ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 9, Issue 1, pp: (28-33), Month: April 2022 – September 2022, Available at: www.paperpublications.org

Cryptography Using Linear Diophantine Equation

Mark Kenneth C. Engcot[1]

[1]University of San Carlos, Philippines

DOI: https://doi.org/10.5281/zenodo.6974146

Published Date: 08-August-2022

Abstract: **This study is focused on the encrypting and decrypting of messages using the Linear Diophantine Equation: $ax + by = c$ where $\gcd(a, b) = 1$, that is the integers a and b are relatively prime. Like any encrypting and decrypting process, a number code, the integers a and b, and the flow of the process must be known to both the messenger and the receiver of the message. In this particular study, the message is encrypted by using the number code that results when the values of x and y are solved from the equations: (1) $x = x_0 + bt$ and (2) $y = y_0 - at$, where $t \in Z$ and (x_0, y_0) is a particular solution of the Linear Diophantine Equation ($ax + by = c$ where $\gcd(a, b) = 1$). The values of x and y are solved by substituting t with the specific number code assigned to each letter in the message. Since the encrypted message is dependent on the coding agreed both by the messenger and the receiver, the receiver is able to decrypt the message by finding the value of t and use the corresponding number code, and the schematic diagram.**

Keywords: **cryptography, linear Diophantine equation, encrypt, decrypt, encode, decode.**

I. INTRODUCTION

Number Theory may be one of the "purest" branches of mathematics, but it has turned out to be one of the most useful when it comes to computer security [3]. Unfortunately, algorithms based on number theory are often treated as a kind of black box where the understanding of the underlying mathematics is secondary to the actual application of the algorithm [5].

For thousands of years people have searched for ways to send messages secretly. A story in ancient times, stated that a king needed to send a secret message to his general in battle. The king took a servant, shaved his head, and wrote the message on his head. He waited for the servant's hair to grow back and then sent the servant to the general. The general then shaved the servant's head and read the message. If the enemy had captured the servant, they presumably would not have known to shave his head, and the message would have been safe [1].

In cryptography parlance, the message is referred to as plaintext. The process of scrambling the message using a key is called encryption. After encrypting the message, the scrambled version is called ciphertext. From the ciphertext, one can recover the original unscrambled message via a process known as decryption. Figure 1.1 illustrates an encryption and decryption cycle [4].

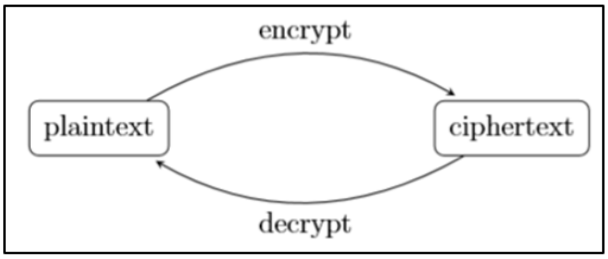


Figure 1.1 The Encryption/Decryption Cycle

II. CRYPTOGRAPHY USING LINEAR DIOPHANTINE EQUATION

A. *Preliminaries*

Let's define the most important concept on this study.

Corollary 1. [2] If a and b are given integers, not both zero, then the set $T = \{ax + by | x, y \text{ are integers}\}$ is precisely the set of all multiples of $d = \gcd(a, b)$.

Theorem 1. [2] **(Euclid)** There is an infinite number of primes.

Theorem 2. [2] The **linear Diophantine equation $ax + by = c$** has a solution if and only if $d|c$, where $d = \gcd(a, b)$. If x_0, y_0 is any particular solution of this equation, then all other solutions are given by $x = x_0 + \left(\frac{b}{d}\right)t$ and $y = y_0 - \left(\frac{a}{d}\right)t$, where t is an arbitrary integer.

Since the $\gcd(a, b) = 1$ then we have now new equations in finding new solutions for x and y, stated in Corollary 2.

Corollary 2. [2] If $\gcd(a, b) = 1$ and if x_0, y_0 is a particular solution of the Linear Diophantine Equation $ax + by = c$, then all solutions are of the form of $x = x_0 + bt$ and $y = y_0 - at$ for integral values of t.

B. *Encoding the message*

Consider the *number code* (Table 2.1) and the *schematic diagram* (Figure 2.1) agreed by the messenger and the receiver.

Letters	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Code	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Table 2.1. Number Code for the different letters on English Alphabet

$$\boxed{x \to y \to x \to y \to x \to y \to x \to y \cdots}$$

Figure 2.1. Schematic Diagram for Encryption and Decryption

In encrypting the message, unique solution x_0 and y_0 of the Linear Diophantine Equation: $ax + by = 1$ is needed to get the other solutions for x and y, where the $\gcd(a, b) = 1$. Since most values of a and b with $\gcd(a, b) = 1$ are relatively prime numbers then we use prime numbers as the values of a and b.

Case 1:

Assume that the messenger and the receiver agreed that $a = 2$ and $b = 3$. Then we have $\gcd(2,3) = 1$ which can be expressed as a linear combination in the form: $2x + 3y = 1$. By Euclidean Algorithm we have,

$$3 = 2(1) + 1$$

$$2 = 1(2) + 0$$

Expressing 1 as a linear combination of 2 and 3 , we have:

$$1 = 3(1) - 2(1)$$

$$1 = 2(-1) + 3(1)$$

Thus, $x_0 = -1$ and $y_0 = 1$. Other solutions are of the form: $x = -1 + 3t$ and $y = 1 - 2t\,; t \in Z$. From the number code presented in Table 2.1., we see that the letters in the message "ATTACK NOW" have the following codes: $A = 1$, $T = 20, C = 3, K = 11, N = 14, O = 15$ and $W = 23$. Substituting these number codes to the equations:

$$x = -1 + 3t \text{ and}$$

$$y = 1 - 2t$$

and taking note of the letter in the message corresponding to the number code, we have the following results; a summary of which is presented in Table 2.2.

A = 1

$$x = -1 + 3(1) = 2$$
$$y = 1 - 2(1) = -1$$

T = 20

$$x = -1 + 3(20) = 59$$
$$y = 1 - 2(20) = -39$$

C = 3

$$x = -1 + 3(3) = 8$$
$$y = 1 - 2(3) = -5$$

K = 11

$$x = -1 + 3(11) = 32$$
$$y = 1 - 2(11) = -21$$

N = 14

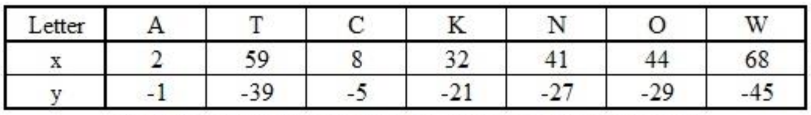
$$x = -1 + 3(14) = 41$$
$$y = 1 - 2(14) = -27$$

O = 15

$$x = -1 + 3(15) = 44$$
$$y = 1 - 2(15) = -29$$

W = 23

$$x = -1 + 3(23) = 68$$
$$y = 1 - 2(23) = -45$$



Letter	A	T	C	K	N	O	W
x	2	59	8	32	41	44	68
y	-1	-39	-5	-21	-27	-29	-45

Table 2.2. A Summary of the Encrypted Results for Case 1

Using the values of x and y presented in Table 2.2 and applying the schematic diagram presented in Figure 2.1, we have:

$$A \to x \to 2 \;\Rightarrow\; A \to 2$$
$$T \to y \to -39 \;\Rightarrow\; T \to -39$$
$$T \to x \to 59 \;\Rightarrow\; T \to 59$$
$$A \to y \to -1 \;\Rightarrow\; A \to -1$$
$$C \to x \to 8 \;\Rightarrow\; C \to 8$$
$$K \to y \to -21 \;\Rightarrow\; K \to -21$$
$$N \to x \to 41 \;\Rightarrow\; N \to 41$$
$$O \to y \to -29 \;\Rightarrow\; \mathrm{O} \to -29$$
$$W \to x \to 68 \;\Rightarrow\; W \to 68$$

Using " / " to separate the words in the encrypted message, the message ATTACK NOW is encrypted as:

$2 \cdot -39 \cdot 59 \cdot -1 \cdot 8 \cdot -21$ / $41 \cdot -29 \cdot 68$.

Case 2:

Suppose that the messenger and the receiver agreed that $a = 3$ and $b = 2$. Then, the $\gcd(a, b) = \gcd(3,2) = 1$ can be express to the form of linear combination $3x + 2y = 1$. By Euclidean Algorithm, we have $x_0 = 1$ and $y_0 = -1$ and all the other solutions are of the form: $x = 1 + 2t$ and $y = -1 - 3t, t \in Z$.

By using the number code in Figure 2.1, ATTACK NOW is encoded using the same codes as in Case 1. Substituting these codes to the equations: $x = 1 + 2t$ and $y = -1 - 3t$, results are as follows and, are summarized in Table 2.3.

A = 1

$$x = 1 + 2(1) = 3$$
$$y = -1 - 3(1) = -4$$

T = 20

$$x = 1 + 2(20) = 41$$
$$y = -1 - 3(20) = -61$$

C = 3

$$x = 1 + 2(3) = 7$$
$$y = -1 - 3(3) = -10$$

K = 11

$$x = 1 + 2(11) = 23$$
$$y = -1 - 3(11) = -34$$

N = 14

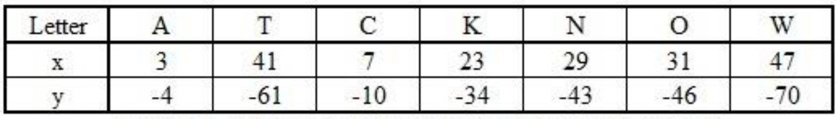
$$x = 1 + 2(14) = 29$$
$$y = -1 - 3(14) = -43$$

O = 15

$$x = 1 + 2(15) = 31$$
$$y = -1 - 3(15) = -46$$

W = 23

$$x = 1 + 2(23) = 47$$
$$y = -1 - 3(23) = -70$$



Letter	A	T	C	K	N	O	W
x	3	41	7	23	29	31	47
y	-4	-61	-10	-34	-43	-46	-70

Table 2.3. A Summary of the Encrypted Results for Case 2

Using the values of x and y presented in Table 2.3 and applying the schematic diagram presented in Figure 2.1, we have:

$$A \rightarrow x \rightarrow 3 \quad \Rightarrow A \rightarrow 3$$
$$T \rightarrow y \rightarrow -61 \quad \Rightarrow T \rightarrow -61$$
$$T \rightarrow x \rightarrow 41 \quad \Rightarrow T \rightarrow 41$$
$$A \rightarrow y \rightarrow -4 \quad \Rightarrow A \rightarrow -4$$
$$C \rightarrow x \rightarrow 7 \quad \Rightarrow C \rightarrow 7$$
$$K \rightarrow y \rightarrow -34 \quad \Rightarrow K \rightarrow -34$$
$$N \rightarrow x \rightarrow 29 \quad \Rightarrow N \rightarrow 29$$
$$O \rightarrow y \rightarrow -46 \quad \Rightarrow \mathrm{O} \rightarrow -46$$
$$W \rightarrow x \rightarrow 47 \quad \Rightarrow W \rightarrow 47$$

Using " / " to separate the words in the encrypted message, the message ATTACK NOW is encrypted as:

$3 \cdot -61 \cdot 41 \cdot -4 \cdot 7 \cdot -34 \,/\, 29 \cdot -46 \cdot 47$.

C. *Decoding the message*

The receiver decrypts the message using the agreed number code (Table 2.1) and the schematic diagram (Figure 2.1). The following cases illustrates how the decryption of the message is done.

Case 1:

In this case, the message received: $2 \cdot -39 \cdot 59 \cdot -1 \cdot 8 \cdot -21 \,/\, 41 \cdot -29 \cdot 68$ is decrypted by using the equations $x = -1 + 3t$ and $y = 1 - 2t$. Thus we have the following results:

$\boldsymbol{x = 2}$

$$2 = -1 + 3t \Rightarrow t = 1 \rightarrow \boldsymbol{A}$$

$\boldsymbol{y = -39}$

$$-39 = 1 - 2t \Rightarrow t = 20 \rightarrow \boldsymbol{T}$$

$\boldsymbol{x = 59}$

$$59 = -1 + 3t \Rightarrow t = 20 \rightarrow \boldsymbol{T}$$

$\boldsymbol{y = -1}$

$$-1 = 1 - 2t \Rightarrow t = 1 \rightarrow \boldsymbol{A}$$

$\boldsymbol{x = 8}$

$$8 = -1 + 3t \Rightarrow t = 3 \rightarrow \boldsymbol{C}$$

$\boldsymbol{y = -21}$

$$-21 = 1 - 2t \Rightarrow t = 11 \rightarrow \boldsymbol{K}$$

$\boldsymbol{x = 41}$

$$41 = -1 + 3t \Rightarrow t = 14 \rightarrow \boldsymbol{N}$$

$\boldsymbol{y = -29}$

$$-29 = 1 - 2t \Rightarrow t = 15 \rightarrow \boldsymbol{O}$$

$\boldsymbol{x = 68}$

$$68 = -1 + 3t \Rightarrow t = 23 \rightarrow \boldsymbol{W}$$

Case 2:

In this case, the message received: $3 \cdot -61 \cdot 41 \cdot -4 \cdot 7 \cdot -34 \,/\, 29 \cdot -46 \cdot 47$ is decrypted by using the equations $x = 1 + 2t$ and $y = -1 - 3t$. Thus we have the following results:

$\boldsymbol{x = 3}$

$$3 = 1 + 2t \Rightarrow t = 1 \rightarrow \boldsymbol{A}$$

$\boldsymbol{y = -61}$

$$-61 = -1 - 3t \Rightarrow t = 20 \rightarrow \boldsymbol{T}$$

$\boldsymbol{x = 41}$

$$41 = 1 + 2t \Rightarrow t = 20 \rightarrow \boldsymbol{T}$$

$\boldsymbol{y = -4}$

$$-4 = -1 - 3t \Rightarrow t = 1 \rightarrow \boldsymbol{A}$$

$\boldsymbol{x = 7}$

$$7 = 1 + 2t \Rightarrow t = 3 \rightarrow \boldsymbol{C}$$

$\boldsymbol{y = -34}$

$$-34 = -1 - 3t \Rightarrow t = 11 \rightarrow \boldsymbol{K}$$

$\boldsymbol{x = 29}$

$$29 = 1 + 2t \Rightarrow t = 14 \rightarrow \boldsymbol{N}$$

$\boldsymbol{y = -46}$

$$-46 = -1 - 3t \Rightarrow t = 15 \rightarrow \boldsymbol{O}$$

$\boldsymbol{x = 47}$

$$47 = 1 + 2t \Rightarrow t = 23 \rightarrow \boldsymbol{W}$$

Proposition 1. The total number of possible encrypted messages is 2^n, where n is the exact number of letters in the original text.

Proof. There are only two possible encrypted values denoted as $x\ or\ y$ in every letter. If we have n letters in the message, then we have $\underbrace{(2)(2)(2)\ldots(2)}_{n\ factors\ of\ 2} = 2^n$ total number possible of encrypted messages. This implies that we have 2^n different encrypted messages.

In the examples presented, the message "ATTACK NOW" consists of 9 letters, then the total number of possible encrypted message sets is $2^9 = 512$. If the messenger and the receiver agreed that they used the encrypted letter alternately starting with x as shown in Figure 2.1, then the resulting encryptions is one of the possible sets of the encrypted message.

III. CONCLUSION

In the process of encrypting and decrypting messages using Linear Diophantine Equation of the form $ax + by = 1$ the following were found:

(i) all other solutions are of the form: $x = x_0 + bt$ and $y = y_0 - at$, where t is the number corresponding to a letter in the number code agreed by both the messenger and the receiver;

(ii) the encrypted letter will be any of the values of x or y, which also depends on the schematic diagram that the messenger and receiver agreed;

(iii) the longer the message the more number of sets of encrypted messages there will be;

(iv) the total possible number of encrypted messages is 2^n.

REFERENCES

[1] K. Bogart, et.al., *Cryptography and Number Theory*, 2003.

[2] Burton, *Elementary Number Theory*, The McGraw-Hill Companies, Inc., New York, 2007.

[3] B. Kaliski, *The Mathematics of the RSA Public-Key Cryptosystem*, 2005.

[4] M. Nguyen, *Exploring Cryptography Using the Sage Computer Algebra System*, 2009.

[5] Sutanyo, *Elementary and Analytic Methods in Number Theory*, 2007.