El CNI i el -no tan secret- codi del Gran Capità

Autor:
Data de publicació: 03-02-2018

GamesGoldSilverBronze

1956 Melbourne
details
New Zealand
Peter Mander
Jack Cropp
Australia
Rolly Tasker
John Scott
Great Britain
Jasper Blackall
Terence Smith

Venditore ambulante, in Thesaurus del Nuovo soggettario, BNCF.

Aquesta vegada va de història, de la història estafada descoberta per un castellà

http://elprofedefisica.naukas.com/2018/02/02/el-cni-y-el-no-tan-secreto-codigo-del-gran-capitan/

[Ver Actualización al final del artículo]

Hoy viernes me ha llegado una noticia muy interesante. Según parece, el CNI ha descifrado uno de los códigos secretos usados por Gonzalo Fernández de Córdoba, el Gran Capitán (aquí y aquí; también aparece en El Mundo, El País, Público y suma y sigue). La noticia ha sido desvelada por cortesía del Museo del Ejército, que al parecer ha dado una rueda de prensa para presentar el hallazgo, obtenido a partir de cartas inéditas conservadas por los duques de Maqueda.

Según el diario ABC, de donde leí la noticia por primera vez, dicho código estaba “muy bien pensado” y “es un precursor del sistema Vigenère”, y la opinión de José Enrique Ruiz-Domènec, un experto en el Gran Capitán, es que “estamos ante un hallazgo fundamental para revisar uno de los momentos más importantes de la historia de España”

Bien, pues me alegro porque yo soy aficionado a la criptografía, con especial interés en la historia de la cripto en España. Mi viejo Taller de Criptografía sigue en pie (aquí), y todavía recuerdo haber leído algunas cartas intercambiadas entre el Gran Capitán y el rey Fernando el Católico. Acabo de revisarlas y he llegado a una interesante conclusión: el CNI ha descubierto un código que ya se conoce desde hace más de un siglo.

Escribí sobre dicho código en 2006 y en 2010. Para resumir la historia, resulta que un historiador inglés llamado

Gustave Bergenroth estuvo en el Archivo de Simancas a mediados del siglo XIX. Buscaba información sobre las relaciones entre España e Inglaterra y encontró un montón de legajos. Un buen número de ellos estaba cifrado, así que Bergenroth tuvo que descifrarlos personalmente. Sus experiencias como criptoanalista pasaron a un conjunto de documentos llamados State Papers, y puede usted leer aquí algunas clave sobre cómo logró descifrarlos. No se trata de usar ordenadores sofisticados sino papel, lápiz y paciencia.

Aquí tenéis la copia de la clave, tal como la descubrió Bergenroth. Se encuentra, junto con diversos documentos originales y copias descifradas por él, en la Biblioteca Nacional, signatura MSS 20.211. No sé si el original se encuentra disponible para el público, pero si van a la sección de microfilmes gustosamente le dejarán ver la versión en microfilm y hasta podrán sacar una copia en papel:

Puede comprobarse cómo los símbolos que representan letras individuales coinciden con las descubiertas por el CNI (aquí y aquí). No está completa, ya que muchos de los signos que indican palabras completas no aparecen, pero Bergenroth pudo obtener buen número de ellas. El descifrado del CNI, según el diario ABC, revela un total de 88 símbolos y 237 códigos de letras; yo he conseguido (bueno, Bergenroth consiguió) listar un total de 198 símbolos, de los cuales 89 tienen significado conocido. Por ejemplo, LUQ significa “Capitán”, TA representa “Turco” y UAE es “Papa”:

Ahora, en lo tocante a la clave en sí, debo decir algunas cosas.

En primer lugar, y en contra de lo que afirma ABC, este código no es de gran sofisticación. Se trata de un sistema de sustitución monoalfabética con homófonos al que se le ha añadido un conjunto de términos de lenguaje convenido. Tengo un buen puñado de códigos españoles de la época y puedo asegurar que los hay más sofisticados que éste. Por ejemplo, la llamada Clave de las Capitulaciones es similar en forma y estructura, siendo al menos diez años más antigua; y la Cifra General de los Reyes Católicos, de fecha similar a la del Gran Capitán, tenía nada menos que 670 términos en lenguaje convenido.

Segundo: tampoco creo que sea correcto decir que este sea un “precursor del sistema Vigenère”, a menos que con “precursor” se quiera decir “apareció antes de”. Ambos sistemas son diferentes, y por cierto, no recuerdo haber visto un solo mensaje de archivos españoles cifrado con sistema Vigenère (bueno, quizá uno).

En tercer lugar, ese tipo de claves ya era vulnerable a ataques criptoanalíticos en aquella época. Manías como la de cifrar solamente una parte de la carta, o repetir los términos cifrados usados, hacía que fuesen relativamente fáciles de descifrar por usuarios no autorizados. Como ejemplo, vamos a ver un fragmento de una carta enviada por el Gran Capitán hacia 1496. Está cifrada casi por completo (con una clave distinta a la que acaba de “descubrir” el CNI pero similar en estructura). Fíjese cómo el “casi” estropea la seguridad del sistema:

En la sexta fila aparece recuadrada la expresión “de manera” seguida de varios símbolos, cada uno de ellos representando una letra. ¿Qué puede ir tras las palabras “de manera”? La opción más lógica que se me ocurre es la palabra “que”. Si hacemos esa hipótesis no será raro encontrar algún otro trío de esos tres símbolos que representan la palabra “que”. Y en efecto, ahí pueden ver uno, resaltado al comienzo de la cuarta línea.

Algunas letras son más probables que otras, y aunque las más probables tienen más de un signo para cifrar, eso no es garantía de éxito. En el ejemplo anterior, la letra E tiene seis símbolos para cifrarla. Se supone que cada vez hay que usar un símbolo distinto precisamente para evitar los ataques de análisis por frecuencias, pero en la práctica los copistas no se complicaban mucho la vida y echaban mano de atajos, con la consecuencia de que el secreto de la carta puede desaparecer, como hemos visto en ese ejemplo.

Hay otras técnicas matemáticas y lingüísticas que pueden usarse y créanme, no son nada complejas. Cualquier estudiante de primer curso podría reventar esa carta y revelar su contenido, no hay que echar mano del CNI. Bergenroth lo hizo hace siglo y medio; si quiere verlo, aquí tiene un ejemplo del mismo legajo. El inglés no tuvo otra ocurrencia que escribir el texto descifrado sobre la misma carta original, algo que ahora le valdría un tirón de orejas frente a la Biblioteca Nacional pero que hace siglo y medio era algo normal.

Finalmente, y sin ánimo de criticar el trabajo de nadie, me resulta increíble que historiadores expertos y profesionales de inteligencia puedan pasar por alto los documentos que sobre el Gran Capitán se guardan en la Biblioteca Nacional. Yo tuve que pedir una tarjeta de investigador, desplazarme a Madrid y pasar varios días leyendo legajos, pero ahora mucho de ese trabajo puede hacerse online. No hay más que irse al catálogo online de la BME, teclear “Gonzalo

Fernández de Córdoba” y obtener un montón de referencias. Yo acabo de hacerlo, y la primera que me sale es un DVD de la serie Águila Roja, pero el legajo MSS 20.211 aparece ya en la tercera página de resultados.

Incluso podrían haberme preguntado a mí, que aparezco en la segunda página de resultados cuando metes “claves del gran capitán” en Google (imagino que salía en la primera página antes de salir esta noticia). Pero da igual, y como no quiero ser un destroyer, a continuación adjunto unos apuntes que tengo sobre los sistemas de cifrado del Gran Capitán. Si el Museo del Ejército o el CNI desean más detalles, estoy a su disposición.

“LAS CLAVES DEL GRAN CAPITAN” (Notas inéditas, Arturo Quirantes Sierra)

Tras la conquista de Granada, los principales campos de intervención de la nueva España se trasladan a Francia e Italia. Las pretensiones francesas sobre Italia en general y sobre el reino de Nápoles en particular chocan con los intereses españoles. Esto conllevó la aparición de nuevas aplicaciones criptográficas.

Como vimos anteriormente, ya durante la década de 1470 Fernando de Aragón mantuvo correspondencia cifrada con su padre Juan II en asuntos de índole política y militar. Sin embargo, el uso de sistemas de cifrado durante las campañas militares recibió un fuerte impulso de la mano del mejor soldado de Fernando: Gonzalo Fernández de Córdoba, el Gran Capitán. Dispuesto a negarle el reino de Nápoles a Carlos VIII de Francia –quien reivindicaba los derechos de la casa de Anjou por haber reinado en Nápoles anteriormente-, Fernando reaccionó despachando un ejército a Italia bajo el mando del Gran Capitán, quien desembarcó en la península en el año 1495. En apenas un año había derrotado al ejército francés y conquistado todo el Reino de Nápoles.

Durante la primera campaña italiana (1495-1497), el Gran Capitán llevaba consigo una cifra de sustitución monoalfabética homofónica, es decir, la cifra “estándar” en la España de la época, aunque sin diccionario ni listas de lenguaje convenido. Don Gonzalo no perdía mucho tiempo en enviar mensajes cifrados a sus majestades católicas, y cuando lo hacía era por intermedio de algún secretario. Ciertamente no escribía él mismo sus propios despachos cifrados; lo cual es hasta cierto punto una ventaja, ya que su firma resulta prácticamente ilegible.

Existió también un conjunto de cifras para los principales embajadores españoles en Italia, como Garcilaso de la Vega, embajador en Roma (y padre del famoso poeta); Juan Claver, embajador en Nápoles; y Alfonso de Fonseca. Son cifras similares a la del Gran Capitán aunque en algunos casos contaban con la adición de un pequeño diccionario. Según parece, el uso de diccionarios más o menos largos puede resultar adecuado en el ambiente diplomático, donde una embajada proporciona seguridad, tranquilidad y espacio, pero no resultaba idóneo en una campaña militar. Lo que no evita errores ni siquiera en las embajadas: una carta cifrada del representante en Milán, Juan Claver, está cifrada casi correctamente … salvo porque el embajador dejó los espacios entre palabras, otra gran ayuda para el criptoanalista enemigo.

La primera campaña italiana del Gran Capitán terminó con la completa conquista del reino de Nápoles. Por consideraciones de política internacional se procedió a un reparto, quedándose los franceses con las regiones de Campania y los Abruzos, y los españoles con las de Abulia y Calabria. No duró mucho la concordia entre Fernando de Aragón y Luis XII de Francia, sucesor de Carlos VIII, dando con ello comienzo la segunda campaña italiana de 1501-04. Para entonces, el Gran Capitán disponía de una nueva cifra, que usó con más asiduidad. Esta Gran Cifra (permítasenos llamarla así) era el sistema criptográfico más sofisticado utilizado en España hasta la fecha. Incluía la habitual tabla de sustitución monoalfabética con hasta siete homófonos, que se completaba con diversos signos nulos. Como novedad, por primera vez en la historia de la criptografía española, se utilizaba un signo anulante, cuya propiedad era la de dejar sin valor a los signos que se encuentran a su alrededor.

Como complemento, la Gran Cifra tenía un diccionario de más de doscientos términos (se desconoce el número exacto). Las palabras se cifraban como conjuntos de tres letras (sólo en raras ocasiones eran dos o cuatro), lo que resultaba bastante menos engorroso que recurrir a números romanos. Como particularidad, debe mencionarse que el diccionario no estaba ordenado en forma alfabética. Si el signo mad significaba como, mit significaba Italia y mun se transformaba en certifica. No era un diccionario totalmente desordenado, pero se apartaba bastante del orden alfabético. Tanto esto como la introducción de un signo anulante eran claros indicios de que el redactor de la Gran Cifra –cuyo nombre, por desgracia, se desconoce- era plenamente consciente de las capacidades criptoanalíticas de la época. A fin de cuentas, Italia era la cuna de la criptografía moderna, y Fernando se jugaba mucho para arriesgarse a dejar que sus secretos cayesen en otras manos, amigas o enemigas.

Hay constancia de que la Gran Cifra fue usada por entre 1500 y 1504, es decir, toda la segunda campaña italiana, para comunicarse con los Reyes Católicos Las cartas que escribía estaban sólo parcialmente cifradas, y aun entonces se dejaban palabras en claro. Es evidente que don Gonzalo no comprendía las sutilezas de la criptografía, aunque ello no

le impidió triunfar plenamente en el campo de batalla y ganarse el sobrenombre de Gran Capitán.

ACTUALIZACIÓN (3 febrero 2018, 18:00 horas)

Comentario al artículo “Un investigador del XIX resolvió parte del código del Gran Capitán” de Bruno Pardo Porto (diario ABC)

Estimado Sr. Pardo,

Soy Arturo Quirantes, y le adjunto la siguiente información por si le resulta de utilidad.

La misiva de la Biblioteca Nacional MSS 20.211/52, que incluye la cifra de sustitución homofónica, no es un “intento de resolver el enigma” sino, en efecto, su resolución, y sí llegaron a buen puerto, tanto es así que coinciden casi exactamente con las que ha redescubierto el CNI. Julio Martín, de El Confidencial, ha publicado un artículo con mucha información al respecto, entre otros una copia de la cifra que le he proporcionado yo mismo; por cierto, no entiendo el motivo por el que no se ha incluido esa referencia en el artículo que estoy contestando ahora mismo, pero creo que sería conveniente hacerlo.

El descifrador original, Gustave Bergenroth, ni siquiera era “estudioso de la criptografía”. Era un historiador que se vio en la obligación de improvisar un trabajo de criptoanalista para poder acceder a la información que necesitaba. Consiguió obtener la cifra de sustitución monoalfabética homofónica, y al menos un centenar de símbolos de lenguaje convenido; puede que la cifra supere los dos centenares, pero no podemos saberlo porque esa parte de su descubrimiento parece haberse perdido. Esos símbolos pueden verse en el resto de las cartas del antedicho legado 20.211, donde Bergentoth anota el descifrado sobre la propia carta.

Debo reconocer que lamento la forma en que se trata el trabajo del señor Bergenroth. Le recuerdo que él solo, sin ayuda de nadie y sin conocimientos criptoanalíticos, consiguió el mismo resultado que el CNI, y lo hizo en condiciones penosas.

Menciona usted que “Incomprensiblemente, el hallazgo que relata el profesor [Quirantes] no fue puesto a disposición de los especialistas en esta época” Mis descubrimientos sobre el tema fueron publicados en mi web Taller de Criptografía en 2006 y en 2010). No se me ocurrió compartirlos con ningún historiador porque a) no soy historiador yo y no conozco a ninguno, y b) creí que, si yo la había descubierto, cualquier otro podría. No he resultó tan difícil, sinceramente.

Sin perjuicio de ello, no tengo inconveniente en compartir información con quien me la pida, cosa que por ejemplo hice con los señores Julio Marín (quien hizo el artículo de El Confidencial) y Jesús García Calero (co-autor de los artículos del ABC sobre el descubrimiento). Teniendo en cuenta que una búsqueda en Google de “claves del Gran Capitán” ya incluye un boletín mío sobre el tema en la página 2, creo que cualquier persona interesada podría haber contactado conmigo hace años.

Respecto a su comentario “De hecho, en la encuesta realizada por ABC hoy entre los más destacados conocedores del siglo XVI español se constata que ninguno de ellos tenía noticia de la tabla”, debo reconocer que también a mí me ha sorprendido que ninguno de los expertos supiese que esa cifra ya estaba descubierta. Si yo, aficionado a la historia de la criptografía, fui capaz de encontrarlos en la Biblioteca Nacional, pensé que los expertos ya lo habrían hecho. Sinceramente, me siento tentado a escribir un libro sobre el tema, ya que al parecer he tenido en mis manos información de gran valor histórico durante años.

Estoy de acuerdo con usted en que conseguir las claves para poder leer mensajes cifrados antiguos es abrir una ventana al conocimiento histórico, y que pueden esperarse grandes descubrimientos en el futuro. En ese sentido, una revisión de los archivos actuales en busca de tales claves será una gran ayuda. Tengo en mi archivo personal varios centenares de esas claves, y gustosamente prestaré mi ayuda a cualquier historiador profesional que lo desee. Arturo Quirantes.