Aplicaciones del álgebra matricial en los cifrados por transposición

PhD. Cristian David Barría Huidobro[1]
Universidad Mayor - Chile
cristian.barria@mayor.cl

Msc. Álvaro Andrés Toledo San Martín[2]
Universidad Mayor - Chile
alvaro.toledo@mayor.cl

Lic. Daniel Montenegro Tobar[3]
Universidad Mayor - Chile
symmtec@icloud.com

Fecha Recepción: 20/04/18 - Fecha Aprobación: 16/06/18

Resumen: Desde los comienzos de la comunicación en la humanidad se ha visto la necesidad de transmitir mensajes de manera que sean ocultos para aquellos que no sean el destinatario. Las metodologías de cifrado de mensajes han sido desarrolladas desde tiempos remotos, lo cual ha permitido diversos métodos y algoritmos matemáticos; de hecho algunos de ellos en la actualidad aún no han logrado ser totalmente descifrados. En este artículo se desarrolla una metodología y algoritmo que modela el cifrado mediante el sistema de transposición conocido como de doble transposición mediante los fundamentos matemáticos del álgebra lineal. Se establece una aplicación de un método de cifrado, basado en la factorización matricial especial PALU, dejando la puerta abierta para nuevas metodologías por factorizaciones de distinto orden y complejidad de acuerdo con el álgebra matricial.

Palabras clave: : Cifrado, Matrices, PALU, Transposición.

Abstract: Since the beginning of communication in humanity has seen the need to convey messages in a way that are hidden for those who are not the recipient. Message encryption methodologies have been developed since ancient times, which has allowed various methods and mathematical algorithms, in fact some of them at present have not yet been fully deciphered. In this article we develop a methodology and algorithm that models the encryption through the transposition system known as double transposition through the mathematical foundations of linear algebra. An application of an encryption method is established, based on the PALU special matrix factorization, leaving the door open for new methodologies by factorizations of different order and complexity according to the matrix algebra.

Keywords: : Encryption, Transposition, Matrix, PALU.

1. INTRODUCCIÓN

La criptografía es la ciencia que estudia los métodos y procedimientos, mediante algoritmos matemáticos, que permiten la confiabilidad, integridad y confidencialidad de la información. Triana Laverde, en su trabajo: aplicaciones matriciales a la criptografía, señala: "existen diversos métodos para encriptar o cifrar un mensaje" [1], Giovanni Battista della Porta en su texto de cuatro volúmenes furtivis literarum notis-

1.Doctor en Ingeniería Informática, Magister en Ciencias de la Ingeniería Informática y Magister en Planificación y Gestión Educacional, Licenciado en Informática, y Licenciado en Ciencias de la Ingeniería, cuenta con la Ingeniería en Informática, e Ingeniería en Administración. Docente Investigador Universidad Mayor.
2.Estadístico, Licenciado en Matemáticas y Magíster en Estadística de la Pontificia Universidad Católica de Chile. Doctorando en Ingeniería Industrial e Investigación de Operaciones en Universidad Adolfo Ibáñez. Coordinador Docente del área de Estadística del Departamento de Matemáticas y Física, Universidad Bernardo O'Higgins. Docente de la Escuela de Ingeniería en Computación e Informática, Universidad Mayor.
3.Licenciado en matemáticas. Director ejecutivo de SYMMTEC Consulting, empresa dedicada a la simulación y modelación matemática y estadística. Especialista en dinámica de sistemas y teoría de números.

vulgo de ziferis clasifica las técnicas de cifrado en tres grupos, que constituyen la criptografía clásica: cifrado por transposición, cifrado por sustitución y cifrado de sustitución por símbolos. Un cifrado clásico es un canal para ocultar un mensaje, conocido como mensaje en claro, donde las letras son sustituidas o transpuestas por otras letras, pares de letras y algunas veces por muchas letras [2]. En criptografía, el cifrado clásico fue utilizado históricamente y en la actualidad la mayoría de ellos se desarrollan mediante aplicaciones informáticas [3]. Los métodos más modernos usan ordenadores u otras tecnologías digitales, que operan con bits y bytes. Muchos cifrados clásicos fueron usados por personajes muy conocidas como Julio César y Napoleón, quienes crearon sus propios cifrados que después han sido usados popularmente, muchos tienen un origen militar. Algunas veces se agrupan junto con los cifrados clásicos otras máquinas mecánicas o electromecánicas, como Enigma.

En la actualidad los métodos de cifrado son mucho más sofisticados [4], entre ellos el más utilizado es el algoritmo RSA, creado por Rivest, Shamir, Adleman publicado en 1977 en la revista Scientific American, basado en números primos de gran magnitud, el cual emplea el modelo de una clave pública y otra privada (cifrado asimétrico) [5]. La confiabilidad que ofrece el algoritmo RSA permitió a Phil Zimmerman en 1991 [6] desarrollar el PGP (Pretty Good Privacy) que es un algoritmo de cifrado que funciona fácilmente en computadores domésticos. PGP utiliza conceptos de criptografía clásica y los combina con el algoritmo RSA [7], [8].

En la mayoría de los cifrados clásicos, los algoritmos desarrollados se sustentan en fundamentos matemáticos, por ejemplo, la aritmética modular, el teorema fundamental de la aritmética y sus aplicaciones a números primos, como la función de Euler y el teorema chino del resto, entre otros. Para el sistema de cifrado por transposición se puede determinar un algoritmo de cifrado y descifrado cuya base matemática se sustente en el álgebra de matrices [9].

En este artículo se propone un algoritmo para cifrar y descifrar mensajes por el sistema de doble transposición basado en los pilares del álgebra lineal, con lo cual se representaría un modelo matemático con sustento en el álgebra matricial para el método de cifrado de este criptosistema clásico [10], [11]. Mediante el desarrollo de los fundamentos matemáticos basados en el álgebra matricial y su implementación en el cifrado y descifrado mediante el sistema de doble transposición, se propone una nueva metodología para la generación de algoritmos y funciones de cifrado y de descifrados basados en factorizaciones o descomposiciones matriciales, como es el caso de la factorización PALU.
Para tal fin, este artículo se divide de tal manera que el lector podrá encontrar en el capítulo dos, el desarrollo del sistema de cifrado por transposición para el caso particular del cifrado por el método conocido como de doble transposición, fundamentado en el álgebra matricial. Las consideraciones adicionales que permiten generar nuevas aplicaciones de las factorizaciones especiales en matrices para el desarrollo de nuevos algoritmos de cifrado y de descifrado son tratados con detalle en el capítulo tres, para el caso aplicado de la factorización PALU. En el capítulo cuatro se encuentran las conclusiones.

2. EL SISTEMA DE CIFRADO POR TRANSPOSICIÓN

En el sistema de cifrado por transposición, las letras de un mensaje cifrado mediante esta metodología siguen siendo las mismas que en el mensaje en claro, sin embargo se hallan reorganizadas de acuerdo a un modelo previo o método definido, generando así un anagrama. Un célebre ejemplo de esto último es el seudónimo Voltaire, que, según una teoría, fue escogido por ser anagrama de Arouet, con la consideración de que i y j son la misma letra, al igual que u y v, como ocurre en latín. Desde un punto de vista criptoanalista, para un alfabeto de 27 caracteres (como es el caso del alfabeto español, incorporando la ñ), si se eligen cinco letras para establecer una clave de acceso de ordenamiento lineal sin repetición, el número de disposiciones (palabra clave, pues indica la importancia del orden) lineales de letras que son posibles de generar, o permutación, de acuerdo al principio de elección (o del producto) es de 27!/(27-5)!=9.687.600 disposiciones lineales posibles sin repetición ¡impresionante!, si se recuerda que sólo se está considerando la elección de cinco letras de un alfabeto de 27. A diferencia del primer caso, el número de disposiciones (lineales) de las cuatro letras de la palabra BALL es 12 y no 4! = 24. La razón es que no se tiene que ordenar cuatro letras distintas. Si las dos letras L se distinguen como L1, L2, entonces se puede utilizar las permutaciones de objetos distintos; con los

cuatro símbolos B, A, L1, L2, obteniendo así, 4! = 24 permutaciones. Sin embargo a cada disposición en la que las letras L son indistinguibles le corresponde una pareja de permutaciones con letras L distintas. En consecuencia se tienen permutaciones con repetición: si existen n objetos con n_{-1} de un primer tipo, n_{-2} de un segundo tipo, ... y n_{-r} de un r - ésimo tipo (los objetos del mismo tipo son indistinguibles), donde $n_1+n_2+...+n_r = n$, entonces existen n!/ (n_1! n_2! .. n_r!) disposiciones (lineales) de los n objetos dados.

En el libro de Matemáticas discretas de Ralph Grimaldi, se relata de forma genial la rapidez con que crecen los valores de n!: " se puede calcular que 10! = 3.628.800, y éste es precisamente el número de segundos que hay en seis semanas. En consecuencia, 11! es superior al número de segundos que tiene un año, 12! supera el número que hay en 12 años, y 13! sobrepasa la cantidad de segundos que tiene un siglo". Lo anterior demuestra que el método de transposición es un sistema que requiere haberse puesto previamente de acuerdo en todos los extremos del criptosistema.

2.1. Técnicas de cifrado por transposición: el método de doble transposición.

Este método consiste en ordenar por filas y columnas el texto del mensaje en claro, creando una tabla que se puede completar con letras nulas (se puede establecer una clave sobre el alfabeto, que puede ser numérica, para cifrar las letras de acuerdo a su orden en el mismo). Una vez dispuestos todos las letras (o números) que representan el texto del mensaje formando la tabla, se efectúan permutaciones por filas y columnas, una o varias veces. Se tendría así lo que se conoce como método de doble transposición. En el siguiente ejemplo considerando el mensaje cifrado doble transposicion. Se pasa el mensaje a una tabla cuadrada de 5 x 5 entradas (pues son 25 letras en el mensaje), numeradas por filas y columnas.

Tabla I. Tabla del mensaje en claro: cifrado doble transposición.

.	1	2	3	4	5
1	c	i	f	r	a
2	d	o	d	o	b
3	l	e	t	r	a
4	n	s	p	o	s
5	i	c	i	o	n

A continuación, se intercambia el orden de las columnas de manera aleatoria, sabiendo que el receptor del mensaje conoce la disposición final en la que va a quedar. Suponiendo que el orden escogido es (5-3-1-4-2). Además del orden de las columnas se ha de cambiar también el de las filas, siguiendo el mismo orden de numeración, sólo para este ejemplo. Ambas disposiciones (filas y columnas) corresponden a las llaves del criptosistema k_1,k_2, siendo estas presentadas en forma numérica o por medio de la palabra asociada a la asignación numérica del alfabeto utilizado, que para este ejemplo, la disposición (5,3,1,4,2) corresponde a k_1=k_2= FDBEC. Un intercambio sólo en el orden de las columnas o el de las filas se conoce como método de transposición sencilla. La siguiente tabla muestra las permutaciones propuestas.

Tabla 2. Tabla del mansaje en claro cifrado por doble transposición con clave 5-3-1-4-2 (en filas y columnas).

.	5	3	1	4	2
5	a	f	c	r	i
3	b	d	d	o	o
1	a	t	l	r	e
4	s	p	n	o	s
2	n	i	i	o	c

El cifrado del mensaje se obtiene transcribiendo de izquierda a derecha y de arriba a abajo, por filas, las letras de esta última tabla. Presentando, por ejemplo, en grupo de cierta profundidad. Utilizando grupos de cinco caracteres, el mensaje encriptado resulta así,

afcri bddoo atlre spnos niioc

El mensaje cifrado obtenido contiene 25 letras de las cuales existen repeticiones, como son el caso de la a, c, r, d, s, n con una frecuencia de dos, la i con frecuencia de tres, o con frecuencia de cuatro y finalmente las letras f, b, t, l y e con sólo una aparición en el mensaje en claro. El número de permutaciones (o disposiciones) con repetición, lineales del mensaje, es de $25!/2!^6 \cdot 3! \cdot 4!) = 1.68 \cdot 10^{21}$, ¡de aquí la importancia de la clave! Sin embargo, al disponer el mensaje en una tabla, las permutaciones posibles de filas y columnas que se pueden generar son de (se está analizando

el número de disposiciones lineales). Este método también es vulnerable a análisis de frecuencia

2.2. Fundamentos matemáticos matriciales en la formulación del método de cifrado por doble transposición.

Uno de los primeros objetivos de este artículo consiste en formalizar matemáticamente mediante el uso del álgebra matricial el sistema de cifrado por doble transposición. Para ello, se inicia con las siguientes definiciones y tipos de matrices especiales,

Definición 2.1 Matriz Triangular Superior (U): Sea U= [u_(i,j)]_(n^2) matriz cuadrada de orden n. U se dice matriz triangular superior si:

$$u_{i,j}\begin{cases}=0 \;\; si \;\; i>j\\ \neq 0 \; si \;\; i\leq j\end{cases} \quad (2.1)$$

Definición 2.2 Matriz Triangular Inferior (L): Sea L= [l_(i,j)]_(n^2) matriz cuadrada de orden n. L se dice matriz triangular inferior si:

$$l_{i,j}\begin{cases}=0 \;\; si \;\; i<j\\ \neq 0 \; si \;\; i\geq j\end{cases} \quad (2.2)$$

Definición 2.3 Matriz Diagonal (D): Sea D= [d_(i,j)]_(n^2) matriz cuadrada de orden n. D se dice matriz diagonal si:

$$d_{i,j}\begin{cases}=0 \;\; si \;\; i\neq j\\ \neq 0 \; si \;\; i=j\end{cases} \quad (2.3)$$

Un caso particular de matriz diagonal es la matriz identidad de orden n, denotada por I_n, la cual tiene valores unitarios en su diagonal principal.

Definición 2.4 Operaciones elementales: Sea Amxn matriz de m filas y n columnas (o dimensiones m x n). Sobre la matriz A se definen tres operaciones llamadas elementales:

1. Intercambiar la fila (o columna) i por la fila (o columna) j. Simbólicamente se adopta la notación para la permutación de filas y columnas, respectivamente, por $F_i \updownarrow F_j$, $[\![(C]\!]_i \updownarrow C_j$).

2. Multiplicar la fila (o columna) i por un escalar $\propto \neq 0$. Simbólicamente, $\propto F_i$,($\propto C_j$) para el caso de la aplicación del escalar a una columna.

3. Sumar k veces la fila (columna) i a la fila (columna) j, i≠j. Simbólicamente $F_i+k^* F_j$, $[\![(C]\!]_i+k^*C_j$)

Las operaciones elementales (operaciones-elementales) permiten definir las matrices elementales,

Definición 2.5 Matriz Elemental: Una matriz elemental es aquella matriz cuadrada que se obtiene a partir de la matriz identidad, mediante la aplicación de una sola operación elemental fija o columna de acuerdo con (2.2) sobre In, lo cual se denota por Ei y Fj, respectivamente.

Una matriz elemental es no singular.

En (operaciones-elementales) se encuentran los fundamentos matemáticos para la formulación matricial del cifrado y descifrado por doble transposición. Se calculan las operaciones y matrices elementales al ejemplo considerado en la sección de cifrado por transposición mediante el método de doble transposición al mensaje cifrado doble transposicion pasado a una matriz (tabla) cuadrada de 5 x 5. El orden de las columnas y filas dispuestas de manera aleatoria es (5-3-1-4-2). Las operaciones y las matrices elementales asociadas están dadas por,

$$C_1 \updownarrow C_5, F_1 \updownarrow F_5, F_1 = E_1 = \begin{bmatrix}0&0&0&0&1\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\1&0&0&0&0\end{bmatrix}$$

$$C_2 \updownarrow C_3, F_2 \updownarrow F_3, F_2 = E_2 = \begin{bmatrix}1&0&0&0&0\\0&0&1&0&0\\0&1&0&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}$$

$$C_3 \updownarrow C_5, F_3 \updownarrow F_5, F_3 = E_3 = \begin{bmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&0&0&1\\0&0&0&1&0\\0&0&1&0&0\end{bmatrix}$$

Para finalizar el análisis del algebra matricial en cuanto a los fundamentos matemáticos en el cifrado por transposición mediante el método de doble transposición, en relación con las definiciones (operaciones-elementales) y (matriz-elemental) se plantean los siguientes resultados,

Definición 2.6 Relación de congruencia matricial: Si sobre A ∈ M mxn se efectúa una sucesión finita de operaciones elementales, se obtiene una matriz B ∈ M mxn que se dice congruente con la matriz A y se denota por A ~B.

Teorema 2.1. La relación (2.2) es una relación de equivalencia entre matrices.

Esto es: sea A∈M_(m x n) (R) y E una matriz elemental que proviene de I_m, la multiplicación por la izquierda de A por E efectúa la misma operación elemental en las filas de A que la realizada en la matriz identidad para obtener E. Análogamente la multiplicación por derecha de A por F efectúa la misma operación elemental en las columnas de A que la realizada en la matriz identidad para obtener F.

En conclusión: la tabla asociada al mensaje en claro dispuesto en filas y columnas mediante un cifrado de doble transposición, y luego la aplicación de permutaciones de filas y columnas, corresponden a operaciones elementales de permutación de filas y columnas (operaciones-elementales) sobre la tabla vista como matriz del mensaje a cifrar. Es decir, una aplicación finita de matrices elementales (matriz-elemental) por izquierda y por derecha.

Continuando con el ejemplo de la aplicación de las operaciones y matrices elementales sobre la tabla (tabla-ejemplo-doble-transposicion) se obtiene,

$$A=\begin{bmatrix} C & I & F & R & A \\ D & O & D & O & B \\ L & E & T & R & A \\ N & S & P & O & S \\ I & C & I & O & N \end{bmatrix}$$

$$E3*E2*E1*A*F1*F2*F3$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} C & I & F & R & A \\ D & O & D & O & B \\ L & E & T & R & A \\ N & S & P & O & S \\ I & C & I & O & N \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Obteniéndose así la matriz del mensaje encriptado,

$$A=\begin{bmatrix} A & F & C & R & I \\ B & D & D & O & O \\ A & T & L & R & E \\ S & P & N & O & S \\ N & I & I & O & C \end{bmatrix}$$

Que de acuerdo con (mensaje-ejemplo-encriptado) comprueba la aplicación. (teorema-no-singularidad) permite la inversión de cada matriz de permutación, lo que resuelve el problema de descifrar el mensaje cifrado para la obtención del mensaje en claro.

En el siguiente capítulo se propone la generalización de la aplicación de las matrices en el cifrado de mensajes en un criptosistema. Esta aplicación consiste en la factorización especial PALU.

3. CIFRADO MEDIANTE FACTORIZACIONES MATRICIALES ESPECIALES: CIFRADO POR FACTORIZACIÓN PALU

Este método consiste en ordenar por filas y columnas el texto del mensaje en claro, creando una matriz que se puede completar con caracteres o símbolos nulos para generar una matriz cuadrada. Cada entrada de esta matriz tiene asignado de manera única un caracter del correspondiente alfabeto utilizado por los extremos del criptosistema. Si n∈Z^+ corresponde a la longitud del alfabeto, entonces n debe ser primo. Se asigna a cada caracter de este alfabeto ordenado un elemento del conjunto $(Z_n,+,\cdot)$, que tiene estructura de cuerpo para n primo. Esta consideración permite la generalización del alfabeto utilizado en otros sistemas criptográficos clásicos, por ejemplo, la posibilidad de considerar el espacio entre las palabras que componen el mensaje, diferenciación entre mayúsculas y minúsculas, números o letras acentuadas, entre otras posibilidades, enriquecen la codificación del mensaje en claro y con ello dificulta el trabajo del criptoanalista.

Una vez dispuestos todos los números que representan el texto del mensaje en claro formado en la matriz, el cifrado consiste en la permutaciones de filas y/o columnas, una o varias veces, lo que se conoce como método de doble transposición y la eliminación de parte de este mensaje mediante la transformación por equivalencia de la matriz del mensaje en claro en

una matriz triangular superior (triangular-superior) logrando así un mensaje encriptado de menor longitud que el mensaje original y con triple llave de seguridad, dos asociadas al método de doble transposición y una correspondiente a la reducción por escalonamiento.

Sea la matriz del mensaje en claro $A=[a_{ij}]_{m^2}$),mod(n), donde $m^2=m\times m, m\in Z^+$ corresponden al número de filas (y columnas) de la matriz A cuadrada. Aplicando el algoritmo de factorización PALU como sigue: se comprueba que el elemento $d_{ij}=a_{ij}, i=j$ (elemento de la diagonal principal de la matriz) denominado elemento pivote no es cero. En caso de serlo, se aplica permutación de filas, de acuerdo a las operaciones elementales (operación-elemental}) definidas. Si es distinto de cero, se eliminan los elementos de la columna j por debajo del pivote, para ello, se definen para cada fila i=j+1,j+2,...,m-1,m los factores o multiplicadores, para cada columna (fija) j. Dado que $a\_ij\in Z_n \forall i,j$ y $(Z_{n'},+,\cdot)$ tiene estructura algebraica de cuerpo, se asegura la existencia y unicidad de los elementos simétricos para amabas operaciones definidas en el conjunto. Sean $(-a_{ij})$ el elemento simétrico respecto a $(Z_{n'},+)$ o inverso aditivo de a_{ij} y d_j^{-2} el elemento simétrico respecto a $(Z_{n'},\cdot)$ o inverso multiplicativo (recíproco) de d_j, definiendo así el multiplicador para cada fila i, para una columna j,

$$r_{ij}=-a_{ij}*d_j^{-1},\ \forall j=1,2,3,\dots,m \forall i=j+1,j+2,\dots,m$$

Se aplican las operaciones elementales (operaciones-elementales) mediante el siguiente algoritmo: todos los elementos debajo de la diagonal principal de la columna j se anularan, los demás elementos de la matriz debajo de la fila j también se verán afectados de acuerdo con la operación,

$$F_{i+1}+\ r_{i+1,j}*F_i \rightarrow F_i, \forall j=1,2,3,\dots,m \forall i=j,j+1,\dots,m$$

El algoritmo de reducción culmina cuando la matriz A queda representada como una matriz triangular superior denotada por U (de Up). La reducción de una matriz cuadrada a una de las formas triangulares se puede lograr por multiplicaciones sucesivas por izquierda (o derecha) de matrices elementales adecuadas. Es decir, si A se puede reducir a una matriz triangular superior U mediante operaciones elementales filas, entonces existen matrices elementales $E_1,E_2,\dots,E_k$ tales que $U=E\_k\cdots E_2\cdot E_1\cdot A$.

Por otra parte, la matriz triangular inferior L (2.2) asociada a la matriz A se obtiene mediante el producto $E_1^{-1}*E_2^{-1}\dots E_{j-1}^{-1}*E_j^{-1}$. Las matrices Ei son triangulares inferiores, con unos en su diagonal principal, por lo tanto también $E_1^{-1} \forall i=1,2,\dots,j$ son también triangulares inferiores y el producto de triangulares inferiores se sabe que es triangular inferior, por lo tanto L es una matriz triangular inferior con unos en su diagonal principal. Sin embargo y de acuerdo a lo anterior, los elementos li,j= -ri,j para i > j. Para i=j, li,j=1 y i < j, li,j=0. Esta matriz configura lo que se llama la matriz llave del descifrado y es entregada mediante los factores (Tabla 3) organizados como elementos de una matriz triangular inferior para su aplicación inversa mediante (Tabla 3).

Finalmente, las permutaciones realizadas sobre la matriz representante del mensaje en claro generan las matrices de permutación P_1,P_2 que se construye de acuerdo a lo revisado para el método de doble transposición (tabla-ejemplo-doble-transposicion). Las permutaciones en filas que generan a la matriz P_1 y columnas P_2 establecen las dos primeras llaves del sistema, respectivamente.

3.1. Aplicación del cifrado mediante factorización PALU.

Considerando la matriz del mensaje en claro **CiFrAdO aPlIcAnDo FaCtOrIzAcIoN PALU,**

Tabla 3. Matriz del mensaje en claro CiFrAdO aPlIcAnDo FaCtOrIzAcIoN PALU.

.	1	2	3	4	5	6
1	C	i	F	r	A	d
2	O	.	a	P	l	I
3	c	A	n	D	o	.
4	F	a	C	t	O	r
5	I	z	A	c	I	o
6	N	.	P	A	L	U

Cada carácter del mensaje en claro, elemento de la matriz (tabla-ejemplo-LU), tiene asociado numéricamente un elemento de Z_{59}. De la clase del [0] hasta la clase del [28] el alfabeto español en mayúsculas, considerando la incorporación de las letras CH, LL y Ñ, en las clases [3], [13] y [16] respectivamente. Al espacio entre

palabras se le asigno la clase del [29] y el alfabeto en minúsculas desde la clase [30] hasta la clase [58], en el mismo orden que el anterior.

Tabla 4. Matriz con la asignación numérica con aritmética Z_{59} del mensaje en claro (Tabla 3).

.	1	2	3	4	5	6
1	2	39	6	50	0	34
2	17	29	30	18	42	9
3	32	0	45	4	47	29
4	6	30	2	52	17	50
5	9	58	0	32	9	47
6	15	29	18	0	12	23

Se aplica sobre la matriz (tabla-numérica-ejemplo-LU) el cifrado de doble transposición, mediante una permutación en filas y columnas, generando así, las primeras dos llaves k_{1},k_{2}, respectivamente del cifrado: k_{1}=(6,5,3,1,2,4)= FECHBCD y k_{2}=(3,1,6,2,5,4)= CHBFCED. La matriz P_1 AP_2, donde las matrices de permutación P_1,P_2 están modeladas mediante la formulación matricial del método de doble transposición.

Tabla 5. Matriz (Tabla 4) con la aplicación de permutaciones en filas y columnas.

.	3	1	6	2	5	4
6	18	15	23	29	12	0
5	0	9	47	58	9	32
3	45	32	29	0	47	4
1	6	2	34	39	0	50
2	30	17	9	29	42	18
4	2	6	50	30	17	52

Los multiplicadores (elemento-L) correspondientes al proceso de congruencia matricial a U corresponden a:

$r_{3,1}$= 14*23=27 mód 59
$r_{4,1}$= 53*23=39 mód 59
$r_{5,1}$= 29*23=18 mód 59
$r_{6,1}$= 57*23=13 mód 59
$r_{3,2}$= 35*46=17 mód 59
$r_{4,2}$= 3*46 =20 mód 59
$r_{5,2}$= 8*46 =14 mód 59
$r_{6,2}$= 35*46=17 mód 59
$r_{4,3}$= 17*34=47 mód 59
$r_{5,3}$= 40*34=3 mód 59
$r_{6,3}$= 32*34=26 mód 59
$r_{5,4}$= 56*36=10 mód 59
$r_{6,4}$= 49*36=53 mód 59

La matriz triangular superior obtenida corresponde a,

$$U = \begin{bmatrix} 18 & 15 & 23 & 29 & 12 & 0 \\ 0 & 9 & 47 & 58 & 9 & 32 \\ 0 & 0 & 33 & 58 & 52 & 17 \\ 0 & 0 & 0 & 41 & 24 & 14 \\ 0 & 0 & 0 & 0 & 13 & 8 \\ 0 & 0 & 0 & 0 & 0 & 10 \end{bmatrix}$$

El mensaje cifrado se obtiene transcribiendo de izquierda a derecha y de arriba a abajo, por filas, de acuerdo con la asignación numérica del alfabeto utilizado. Así, el mensaje está dado por PNU LAIozIcchztOkVALLne. Presentando en bloques de tres caracteres, como es habitual para su envío, resulta así:

PNU LAI ozI cch ztO kVA LLne

La tercera llave del cifrado k_3 corresponde a la colección de los factores (o multiplicadores) r_ij, que permiten la determinación de la matriz triangular inferior asociada a la factorización LU. De acuerdo a su posición en la matriz (i,j) transcribiendo de izquierda a derecha y de arriba a abajo, por filas, se tiene para esta aplicación: **AYOijoPMCHJLLOXwa**

$$L = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ -27 & -17 & 1 & 0 & 0 & 0 \\ -39 & -20 & -47 & 1 & 0 & 0 \\ -18 & -14 & -3 & 10 & 1 & 0 \\ -13 & -17 & -26 & -53 & 0 & 1 \end{bmatrix} \text{mód } 59$$

Desde el punto de vista criptoanalista, existen algoritmos de forma tal que la matriz U y la matriz L queden en una misma matriz cuadrada. La estrategia radica en que siendo todos los elementos de la

diagonal principal de U unos, no se requiere el espacio para almacenarlos. Este procedimiento se puede aplicar en virtud de la estructura de cuerpo de $(Z_{n'}+,\cdot)$ para n primo. También hay formas de programar el algoritmo para que las matrices de permutaciones, que gobierna el método de doble transposición P1, P2 se presenten por un sólo vector (de forma independiente, claro está) con n valores, numerados, que indican cómo deben permutarse los reglones de la identidad. Esto es muy conveniente pues las matrices P_i es tal que de sus n^2 valores todos son cero excepto n que son 1. Usando estas técnicas de almacenamiento requerido por el algoritmo de factorización PALU puede reducirse de $[\![3n]\!]^2$ a n^2+n números de punto flotante, lo que significa un ahorro de espacio aproximadamente de un 66%. Respecto a la aritmética modular utilizada, la determinación de los elementos simétricos aditivos y multiplicativos en $(Z_{n'}+,\cdot)$ tiene un grado de complejidad del orden de $([\![\log]\!]_2\ a)^3$, siendo $a \in Z_n$ la clase a la cual se necesitan sus simétricos. Lo anterior, pues en la utilización del algoritmo de Euclides extendido los números decaen a la mitad (al menos) a cada dos pasos.

4. CONCLUSIONES

El método de cifrado y descifrado, con fundamentos matemáticos desarrollados en el álgebra matricial que se propone en este artículo, inicia con la revisión del sistema de transposición, específicamente con el método de doble transposición. Esta metodología permite la extrapolación a nuevas técnicas de cifrado. La factorización matricial PALU es una de estas nuevas metodologías propuestas. Entre los alcances, se encuentra la posibilidad de generalización del alfabeto incorporando nuevos caracteres. La posibilidad de ocultar y sustituir parte del mensaje que se quiere comunicar en el criptosistema permite elevar el grado de seguridad e integridad de la información, de este modo se obtiene una mejora en la eficiencia de los métodos de cifrado en la línea de los sistemas de transposición, incorporando además un número de llaves mayor. El resultado obtenido nos muestra un buen rendimiento de cifrado, debido a la longitud del alfabeto utilizado, los órdenes de los cálculos matriciales y el uso de la aritmética modular.

Referencias Bibliográficas

[1] Triana Laverde, J. Aplicaciones matriciales a criptografía, 2011.

[2] Della Porta, G. De furtivis literarum notis vulgo de ziferis libri IIII. Mariam Scotum. Londres, 1591.

[3] Pousa, A., Diaz, J.,Giusti, A. Algoritmo de cifrado simétrico AES. Aceleración de tiempo de cómputo sobre arquitecturas multicore. Universidad Nacional de la Plata, 2011.

[4] Mao, W. Modern cryptography: theory and practice. https://doi.org/10.1093/aje/kwp410, 2004.

[5] Ron Rivest, Adi Shamir y Leonard Adleman. RSA algorithm. en: Revista Scientific American, 1977.

[6] Zimmermann, P. PGP(Pretty Good Privacy): Source Code and Internals Hardcover, 1995.

[7] Solís, F., León, W. El algoritmo criptográfico estándar avanzado de cifrado: bases e implementación. Congreso Internacional de Investigación Academia Journals, 2015.

[8] Maricela, J., Octavio F. Sistema para codificar información implementando varias órbitas caóticas. Ingeniería, Investigación y Tecnología. https://doi.org/10.1016/j.riit.2015.05.004, 2015.

[9] Raplh G. Matemáticas Discretas. Edición, 2011.

[10] Nakos. Álgebra lineal con aplicaciones. Edición 2007.

[11] Jorgensen, P. Applied cryptography: protocolos, algorithm and source code in C. Goverment Information Quarterly. https://doi.org/10.1016/S0740-624X(96)90083-0. 1996.