RESEARCH ARTICLE OPEN ACCESS

Application of Diophantine Equations in Crytography

V. Pandichelvi[1], R. Vanaja [2]

[1]PG & Research Department of Mathematics, Urumu Dhanalakshmi College, Trichy.

(Affiliated to Bharathidasan University)

E-mail: mvpmahesh2017@gmail.com

[2]PG & Department of Mathematics, Shrimati Indira Gandhi College, Trichy.

(Affiliated to Bharathidasan University)

E-mail: vanajvicky09@gmail.com

--************************----------------------------------

Abstract:

In this paper, the algorithm for the transmission of a message from the despatcher to the receiver is enlightened by employing second-degree Diophantine equations and simultaneous Diophantine equations.

***Keywords* —** Cryptography, Diophantine equations, Simultaneous Diophantine equations, quotient ring**.**

--************************----------------------------------

I. INTRODUCTION

Cryptography is the study of secure communication techniques that restrict message contents to only the recipient and intended sender. Many authors have discussed public-key cryptosystems based on integer factorization, discrete logarithm, or elliptic curve techniques [1–10]. In this article, the process of conveying a message from one person to another is exposed by using second-degree Diophantine equations and a system of Diophantine equations.

II. Application of second-degree Diophantine equations in cryptography

this section exemplifies the ability to use second-order Diophantine equations in cryptography

A. Communication Of A Message Between Two Persons Over A Second-Degree Diophantine Equation

The communication of message 4563 between the sender and the recipient is explained through the following algorithm:

STEP 1: The recipient sets the integer values of variables x, y to $x = 13, y = 3$ (1)

and using those variables, the recipient constructs his public key as a Diophantine equation $x^2 - 6y^3 - 17 = 0$ (2)

STEP 2:The recipient sends the Diophantine equation (2) to the sender by keeping the values of the variables 13 and 3 secret.

STEP 3: The sender inserts an element $g(x, y) = x^2y^3$ into the quotient ring $Z(x, y) / x^2 - 6y^3 - 17$ and describes the following operator on that quotient ring

$T[a, b, c]: x \rightarrow x^a + bc$ (3)

where $a, b,$ and c are integers. The sender places an element x^2y^3on the quotient ring and practises the operator repeatedly on this element, as offered below

$$T_{[2,1,3]}\left(T_{[1,4,2]}(x^2y^3)\right)$$
$$= T_{[2,1,3]}(x^2y^3 + 8)$$
$$= x^4y^6 + 16x^2y^3 + 67$$
$$= 36y^{12} + 84y^9 + 49y^6 + 16x^2y^3 + 6 \quad (4)$$

STEP 4: The sender maintains $h(x, y) = 36y^{12} + 84y^9 + 49y^6 + 16x^2y^3 + 6$ and fixes the element $g(x, y) = x^2y^3$ as public key and sustains the parameters operator as a private key.

STEP 5: The recipient upholds the premeditated value $h(13,3) = 20894044$ as public and $(13,3) = 4563$ as secret.

STEP 6: The recipient returns the value 20894044 to the sender while concealing the value 4563.

STEP 7: The sender recovers the value of $g$as

$$g = T_{[1,4,2]}{}^{-1}\left(T_{[2,1,3]}{}^{-1}(20894044)\right)$$
$$= T_{[1,4,2]}{}^{-1}(4571) = 4563. \quad (5)$$

STEP 8:As a result, the recipient and sender might be able to share the secret.

B. **Communication of the message between three persons through the second-degree Diophantine equation**

The communication of message 16125 between the despatcher and two receivers is exemplified as follows.

STEP 1: The receiver R_1 sets the integer values $5, 11$ as private keys and create the public key as the Diophantine equation $x^3 - y^2 - 4 = 0$ (6)

The receiver R_2 retains $x = 5$ and $y = 55$ as private keys and the public key as the corresponding Diophantine equation $x^3 - 2y - 15 = 0$ (7)

STEP 2: R_1 and R_2 both share their public keys with the dispatcher S.

STEP 3: As in section II (A), the despatcher uses the operator given in (3) repeatedly by placing an element x^3y^2 on the quotient ring, as mentioned below.

$$T_{[2,3,-2]}\left(T_{[1,5,3]}(x^3y^2)\right)$$
$$= T_{[2,1,3]}(x^3y^2 + 15)$$
$$= x^6y^4 + 30x^3y^2 + 219$$
$$= x^{12} - 8x^9 + 16x^6 + 30x^3y^2 + 219 \quad (8)$$

The Dispatcher S holds $j(x, y) = x^{12} - 8x^9 + 16x^6 + 30x^3y^2 + 219$ and $i(x, y) = x^3y^2$ as public keys by keeping the parameter operator $[2,3, -2]$ private for the receiver R_1.

The Dispatcher S inserts an element $k(x, y)$ into the quotient ring $Z(x, y)\ /\ x^3 - 2y - 15 = 0$ and express the given operator repetitively by placing an element xy^2on the quotient ring, as revealed below.

$$T_{[2,4,1]}\left(T_{[1,3,2]}(xy^2)\right)$$
$$= T_{[2,4,1]}(xy^2 + 6)$$
$$= x^2y^4 + 12xy^2 + 40$$
$$= x^2y^4 + 3y^7 - 90x^4 + 675x + 40$$
$$= l(x, y) \quad (9)$$

The despatcher makes $l(x, y)$ and $k(x, y) = xy^2$ as public by sustaining the operator parameters private for the receiver R_2.

STEP 4:

The receiver R_1 directs the value of $j(5,11) = 229219594$ to the dispatcher and possess $i(5,11) = 15125$ secret.

The receiver R_2 computes $k(5,55)$ and $l(5,55)$ and sends $l(5,55) = 228947165$ to the sender by upholding $k(5,15) = 15125$ secret.

STEP 5: The dispatcherrecovers the value i by using the value of $j(x, y)$as

$$i = T_{[1,5,3]}{}^{-1}\left(T_{[2,3,-2]}{}^{-1}(229219594)\right)$$
$$= T_{[1,5,3]}{}^{-1}(15140) = 15125. \quad (10)$$

The despatcher convalesces the value $k$by applying $l(x, y)$ as

$$k = T_{[1,3,2]}{}^{-1}\left(T_{[2,4,1]}{}^{-1}(228947165)\right)$$
$$= T_{[1,3,2]}{}^{-1}(15131) = 15125. \quad (11)$$

STEP 6:Finally, the dispatcher and receivers $R_1$and R_2 could share the secret.

III. Application of Simultaneous Diophantine Equations in Cryptography

This section describes the application of simultaneous Diophantine equations in cryptography.

A. **Transmission of a message between two persons through simultaneous Diophantine equations**

The transmission of a message 1225 between two adherents by means of simultaneous Diophantine equations is explicated by the following algorithm.

STEP 1:The recipient creates the following simultaneous Diophantine equations as his public key by giving integer values to the variables x and y by$x = 7, y = 5$ (12)

$$\left.\begin{array}{l} x^2 - 2y^2 + 1 = 0 \\ 2x^2 - 3y^2 - 23 = 0 \end{array}\right\} \quad (13)$$

Here, 7, 5 are kept secret by the recipient.

STEP 2:The sender collects the Diophantine equation (13) from the recipient.

STEP 3:As in section II (A), the sender uses the operator specified in (3) repeatedly by employing an element x^2y^2on the quotient ring as follows.

$$T_{[3,2,1]}\left(T_{[1,2,3]}(x^2y^2)\right)$$
$$= T_{[3,2,1]}(x^2y^2 + 16)$$
$$= x^6y^6 + 18x^4y^4 + 108x^2y^2 + 214$$
$$= x^6y^6 + 18x^4y^4 + 180y^4 + 792y^2 + 214$$
$$= n(x, y) \quad (14)$$

STEP 4:The sender makes $n(x, y)$ and the fixed element $m(x, y) = x^2y^2$ public and the operator parameters private.

STEP 5:The recipient calculates $m(7,5)$ and $n(7,5)$ and displays $n(7,5) = 1865409389$ in public while preserving $m(7,5) = 1225$ in secret.

STEP 6:The recipient returns the value 1865409389to the sender while concealing the value of n.

STEP 7:The sender recovers the value $m$as

$$m = T_{[1,2,3]}{}^{-1}\left(T_{[3,2,1]}{}^{-1}(1865409389)\right)$$
$$= T_{[1,2,3]}{}^{-1}(1231) = 1225. \quad (15)$$

STEP 8: Finally, the recipient and sender interchange the secret m

B. **Sharing of the message among the sender and two recipients over simultaneous Diophantine Equations**

Sharing of message 1728 between the sender and two recipients over simultaneous Diophantine equations are illustrated below.

STEP 1:The recipient T_1generates simultaneous Diophantine equations as his public key by engaging the integer values of variables 3 and 4 as his private keys.

$$\left.\begin{aligned} 2x^2 - y^2 - 2 &= 0 \\ x^2 - 2y^2 + 23 &= 0 \end{aligned}\right\} \quad (16)$$

The receiver T_2 preserves the relevant simultaneous Diophantine equation

$$\left.\begin{aligned} x^2 - 8y^2 - 8 &= 0 \\ 2x^2 - 13y^2 - 11 &= 0 \end{aligned}\right\} \quad (17)$$

as public key and the private keys are $x = 8$ and $y = 3$

STEP 2:T_1 and T_2 directed their public keys to sender U.

STEP 3:As in section II (A), the sender repeats the operator (3) by engaging an element x^3y^3 on the quotient ring as mentioned below.

$$T_{[3,1,-1]}\left(T_{[1,5,4]}(x^3y^3)\right)$$
$$= T_{[3,1,-1]}(x^3y^3 + 20)$$
$$= x^9y^9 + 60x^6y^6 + 1200x^3y^3 + 7999$$
$$= x^9y^9 + 60y^{12} - 1260y^{10} + 8820y^8 - 20580y^6 + 1200x^3y^3 + 7999$$
$$= p(x,y) \quad (18)$$

The sender U retains $p(x,y)$ and $o(x,y) = x^3y^3$ public with the operator, and the parameters are private for the recipient T_1.

The sender U inserts an element $q(x,y) = x^2y^3$ into the quotient ring$Z(a,b,c)\,/\,x^2 - 8y^2 - 8 = 0$ and$2x^2 - 13y^2 - 11 = 0$ and delineates the given operator on that quotient ring,such as

$$T_{[3,3,-2]}\left(T_{[1,2,3]}(x^2y^3)\right)$$
$$= T_{[3,3,-2]}(x^2y^3 + 6)$$
$$= x^6y^9 + 18x^4y^6 + 108x^2y^3 + 210$$
$$= x^6y^9 + 18x^4y^6 + 756y^5 + 108y^3 + 210 = r(x,y) \quad (19)$$

The sender possesses $r(x,y)$ and $q(x,y) = x^2y^3$as public and the operator parameters as private for the receiver T_2.

STEP 4: The recipient T_1 leads the value of $p(3,4) = 5341020991$ to the sender by reserving$o(3,4) = 1728$ secret. The recipient T_2 estimates $l(8,3)$ and $m(8,3)$ and refers $r(8,3) = 5213714898$ to the sender by sustaining$q(8,3) = 1728$ secret.

STEP 5: The senderrecuperates the value o by using $p(x,y)$ as

$$o = T_{[1,5,4]}{}^{-1}\left(T_{[3,1,-1]}{}^{-1}(5341020991)\right)$$
$$= T_{[1,5,4]}{}^{-1}(1748) = 172(20)$$

The sender improves the value q by using $r(x,y)$ as

$$q = T_{[1,2,3]}{}^{-1}\left(T_{[3,3,-2]}{}^{-1}(5213714898)\right)$$
$$= T_{[1,2,3]}{}^{-1}(1734) = 1728. \quad (21)$$

STEP 6: The sender U and recipients T_1 and T_2 might be capable of conveying the secret.

IV. Conclusion

The encryption method was discussed in this work by using second-degree Diophantine equations and simultaneous Diophantine equations. Through this method, how messages can be sent from one person to another using a variety of operators is explained in detail. In a similar way, one can search for the application of higher-degree Diophantine equations in Cryptography.

V. References

[1] R. Bose, "Novel Public Key Encryption Techniques Based on Multiple Chaotic Systems", *Physic Review Letters*, vol. 95(9), 2005.

[2] J. Hoffstein, J. Pipher, and J.H. Silverman, "An Introduction to Mathematical Cryptography", *Springer, New York*, 2008.

[3] Basu, M. and Prasad, B., "The generalized relations among the code elements for Fibonacci coding theory", *Chaos Solitons Fractals*, vol. 41(5), pp. 2517-2525, 2009.

[4] M.R.K. Ariffin, N.A. Abu and A. Mandangan, "Strengthening the-cryptosystem" *Proc. Second International Cryptology Conference 2010*, 2010, 16 - 26.

[5] Harry Yosh, "The Key Exchange Cryptosystem Used with Higher Order Diophantine Equations", *International Journal of Network Security and its Applications (IJNSA)*, vol. 3(2), March 2011.

[6] J. S. Armand Eyebe Foudaa, J. Yves Effab, Bertrand Bodoa and Maaruf Alic, "Diophantine Solutions Based Permutation for Image Encryption", *Journal of Algorithms and Computational Technology,*vol. 7(1), pp. 65-86, June 2012.

[7] N. Hirata-Kohno and A. Petho, "On a key exchange protocol based on Diophantine equations", *Info communications Journal*, vol. 5, pp. 17–21, 2013.

[8] Prasad, B., "Coding theory on Lucas p-numbers", *Discrete Math. Algorithms Appl.,*vol. 8(4), pp. 17, 2016.

[9] T.Logeswar, "Data Security in Cryptography using Mathematics", *National Conference on Contemporary Research and Innovations in Computer Science (NCCRICS)*, Dec 2017.

[10] Sümeyra Uçar, Nihal Tas and Nihal Yılmaz Özgür, "A New Application to Coding Theory via Fibonacci and Lucas Numbers", *Mathematical Sciences and Applications E-Notes*, vol. 7(1), pp. 62-70, 2019.