Morfismos, Vol. 19, No. 2, 2015, pp. 61–72

Ataque matricial a cifrados de sustitución monoalfabética*

Juan Gabriel Triana Laverde Jorge Mauricio Ruiz Vera

Resumen

Desde los inicios de la escritura se ha visto la necesidad de transmitir mensajes de manera que el significado permanezca oculto para aquellos que no sean el destinatario, para tal fin han sido desarrollados diversos métodos de cifrar mensajes, entre ellos el cifrado por sustitución monoalfabética, uno de los métodos clásicos de cifrado. En este artículo se establece un algoritmo, basado en herramientas computacionales y álgebra lineal numérica, con el cual es posible atacar mensajes cifrados por sustitución monoalfabética, mejorando los resultados obtenidos al atacar mediante un análisis de frecuencias.

2010 Mathematics Subject Classification: 65F30,11T71, 68U15.
Keywords and phrases: Algebra lineal numérica, criptografía, procesamiento de texto.

1 Introducción

La criptografía históricamente ha sido clasificada en dos etapas: criptografía clásica y criptografía moderna [11, pág. 3]. Según Giovanni Battista della Porta (1535-1615), en su texto de cuatro volúmenes *furtivis literarum notis-vulgo de ziferis*, uno de los primeros textos formales de criptografía [12, pág. 18], las técnicas clásicas de cifrado son de dos tipos: sustitución y trasposición, explicadas detalladamente en [15, pág. 9]; dichas técnicas continúan vigentes e incluso han sido utilizadas en el

*Este artículo corresponde a la tesis del primer autor, asesorada por el segundo autor, realizada para optar al título de Magister en Ciencias - Matemática Aplicada, otorgado el día 16 de febrero de 2012 por la Universidad Nacional de Colombia.

desarrollo de métodos modernos de cifrado, prueba de ello el uso de sustituciones y trasposiciones en el desarrollo de cifrados por bloques, con el fin de inducir confusión y difusión [15, pág. 147].

En el presente artículo se consideran los métodos de sustitución monoalfabética, también conocida como sustitución simple [13, pág. 17], explicada detalladamente en [3, pág. 3-8], en los cuales cada letra del alfabeto del mensaje es sustituido por un caracter del alfabeto de cifrado, de manera inyectiva; por lo tanto dado un mensaje cifrado por sustitución monoalfabética, en un alfabeto de n caracteres, se obtienen $n!$ posibles mensajes descifrados [19, pág. 8]; en el caso del español hay $n = 27$ caracteres, obteniendo así 27! posibles mensajes, del orden de 10^{28}, lo cual hace inviable un ataque por fuerza bruta [10, pág. 155-185].

El proceso para descifrar un mensaje cifrado por sustitución monoalfabética se basa en el uso de la tabla de frecuencias correspondiente a cada idioma, combinado con el análisis de frecuencias del mensaje; sin embargo, en mensajes cortos las frecuencias pueden no corresponder a las previstas en la tabla de frecuencias, por tal razón se propone un método para descifrar mensajes en español, cifrados mediante sustitución monoalfabética, en el cual se diferencian los caracteres cifrados que corresponden a vocales y consonantes; para tal fin, es necesaria la descomposición de valores singulares de la matriz de frecuencias correspondiente al mensaje, siguiendo la estrategia propuesta en [14] para mensajes en inglés.

2 Matriz de Frecuencias

El proceso de descifrado de un mensaje inicia con el estudio de la frecuencia con la que aparecen los caracteres en el mensaje, técnica conocida como análisis de frecuencias, descrita en términos de su creador, Al-kindi (801-873), en [4, pág. 125]. La efectividad del análisis de frecuencias radica en que distintas letras no aparecen con la misma frecuencia en un mensaje, esto hace que algunas de ellas destaquen por su abundancia, por ejemplo las letras e,a, y otras por su escasez como es el caso de k y x; en el caso de un mensaje en español. En particular, los mensajes cifrados por sustitución son susceptibles al análisis de frecuencias, como se explica en [12, pág. 239] y [3, pág. 3].

La información del análisis de frecuencias es almacenada en una matriz, denominada *matriz de frecuencias*, ya que permite un almacenamiento eficiente, además de las facilidades que ofrece para extraer

la información y la posibilidad de aplicar técnicas de álgebra lineal numérica. El proceso de construcción de la matriz de frecuencias se presenta en el siguiente algoritmo.

Algorithm 1 Algoritmo para construir la matriz de frecuencias

Require: Mensaje a descifrar
Ensure: Matriz de frecuencias
1: Enumerar los caracteres del alfabeto de cifrado
2: Tomar n, número de caracteres del alfabeto considerado
3: Crear una matriz $A_{n\times n}$.
4: Asignar la i-ésima fila para el i-ésimo carácter del alfabeto
5: Asignar la j-ésima columna para el j-ésimo carácter del alfabeto
6: **for** $i = 1 : n$ **do**
7: **for** $j = 1 : n$ **do**
8: $A_{ij} \leftarrow$ veces que el carácter i-ésimo es seguido por el carácter j-ésimo
9: **end for**
10: **end for**

La descomposición en valores singulares, cuyo algoritmo es presentado en [2, pág. 234], permite aproximar la matriz de frecuencias mediante matrices de rango menor, de este modo se obtiene la siguiente factorización

$$A = X\Sigma Y^T \tag{1}$$

donde X y Y son matrices unitarias y Σ es una matriz diagonal que contiene los valores singulares σ_i de la matriz de frecuencias A, ordenados de mayor a menor. Los valores singulares de la matriz A son definidos como las raíces cuadradas de los valores propios de la matriz A^tA [8, pág. 205]; debido a que A^tA es simétrica y definida positiva los valores singulares son reales positivos; además, como las componentes de la matriz de frecuencias son reales, X y Y son matrices ortogonales [6, pág. 70]. Realizando el producto propuesto en la ecuación 1, se obtiene que la matriz de frecuencias A puede escribirse como

$$A = \sum_{i=1}^{n} \sigma_i X_i Y_i^t \tag{2}$$

Los vectores X_i y Y_i se denominan vectores singulares a izquierda y derecha respectivamente [20, pág. 264]. Si en la ecuación 2 se considera

la suma hasta un valor $r \leq n$ se obtiene una aproximación de rango bajo [2, pág. 35] o reducida [9, pág. 83]; en particular si $r = 1$, la matriz de frecuencias A queda descrita en términos del primer valor singular σ_1, esta aproximación se denomina *aproximación de rango* 1 de la matriz de frecuencias A. Luego

$$A \approx \sigma_1 X_1 Y_1^t \tag{3}$$

Cabe destacar que la matriz de frecuencias tiene todas sus entradas mayores o iguales que 0, por esta razón se puede decir que los vectores singulares asociados a la aproximación de rango 1 poseen todas sus componentes positivas, lo cual es consecuencia del teorema de Perron-Frobenius [18, pág. 330].

Intrínsecamente al tomar la aproximación de rango 1, dada en la ecuación 3, se asume que el alfabeto considerado es un conjunto sin particiones, es decir, no se distinguen vocales ni consonantes. No obstante, pese a esta limitación es posible extraer información de utilidad, por ejemplo la frecuencia con la que aparece un caracter en el mensaje, para ello basta multiplicar la matriz de frecuencias por un vector columna de 1's, obteniendo así un vector columna en cuyas filas se encuentra el número de veces que aparece cada carácter en el mensaje; esto permite ordenar los caracteres por el número de apariciones que tengan en el mensaje. La siguiente tabla, denominada tabla de frecuencias, muestra la frecuencia de aparición de cada letra en el idioma español.

A	11,96%	B	0,92%	C	2,92%
D	6,87%	E	16,78%	F	0,52%
G	0,73%	H	0,89%	I	4,15%
J	0,30%	K	0,01%	L	8,37%
M	2,12%	N	7,01%	Ñ	0.29%
O	8,69%	P	2,77%	Q	1,53%
R	4,94%	S	7,88%	T	3.31%
U	4.80%	V	0.39%	W	0.01%
X	0.06%	Y	1.54%	Z	0.15%

Table 1: Tabla de frecuencias del idioma español. Tomado de [7, pág. 39]

Dado un mensaje cifrado, al ordenar los caracteres por el número de apariciones, es posible relacionar el carácter más frecuente del mensaje con la letra *e*, la más frecuente según la tabla de frecuencias dada en la tabla 1; siguiendo con esta idea se relacionaría el segundo carácter más

frecuente del mensaje con la letra a, la segunda más frecuente según la tabla de frecuencias dada en la tabla 1, y así sucesivamente para cada carácter.

La técnica descrita no siempre será efectiva, pero es un buen punto de partida ya que posiblemente algunos caracteres sean descifrados. El conocer cuántas veces un carácter es seguido por otro es conveniente, pues hay combinaciones de dos letras, denominadas bigramas, que se presentan a menudo, por ejemplo *en*, *es*, *el*, son las más comúnes en español [5, pág. 32], así como también hay combinaciones que no se presentan, *ñt*,*fg*. Dicho esto, al identificar algún carácter en el mensaje descifrado, se obtiene información acerca del carácter que más veces le sigue.

Dado que ninguna letra del alfabeto es consonante y vocal a la vez, y además al unir el conjunto de las vocales con el de las consonantes se forma todo el alfabeto, se obtiene que el conjunto de vocales y el de consonantes particionan el alfabeto. Con el fin de representar que el alfabeto es particionado por dos tipos de elementos, se considera la aproximación de rango 2 dada por:

$$A \approx \sigma_1 X_1 Y_1^t + \sigma_2 X_2 Y_2^t \tag{4}$$

Debido a que se considera el segundo valor singular de la matriz de frecuencias, no es posible garantizar que los vectores propios asociados tengan siempre términos positivos, ya que el Teorema de Perron Frobenius [18, pág. 330] establece una condición solo para el mayor valor singular y su correspondiente vector singular asociado. Considerando lo anterior, se construyen los vectores V y C, en términos de la aproximación de rango 2, de la siguiente manera:

$$V(i) = \begin{cases} 1, & \text{si } X_2(i) < 0,\ Y_2(i) > 0; \\ 0, & \text{en otro caso.} \end{cases}$$

$$C(i) = \begin{cases} 1, & \text{si } X_2(i) > 0,\ Y_2(i) < 0; \\ 0, & \text{en otro caso.} \end{cases}$$

Aquí $V(i) = 1$ si la letra i-ésima es vocal, $C(i) = 1$ si la letra i-ésima es consonante. Considerando la matriz de frecuencias A, y los vectores V y C se obtiene que:

$C^t AV =$ Número de ocasiones en que una consonante es seguida de una vocal

$V^tAV =$ Número de ocasiones en que una vocal es seguida de una vocal

$V^tAC =$ Número de ocasiones en que una vocal es seguida de una consonante

$C^tAC =$ Número de ocasiones en que una consonante es seguida de una consonante

$V^tAe =$ Número de vocales

$C^tAe =$ Número de consonantes

Adicionalmente $V^tAe + C^tAe$ es el número de caracteres que son usados en el mensaje.

Con el objetivo de reducir el conjunto de posibles soluciones se debe agregar una restricción, inherente al idioma, que permita ajustar el método a la realidad. En particular existe una regla que cumple el idioma español, al igual que el inglés y otros idiomas, conocida como *regla vfc*, por sus iniciales en inglés, la cual enuncia que es más frecuente que las consonantes sean seguidas por vocales y no que las vocales sean seguidas por vocales. Matemáticamente, la condición *vfc* se puede escribir, según [14], como:

$$\frac{\text{Número vocales seguidas por vocal}}{\text{Número de vocales}} - \frac{\text{Número consonantes seguidas por vocal}}{\text{Número de consonantes}} < 0,$$

lo cual puede escribirse en términos de los vectores V, C y la matriz de frecuencias como:

$$\begin{aligned} \frac{V^tAV}{V^tA(V+C)} - \frac{C^tAV}{C^tA(V+C)} &< 0 \\ \frac{[V^tAV][C^tA(V+C)] - [C^tAV][V^tA(V+C)]}{[V^tA(V+C)][C^tA(V+C)]} &< 0 \\ [V^tAV][C^tAV] + [V^tAV][C^tAC] - ([V^tAV][C^tAV] + [V^tAC][C^tAV]) &< 0 \\ [V^tAV][C^tAC] - [V^tAC][C^tAV] &< 0 \end{aligned}$$

Entonces, para que la partición satisfaga la regla *vfc* se debe cumplir

$$[V^tAV][C^tAC] - [V^tAC][C^tAV] < 0. \tag{5}$$

Por lo tanto, dado un mensaje con matriz de frecuencias A, es necesario encontrar una partición tal que la ecuación 5 se cumpla; en particular la definición dada para V y C satisface la desigualdad, incluso si se sustituye A por su aproximación de rango 2 [14].

Debido a que la clasificación de caracteres, como vocales o consonantes, es llevada a cabo mediante una estrategia numérica es posible

que tenga errores de precisión, por ello se considera un caso para el cual no halla suficiente evidencia para clasificar un carácter, ya sea como vocal o consonante, este caso es considerado en el vector N dado por

$$N(i) = \begin{cases} 1 & \text{si } X_2(i)Y_2(i) > 0; \\ 0 & \text{en otro caso,} \end{cases}$$

en el cual $N(i) = 1$ si el criterio no clasifica la letra i-ésima.

Ejemplo 2.1. Considerando el poema Nocturno [17], publicado en 1894, escrito por José Asunción Silva (1865-1898), la clasificación de las letras en los vectores V, C y N es dada por:

	V	C	N		V	C	N		V	C	N
A	1	0	0	J	0	1	0	R	0	1	0
B	0	1	0	K	0	0	0	S	0	1	0
C	0	1	0	L	0	1	0	T	0	0	1
D	0	1	0	M	0	1	0	U	1	0	0
E	1	0	0	Ñ	0	0	0	V	0	1	0
F	0	0	1	N	0	1	0	W	0	0	0
G	0	1	0	O	1	0	0	X	0	0	0
H	0	0	1	P	0	1	0	Y	0	1	0
I	0	0	1	Q	0	1	0	Z	0	1	0

Table 2: Asignación de letras en el poema *Nocturno*.

Las letras que no aparecen, k, ñ, w, x, tienen asignación 0 para V, C y N; las 19 letras que fueron clasificadas como vocal o consonante se asignaron correctamente; para 4 de las letras el criterio no realiza asignación.

Dado que la matriz de frecuencia contiene la información de los bigramas, o 2-gramas, se puede implementar en el método de descifrado la información correspondiente a los bigramas más frecuentes en un texto en español [1, pág. 115-125], en general esto puede hacerse con los k-gramas más frecuentes en cada idioma, con el fin de mejorar la precisión del descifrado. Matemáticamente, un texto puede ser modelado como una secuencia de k-gramas, con una probabilidad de transición entre los distintos k-gramas, que denominamos palabras, lo cual es descrito mediante una cadena de Markov [16, pág. 36]; sin embargo considerar más allá de bigramas implicaría mayor costo computacional y mayores consideraciones teóricas para obtener una mejora leve [16, pág. 43].

Por tal razón se consideran solo algunos bigramas asociados a la letra de mayor frecuencia, ya que es la letra más probable de ubicar en un mensaje cifrado.

3 RESULTADOS

A continuación se propone el siguiente procedimiento de descifrado, para mensajes cifrados mediante sustitución monoalfabética

Algorithm 2 Algoritmo para aplicar el método de descifrado.

Require: Mensaje a descifrar
Ensure: Mensaje descifrado
1: Construir la matriz de frecuencias del mensaje
2: Aplicar la tabla de frecuencias.
3: **if** el mensaje es legible **then**
4: Proponer el mensaje obtenido como solución.
5: **return**
6: **end if**
7: Construir V, C y N.
8: Combinar V, C y N con la frecuencia de caracteres y bigramas.
9: Proponer el mensaje obtenido como solución.
10: **return**

El resultado, una vez aplicado el procedimiento anterior, es una predicción de si cada carácter se trata de una consonante, una vocal o si no es posible determinarlo, junto con un posible mensaje descifrado que, aunque no es exacto siempre, es de gran utilidad en el proceso de descifrado del mensaje. Con el fin de establecer la efectividad del método propuesto se tomará un texto cifrado, posteriormente se presentan los resultados obtenidos al aplicar el método de descifrado propuesto

Ejemplo 3.1. Considere el siguiente texto cifrado, mediante sustitución monoalfabética, con una palabra clave aleatoria de longitud aleatoria.

"Vp wkhzwkp hg hv wbzxlzjb ih wbzbwkykhzjbg gkgjhypjkwpyhzjh hgjflwjlfpibg bÑjhzkibg yhikpzjh vp bÑghfnpwkbz ih cpjfbzhg fhqlvpfhg,ih fpubzpykhzjbg t ih hrchfkyhzjpwkbz hz pyÑkjbg hgchwkekwbg ih vbg wlpvhg gh qhzhfpz cfhqlzjpg gh wbzgjflthz skcbjhgkg gh ihilwhz cfkzwkckbg t gh hvpÑbfpz vhthg qhzhfpvhg t hgdlhypg yhjbikwpyhzjh bfqpzkupibg Vp wkhzwkp ljkvkup ikehfhzjhg yhjbibg t jhwzkwpg cpfp

VP PIDLKGKWKBZ T BFQPZKUPWKBZ IH WBZBWKYKHZJBG GBÑFH VP HGJ- FLWJLFP IH LZ WBZXLZJB IH SHWSBG GLEKWKHZJHYHZJH BÑXHJKNBG T PWWHGKVHG P NPFKBG BÑGHFNPI- BFHG PIHYPG IH ÑPGPFGH HZ LZ WFKJHFKB IH NHFIPI T LZP WBFFHWWKBZ CHFYPZHZJH VP PCVKWPWKBZ IH HGBG YHJBIBG T WBZBWKYKHZJBG ÑLGWP VP QHZHFPWKBZ IH YPG WBZBWKYKHZJB BÑXHJKNB HZ EBFYP IH CFHIKWWKBZHG WBZWFHJPG WLPZJKJPJKNPG T WBYCFBÑPÑVHG FHEHFKIPG P SHWSBG BÑGHFNPÑVHG CPGPIBG CFHGHZJHG T ELJLFBG WBZ EFHWLHZWKP HGPG CFHIKWWKBZHG CLHIHZ EBFYLVPFGH YHIKPZJH FPUBZPYKHZJBG T HGJFLWJLFPFGH WBYB FHQVPG B VHTHG QHZHFPVHG DLH IPZ WLHZJP IHV WBYCBFJPYKHZJB IH LZ GKGJHYP T CFHIKWHZ WBYB PWJLPFP IKWSB GKGJHYP HZ IHJHFYKZPIPG WKFWLZGJPZWKPG PVQLZBG IHGWLÑFKYKHZJBG WKHZJKEKWBG CLHIHZ FHGLVJPF WBZJFPFKBG PV GHZJKIB WBYLZ HXHYCVBG IH HGJB GBZ VP JHBFKP PJBYK- WP B VP YHWPZKWP WLPZJKWP DLH IHGPEKPZ ZBWKBZHG WBYLZHG GBÑFH VP YPJHFKP YLWSPG WBZWHCWKBZHG KZJLKJKNPG IH VP ZPJLFPVHUP SPZ GKIB JFPZGEBFYPIPG P CPFJKF IH SPVVPUQBG WKHZ- JKEKWBG WBYB HV YBNKYKHZJB IH JFPGVPWKBZ IH VP JKHFFP PVFHIHIBF IHV GBV"

Aplicando el análisis de frecuencias, basado en la aproximación de rango 1, se obtiene

"MA INERINA ES EM IORZTRLO CE IOROINUNERLOS SNSLEUALNIAUERLE ESLDTILTDACOS OBLERNCOS UECNARLE MA OBSEDQAINOR CE PALDORES DEYTMADES, CE DAFORAUNERLOS G CE EXPEDNUERLAINOR, ER AUBNLOS ESPEINVNIOS CE MOS ITAMES SE YEREDAR PDEYTRLAS, SE IORSLDTGER HNPOLESNS, SE CECTIER PDNRINPNOS G SE EMABODAR MEGES YEREDAMES G ESJTEUAS UELOCNIAUERLE ODYARNFACOS. MA INERINA TLNMNFA CNVEDERLES UELOCOS, G LEIRNIAS PADA MA ACJTNSNINOR G ODYARNFAINOR CE IOROINUNERLOS SOBDE MA ESLDTILTDA CE TR IORZTRLO CE HEIHOS STVNINERLEUERLE OBZELNQOS G AIIESNBMES A QADNOS OBSEDQACODES, ACEUAS CE BASADSE ER TR IDNLEDNO CE QEDCAC G TRA IODDEIINOR PEDUARERLE. MA APMNIAINOR CE ESOS UELOCOS G IOROINUNERLOS BTSIA MA YEREDAINOR CE UAS IOROINUNERLO OBZELNQO ER VODUA CE PDECNIINORES IORIDELAS, ITARLNLALNQAS G IOUPDOBABMES, DEVEDNCAS A HEIHOS OBSEDQABMES PASACOS, PDESERLES, G VTLTDOS. IOR VDEITERINA ESAS PDECNIINORES PTECER VODUTMADSE UECNARLE DAFORAUNERLOS G ESLDTILTDADSE IOUO DEYMAS O MEGES YEREDAMES, JTE CAR ITERLA CEM IOUPODLAUNERLO CE TR SNSLEUA, G PDECNIER IOUO AIL-

tada cniho snsleua er celedunracas inditrslarinas. Amytros cesitbdnunerlos inerlnvnios ptecer destmlad iorldadnos am serlnco ioutr. Ezeupmos ce eslo sor ma leodna alounia o ma ueiarnia itarlnia jte cesavnar roinores ioutres sobde ma ualedna. Utihas ioriepinores nrltnlnqas ce ma raltdamefa har snco ldarsvoduacas a padlnd ce hammafyos inerlnvnios iouo em uoqnunerlo ce ldasmainor ce ma lnedda amdececod cem som"

Aplicando el método propuesto, basado en la aproximación de rango 2, se obtiene

"Pa ciencia es ep conjunto de conocimientos sistematicamente estructurados ogtenidos mediante pa ogserhacion de batrones requpares,de razonamientos v de exberimentacion en amgitos esbeciyicos de pos cuapes se qeneran brequntas se construven fibotesis se deducen brincibios v se epagoran peves qenerapes v esñuemas metodicamente orqanizados Pa ciencia utipiza diyerentes metodos v tecnicas bara pa adñuisicion v orqanizacion de conocimientos sogre pa estructura de un conjunto de fecfos suyicientemente ogjetihos v accesigpes a harios ogserhadores ademas de gasarse en un criterio de herdad v una correccion bermanente Pa abpicacion de esos metodos v conocimientos gusca pa qeneracion de mas conocimiento ogjetiho en yorma de bredicciones concretas cuantitatihas v combrogagpes reyeridas a fecfos ogserhagpes basados bresentes v yuturos Con yrecuencia esas bredicciones bueden yormuparse mediante razonamientos v estructurarse como reqpas o peves qenerapes ñue dan cuenta dep combortamiento de un sistema v bredicen como actuara dicfo sistema en determinadas circunstancias Apqunos descugrimientos cientiyicos bueden resuptar contrarios ap sentido comun Ejembpos de esto son pa teoria atomica o pa mecanica cuantica ñue desayian nociones comunes sogre pa materia Mucfas concebciones intuitihas de pa naturapeza fan sido transyormadas a bartir de fappazqos cientiyicos como ep mohimiento de traspacion de pa tierra aprededor dep sop"

La aproximación de rango 1 obtiene un mensaje descifrado muy pobre, como se observa al intentar leer, pues la longitud del mensaje no garantiza la convergencia de las frecuencias de aparición en el mensaje

a las mostradas en la tabla de frecuencias, presentada en la tabla 1. Por otra parte, el resultado obtenido por el método propuesto, presentado en el algoritmo 2, muestra una clara mejoría ya que al aplicar aproximaciones algebraicas y bigramas se logra extraer más información, lo cual permite mejorar significativamente los resultados obtenidos para mensajes cuya longitud es corta, por ejemplo mensajes de longitud inferior a una página.

Juan Gabriel Triana Laverde
Departamento de matemáticas,
Universidad Nacional de Colombia,
Bogotá, Colombia
jtrianal@unal.edu.co

Jorge Mauricio Ruiz Vera
Departamento de matemáticas,
Universidad Nacional de Colombia,
Bogotá, Colombia
jmruizv@unal.edu.co

Referencias

[1] Alvarez, C., Carreiras, M., De Vega, M. Estudio estadístico de la ortografía castellana (1): Frecuencia de bigramas, Cognitiva 4(1) (1992) 107-125.

[2] Bau, D., Trefethen, L. Numerical linear algebra, society for industrial and applied mathematics. 1997.

[3] Bishop, D. Introduction to cryptography with java applets, Jones & Bartlett Learning. 2003.

[4] Fernandez, S. La criptografía clásica, Revista SIGMA 24 (2004) 119-141.

[5] Garcia, E., Lopez, M., Ortega, J. Introducción a la criptografía. Historia y actualidad. Colección monografías, ediciones de la Universidad de Castilla. 2006.

[6] Golub, G., Van Loan, C. Introduction to scientific computing, Prentice Hall. 1996.

[7] Gómez, J. Matemáticos, espías y piratas informáticos, RBA Libros S.A. 2010.

[8] Horn, R., Johnson, C. Matrix analysis, Cambridge University Press. 1990.

[9] Ipsen, I. Numerical matrix analysis, society for industrial and applied math. 2009.

[10] Joux, A. algorithmic cryptanalysis, Chapman and Hall. 2009.

[11] Katz, J., Lindell, Y. Introduction to modern cryptography. Chapman & Hall/CRC. 2007.

[12] Konheim, A. Computer security and cryptography, Wiley. 2007.

[13] Menezes, A., Oorschot, P., Scott, V. Handbook of applied cryptography, CRC Press. 2010.

[14] Moler, C. Singular value analysis of cryptograms, The american mathematical monthly, 90(2) (1983) 78-87.

[15] Mollin, R. An introduction to cryptography, Chapman and Hall. 2007.

[16] Mumford, D. Desolneux, A. Pattern Theory: The stochastic analysis of real-world signals, CRC Press. 2010.

[17] Orjuela, H. La primera versión del nocturno de Silva, Thesaurus 34 (1974) 118-128.

[18] Poole, D. Álgebra lineal, una introducción moderna, Cengage learning editores. 2007.

[19] Stinson, D: Cryptography theory and practice, Chapman & Hall. 2006.

[20] Watkins, D. Fundamentals of matrix computations, John Wiley & sons. 2002.