\ 3 & 17 \end{pmatrix}, B_3 = \begin{pmatrix} 12 & 6 \\ 7 & 4 \end{pmatrix}, B_4 = \begin{pmatrix} 8 & 3 \\ 28 & 3 \end{pmatrix}$ *from E.*

8. *Hence* $B = \begin{pmatrix} H & A & V & E \\ \theta & A & \theta & N \\ I & C & E & \theta \\ D & A & Y & \theta \end{pmatrix}$

Example 2.3. *The message to be encrypted is " THE SUN RISES IN THE EAST "*

Encryption:

1. $B = \begin{pmatrix} T & H & E & \theta & S & U \\ N & \theta & R & I & S & E \\ S & \theta & I & N & \theta & T \\ H & E & \theta & E & A & S \\ T & \theta & \theta & \theta & \theta & \theta \\ \theta & \theta & \theta & \theta & \theta & \theta \end{pmatrix}$

2. *Here there are nine blocks. So* $B_1 = \begin{pmatrix} T & H \\ N & \theta \end{pmatrix}, B_2 = \begin{pmatrix} E & \theta \\ R & I \end{pmatrix}, B_3 = \begin{pmatrix} S & U \\ S & E \end{pmatrix}, B_4 = \begin{pmatrix} S & \theta \\ H & E \end{pmatrix}, B_5 = \begin{pmatrix} I & N \\ \theta & E \end{pmatrix},$
$B_6 = \begin{pmatrix} \theta & T \\ A & S \end{pmatrix}, B_7 = \begin{pmatrix} T & \theta \\ \theta & \theta \end{pmatrix}, B_8 = \begin{pmatrix} \theta & \theta \\ \theta & \theta \end{pmatrix}, B_9 = \begin{pmatrix} \theta & \theta \\ \theta & \theta \end{pmatrix}$ *and* $b = 9$

3. *Choose* $n = 9$

4. *Thus* $B_1 = \begin{pmatrix} 28 & 16 \\ 22 & 8 \end{pmatrix}, B_2 = \begin{pmatrix} 13 & 8 \\ 26 & 17 \end{pmatrix}, B_3 = \begin{pmatrix} 27 & 29 \\ 27 & 13 \end{pmatrix}, B_4 = \begin{pmatrix} 27 & 8 \\ 16 & 13 \end{pmatrix}, B_5 = \begin{pmatrix} 17 & 22 \\ 8 & 13 \end{pmatrix}, B_6 = \begin{pmatrix} 8 & 28 \\ 9 & 27 \end{pmatrix}, B_7 = \begin{pmatrix} 28 & 8 \\ 8 & 8 \end{pmatrix}, B_8 = \begin{pmatrix} 8 & 8 \\ 8 & 8 \end{pmatrix}, B_9 = \begin{pmatrix} 8 & 8 \\ 8 & 8 \end{pmatrix}$ *and so*

$i=1$	$\mathbf{b_{11}}$	$\mathbf{b_{12}}$	$\mathbf{b_{13}}$	$\mathbf{b_{14}}$
$i=1$	*28*	*16*	*22*	*8*
$i=2$	$\mathbf{b_{21}}$	$\mathbf{b_{22}}$	$\mathbf{b_{23}}$	$\mathbf{b_{24}}$
$i=2$	*13*	*8*	*26*	*17*
$i=3$	$\mathbf{b_{31}}$	$\mathbf{b_{32}}$	$\mathbf{b_{33}}$	$\mathbf{b_{34}}$
$i=3$	*27*	*29*	*27*	*13*
$i=4$	$\mathbf{b_{41}}$	$\mathbf{b_{42}}$	$\mathbf{b_{43}}$	$\mathbf{b_{44}}$
$i=4$	*27*	*8*	*16*	*13*
$i=5$	$\mathbf{b_{51}}$	$\mathbf{b_{52}}$	$\mathbf{b_{53}}$	$\mathbf{b_{54}}$
$i=5$	*17*	*22*	*8*	*13*
$i=6$	$\mathbf{b_{61}}$	$\mathbf{b_{62}}$	$\mathbf{b_{63}}$	$\mathbf{b_{64}}$
$i=6$	*8*	*28*	*9*	*27*
$i=7$	$\mathbf{b_{71}}$	$\mathbf{b_{72}}$	$\mathbf{b_{73}}$	$\mathbf{b_{74}}$
$i=7$	*28*	*8*	*8*	*8*
$i=8$	$\mathbf{b_{81}}$	$\mathbf{b_{82}}$	$\mathbf{b_{83}}$	$\mathbf{b_{84}}$
$i=8$	*8*	*8*	*8*	*8*
$i=9$	$\mathbf{b_{91}}$	$\mathbf{b_{92}}$	$\mathbf{b_{93}}$	$\mathbf{b_{94}}$
$i=9$	*8*	*8*	*8*	*8*

5. *The determinants are found as*

i	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
d_i	*-128*	*13*	*-432*	*223*	*45*	*-36*	*160*	*0*	*0*

6. $E = \begin{pmatrix} -128 & 28 & 16 & 8 \\ 13 & 13 & 8 & 17 \\ -432 & 27 & 29 & 13 \\ 223 & 27 & 8 & 13 \\ 45 & 17 & 22 & 13 \\ -36 & 8 & 28 & 27 \\ 160 & 28 & 8 & 8 \\ 0 & 8 & 8 & 8 \\ 0 & 8 & 8 & 8 \end{pmatrix}$

Decryption:

1. $\left(Q^{3*}\right)^9 = \begin{pmatrix} x_9 & 3y_9 \\ y_9 & x_9 \end{pmatrix} = \begin{pmatrix} 70226 & 121635 \\ 40545 & 70226 \end{pmatrix}$

2. $q_1 = 70226, q_2 = 121635, q_3 = 40545, q_4 = 70226$

3.

e_{11}	e_{21}	e_{31}	e_{41}	e_{51}	e_{61}	e_{71}	e_{81}	e_{91}
2615048	1237298	3071907	2220462	2085832	1697068	2290688	886168	886168

4. $e_{12} = 2236, e_{22} = 4976, e_{32} = 2598, e_{42} = 1635$

e_{11}	e_{21}	e_{31}	e_{41}	e_{51}	e_{61}	e_{71}	e_{81}	e_{91}
4529396	2143063	5320699	3845953	3612767	2939408	3967588	1534888	1534888

5. *Solving the equations* $d_i = e_{i1}(q_2 t_i + q_4 b_{i4}) - e_{i2}(q_1 t_i + q_3 b_{i4})$, *one can get*

$$t_1 = 22, t_2 = 26, t_3 = 27, t_4 = 16, t_5 = 8, t_6 = 9, t_7 = 8, t_8 = 8, t_9 = 8$$

6. $b_{13} = t_1 = 13$

$b_{23} = t_2 = 26$

$b_{33} = t_3 = 27$

$b_{43} = t_4 = 16$

$b_{53} = t_5 = 8$

$b_{63} = t_6 = 9$

$b_{73} = t_7 = 8$

$b_{83} = t_8 = 8$

$b_{93} = t_9 = 8$

7. *Thus* $B_1 = \begin{pmatrix} 28 & 16 \\ 22 & 8 \end{pmatrix}, B_2 = \begin{pmatrix} 13 & 8 \\ 26 & 17 \end{pmatrix}, B_3 = \begin{pmatrix} 27 & 29 \\ 27 & 13 \end{pmatrix}, B_4 = \begin{pmatrix} 27 & 8 \\ 16 & 13 \end{pmatrix}, B_5 = \begin{pmatrix} 17 & 22 \\ 8 & 13 \end{pmatrix}, B_6 = \begin{pmatrix} 8 & 28 \\ 9 & 27 \end{pmatrix}$,
$B_7 = \begin{pmatrix} 28 & 8 \\ 8 & 8 \end{pmatrix}, B_8 = \begin{pmatrix} 8 & 8 \\ 8 & 8 \end{pmatrix}, B_9 = \begin{pmatrix} 8 & 8 \\ 8 & 8 \end{pmatrix}$ *from* E.

8. *Hence* $B = \begin{pmatrix} T & H & E & \theta & S & U \\ N & \theta & R & I & S & E \\ S & \theta & I & N & \theta & T \\ H & E & \theta & E & A & S \\ T & \theta & \theta & \theta & \theta & \theta \\ \theta & \theta & \theta & \theta & \theta & \theta \end{pmatrix}$

3. Conclusion

In this paper, using the solutions of the Pell equation $x^2 - 3y^2 = 1$, the matrix Q^{3*} is defined. This play its role in the decryption phase. The main theme is to convert the message into a single matrix of even order and then into blocks of size 2. The strong secrecy depends on the fact that the entries of Q^{3*} becomes much larger and larger. One may consider another Pell equation of the form $x^2 - Dy^2 = 1$ and determine Q^{D*}. Using that some other algorithms also be developed.

References

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

[2] C. J. R. Berges, *A history of the Fibonacci* $Q-$*matrix and a higher-dimensional problem*, Fibonacci Quart, 19(3)(1981), 250-257.

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

[4] 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.

[5] Manju Somanath, K. Raja, J. Kannan and B. Jeyashree, *Non Trivial Integral Solutions of Ternary Quadratic Diophantine Equation*, Advances and Applications in Mathematical Sciences, 19(11)(2020), 1105-1112.

[6] Manju Somanath and J. Kannan, *On a Class of Solutions for a Diophantine Equation of Second Degree*, International Journal of Pure and Applied Mathematics, 117(2)(2017), 55-62.

[7] Manju Somanath and J. Kannan, *Congruum Problem*, International Journal of Pure and Applied Mathematical Sciences, 9(2)(2016), 123-131.

[8] Manju Somanath, J. Kannan and K. Raja, *Congruum Problem*, International Journal of Pure and Applied Mathematical Sciences, 9(2)(2016), 123-131.

[9] Manju Somanath and J. Kannan, *Lattice Points of an Infinite Cone* $x^2 + y^2 = (\alpha^{2n} + \beta^{2n})z^2$, International Journal of Mathematical Trends and Technology, 38(2)(2016), 95-98.

[10] N. Tas, S. Uçar, N. Y. Ozgur, and O. O. Kaymak, *A new coding/decoding algorithm using Fibonacci numbers*, Discrete Mathematics, Algorithms and Applications, 10(2)(2018), 1850028.

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

[12] W. Trappe and L. C. Washington, *Introduction to Cryptography*, Prentice Hall, (2006).