International Journal of
Science and Engineering Investigations
vol. 9, issue 103, August 2020
Received on August 22, 2020
ISSN: 2251-8843

The Encryption and Decryption Using a Constraint Matrix of a Linear Programming Problem

François Ndayiragije[1], Servat Nyandwi[2], Espérance Hatungimana[3]
[1,2]Prof., Department of Mathematics, Faculty of Sciences, University of Burundi, Bujumbura, Burundi
[3]Gihosha Fundamental School, DCE Ntahangwa, Bujumbura, Burundi
([1]francois.ndayiragije@ub.edu.bi, [2]servat.nyandwi@ub.edu.bi, [3]esperancehatungi@gmail.com)

Abstract-In this paper, after recalling the concepts of encryption, decryption and linear programming, we use the constraint matrix of a Linear Programming Problem (LPP) as a key to encrypting a coded message.

Keywords- *Encryption, Decryption, LPP*

I. INTRODUCTION

Cryptology [1,2,3,4,5], a science governing the coding of information, experienced a real explosion with the development of computer systems, Passing from an artisanal and confidential era to very high-tech technology requiring a significant amount of computational power. It has seen a wider expansion again with the advent of communications systems (Internet, etc.) where there is a need absolute to protect the data exchanged individuals.

In a context where the exchange of information dematerialized products are developing, it is essential to be able to benefit from secure systems to protect personal or confidential data. It is therefore necessary to have access to tools better protection against arbitrary intrusions data privacy. Encryption is often the only effective way to respond to these Requirements.

Cryptography is the set of processes lockdown to protect access to certain Data to make them incomprehensible to unauthorized persons. Technology cryptographic devices are thus recognized as being essential data security tools and data security trust in communications and trade Electronic.

II. ENCRYPTION AND DECRYPTION

During an encryption, each letter is represented by a number modulo 26. Though this is not an essential feature of the cipher, this simple scheme is often used:

TABLE I. FRENCH ALPHABET ASSOCIATED WITH INTEGERS

a	0
b	1
c	2
d	3
e	4
f	5
g	6
h	7
i	8
j	9
k	10
l	11
m	12
n	13
o	14
p	15
q	16
r	17
s	18
t	19
u	20
v	21
w	22
x	23
y	24
z	25

To encrypt a message, each block of n letters is multiplied by an invertible $n \times n$ matrix, against modulus 26. We group the numbers thus obtained by n (let's take for example n=3).

The letters ξ_k, ξ_{k+1} and ξ_{k+2} of the clear text will be encrypted λ_k, λ_{k+1} and λ_{k+2} with the following formula:

$$\begin{pmatrix} \lambda_k \\ \lambda_{k+1} \\ \lambda_{k+2} \end{pmatrix} = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} \xi_k \\ \xi_{k+1} \\ \xi_{k+2} \end{pmatrix} \text{(modulo 26).} \quad (1)$$

Where a, b, c, d, e, f, g, h, i are integers, λ_k, λ_{k+1} and λ_{k+2} will also be integers. The choice of the key here corresponds to the choice of a number n, and the choice of linear combinations to be made (this are always the same blocks in blocks).

To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption. The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible $n \times n$ matrices (modulo 26). The cipher can, of course, be adapted to an alphabet with any number of letters; all arithmetic just needs to be done modulo the number of letters instead of modulo 26.

In short, to decipher, the principle is the same as for the encryption: we take the letters two by two, and then we multiplies them with a matrix:

$$\begin{pmatrix} \xi_k \\ \xi_{k+1} \\ \xi_{k+2} \end{pmatrix} = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}^{-1} \begin{pmatrix} \lambda_k \\ \lambda_{k+1} \\ \lambda_{k+2} \end{pmatrix} \text{(modulo 26).} \quad (2)$$

During the decryption, a complication exists in picking the encrypting matrix: the determinant of the encrypting matrix must not have any common factors with the modular base.

Thus, if we work modulo 26 as above, the determinant must be nonzero, and must not be divisible by 2 or 13.

$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}^{-1}$ (modulo26) exists if $\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix}^{-1}$ (modulo 26) exists. Now, $\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}^{-1}$ (modulo 26) exists if $\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix}$ and 26 are prime numbers between them. It is therefore necessary to control that $\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix}$ is odd and is not multiple of 13. The following table gives the reverse modulo 26:

TABLE II. THE REVERSE MODULO 26

1	1
3	9
5	21
7	5
9	3
11	19
15	7
17	23
19	11
21	5
23	17
25	25

III. LINEAR PROGRAMMING

The origins of the subject of Operations Research date back to the Second World War (1939-1945) of the last century [K Bose]. In Linear Programming, the objective function and constraints are all linear expression in some unknown variables. G.B. Dantzig [6] who was working in the United Air Force formulated the general LPP. The term Linear Programming (LP) was coined by Koopmans and Dantzig in the summer of 1948 [7] during the course of their respective work.

The general form of mathematical programming problem is [6]:

Optimize Z= f(X)

Subject to

$$g_i(X) (\leq, =, \geq) 0, \text{ i} = 1, \ldots, \text{m}$$

$$X \geq 0$$

Where f(X) and g(X) are functions of the vector X = (x_1, …, x_n).

IV. PROBLEM , MATHEMATICAL FORMULATION AND METHODOLOGY

A. *Problem and mathematical formulation*

A company manufactures three types of bicycles: hiking bicycles, mountain bicycles and racing bicycles. Every hiking bicycle requires 1 hours of manufacturing, 3 hour of painting and 2 hour of assembly; each mountain bicycle requires 1 hour of manufacturing, 1 hours of painting and 5 hours of assembly and, finally, every racing bicycle requires 2 hours of manufacturing, 1 hour of painting and 3 hours assembly.

If the company has 120 hours of manufacturing, 100 hours of painting and 140 hours of assembly per week and that every hiking bicycle brings 40$, every mountain bicycle, 30$, and every racing bicycle, 50$,

The linear program to determine the number of bicycles each type that must be manufactured weekly to maximize profit is given the following LPP:

Max Z = 40 x_1 +30 x_2 +50 x_3

Subject to

$$x_1 + x_2 + 2x_3 \leq 120 \quad (3)$$

$$3x_1 + x_2 + x_3 \leq 100$$

$$2x_1 + 5x_2 + 3x_3 \leq 140$$

$$x_1, x_2, x_3 \geq 0$$

where x_1 , x_2 and x_3 are the number of hiking bicycles, mountain bicycles and racing bicycles, respectively.

B. *Methodology*

We encrypt the message: PUBLISH OR PERISH and we take as a cipher key the constraint matrix given by "(3)":

$\begin{pmatrix} 3 & 1 & 2 \\ 1 & 1 & 2 \\ 1 & 3 & 2 \end{pmatrix}$ and we use "(1)". To decrypt the message we sent, we use "(2)".

V. RESULTS

By the formula "(1)", we have table III.

To decrypt the sent message (L O D D H M D A F B O X O X X), we use "(2)" and the decryption matrix is: $\begin{pmatrix} 6 & 5 & 3 \\ 21 & 3 & 11 \\ 13 & 9 & 6 \end{pmatrix}$. We obtain the table IV.

TABLE III. THE ENCRYPTION TABLE

Letters	ξ_k	λ_k	Encrypted letters
P	15	11	L
U	20	14	O
B	1	3	D
L	11	3	D
I	8	7	H
S	18	12	M
H	7	3	D
O	14	0	A
R	17	5	F
P	15	1	B
E	4	14	O
R	17	23	X
I	8	14	O
S	18	23	X
H	7	23	X

TABLE IV. THE DECRYPTION TABLE

Encrypted letters	λ_k	ξ_k	Letters
L	11	15	P
O	14	20	U
D	3	1	B
D	3	11	L
H	7	8	I
M	12	18	S
D	3	7	H
A	0	14	O
F	5	17	R
B	1	15	P
O	14	4	E
X	23	17	R
O	14	8	I
X	23	18	S
X	23	7	H

VI. CONCLUSION AND FUTURE WORK

In this paper, we used a constraint matrix of a LPP to encrypt the message "PUBLISH OR PERISH". In the future, we could use a constraint matrix of a dynamic programming problem, in the operations of encryption and decryption.

REFERENCES

[1] Bruce Schneir, "Applied Cryptography, Protocols, Algorithms, and source Code in C", edition John Wiley & Sons Inc., 1994.

[2] Beckett Brian, "Introduction aux méthodes de la cryptologie ", Editions Masson, 1990.

[3] Hill Lester S., "Cryptography in Algebraic Alphabet," American Mathematical Monthy, 36, 1929,pp.306-312.

[4] Stinson Douglas, "Cryptographie, Théorie et pratique" , Vuibert, 2001, pp. 12-16.

[5] D.Müller, "Une application intéressante des matrices: le chiffre de Hill" , bulletin No 90 de SSPMP (www.vsmp.ch),Octobre 2002.

[6] K.C.RAO and S.L.MISHRA, "Operations research" Alpha Science, Harrow, U.K. (2005).

[7] S.K. Bose, "Operations Research Methods", Alpha Science International Lld, Harrow, UK. (2005).

Prof. **François Ndayiragije** has a PhD in Mathematics, obtained 10 July2012 at the University of Leuven (in Belgium). His Supervisor is Professor Walter Van Assche.

He is presently working as Associate professor and researcher at the Department of Mathematics, Faculty of Sciences, University of Burundi, Bujumbura, Burundi. He has 17 years' experience in teaching.

Nowadays, he is the Director of the Center for Research in Mathematics and Physics (CRMP).

His subjects of interest include multiple orthogonal polynomials and applied mathematics, especially Operations Research.

Outside the Science, he is an Evangelist and Servant of God in the Pentecostal Church of Kiremba, Bururi Province, Burundi. He believes in Jesus Christ and the Holy Bible is his favoured Book.

How to Cite this Article:

Ndayiragije, F., Nyandwi, S. & Hatungimana, E. (2020). The Encryption and Decryption Using a Constraint Matrix of a Linear Programming Problem. International Journal of Science and Engineering Investigations (IJSEI), 9(103), 62-64. http://www.ijsei.com/papers/ijsei-910320-13.pdf