Journal of Indian Acad. Math. ISSN: 0970-5120
Vol. 48, No. 1 (2026) pp. 16–22.

CRYPTOGRAPHIC ALGORITHM BASED ON GENERALIZED PELL EQUATION INVOLVING SPHENIC NUMBERS

J. Kannan[1*], K. Kaleeswari[2], and A. Deepshika[3]

Abstract. One of the key components for the secure transmission of messages is cryptography. Strong algorithms are now required in order to convey a message to another person. For encryption and decryption, modern academics use several mathematical ideas, most notably number theory. In this study, we developed a method that fixes d as a prime integer and n as the square of the sphenic numbers, utilizing the well-known generalized Pell equation as $x^2 - dy^2 = n$.

Keywords: encryption, decryption, the matrix Q^{p*}, generalized Pell equation, Sphenic numbers.

2010 AMS Subject Classification: 11A05, 11A07, 11B37, 11D09, 11D99.

1. Introduction

Number theory - a basket of properties of numbers, especially integers, is one of the most widely used and most attractive theories in Mathematics. It is more advantageous subject to master because it encompasses a variety of elements. The creation of Diophantine equations is one example. These equations are polynomial equations with integer coefficients and two or more unknowns such that the only solutions of interest are the integer ones.

Diophantine analysis, the mathematical study of Diophantine problems, comprises of a special type of equation, commonly known as Pell equation [1]. It is one among the various Diophantine equations and it takes the form

$$x^2 - dy^2 = 1 \tag{1}$$

where d is a fixed positive integer, not a perfect square. It also has been proved that equation (1) has infinitely many solutions in positive integers. This Pell equation is generalized as

$$x^2 - dy^2 = n \tag{2}$$

for some integer n.

Let p be a prime and (x_k, y_k) be positive integer solutions of the equation $x^2 - py^2 = 1$. Using these solutions we can define the matrix Q^{p*} as $Q^{p*} = \begin{pmatrix} x_1 & py_1 \\ y_1 & x_1 \end{pmatrix}$ [3]. The speciality of this matrix is its k^{th} power can be obtained directly from the k^{th} solution (x_k, y_k) of equation $x^2 - py^2 = 1$. That is, $(Q^{p*})^k = \begin{pmatrix} x_k & py_k \\ y_k & x_k \end{pmatrix}$.

In this paper, we construct a similar matrix $Q_a^{p*} = \begin{pmatrix} x_1 & py_1 \\ y_1 & x_1 \end{pmatrix}$ for the equation $x_1^2 - py_1^2 = a^2$, where $a \in \mathbb{Z}$. The r^{th} power of this matrix is $(Q_a^{p*})^r = a^{r-1}\begin{pmatrix} x_r & py_r \\ y_r & x_r \end{pmatrix}$ where (x_r, y_r) is a positive integer solution of $x^2 - py^2 = a^2$.

In [3], an encryption and decryption algorithms are developed using the Pell equation $x^2 - py^2 = 1$ and its corresponding matrix Q^{p*}. Likewise, in this work, we deal with the same algorithm with little modifications but we employ the generalized Pell equation $x^2 - py^2 = a^2$ and its corresponding matrix Q_a^{p*}. In particular, here we restrict a as a Sphenic number, a number which is a product of three distinct primes. The algorithm is made more secure by the sphenic number that is employed here. In this work, we made several modifications to the algorithm. The table below shows the differences between the suggested method and the current approach.

Proposed method	Existing method
Cryptographic Algorithm Based on Generalized Pell Equation involving Sphenic numbers	Cryptographic algorithm involving the matrix Q^{p*}[3]
In this algorithm, we uses the generalized Pell equation $x^2 - dy^2 = a^2$ where x, y are integers, d as non square positive integer and a is the sphenic number	Here the authors use the Pell equation $x^2 - dy^2 = 1$ where x, y are integers , d as a non square positive integer
We use the $(Q_q^{p*})^r = a^{r-1}\begin{pmatrix} x_r & p_r \\ y_r & x_r \end{pmatrix}$ for decryption	We use the $(Q_q^{p*})^r = \begin{pmatrix} x_r & p_r \\ y_r & x_r \end{pmatrix}$ for decryption

2. Notations

In this section, we display the notations and position of characters needed for the encryption and decryption.

- $\mathbb{B}$ - $2n \times 2n$ matrix which is constructed using the given message.
- $\mathbb{B}_k$ - k^{th} block of $\mathbb{B}$ with the size 2 (ie, 2×2 matrix).
- b - number of blocks of the matrix $\mathbb{B}$.
- $p = \begin{cases} 2 & if\ b\ is\ 1\ or\ 2n\ (n \in \mathbb{N}) \\ smallest\ prime\ divides\ b & if\ b\ is\ 2n+1 (n \in \mathbb{N}) \end{cases}$
- $r = \begin{cases} b & if\ b \leq p \\ p & if\ b > p \end{cases}$
- d_k - determinant of the matrix $\mathbb{B}_k$.
- $\begin{pmatrix} b_{k1} & b_{k2} \\ b_{k3} & b_{k4} \end{pmatrix}$- elements of $\mathbb{B}_k$
- $\mathbb{E}$=$[d_k, b_{ki}]_{i=1,2,4}$ - encrypted matrix.

- $\begin{pmatrix} q_1 & q_2 \\ q_3 & q_4 \end{pmatrix}$ - elements of $(Q_a^{p^*})^r$
- δ -notation for space.
- (x, y) - Positive integer solutions of $x^2 - py^2 = a^2$
- a - Sphenic number

2.1. **Character's Position.**

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

3. ALGORITHM

In this section, we present the encryption and decryption algorithms.

3.1. **Encryption.**

(1) Using the given text we have to construct the matrix $\mathbb{B}$ of order $2n \times 2n$.
(2) Convert the matrix $\mathbb{B}$ into the block matrix $\mathbb{B}_k$ of the order 2×2.
(3) Finding the number of blocks b and select r using p and b.
(4) p can be choosen in two ways as given above.
(5) Choose any Sphenic number a.
(6) Instead of using the characters in $\mathbb{B}_k$ we apply their positions using the above table to find the elements of $\mathbb{B}_k$.
(7) Find the determinant d_k of the matrix $\mathbb{B}_k$.
(8) Using the elements of $\mathbb{B}_k$ and their determinant we construct $\mathbb{E}$.

3.2. **Decryption.** Using the encrypted matrix $\mathbb{E}$ we have to decrypt.

(1) Construct the $(Q_a^{p^*})^r$.
(2) We have the elements of $(Q_a^{p^*})^r$ as $q_k's$.
(3) Find ω_{k1} and ω_{k2}, where $\omega_{k1} = q_1b_{k1} + q_3b_{k2}$,$\omega_{k2} = q_2b_{k2} + q_4b_{k2}$.
(4) Solve for t_k using $a^{2r}d_k = \omega_{k1}(q_2t_k + q_4b_{k4}) - \omega_{k2}(q_1t_k + q_3b_{k4})$.
(5) Now substitute b_{k3} instead of t_k.
(6) At last we construct $\mathbb{B}_k$ and $\mathbb{B}$.

4. EXAMPLES

Let us see some examples for two different values of a.

4.1. **Encryption and Decryption of BETA.** . **Encryption**:

(1) $\mathbb{B} = \begin{pmatrix} B & E \\ T & A \end{pmatrix}$

(2) There is only one block and so $b = 1$.

(3) By definition of p and r, we have $p = 2$ and $r = 1$. Choose $a = 105$.

(4) Thus $\mathbb{B}_1 = \begin{pmatrix} 211 & 214 \\ 229 & 210 \end{pmatrix}$ and so $b'_{1k}s$ are given by $b_{11} = 211, b_{12} = 214, b_{13} = 229, b_{14} = 210$.

(5) $d_1 = \begin{vmatrix} 211 & 214 \\ 229 & 210 \end{vmatrix}$= -4696

(6) $\mathbb{E} = \begin{pmatrix} -4696 & 211 & 214 & 210 \end{pmatrix}$

Decryption

(1) $Q_{105}^{2^*} = \begin{pmatrix} 315 & 420 \\ 210 & 315 \end{pmatrix}$.

(2) Here $q_1 = 315, q_2 = 420, q_3 = 210, q_4 = 315$

(3) $\omega_{11} = q_1b_{11} + q_3b_{12} = 111405$ and $\omega_{12} = q_2b_{12} + q_4b_{12} = 156030$.

(4) $a^1d_1 = \omega_{11}(q_2t_1 + q_4b_{14}) - \omega_{12}(q_1t_1 + q_3b_{14}) \Rightarrow t_1 = 229$

(5) $b_{13} = t_1 = 229$

(6) Hence we get $\mathbb{B}_1 = \begin{pmatrix} 211 & 214 \\ 229 & 210 \end{pmatrix}$ from $\mathbb{E}$.

(7) $\mathbb{B} = \begin{pmatrix} B & E \\ T & A \end{pmatrix}$

4.2. **Encryption and Decryption of My favourite subject is mathematics. Encryption:**

(1) Now $\mathbb{B} = \begin{pmatrix} M & Y & \delta & F & A & V \\ O & U & R & I & T & E \\ \delta & S & U & B & J & E \\ C & T & \delta & I & S & \delta \\ M & A & T & H & E & M \\ A & T & I & C & S & \delta \end{pmatrix}$

(2) Here $b = 9$. We get $\mathbb{B}_1 = \begin{pmatrix} M & Y \\ O & U \end{pmatrix}$, $\mathbb{B}_2 = \begin{pmatrix} \delta & F \\ R & I \end{pmatrix}$, $\mathbb{B}_3 = \begin{pmatrix} A & V \\ T & E \end{pmatrix}$, $\mathbb{B}_4 = \begin{pmatrix} \delta & S \\ C & T \end{pmatrix}$,

$\mathbb{B}_5 = \begin{pmatrix} U & B \\ \delta & I \end{pmatrix}$, $\mathbb{B}_6 = \begin{pmatrix} J & E \\ S & \delta \end{pmatrix}$, $\mathbb{B}_7 = \begin{pmatrix} M & A \\ A & T \end{pmatrix}$, $\mathbb{B}_8 = \begin{pmatrix} T & H \\ I & C \end{pmatrix}$, $\mathbb{B}_9 = \begin{pmatrix} E & M \\ S & \delta \end{pmatrix}$

(3) We have $p = 3 < b$ and $r = 3$. Choose $a = 30$.

(4) Hence $\mathbb{B}_1 = \begin{pmatrix} 822 & 834 \\ 824 & 830 \end{pmatrix}, \mathbb{B}_2 = \begin{pmatrix} 809 & 815 \\ 827 & 818 \end{pmatrix}, \mathbb{B}_3 = \begin{pmatrix} 810 & 831 \\ 829 & 814 \end{pmatrix}, \mathbb{B}_4 = \begin{pmatrix} 809 & 828 \\ 812 & 829 \end{pmatrix},$

$\mathbb{B}_5 = \begin{pmatrix} 830 & 811 \\ 809 & 818 \end{pmatrix}, \mathbb{B}_6 = \begin{pmatrix} 819 & 814 \\ 828 & 809 \end{pmatrix}, \mathbb{B}_7 = \begin{pmatrix} 822 & 810 \\ 810 & 829 \end{pmatrix},$

$\mathbb{B}_8 = \begin{pmatrix} 829 & 817 \\ 818 & 812 \end{pmatrix}, \mathbb{B}_9 = \begin{pmatrix} 814 & 822 \\ 828 & 809 \end{pmatrix}$

(5) The determinants d_k are given by

k	1	2	3	4	5	6	7	8	9
d_k	-4956	-12243	-29559	-1675	22841	-11421	25338	4842	-22090

(6) The Encrypted matrix, $\mathbb{E} = \begin{pmatrix} -4956 & 822 & 834 & 830 \\ -12243 & 809 & 815 & 818 \\ -29559 & 810 & 831 & 814 \\ -1675 & 809 & 828 & 829 \\ 22841 & 830 & 811 & 818 \\ -11421 & 819 & 814 & 809 \\ 25338 & 822 & 810 & 829 \\ 4842 & 829 & 817 & 812 \\ -22090 & 814 & 822 & 809 \end{pmatrix}$

Decryption

(1) $(Q_{30}^{3^*})^3 = \begin{pmatrix} 702000 & 1215000 \\ 405000 & 702000 \end{pmatrix}$

(2) The $q_k's$ are

k	1	2	3	4
q_k	$702(10)^3$	$1215(10)^3$	$405(10)^3$	$702(10)^3$

(3)

ω_{11}	ω_{12}	ω_{21}	ω_{22}	ω_{31}
$10^3(914814)$	$10^3(1584198)$	$10^3(897993)$	$10^3(1555065)$	$10^3(905175)$
ω_{32}	ω_{41}	ω_{42}	ω_{51}	ω_{52}
$10^3(1567512)$	$10^3(903258)$	$10^3(1564191)$	$10^3(911115)$	$10^3(1577772)$
ω_{61}	ω_{62}	ω_{71}	ω_{72}	ω_{81}
$10^3(904608)$	$10^3(1566513)$	$10^3(905094)$	$10^3(1567350)$	$10^3(912843)$
ω_{82}	ω_{91}	ω_{92}		
$10^3(914814)$	$10^3(1584198)$	$10^3(897993)$		

(4) Solving this equation $a^{2r}d_k = \omega_{k1}(q_2t_k + q_4b_{k4}) - \omega_{k2}(q_1t_k + q_3b_{k4})$, we get

k	1	2	3	4	5	6	7	8	9
t_k	824	827	829	812	809	828	810	818	828

(5) Thus we get $\mathbb{B}_1 = \begin{pmatrix} 822 & 834 \\ 824 & 830 \end{pmatrix}$, $\mathbb{B}_2 = \begin{pmatrix} 809 & 815 \\ 827 & 818 \end{pmatrix}$, $\mathbb{B}_3 = \begin{pmatrix} 810 & 831 \\ 829 & 814 \end{pmatrix}$, $\mathbb{B}_4 = \begin{pmatrix} 809 & 828 \\ 812 & 829 \end{pmatrix}$,

$\mathbb{B}_5 = \begin{pmatrix} 830 & 811 \\ 809 & 818 \end{pmatrix}$, $\mathbb{B}_6 = \begin{pmatrix} 819 & 814 \\ 828 & 809 \end{pmatrix}$, $\mathbb{B}_7 = \begin{pmatrix} 822 & 810 \\ 810 & 829 \end{pmatrix}$, $\mathbb{B}_8 = \begin{pmatrix} 829 & 817 \\ 818 & 812 \end{pmatrix}$,

$\mathbb{B}_9 = \begin{pmatrix} 814 & 822 \\ 828 & 809 \end{pmatrix}$ from the encrypted matrix $\mathbb{E}$.

(6) Hence $\mathbb{B} = \begin{pmatrix} M & Y & \delta & F & A & V \\ O & U & R & I & T & E \\ \delta & S & U & B & J & E \\ C & T & \delta & I & S & \delta \\ M & A & T & H & E & M \\ A & T & I & C & S & \delta \end{pmatrix}$

Note 1. *The R program was also used to validate these examples.*

5. Conclusion

In this paper, $(Q_a^{p^*})^r$ constructed using the solutions of $x^2 - py^2 = a^2$ using the choices of a and p. By using very high prime numbers can further secure the process. We encrypt and decrypt the message using the generalized Pell Equation of the form $x^2 - dy^2 = n$ where d and n are prime (p) and square of a sphenic number (a^2) respectively. This content is the generalization of [3]. We may also extend this with any other Diophantine Equation or we may use any other choices of a.

REFERENCES

[1] Dickson, L. E.,History of the Theory of Numbers, Volume- II Diophantine Analysis, Dover Publications, New York (2015).

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

[3] Kannan, J., Mahalakshmi, M., & Deepshika, A., Cryptographic algorithm involving the matrix Q^{p^*}, Korean J. Math, 30(3), 533-538, (2022).

[4] Kannan, J., & Manju Somanath, Fundamental Perceptions in Contemporary Number Theory *Nova Science Publisher, New York*, (2023).
[5] Kannan, J., Manju Somanath., Mahalakshmi, M., & Raja, K., Encryption decryption algorithm using solutions of pell equation. *International Journal for Research in Applied Science and Engineering Technology*, 10(1), 1-8, (2022).
[6] Sumeryra, 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), 62-70, (2019).
[7] Titu Andreescu., Dorin Andrica., & Ion Cucurezeanu, An introduction to Diophantine equations: a problem - based approach. Birkhauser Boston, (2010).

(Received, July 21, 2025)
(Revised, August 02, 2025)

[1]Department of Mathematics,
Ayya Nadar Janaki Ammal College,
(Autonomous, affiliated to Madurai
Kamaraj University), Sivakasi.
Email[1]: jayram.kannan@gmail.com

[2,3]Ayya Nadar Janaki Ammal College,
(Autonomous, affiliated to Madurai
Kamaraj University), Sivakasi.