novática
CEPIS UPGRADE Revista de la Asociación de Técnicos de Informática

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática), organización que edita también la revista **REICIS** (Revista Española de Innovación, Calidad e Ingeniería del Software). ***Novática*** co-edita asimismo **UP**GRADE, revista digital de **CEPIS** (*Council of European Professional Informatics Societies*), en lengua inglesa, y es miembro fundador de **UP**ENET (***UP****GRADE* **E***uropean* **NET***work*).

<http://www.ati.es/novatica/>
<http://www.ati.es/reicis/>
<http://www.cepis.org/upgrade>

ATI es miembro fundador de **CEPIS** (*Council of European Professional Informatics Societies*) y es representante de España en **IFIP** (*International Federation for Information Processing*); tiene un acuerdo de colaboración con **ACM** (*Association for Computing Machinery*), así como acuerdos de vinculación o colaboración con **AdaSpain**, **AI2**, **ASTIC**, **RITSI** e **Hispalinux**, junto a la que participa en **ProInnova**.

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Padilla 66, 3º, dcha., 28006 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Composición, Edición y Redacción ATI Valencia
Av. del Reino de Valencia 23, 46005 Valencia
Tlfn./fax 963330392 <secreval@ati.es>
Administración y Redacción ATI Cataluña
Via Laietana 46, ppal. 1ª, 08003 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>
Redacción ATI Aragón
Lagasca 9, 3-B, 50006 Zaragoza.
Tlfn./fax 976235181 <secreara@ati.es>
Redacción ATI Andalucía <secreand@ati.es>
Redacción ATI Galicia <secregal@ati.es>
Suscripción y Ventas <http://www.ati.es/novatica/interes.html>, ATI Cataluña, ATI Madrid
Publicidad
Padilla 66, 3º, dcha., 28006 Madrid
Tlnf.914029391; fax.913093685 <novatica@ati.es>
Imprenta: Derra S.A., Juan de Austria 66, 08005 Barcelona.
Depósito legal: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Portada: Resolución en marcha - Concha Arias Pérez / © ATI
Diseño: Fernando Agresta / © ATI 2003

Nº 211, mayo-junio 2011, año XXXVII

sumario

Tema del próximo número: "*Innovación y emprendimiento en Informática*"

Tomás F. Tornadijo Rodríguez
Analista informático; Encargado del dpto. de informática de Cartonajes Vir, S.A.

<tornadijo@telecable.es>

Criptoanálisis mediante algoritmos genéticos de una comunicación cifrada en la Guerra Civil

Resumen: *El propósito de este artículo es mostrar la aplicación de un algoritmo genético, asistido con información de contexto del mensaje, al desciframiento de un radiotelegrama cifrado mediante una tabla de substitución homofónica al comienzo de la guerra civil española.*

Palabras clave: *Algoritmo genético, cifra homofónica, criptoanálisis.*

1. Introducción

Entre los diferentes métodos de cifrado utilizados durante la Guerra Civil, uno de los más empleados por ambos contendientes fue una variante del cifrado por tabla de homófonos: el criptógrafo de cinta. Este sistema consiste en una tabla que tiene un alfabeto ordenado en la fila superior, bajo el que se dispone una cinta móvil con otro alfabeto doble aleatorio que encabeza las columnas de homófonos, que son las cifras de un par de dígitos que substituirán a las letras en el mensaje cifrado.

El emisor y el receptor del mensaje convienen una correspondencia determinada entre una letra de la primera fila y otra de la fila inferior, desplazando la cinta móvil para alinearlas. Entonces, para cifrar un mensaje se busca cada letra del mismo en la cinta móvil, substituyéndola en el texto cifrado por uno cualquiera de los homófonos de su columna, variación que hará menos susceptible esta cifra a los intentos de ruptura mediante la técnica del análisis de frecuencias.

El 29 de julio de 1936 el general Mola envió al general Franco un radiotelegrama cifrado pero con partes del texto en claro, de cuyo contenido se desprende que es un parte de operaciones de varios teatros bélicos. Este radio fue interceptado por los republicanos y una copia del mismo se puede ver en el *Taller de criptografía* [1], la extensa página Web sobre el particular del profesor Arturo Quirantes Sierra.

El encabezado del mensaje aclara que se utiliza la clave *Regidor*, que es un cifrado homofónico, sin cinta móvil [2, pág. 43], de modo que las columnas de homófonos se corresponden con un único alfabeto. Vamos a intentar romper la cifra de esta comunicación militar utilizando un algoritmo genético, ayudándolo con algún término que podamos conjeturar a partir de los fragmentos de texto en claro.

2. Metodología

2.1. Datos de partida

Supondremos que el documento que vamos a tratar de descifrar, está cifrado con una clave homofónica, de manera que cada número de dos dígitos se corresponde con una única letra en el texto en claro, en tanto que cada letra puede estar representada por varios números. Los cinco bloques en cifra se agruparán en uno solo para su descifrado.

Por otra parte, se observa que el último homófono del mensaje es el 00, que no se repite en ninguna otra posición, por lo que parece razonable suponer que se trate de algún de indicativo de fin de comunicación, así que se considerará, en principio, que no codifica ninguna letra.

El mensaje se presenta tal cual se publica en la Web, no se ha investigado en los archivos militares si el documento está descifrado, ni se ha buscado por otros medios la clave del mismo.

2.2. Método de descifrado

Para establecer esta correspondencia entre cifras y letras del alfabeto vamos a utilizar un algoritmo genético, que es un método de ataque ampliamente utilizado en el criptoanálisis moderno [3], y que, además, ya ha sido aplicado al desencriptado de documentos cifrados durante la guerra civil [2].

Sin embargo los esfuerzos desarrollados hasta el momento solo permiten atacar con éxito aquellos documentos cifrados de los que se conozca la tabla de homófonos pero no el alfabeto de cinta móvil, es decir cuando se sabe que cifras van juntas, pero no a que letra corresponden, pues de otra manera el espacio de búsqueda resulta demasiado amplio [2, pág. 17).

Para intentar resolver esta dificultad proponemos un algoritmo genético con una función objetivo que valore la diferencia entre las frecuencias encontradas de letras y bigramas y las frecuencias esperadas procedentes de un texto de referencia. Además este algoritmo tendrá un operador que permitirá vincular una palabra o texto corto a un determinado fragmento del mensaje, de forma que si esa palabra o texto corto realmente figurase en el texto en claro y en esa misma posición, entonces los homófonos correspondientes a sus letras quedarían bien asignados, resolviéndose correctamente otras porciones del mensaje y disminuyendo, en principio, la diferencia de frecuencias, mejorándose así el valor de la función objetivo.

El programa analizará la palabra clave, colocándola sucesivamente en todas las posiciones del texto y lanzará el algoritmo genético para cada una de ellas, guardando el valor de la función objetivo en una tabla, junto con texto descifrado, para obtener una estadística del desempeño.

Finalizado el análisis, comprobaremos si el texto en claro resulta inteligible, aunque sea de forma parcial, para los mejores valores de aptitud conseguidos. Si no es así, pensaremos en una nueva palabra y prepararemos el programa para realizar un nuevo análisis.

Hay que observar que este procedimiento es solo semiautomático, pues necesitamos conocer ciertos detalles pertenecientes al contexto del mensaje, por lo que resulta más apropiado para el criptoanálisis de documentos que alternen el texto en cifra con zonas en claro, como es el que nos ocupa.

3. Algoritmo genético

3.1. Introducción

Los algoritmos genéticos son unos métodos heurísticos de búsqueda y optimización, basados en la teoría de la evolución de Darwin, de acuerdo a la cual los individuos con mejor grado de adaptación al medio (*eficacia biológica* o *fitness*) sobreviven en mayor número, transmitiendo a la descendencia los rasgos adaptativos expresados por sus cromosomas.

3.2. Descripción de un algoritmo genético

Los algoritmos genéticos [4] imitan la acción de la selección natural a partir de una población de partida, cuyos individuos codifican en una cadena (cromosoma) una solución inicial a un problema, normalmente aleatoria. El algoritmo actúa sobre esta población sometiéndola a unas operaciones similares a los mecanismos evolutivos naturales:

- Selección. Los individuos más aptos tienen mayor probabilidad de pasar a la siguiente generación.
- Cruce. Consiste en combinar las características de los cromosomas de dos individuos

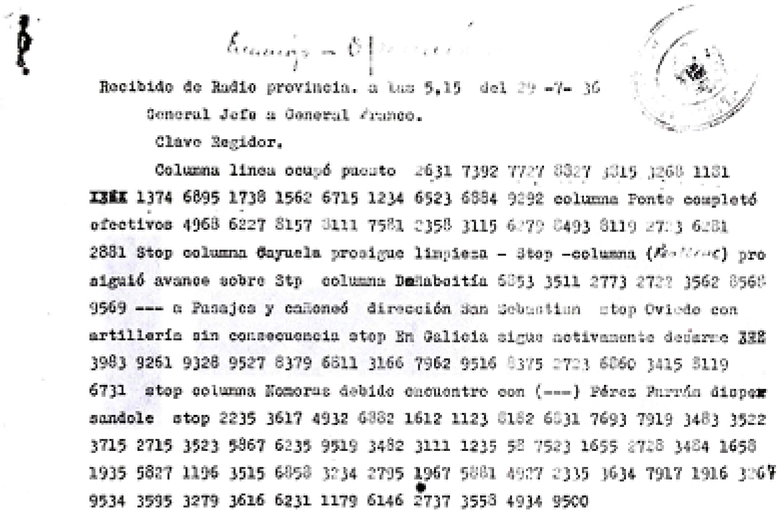
Recibido de Radio provincia. a las 5,15 del 29 -7- 36
General Jefe a General Franco.
Clave Regidor.
Columna linea ocupó puesto 2631 7392 7727 8327 3315 3268 1131
1374 6895 1738 1562 6715 1234 6523 6884 9292 columna Ponte completó
efectivos 4968 6227 8157 3111 7581 2358 3115 6279 8493 8119 2723 6281
2881 Stop columna Cayuela prosigue limpieza - Stop -columna ([illegible]) pro
siguió avance sobre Stp columna Dalabeitía 6853 3511 2773 2722 3562 8568
9569 --- a Pasajes y cañoneó dirección San Sebastian stop Oviedo con
artillería sin consecuencia stop En Galicia sigue activamente desarme
3983 9261 9328 9527 8379 6611 3166 7962 9516 8375 2723 6060 3415 8119
6731 stop columna Nomorus debido encuentro con (---) Pérez Farrás disper
sandole stop 2235 3617 4932 6882 1612 1123 8182 6831 7693 7919 3483 3522
3715 2715 3523 5867 6235 9519 3482 3111 1235 52 7523 1655 2728 3484 1658
1935 5827 1196 3515 6858 3234 2795 1967 5881 4927 2335 3634 7917 1916 3267
9534 3595 3279 3616 6231 1179 6146 2737 3558 4934 9500

Figura 1. Radiotelegrama cifrado. Fuente: Arturo Quitantes [1].

para obtener uno nuevo.

- Mutación. Con cierta probabilidad se altera aleatoriamente el cromosoma de un individuo, incrementando con ello la diversidad genética de la población.

Un algoritmo genético canónico suele seguir el siguiente esquema:

{Generar la población inicial, P_i
  Evaluar aptitud P_i
  Repetir hasta g generaciones
    {Seleccionar los individuos de P_i que pasarán a P_{i+1}
    Cruzar individuos de Pi y colocar en P_{temp}
    Mutar individuos de P_{temp} y colocar en P_{i+1}
    $P_i = P_{i+1}$
    Evaluar aptitud P_i
  }
}

Si el algoritmo está correctamente diseñado, la población convergerá hacia el mejor resultado que quedará registrado en el cromosoma del individuo más apto de la última generación.

3.3. Codificación

Cada individuo de la población representará una posible clave del mensaje, es decir: la relación de la tabla de homófonos con las letras del abecedario. Los cromosomas estarán formados por una cadena de texto con tantas letras del abecedario como homófonos diferentes existan en el mensaje, estando relacionada cada posición del cromosoma con una cifra determinada. Esta representación permitirá al programa atacar indistintamente tanto la cifra homofónica convencional como la de cinta móvil, pues al final ambas no pasan de ser una correspondencia donde se relaciona cada letra con varias cifras. Por otra parte, al no utilizar todos los números del 0 al 99, sino solo los presentes en el mensaje, evitaremos generar combinaciones improductivas y ahorraremos tiempo de proceso. En la **figura 2** se muestra un ejemplo con los cromosomas de dos individuos.

3.4. Selección

El algoritmo emplea una selección por torneo binario determinístico, procedimiento que consiste en tomar al azar dos individuos de la población seleccionando al más apto de ellos. Además se utiliza el elitismo, para asegurar que los individuos mejor adaptados de una generación pasen siempre a la siguiente.

3.5. Función objetivo

Para evaluar la aptitud de un individuo, el algoritmo utiliza sus cromosomas como clave para decodificar el texto cifrado. A continuación, con el texto conseguido, calcula la diferencia entre las frecuencias encontradas de letras y bigramas y las frecuencias esperadas, procedentes de un texto de referencia (se utilizó la novela *La Primera República*, de B. Pérez Galdós). Con objeto de disminuir el tiempo de localización de los bigramas se implementó un procedimiento de búsqueda binaria en un vector ordenado.

La suma de las diferencias de letras y bigramas supone el error entre el texto descifrado y el paradigma, de manera que la idoneidad de la clave analizada, *k*, vendrá dada por la siguiente función [3, pág 43]:

$$C_k = \alpha \bullet \sum_{i \in A} |K^u_{(i)} - D^u_{(i)}| + \beta \bullet \sum_{i,j \in A} |K^b_{(i,j)} - D^b_{(i,j)}|$$

Donde *A* denota el alfabeto [A..Z], *K* denota las frecuencias de referencia, *D* las del texto analizado, los subíndices *u* y *b* las frecuencias de letras y bigramas respectivamente, en tanto que α y β son los pesos asignados a letras y bigramas, no resultando práctico introducir las frecuencias de los trigramas [3, pág 43]. Para este problema el algoritmo mejora la convergencia utilizando como pesos los valores 1 y 2 respectivamente. Además, para conseguir una función creciente, a medida que disminuye el error, se ha aplicado:

$$C_k = 5 - C_k$$

3.6. Población inicial

Rellenaremos cada posición del cromosoma con letras del abecedario tomadas aleatoriamente hasta la última posición, la 50, que es el total de homófonos diferentes (excluyendo el último, como se ha dicho anteriormente) que hay en el mensaje cifrado.

3.7. Mutación

Con cierta probabilidad, un individuo seleccionado sufre una operación de mutación, que consiste en elegir al azar un gen, un carácter de su cromosoma, y a continuación substituirlo por una letra tomada aleatoriamente del abecedario.

3.8. Cruce

El algoritmo utiliza uno de los operadores más sencillos, el cruce de un punto, que consiste en cortar dos cromosomas por una posición escogida al azar, generando cada uno un segmento de cabeza y otro de cola. Entonces el segmento de cabeza de un progenitor y el de de cola de otro se unen para dar lugar a un nuevo individuo.

3.9. Texto supuesto

Una vía para disminuir el elevadísimo número de combinaciones con las que tiene que trabajar el programa consiste en asociar un frag-

C	A	H	G	I	E	O	D	A	N	K	Z	B	E	O	S	N	..
00	11	12	15	16	17	19	22	23	26	27	28	31	32	34	35	36	..

A	O	J	E	C	B	V	Y	S	C	E	I	N	F	E	A	S	..
00	11	12	15	16	17	19	22	23	26	27	28	31	32	34	35	36	..

Figura 2. Dos cromosomas.

mento del mensaje cifrado con un texto en claro, una palabra o una frase corta supuesta a partir de la información que nos proporcionan las zonas en claro del mensaje, un procedimiento análogo a los rastreos de contenidos estereotipados que efectuaban los criptoanalistas británicos en los partes meteorológicos cifrados de la marina alemana durante la segunda guerra mundial, con la diferencia de que, en este caso, no podemos saber donde está ese fragmento de texto, por lo que probaremos en todas las posiciones, lanzando el algoritmo genético para cada una de ellas, de acuerdo al siguiente esquema:

```
{  t = longitud del texto cifrado
   b = longitud del texto de búsqueda
   x = 0
   Repetir hasta que x  = t - b + 1
  {x = x  + 1
    Lanzar algoritmo genético [x, texto de
búsqueda]
    Guardar x
    Guardar aptitud
    Guardar texto en claro
    }
}
```

Además el algoritmo genético cuenta con un operador adicional que modifica los cromosomas de los individuos en cada nueva generación, de forma que el mensaje en claro contenga el texto supuesto en la posición indicada.

4. Ajuste

4.1. Ensayos

Para ajustar los parámetros del algoritmo genético, se codificó un mensaje de la misma longitud que el radiotelegrama analizado, utilizando una clave con el mismo número de homófonos, y se ejecutó el programa (sin proporcionarle un texto supuesto) para un total de cinco combinaciones de pesos, contando la cantidad de letras coincidentes entre el mensaje descifrado por el programa y el texto original sin cifrar, con la intención de obtener un valor real de aptitud. Para cada combinación se ejecutó el algoritmo 50 veces, calculando el valor medio de la función de coste (ver **figura 3**).

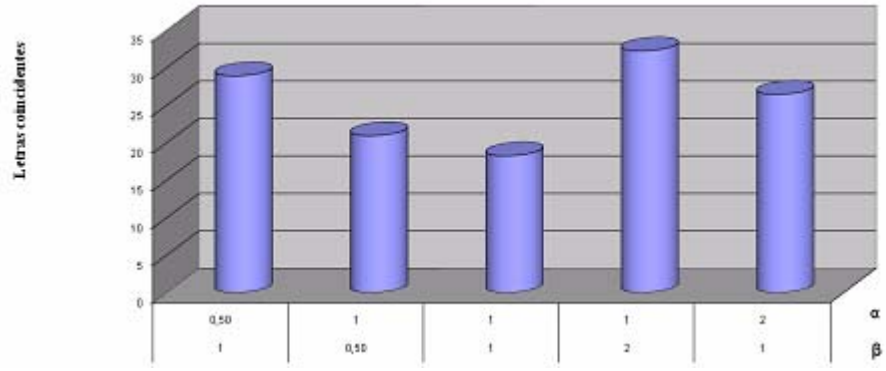

Figura 3. Aptitud real en función de los pesos α y β.

Los valores de las combinaciones primera y cuarta (ver **figura 3**) muestran una mejora del valor de la función de coste cuando aumenta el peso asignado a los bigramas, lo que resulta coincidente con los estudios de Clark & Dawson [3, pág 44] y otras experiencias [5, pág 19]. Usaremos la mejor combinación, con los valores α = 1 y β = 2.

Asimismo se comprobó que el algoritmo se comportaba bien con un valor de mutación alto: 0,008, y con un reparto de individuos y generaciones no muy elevado, de 500 y 50, respectivamente (ver **figura 4**). Todos estos parámetros serán los que utilicemos en el descifrado del mensaje de la guerra civil.

5. Resultados

Las primeras pruebas se realizaron sin proporcionar al algoritmo un texto supuesto, pero se observó que, aunque convergía adecuadamente consiguiendo generación tras generación valores de aptitud crecientes, el texto en claro obtenido al final del proceso nunca resultaba legible.

Como en una de las zonas no cifradas del telegrama se hace mención a la columna del general Miguel Ponte y Manso de Zúñiga, que por aquellas fechas intentaba abrirse paso hacia Madrid por la Sierra de Guadarrama, se consideró posible que el texto cifrado contuviese alguna mención a la ciudad de Madrid, objetivo último de la citada columna, información que habría resultado igualmente obvia para algún criptoanalista coetáneo al mensaje.

Sin embargo las pruebas realizadas con esos textos supuestos resultaron infructuosas, y no se pudo obtener ningún texto legible. Otros intentos utilizando algunas palabras típicas de la terminología militar, como *bombardeo*, *artillería*, *aviación*, *posición*, etc., tampoco arrojaron resultados satisfactorios.

Otro de los párrafos en claro hace referencia a la columna del capitán Pablo Díaz Duñabeitia, que por entonces operaba en Guipuzcoa, lo que hacía verosímil la presencia en el texto cifrado de alguna alusión a la capital de la provincia, San Sebastián, donde a la sazón se estaban produciendo importantes acontecimientos.

En este caso, con el valor de aptitud más alto conseguido cuando el texto se asocia a partir de la posición 158 del mensaje cifrado (ver **figura 5**), se obtuvo el siguiente resultado, donde se leen algunas palabras (en negrita) y donde se sugiere alguna otra más: MOMQ JASAPBTANORHANKPBREBSIALAT QQ/QARAOYONCOL**SOBRE**TPODALR OUO/AUENAMALERIANC/UDQFPU NADEANOMERNODCALAFIBODEO/ MLKQTACO SNLOCAOSPEDIDEMV BABELSERENDICONSESCLOSAUITOS **DESANSEBASTIAN**DESOQALELIEK DO**TENIENTE**LORONE FZAVESQIN

Podríamos intentar mejorar la solución mediante un reproceso con un mayor número de generaciones para esta posición del texto de búsqueda, pero también podemos intentar romper la cifra usando las nuevas palabras que conocemos, realizando un criptoanálisis clásico. Por ejemplo, podemos completar TENIENTE CORONEL, que parece una suposición bastante obvia a partir del texto que sigue a TENIENTE, lo que nos proporciona el siguiente mensaje, compuesto únicamente con las letras que hemos ido fijando: *O***A*A*BTAN***AN**BREB*I**A***/

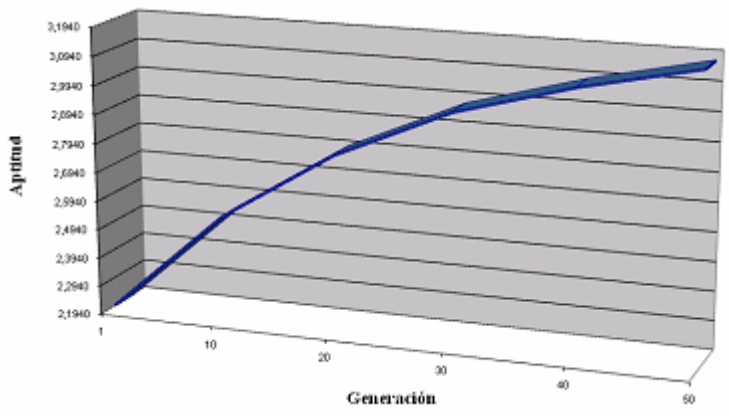

Figura 4. Aptitud en función del número de generaciones.

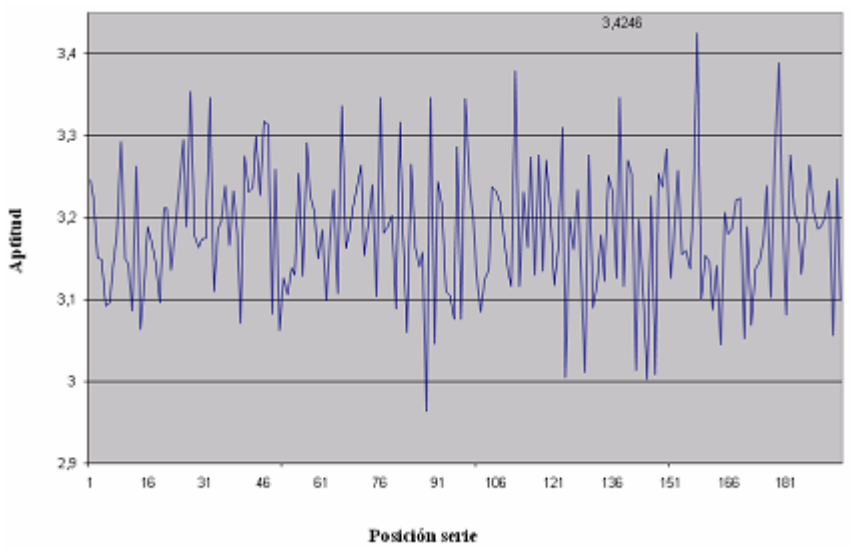

Figura 5. Aptitud en función de la posición del texto supuesto.

*ARA***N***SOBRE***DA*R***/A*ENA*A*ER*AN*/***L**NA*EANO*ERNO**A*A*IB*DEO/*EC**TA*O*N***AO**EDI*E**BABE*SERENDI*ON*ES**O*A*I*OSDESANS EBASTIANDES**A*ECIE*DO**TENIENTECORONEL*A*ES*IN**

El párrafo en negrita es claro que solo puede referirse al teniente coronel Vallespín, oficial al mando de los cuarteles de Loyola en aquella época. Completando VALESPIN, tenemos: *O***A*A* BTAN***AN**BREB*I**A***/PARA***N***SOBRE***DA*R***/A*ENA*A*ER*AN*/***L**NA*EANO*ERNO**A*A*IB*DEO/*EC*PTA*O*N***AO**EDI*E*LBABE*SERENDI*ON*ES**ONA*I*OSDESANSEBASTIAN**DES*PA*ECIE*D O**TENIENTE CORONEL VALESPIN

Completando DESAPARECIENDO: *O***A*A*BTANA**ANN*BREB*I*RA***/PARA**A*AN*AR**SOBRE**ADARRA*A**/A*ENA*ARER*AN*/***L**NA*EANO*ERNO**ARA**IBADEO**/*ECNPTA*O*NRA*AO**EDI*E*LBABERSERENDI*ON*ES*RONA*I*OSDESANSEBASTIANDESAPARECIENDOTENIENTECORONELVALESPIN

Completando AVANZAR GUADARRAMA Y RIBADEO: *O***A*A*BTANA**ANN*BREB*I*RAG**/PARAAVANZARSOBREGUADARRAMA/A*ENA*ARER*AN*/***LUMNA**EANO**ERNO*ZARA**RIBADEO/***ECNPTA*O*N**RA*AO*UEDI*E*LBABERSERENDI*ON*ESZRONAMIGOSDESANSEBASTIANDESAPARECIENDOTENIENTECORONELVALESPIN

Completamos COLUMNA, PERNOCTARA, DETECTADO, UN y vemos que hay varios homófonos confundidos en el texto cifrado: *O*O*A*A*BTANA**ANN*BRE**BUI*RAGO**PARAAVANTARSOBREGUADARRAMA/A*ENA*ARER*AN*/*COLUMNACEANO PERNOCTARARIBA DEO/DECNPTADOUNRADAOQUEDI CEDLBABERSERENDIDONUESTRONAMIGOSDESANSEBASTIANDESAPARECIENDOTENIENTECORONELVALESPIN

Completamos BUITRAGO: *O*O*A*A*BTANA**ANN*BREBUITRAGOO/PARAAVANTARSOBREGUADARRAMA/**A*ENA*A**RER*AN*/*COLUMNACEANOPERNOCTARARIBADEO/DECNPTADOUNRADAOQUEDICEDLBABERSERENDIDONUESTRONAMIGOSDESANSEBASTIANDESAPARECIENDOTENIENTECORONELVALESPIN

Completamos AMENAZA: *OZO*A*A*BTANA**ANN*BREBUITRAGOO/PARAAVANTARSOBREGUADA RRAMA/AMENAZA**RER*AN***/*COLUMNACEANOPERNOCTARARIBADEO/DE CNPTADOUNRADA OQUEDICE DLBA BERSERENDIDONUESTRONAMIGOSDESANSEBASTIANDESAPARECIENDOTENIENTE CORONELVALESPIN

Completamos HERNANI, nuevamente se han confundido homófonos: ***OZO*A***A*BTANA**ANN*BREBUITRAGOO PARAAVANTARSOBREGUADARRAMA/AMENAZARERNANI*COLUMNACEANOPERNOCTARARIBADEO/DECNPTADOUNRADAOQUEDICEDLBABERSERENDIDONUESTR ONAMIGOSDESANSEBASTIANDESAPARECIENDOTENIENTECORONELVALESPIN

Completamos LOZOYA, por ser el valle donde está Buitrago: LOZOYA*A*BTANA**ANN*BREBUITRAGOO/PARAAVANTARSOBREGUADARRAMA/AMENAZARERNANI/*COLUMNACEANOPERNOCTARARIBADEO/DECNPTADOUNRADAOQUEDICEDLBABERSERENDIDONUESTRONAMIGOSDESANSEBASTIANDESAPARECIENDOTENIENTECORONELVALESPIN

El párrafo entre LOZOYA y BUITRAGO no se ha podido resolver, tal vez por la existencia de más errores. El texto descifrado, interpolando los errores evidentes, quedaría así: LOZOYA**********BUITRAGO*/PARA AVANZARSOBREGUADARRAMA/AMENAZAHERNANI/*COLUMNACEANOPERNOCTARARIBADEO/DETECTADOUNRADIOQUEDICEDEHABERSERENDIDONUESTROSAMIGOSDESANSEBASTIANDESAPARECIENDOTENIENTE CORONELVAL LES PIN*

6. Conclusiones

Se ha conseguido romper la cifra de este mensaje y descifrarlo en su mayor parte y, aunque el método aplicado no puede considerarse una solución general para la ruptura de las cifras homofónicas, sí puede resultar de ayuda en los casos en los que se disponga de alguna información sobre el contenido o el contexto del mensaje. Como desarrollos futuros cabe imaginar un programa capaz de probar no una, sino varias palabras clave, tomándolas desde una base de datos, a costa de un importante tiempo de proceso.

Referencias

[1] A. Quirantes Sierra. *Taller de criptografía*, 2010, [2-12-2010]. Disponible en <http://www.cripto.es>.

[2] A.S. Gascón González. *Aplicación de algoritmos genéticos en el ataque de textos cifrados durante la guerra civil española.* Proyecto Fin de Carrera, 2010. <http://www.iit.upcomillas.es/pfc/resumenes/4c8615ad0a2b6.pdf>.

[3] Bethany Delman. *Genetic Algorithms in Cryptography*, 2004, <https://ritdml.rit.edu/bitstream/handle/1850/263/thesis.pdf?sequence=1>.

[4] J.H. Holland. *Adaptation in Natural and Artificial Systems*. Ann Arbor: The University of Michigan Press, 1975.

[5] Pallavi Kanagalakatte Basavaraju. *Heuristic Search Cryptanalysis of the Zodiac 340 Cipher*. Master's Projects. Paper 56, 2009. <http://scholarworks.sjsu.edu/etd_projects/56>.

Bibliografía

A. Clark, Ed. Dawson. Optimisation Heuristics for the Automated Cryptanalysis of Classical Ciphers. *Journal of Combinatorial Mathematics and Combinatorial Computing, 28*, 1998, pp. 63-86.

J. García Carmona. *Tratado de criptografía con aplicación especial al ejército*.Madrid: Sucesores de Rivadeneyra, 1894.

R. Otéeme, S. Arumugam. Applying Genetic Algorithms for Searching Key Space of Polyalphabetic Substitution Ciphers. *The International Arab Journal of Information Technology, vol. 5 (1)*, 2008.