El secreto es el alma de toda empresa. Napoleón I.

Introducción.

Parece un anacronismo estudiar los métodos de cifra antiguos dado el alto nivel al que se ha llegado en el estudio de la Criptología moderna. Sin embargo no es tan descabellado el realizar estudios serios sobre el tema, a ello nos incitan varias razones. En primer lugar son un complemento imprescindible de la ciencia historiográfica. Es muy frecuente por parte de muchos historiadores el dejar de lado ciertos documentos depositados en los Archivos por estar en cifra. Si bien es cierto que el descifrado de documentos es difícil, y que no siempre conlleva el éxito la tarea emprendida, también lo es que los documentos y las comunicaciones verdaderamente importantes se cifran, con lo que al dejar de lado estos documentos estamos menospreciando una parte importante de la Historia.

Otro aspecto a destacar del estudio de los métodos de lápiz y papel es que siguen utilizándose ampliamente. En un artículo publicado en la revista del FBI firmado por Daniel Olson, criptoanalista de este organismo (8), se nos presentan varios de los métodos utilizados por el hampa, y no se diferencian en muchos casos de los métodos ya utilizados en siglos anteriores.

Queremos también en este texto dar un enfoque diferente al que generalmente se ha dado a la criptología española, sin ocultar errores, pero tampoco sin ser chauvinistas. El enfoque, generalmente distorsionado, que hace aparecer a la criptología española como una disciplina pobremente utilizada y de un valor menor, nos parece de una simplicidad rayana en la ingenuidad. Esta visión, muy frecuentemente adoptada por los textos anglosajones, y que en contraposición toma como modelos a Francia e Inglaterra, es, sin ningún tipo de duda falsa. España tuvo épocas en las que la criptología brilló con luz propia, y épocas en las que se tocó fondo, al igual que en Francia e Inglaterra.

El presente texto es un resumen muy breve. A todos los que quieran ampliar sobre el tema les invitamos a que lean nuestro libro "Mensajes secretos" en el que se hace un detallado repaso de la historia de criptología española.

Por último cabe destacar un aspecto a tener en cuenta en el estudio de los métodos criptográficos utilizados en las contiendas. Como en las películas, siempre ganan los "buenos", con lo que la visión que obtenemos siempre es parcial y sesgada en un sentido. El investigador debe ser consciente de ello, así como de que los métodos utilizados por los contrincantes son conocidos, exceptuando algún caso verdaderamente afortunado, por los descriptados realizados por el bando contrario. Las buenas normas hacen que el cifrado se elimine una vez descifrado el documento, con lo que en general, los métodos que sobreviven son los que no han servido para su función, es decir, los que han sido "rotos" por el enemigo. Es importante tener muy en cuenta este hecho, ya que si no somos conscientes de él podemos errar en la apreciación de las capacidades reales de los contendientes.

Los principios de la ocultación de mensajes.

La ocultación de la información se utiliza desde hace muchos siglos en formas de lo más variado. Tradicionalmente este proceso se realiza de dos maneras, ocultando el mensaje en sí, o bien ocultando el significado del mismo. En el primer caso hablamos de esteganografía y en el segundo de criptografía. El ejemplo más antiguo de método esteganográfico, del que tenemos conocimiento, viene detallado en "*los nueve libros de la historia*" de Herodoto. En él se nos cuenta como para enviar un mensaje de forma secreta se

rapa la cabeza a un esclavo y se le tatúa un mensaje en el cuero cabelludo, cuando el pelo crece lo suficiente, se envía el esclavo al destinatario del mensaje.

> Pues como Histieo quería indicar a Aristágoras que se sublevase, y no tenía ningún medio seguro de indicárselo por cuanto los caminos estaban vigilados, rapó la cabeza del más fiel de sus criados, le marcó el mensaje y aguardó hasta que le volviera a crecer el pelo; así que le había vuelto a crecer, lo despachó a Mileto sin más recado que cuando llegara a Mileto pidiera a Aristágoras que le rapara el pelo y le mirara la cabeza(9).

Lo que no sabemos es que fue del portador del mensaje una vez entregado. Si se cumplió la norma no escrita de que el mensaje debe destruirse una vez leído, tememos por la vida del pobre esclavo. Un caso parecido al anterior viene referido en la "*Historia del Perú*" de Diego Fernández (10). En dicha obra se indica como método para esconder el mensaje pintarlo en el brazo de un indio, de forma que a primera vista no se distinguía nada y solo se podía leer después de fregar la piel con "*carbón, tierra u otro polvo*". La esteganografía se ha utilizado ampliamente a través de la historia, aunque generalmente con métodos más rápidos y en algún caso con técnicas que hoy pueden parecernos infantiles. Prácticamente todos los niños han utilizado el zumo de limón para generar textos invisibles que solo aparecen cuando el papel se calienta, sin embargo, lo que generalmente no se sabe es que este era el método utilizado por Don Carlos para comunicarse con los generales Cabrera y Zumalacarregui y con su aliado Don Miguel en las guerras Carlistas entre 1833 y 1839 (11), y que en la primera guerra mundial se llegó a un grado de sofisticación tan grande, sobre todo por los alemanes, que llego a utilizarse agua como método para escribir el mensaje .

Uno de los textos más antiguos en el que se describen varios métodos tanto esteganográficos como criptográficos es *La defensa de las posiciones fortificadas* de Aeneas Tacticus(12). Este general, que vivió en el siglo IV antes de Cristo, escribió toda una serie de reglas militares que van desde la selección y disposición de las tropas, hasta la forma de mantener la fidelidad de éstas y el envío de mensajes secretos. En el capítulo XXXI, dedicado a estos últimos, aparte de contarnos la historia de Histieo y Aristágoras que ya hemos comentado, proponía la sustitución de las vocales de un texto en griego por un número determinado de puntos que identificaban esta vocal. Por ejemplo, en lugar de la letra *a* poner un punto, dos puntos por la *e*, etc. (el texto original era en griego, con lo que habría siete vocales). En el mismo capítulo, se explica un método, que puede considerarse el primer dispositivo de cifrado de la historia, al que posteriormente se le ha dado el nombre de "*plancheta de Eneas"*(13). Sin embargo, no podemos quedarnos con la descripción de la plancheta de Eneas que hace Carmona de ella, ya que reconoce no haber leído nunca la obra. En realidad Eneas habla de un astrágalo, un hueso de oveja, con tantos agujeros como letras, y más adelante refina el dispositivo utilizando una tableta perforada en la que los agujeros representan letras según hayan acordado los comunicantes. Para cifrar se empieza pasando un hilo por el centro y posteriormente por cada una de las letras del mensaje. Una vez cifrado el mensaje se envía el circulo interno con el hilo al destinatario. Éste pone el número convenido correspondiente a la clave con la letra inicial del alfabeto y va desenrollando el hilo, con lo que el mensaje aparece al revés. Eso sí, Eneas recomienda la inserción de más agujeros de los veinticuatro correspondientes a las letras, "para evitar sospechas". Estos agujeros situados por el centro servirían para poder escribir dos veces seguidas la misma letra. Para ello, una vez pasado el hilo por la primera letra, se hace pasar por uno de los agujeros "nulos" y posteriormente se vuelve a pasar por la letra inicial.

Una vez hecha la presentación de los primeros métodos conocidos de la Historia, de los que nos falta por citar, entre otros, el método de Polibio aunque el método original fue desarrollado por Cleoxenus y Democleitus, el de César, aunque César utilizara también el

griego con un objetivo puramente criptográfico[1], y la escítala lacedemonia descrita por Plutarco en su "*Vida de hombre ilustres: Lisandro"* como método para cifrar la información utilizado por los espartanos en el siglo V antes de Cristo[2], vamos a centrarnos en la Criptología española.

La criptología en España.

El primer caso que conocemos de criptografía española, aunque hay algunas referencias a claves anteriores y se sabe que se utilizaron métodos muy sencillos tales como la sustitución de las vocales por puntos y símbolos entre los siglos X y XII, es la clave utilizada para la correspondencia entre Alfonso el Magnánimo y sus embajadores ante el rey de Francia Carlos VII, Guillem Ramón de Montcada y Antoni Amat, en 1437. Dicha clave era una pequeño nomenclador, un tipo de cifra muy utilizado durante varios siglos. En el podemos ver un alfabeto de sustitución simple con símbolos extraños, muy al uso de la época, y varios símbolos que representan personajes destacados, lugares y palabras de uso frecuente(28).

En España la criptografía parece no haber tenido mucha importancia hasta ese momento y solo al final del siglo XV, durante el reinado de los Reyes Católicos, parece expandirse su uso. La primera cifra de la que tenemos constancia de esta época es la utilizada por el doctor Puebla en su correspondencia con los Reyes. Esta cifra, en realidad un diccionario, constaría de unos dos mil cuatrocientos términos, sílabas, palabras o letras, representados por un número romano (13). Sin embargo, en algunos casos no se cifra todo el texto sino solamente determinadas palabras que son las que se pretende mantener ocultas, grave error que se repetirá durante siglos. A continuación vemos una carta enviada en 1491 por Isabel la Católica y dirigida al doctor Puebla, en Londres (15).

> Considerando si la ciudad de 102 debe ser 90 ó 39 90, estamos construyendo una 188 allí-en Santa Fe-, en las que esperamos reunir buenas 97 y todo lo necesario para 94 102 o, al menos, para tenerla tan estrechamente cercada que 39 sea necesario 94 de nuevo.

Una vez descifrada quedaría:

> Considerando si la ciudad de Granada debe ser conquistada ó no conquistada, estamos construyendo una fortaleza allí, en las que esperamos reunir buenas tropas y todo lo necesario para sitiar Granada o, al menos, para tenerla tan estrechamente cercada que no sea necesario sitiarla de nuevo.

Ese mismo año, Miguel Pérez Almazán un judío converso, secretario y consejero de los reyes católicos, perfecciona un sistema criptográfico que convierte los textos a números romanos. Éste, era un sistema muy complejo y difícil de romper ya que combinaba símbolos, palabras y signos. Sin embargo, el sistema no era solo difícil de romper, sino también difícil de utilizar, y aparecen muchos documentos de esa época con la anotación de "Sin sentido", "Ordenar al embajador enviar otro despacho" o "No se entiende". Sin embargo, hay que hacer

[1] Sin perder tiempo, con grandes promesas persuade a uno de la caballería galicana que lleve a Cicerón una carta. Iba ésta escrita en griego, con el fin de que, si la interceptaban los enemigos, no pudiesen entender nuestros designios; previenele, que si no puede dársela en mano, la tire dentro del campo atada con la coleta de un dardo. Julio César, "*Comentarios de la guerra de las Galias"*.

[2] Sin embargo, algunos autores actuales dudan de su utilización como método criptográfico(14).

notar que la calidad de los sistemas criptográficos en España comienza a ser muy elevada. Para ello nos puede bastar ver la "*Cifra General de los Reyes Católicos*" atesorada en la Biblioteca de la Real Academia de la Historia y que se reproduce en (18).

Dicha cifra está formada por cuatro homófonos para cada una de las consonantes y cinco para las vocales, todos ellos símbolos extraños y esotéricos, cosa común en las cifras de la época, un repertorio de 671 palabras, cada una de ellas representada por un grupo de tres letras, un conjunto de nulos y uno de caracteres que toman valor doble. Este esquema es el general de las claves de finales del siglo XV y principios del XVI, con la salvedad en general de un conjunto de homófonos y repertorio más reducidos. Ejemplos de cifras de esta época, todas ellas mucho más simples que la Cifra General, son, entre otras, las utilizadas para la correspondencia de los Reyes católicos con el Obispo Diego de Muros (16), la cifra de Don Juan Manuel con su esposa y la cifra de Don Juan Manuel y el Marqués de Villena. Con la llegada al poder de su nieto, Carlos V, la criptografía española pierde parte de su empuje innovador, que no recuperará hasta que el hijo de éste, Felipe II, le suceda en el trono de España.

Un caso de ocultación de información, que luego se repetirá varias veces en la Historia, es el de los textos acrósticos. El más famoso de la época es sin duda La Celestina de Fernando de Rojas. Los versos finales de la edición de 1501 permiten leer "*El Bachiller Fernando de Rojas acabó la comedia de Calixto y Melibea y fue nacido en La Puebla de Montalbán*". A continuación presentamos los primeros versos.

El silencio escuda y suele encobrir
La falta de ingenio y torpeza de lenguas:
Blasón que es contrario, publica sus menguas
A quien mucho habla sin mucho sentir.
Como hormiga que deja de ir,
Holgando por tierra, con la provisión:
Jactóse con alas de su perdición;
LLeváronla en alto, no sabe donde ir.

El airé gozando ajeno y extraño,
Rapiña es ya hecha de aves que vuelan,
Fuertos más que ella; por cebo la llevan;
En las nuevas alas estaba su daño.
Razón es que aplique a mi pluma este engaño
No despreciando a los que me arguyen,
Así que, a mí mismo mis alas destruyen,
Nublosas y flacas, nacias de hogaño.

Donde ésta gozar pensaba volando,
O yo de escribir cobrar más honor,
.....

En cuanto a la criptografía en las Américas, el primero, del que tenemos noticia, que utilizase el cifrado en el Nuevo Mundo fue precisamente su descubridor Cristóbal Colón. El 23 de agosto del año 1500 llegó a Santo Domingo un nuevo gobernador, Francisco de Bobadilla. Bobadilla se encontró con una situación complicada, la mayoría de los españoles, encabezados por Francisco Roldán, se había rebelado contra la autoridad de los hermanos

Colón. Bobadilla detuvo a los hermanos Colón y los envió a Castilla cargados de cadenas. El hecho fue recogido en las "*Décades*" de Pietro Martire D'Anghiera y allí se cuenta que Bobadilla envió a los Reyes cartas escritas por Colón en caracteres cifrados en las que aconsejaba a su hermano que acudiera con hombres armados para defenderse en el caso de que el nuevo gobernador intentase cometer algún atropello en sus personas.

Hernán Cortés parece ser que utilizó a su vez la criptografía como método de ocultar información a sus rivales (17). Se conservan dos cartas con su apoderado cursadas desde Cuernavaca el 25 de junio de 1532 y desde el Puerto de Santiago el 20 de junio de 1533. La primera de ellas fue descifrada en 1925 por D. Francisco Monterde García-Icazbalceta mostrando un código de sustitución monoalfabético con varios homófonos, en total se utilizaban 49 signos para representar las letras. Todas las representaciones de las letras eran símbolos extraños, que como ya hemos comentado, era un sistema muy utilizado en la época.

Sin embargo, la primera cifra oficial en el virreinato peruano es la utilizada por Pedro de La Gasca. Este miembro de la Santa Inquisición nació en Navarregadilla, Ávila. Era un hombre culto e inteligente, bachiller en derecho, licenciado en teología, juez metropolitano de la catedral de Toledo y vicario de Alcalá en 1537 de donde paso al Consejo de la Suprema Inquisición. Fue enviado al Perú para reprimir la revuelta dirigida por Gonzalo Pizarro quien se enfrentó al primer virrey del Perú Blasco Núñez de la Vela en 1546. Núñez de la Vela murió en la batalla, y su cabeza fue expuesta en Quito, hasta que Gonzalo Pizarro mandó quitarla. Carlos V no podía permitir que la rebelión tomase fuerza y decidió enviar a La Gasca a América para terminar con ella. La primera medida de La Gasca fue ofrecer el perdón para los seguidores de Gonzalo Pizarro. Tal medida logró que muchos de los partidarios de Pizarro se pasaran a su bando, sin embargo Pizarro consideró que en esas circunstancias el perdón era imposible y decidió plantar batalla a La Gasca. Perdida la batalla, Gonzalo Pizarro fue capturado y ejecutado. Una vez realizada su labor, Pedro de La Gasca volvió a España en 1550 con un millón y medio de pesos oro que entregó al emperador muriendo el 13 de Noviembre de 1567.

Como ya hemos comentado, La Gasca era hombre inteligente y ya utilizaba una cifra antes de ir a América. Posteriormente, ya en el Perú, se le asignó una cifra para las comunicaciones oficiales. Ambas cifras eran sistemas de sustitución simple con símbolos extraños, muy al gusto de la época.

A	B	C	D	E	F	G	H	I-J	L	M	N	O	P	Q	R	S	T	U-V
7	9	*n*	*m4*	*q4*	*x*	*co*	*c*	*n4 ro*	*ε*	*3*	*d*	*s*	*g*	*es*	*€*	*ɔ*	*h*	*3º*
Gonzalo Pizarro = tun																		

No fue la única cifra de baja calidad, la casa de contratación en Sevilla era la encargada de proporcionar los códigos a los mandos de las armadas que iban a las Indias, y, al parecer, disponía de códigos propios más sofisticados para informar al rey sobre asuntos concernientes a las Américas. La fragilidad de los códigos de las Armadas puede deberse a la poca importancia dada a la seguridad por medio de cifras, ya que los mandos tenían ordenes de echar al mar la correspondencia delicada ante el menor asomo de peligro. Cifras del mismo estilo, alfabetos de sustitución simple, son los del almirante Aguayo de 1536, del general Juan de Velasco de Barrio de 1566, el almirante Flores de Valdés en 1567 y la del almirante Cristóbal de Eraso en 1568.

En enero de 1556, Carlos V renuncia a las coronas de Castilla, León, Aragón-Cataluña, Cerdeña y Sicilia a favor de su hijo Felipe (1527-1598), que reinará con el nombre de Felipe II y el sobrenombre de "el rey prudente". Uno de sus primeros actos como soberano

fue el de cambiar la clave de su padre por considerarla insegura. Esta afirmación se ve avalada por una carta dirigida a su tío el emperador Fernando el 24 de Mayo de 1556 (19), en la que dice "*que ha resuelto variar la cifra que usaba Carlos V para comunicarse con sus ministros de Italia y de otras partes, no solo por ser antigua y haber muerto muchos y otros mudado de destino, de los que estaban en el secreto, sino por estar también harto divulgada y no convenir por esta razón al buen éxito de los negocios*". El centro neurálgico de las comunicaciones y las cifras es el Despacho Universal. Una vez que Felipe II toma posesión del poder cedido por su padre nombra a D. Gonzalo Pérez secretario de Estado y Jefe del Despacho Universal.

Como hemos comentado lo primero que hizo Felipe II fue cambiar la cifra utilizada hasta el momento. Se remitieron dos clases de cifras a los diplomáticos españoles, la cifra general u ordinaria utilizada para la comunicación del rey con sus ministros en las cortes extranjeras, las cifras particulares para las comunicaciones individualizadas, comunicaciones con el duque de Alba y gobernadores y embajadores en varios países y varios códigos y nomencladores para sus comunicaciones con las posesiones en América. Las cifras eran cambiadas cada tres o cuatro años y todo el proceso de administración de los servicios criptográficos era realizado por el Despacho Universal que se encargaba de enviar correos a todas las tierras de España. Cuando la capital de España fue trasladada a Madrid, el Despacho fue puesto a las órdenes del secretario Gonzalo Pérez en el Alcázar, quien ya había trabajado bajo las órdenes de Carlos V en 1543. A la muerte de éste en 1566 fue reemplazado por Francisco de Eraso, al que sustituyo a su muerte en 1570 Antonio Pérez. Antonio Pérez fue arrestado el 21 de julio de 1579 siendo sustituido por Juan de Idiaquez.

Sin embargo, a pesar de todo este complejo para la organización de los sistemas de cifras, seguimos encontrando cifras de una calidad muy baja, como la del gobernador de la isla de Cuba en 1591, que sigue apegado a una cifra de sustitución simple.

En comparación con las utilizadas por su padre, podemos afirmar que la calidad de las cifras mejora muchísimo, con la inclusión de homófonos, caracteres nulos, codificación de digramas, trigramas y repertorio de las palabras más comunes. Las cifras utilizadas por Felipe II eran francamente buenas para su época, no es de extrañar que el rey español no pudiese creer que Viète las hubiera roto utilizando únicamente su intelecto.

En esta época los secretarios de cifra empezaron a retocar los oficios recibidos. En algunos casos eso daba la posibilidad de modificar el sentido de los despachos. En la acusación fiscal del proceso de Enquesta se acusa a Antonio Pérez de tan grave delito, acusación que éste no niega presentando una carta de D. Juan de Austria en la que le dice "*Diré en este papel aparte, por si fuere ese otro visto por su Majestad, que si en él hubiere algo crudo, que pues va en cifra, lo sazone [se refiere a Pérez] según viere convenir, alargando, quitando y mudando lo que le parezca*".

Sin embargo, las cifras indianas, como ya hemos visto, no mejoraban a una velocidad tan grande, la primera cifra conocida que presentase variaciones para hacerla más compleja, variaciones del todo ineficaces para la época, fue la del virrey de Toledo en 1575, en la que las letras dobles tienen un símbolo propio y aparecen abreviaturas, cinco, para las palabras de uso más común en la correspondencia de la que se trata.

En 1571, Don Diego Fernández, vecino de Palencia, publica en Sevilla su "*Historia del Perú*"(10). En este libro, hay un apartado muy jugoso dedicado a la criptografía. En él se describen un par de ejemplos de confección de discos de Alberti, y su utilización. El autor, presenta la utilización del disco de Alberti para la realización de un cifrado polialfabético, ya que escribe que el índice debe adelantarse una posición en cada letra cifrada. Teniendo en cuenta que como él mismo indica,

> Quiero poner, antes que vuelva a la historia, algunos géneros de cifras secretas y dificultosísimas de ser entendidas de aquellas que son visibles, que algunos autores modernos han escripto.

Parece más que probable que la utilización del cifrado polialfabético estuviese ampliamente generalizado para la época. En el mismo escrito presenta una versión de la "tabula recta", la tabla de Porta, la forma de hacer y utilizar rejillas, así como una tabla biliteral como la de Polibio. Sin embargo lo más importante de este texto son las recetas para dificultar el trabajo a los posibles criptoanalistas.

> Y por causa que para leer estas cifras de alfabetos hay hombres tan expertos que fácilmente los entienden y leen, con ciertos avisos y reglas que para ello tienen, es principal documento que se pongan algunas letras en la cifra que no sean ni denoten cosa alguna, porque esto solo basta para desbaratarles su habilidad; y asimismo las dos NN y dos LL tengan cifra sola; porque por esto sólo se han descubierto muchas cifras. Por manera que se ha de huir de escrebir dos letras juntas, si ya no fuese con cautela y engaño, teniendo la cifra que es ninguna o vacía, gran similitud con otra letra, y que solamente diferénciase en un rasguito o punto, como de una i, que pareciese descuido, para engañar al descifrador. Es también aviso para escrebir cifra que lo que se escribiere no vaya por partes, sino continuadas las letras y sin ortografía alguna, porque esto causa mayor secreto. Y porque hay algunos tan curiosos que tienen gran cuenta con algunas letras que no se ofrecen escrebir tan a menudo como otras, y por ellas sacan muchos vocablos, para mayor secreto muchos no usan la letra X, y en su lugar usan de C S, como los antiguos lo usaron escribiendo Alecsandre por Alexandre, y Anacságoras por Anaxágoras.

Por lo que da a entender el párrafo anterior, en 1571 ya se utilizaba la eliminación de espacios, la utilización de nulos, se conocía el análisis de frecuencia, se cifraban como una letra separada las letras dobles como la LL, se camuflaban las letras de poca utilización como la X, y se eliminaban las reglas ortográficas para dificultar el criptoanálisis. La eliminación de la división de palabras como una forma de reducir el ataque por palabra probable se ha asociado siempre a la familia Argenti, de la que al menos tres miembros sirvieron al Papado como secretarios de cifras entre 1585 y 1605. Sin embargo, como ya hemos visto, Diego Fernández ya lo recomendaba años antes como una práctica útil para la preparación de mensajes cifrados.

Un criptoanalista famoso, tanto por su habilidad como por su poca discreción, que estuvo a punto de causarle la ruina, fue François Viète(1540-1603). Viète nació en Fontenay-le-Comte en 1540 y fue uno de los grandes matemáticos de su época. Enrique IV le llamo a su lado, dada su fama, para que intentase descifrar algunos mensajes cifrados por los españoles que habían sido interceptadas por sus tropas. Viète tuvo éxito en todos los casos. La cifra española utilizada en esa época estaba formada por un alfabeto convencional compuesto de los números 1 al 99, que representaban cada uno de ellos una silaba, y una cuarentena de signos que representaban una palabra o una letra. En (11) puede leerse una carta enviada al rey de España descifrada por Viète.

En uno de los viajes en los que Viète acompañaba al rey ocurrió el hecho que pudo costarle la vida. En tours Viète estaba hablando con el embajador de Venecia, Giovanni Mocenigo, al cual contó que habían interceptado una gran cantidad de despachos cifrados del rey de España, del emperador y de varios príncipes, y que él los había descifrado todos. También dejo entrever que conocía la cifra utilizada por la república de Venecia. El embajador le pidió pruebas y éste le mostró un paquete de mensajes descifrados, ninguno de la república de Venecia, y le contó pormenores de la cifra veneciana. El embajador relató el hecho al Consejo de los Diez en su reunión del cinco de Junio de 1595. El doce de Junio se cambió todo el sistema de cifra de los embajadores de la República, adoptando los sistemas

desarrollados por Pietro Partenio, quien según Bazeries(11), era el más hábil criptólogo de la época.

En España, por su parte, cuando se supo que los franceses habían estado descifrando desde hacía años los mensajes interceptados, no se optó por nada mejor que presentar una denuncia al Vaticano acusando a Viète de brujería y pacto con el diablo. Felipe II presentó la queja al Papa, quien haciendo gala de un cierto sentido del humor, ya que sus propios criptoanalistas sabían descifrar los despachos españoles(20), ordenó que el asunto fuese estudiado por una comisión de cardenales con recomendación de urgencia. Los cardenales debieron entender el mensaje y la investigación a día de hoy todavía no ha sido completada. De todas maneras, no hay que menospreciar la iniciativa del rey español, a pesar de que se le ha intentado ridiculizar por este asunto, Viète estaba protegido por uno de los reyes más influyentes de la época, y Felipe no podía tener acceso a él. La única opción era que el Vaticano lo condenase, y, en ese caso, ni el rey de Francia se hubiese atrevido a contradecir directamente al Papa y el matemático galo seguramente hubiera acabado en la hoguera.

Las ordenes religiosas por su parte también utilizaban cifras que iban cambiando con cierta periodicidad. Un ejemplo es la cifra distribuida por la Compañía de Jesús en octubre de 1601 a los provinciales de la Orden. Dicha cifra estaba formada por seis alfabetos diferentes con una representación numeral en la parte superior. Para cifrar se empezaba a hacerlo con el primer alfabeto y cifrando cada letra consecutivamente con el alfabeto siguiente.

	41	42	43	44	45	46	47	48	49	51	52	53	54	55	56	57	58	59	61	62
1	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	Z	A	B
2	U	Z	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T
3	M	N	O	P	Q	R	S	T	U	Z	A	B	C	D	E	F	G	H	I	L
4	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	Z	A
5	R	S	T	U	Z	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q
6	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	Z	A	B	C	D

Por ejemplo, la palabra JESÚS quedaría cifrada con este código como 47 47 47 59 42.

En España la primera obra publicada sobre criptografía no aparece hasta 1635, la obra, de título *Steganographia*, fue escrita por Juan Caramel y Lobkowitz (Madrid 1606-1682), sin embargo se publicó en Colonia y en latín. Caramel fue uno de los grandes matemáticos de su época, estudiando entre otras cosas los principio generales de los números en base *n*, un sistema de logaritmos base 10^9 y un sistema para determinar la longitud basándose en la posición de la luna. Puede parecer extraño el hecho de que no existan otras obras en España dedicadas a la criptografía dada su indudable capacidad técnica, sin embargo, es muy probable que la delicadeza que debía ofrecerse al tema, así como un excesivo poder de la Inquisición, en muchos casos como método de eliminar problemas al Estado, hiciesen que el escribir sobre estos temas no fuese muy recomendable en la España de esa época. Recientemente ha aparecido un libro con el título *De Zifras*, escrito en español presumiblemente a finales del siglo XVI, y de autor desconocido. Dicho libro, escrito por un criptógrafo al servicio de Martín de Cordova, Virrey de Navarra, y dedicado a Juan Fernández de Velasco, condestable de Castilla, incluye, aparte de una descripción de las cifras basadas en varios aspectos, varios ejemplos de nomencladores, rejillas, tablas de tipo Vigenère, sistemas de disco como el de Alberti y un apartado para "Descifrar sin contracifra", en la que se dan 38 reglas para el criptoanálisis, así como un ejemplo.

A mediados del siglo XVII las cosa no pintan bien para España. La situación internacional es muy delicada, en Inglaterra Cromwell se alía con Francia ya que puede

obtener mayor provecho a costa de España. En 1655 Inglaterra se apodera de la isla de Jamaica y las flotas enemigas infestan las Indias lo que dificulta el comercio y provoca grandes pérdidas. Visto el panorama y las dificultades que se perfilan para las comunicaciones, se decide crear en 1658 un código para la comunicación con las autoridades de Ultramar. La cifra es un repertorio formado por una tabla de homófonos y nulos, complementada con una tabla con los digramas y trigramas más habituales y una lista de 123 palabras que contemplan los conceptos militares, y geográficos más comunes.

En 1664, en España se decide cambiar la clave oficial para las comunicaciones con Ultramar, ésta volvería a cambiar en 1675 y 1770. Sin embargo, las precauciones tomadas sirvieron en general de muy poco debido a la falta de preparación de las personas a la que iba destinada. Un buen ejemplo es el virrey del Perú, el conde de Castellar, quien fue amonestado por el Consejo de Indias por su poca aplicación en el uso de la cifra, pero lo curioso del caso es que tuvo que enseñar a su sucesor Don Melchor de Liñán y Cisneros al ser éste todavía menos ducho en el uso de los despachos cifrados. Esto fue uno de los males endémicos en la España del siglo XVII y XVIII, como caso sintomático tenemos el del virrey de la Nueva Granada que al abandonar el gobierno reconoció no haber utilizado nunca la clave, y que por lo que él sabía sus dos antecesores tampoco lo habían hecho nunca.

En los años 50, J. P. Devos, autor de uno de los libros más importantes sobre la criptografía española, aunque dedicado básicamente al Despacho Universal, encontró un Tratado de criptoanálisis de 83 hojas de la Secretaría de Estado española, de entre los años 1668 y 1714. Dicho tratado, que se publicó unos años más tarde por la Universidad de Louvain con el nombre de "*L'art de deschiffrer. Traité de déchiffrement du XVII siècle de la Secrétarie d'État et de Guerre Espagnole*", es una pequeña joya. En él se explican los principios generales del criptoanálisis, el estudio de frecuencias, digramas, trigramas, y ejemplos de aplicación, tanto en español como en francés, basados en documentos reales interceptados. Formas de resolver cifrados realizados con tablas de homófonos, cifrados geométricos, la cifra de Vigenère, que según explica en el texto se utilizaba en Holanda, pero que no solía utilizarse en las Secretarías de Estado debido al tiempo necesario para cifrar y descifrar una carta, una variante del método de Gronsfeld, que aparece en el apartado de cifras indescifrables y un sistema de cifras basado en un repertorio. El sistema, muy sencillo, consiste en generar un repertorio con todas las letras y sus combinaciones de dos y tres caracteres, asociándosele a cada uno de ellos un número de tres dígitos. El cifrado es tan sencillo como escribir los números correspondientes al cifrado, pero agrupándolos en números de diferentes longitudes. Por ejemplo, si el mensaje cifrado está formado por los números 123.452.135.623.458.223 se enviaría por ejemplo de la siguiente manera, 12 34 521 35 62 64 582 23. Por último, hay que resaltar que el autor no considera excesivamente complicado el criptoanálisis del método de Vigenère, simplemente para descifrarlo recomienda un método de fuerza bruta. El método consiste en buscar la correspondencia de la letra (en el original utiliza una tabla de Vigenère con números), con el resto de las letras que pueden formar la clave. Al hacer esto con las primeras letras del criptograma aparecerá por la fuerza una palabra que será la clave.

A mediados del siglo XVIII, en la época de Fernando VI, seguían utilizándose los libros de códigos, en los que aparecían códigos de 2, 3 o 4 dígitos, con múltiples nulos y valores que anulaban el antecedente o el siguiente signo. En los documentos podía ocurrir que se cifrase todo el documento o solo la parte interior, dejándose sin cifrar las cláusulas de cortesía iniciales. Al igual que en siglos anteriores, como ya habíamos visto en el caso del secretario Antonio Pérez, existían personajes que se encargaba de maquillar el mensaje dotándolo de las formulas de cortesía habituales al receptor.

Un método del que tenemos las primeras noticias de su uso a finales del XVIII y que ha sido profusamente utilizado, entre otros por los espías rusos, por la Resistencia francesa para sus comunicaciones con Londres, y al principio de nuestra guerra civil por la flota republicana, es el cifrado mediante el uso de un libro común. El método, sencillo pero engorroso, consiste en que ambos comunicantes utilicen la misma edición de un libro determinado de fácil adquisición. El cifrado consiste en tres números que indican página, línea y posición de la palabra que queremos representar dentro de la línea. La descripción más antigua de dicho método aparece en una proposición al conde de Floridablanca por parte del aventurero Pedro Resard de Wouves d'Argues en 1787(17). Los números indicativos de la página, línea y palabra irían separados por puntos y delimitados por rayas. Para eliminar el problema de representar determinados términos geográficos o técnicos, el método se complementaba con una tabla de 281 conceptos representados por números. Para indicar que se trataba de conceptos de la tabla, al cifrar se separaban estos conceptos por dos rayas. No sabemos si dicha clave fue puesta en funcionamiento, aunque lo dudamos. Lo que si se supone es que este era el método utilizado por Maria Antonieta para su correspondencia con el marqués de Bouillé(21). El libro utilizado en este caso era un libro de 1788 muy de moda en esa época, "*Paul et Virginie*".

Uno de los acontecimientos más importantes de la Europa del siglo XIX fue la llegada al poder de Napoleón. Para el viejo continente la figura de Bonaparte representó un revulsivo, tanto en el ámbito político, como social. Napoleón, persona inteligente, valiente y gran organizador, supo dotar a su imperio de una estructura moderna, que con los años sería copiada en muchos de sus aspectos por el resto de Europa. Sin embargo, no parece que Napoleón tuviese en la importancia que le debía a la criptología, aunque se le atribuya la frase "*Un homme capable de décrypter des écritures chiffrées vaut plus que cinq généraux*[3]". Las cifras que utilizaba eran de una calidad más bien baja y fueron utilizadas en muchos casos de una manera torpe. Los mariscales de Napoleón eran gente valiente y decidida, pero no eran en general gente culta, lo que hacía que no se diese la suficiente importancia al uso de las cifras y al rigor con que deben realizarse los procesos de cifrado y descifrado.

Más adelante, ya convertido en emperador, Napoleón utilizó dos cifras, la "grande chiffre" para la comunicación de los generales y del estado mayor y la "petite chiffre" o "chiffre banal". En la guerra de España, un español consiguió obtener la cifra de Suchet y la utilizó para facilitar a los españoles la toma de Mequinenza y de Lérida (23). Wellington a su vez, utilizó los servicios del mayor George Scovell, que rompió la "grand chiffre" con la ayuda de los múltiples mensajes cifrados de que le proveían los guerrilleros españoles (24). No debemos olvidar al general Joaquín Navarro Sangrán, uno de los mejores criptoanalistas españoles a quien Wellington felicitó por sus éxitos en diversas ocasiones. Vista la carta de José Bonaparte a su hermano que podemos ver en (21), la afirmación de Bazeries "*Les chiffres de Napoleón I pouvaient être lus sans clef*"[4] está más que justificada.

En España la calidad de la criptografía había llegado a límites verdaderamente bajos, el único libro del que tenemos conocimiento escrito en esa época es el del catedrático de taquigrafía D. Francisco Paula Martí (26). El libro, más bien un libreto, de 56 páginas es editado en 1808 con el título "*Poligrafía o arte de escribir en cifra*". En él se explican un par de métodos criptográficos y la utilización de tintas simpáticas. Criptográficamente hablando, el libro tiene un valor nulo, a no ser por que da una idea de la degeneración a la que había llegado España en cuestión de cifras.

Por parte española conocemos dos de las claves que se utilizaban durante la guerra de

[3] Un hombre capaz de descriptar escrituras cifradas vale más que cinco generales.
[4] Las cifras de Napoleón I podían leerse sin la clave.

la Independencia, la primera, un pequeño nomenclador en el que varias letras se cifran con el mismo símbolo, se utilizaba para la comunicación desde Sevilla(4). La otra era mucho más original, una combinación de método criptográfico y esteganográfico utilizado por el capitán de fragata D. José Cannoch para trasmitir cartas desde España al rey Fernando VII. El sistema consistía en cifrar un mensaje sustituyendo las letras del alfabeto por notas musicales. La equivalencia de las letras variaba según se indicase clave de sol, de do o de fa. Finalmente se insertaba la partitura dentro de otra. Para determinar la parte cifrada se utilizaba una plantilla de cristal.

Poco se sabe de la utilización de la Criptología en las guerras Carlistas. Ya hemos comentado la utilización del zumo de limón por parte de Zumalacarregui, Don Carlos Luis de Borbón utilizaba además una clave en la que se sustituían los términos de la misma por combinaciones de hasta tres dígitos y hasta dos letras (27).

En el año 1894 Cesáreo Huecas Carmona, teniente de infantería, escribe su "*Tratado de criptografía*" a nombre de Joaquín García Carmona. Se trata de uno de los mejores libros sobre el tema escrito en España y que fue premiado en su día por el Ministerio de la Guerra. Según Sacco, el libro de Carmona es uno de los buenos textos de la época, sin embargo indica de él que es más documentado que original. David Khan es más apasionado y dice de él que es el mejor libro de criptografía escrito en español y uno de los mejores escritos en cualquier lengua. Tres años después aparece el libro "Nuevos métodos criptográficos" de D. Manuel Núñez y Muñoz (5), menos documentado que el de Carmona, pero mucho más practico y que tuvo una mayor aceptación en los círculos militares, al menos eso deducimos del hecho de que este libro aparezca en varias bibliotecas militares no apareciendo el primero. Varios de los métodos que allí se explican fueron reproducidos años después en el libro de Pascual Diez de Rivera y Casares, "*Orgánica Naval*" (7).

A finales del siglo XIX, y debido a la popularización del telégrafo como medio de comunicación empresarial, empiezan a aparecer unas versiones de los libros de códigos, especialmente orientados al comercio. Su pretensión es el dotar de seguridad a las comunicaciones y reducir el coste de las trasmisiones. Estas claves telegráficas aparecieron por toda Europa, con la limitación de que la clave solo servía para el idioma en el que se había diseñado. En general, por su estructura, no era posible su traducción a otros idiomas. En realidad, la seguridad del sistema era poca, aunque el ahorro en comunicaciones era evidente.

En España dos de las claves más famosas fueron sin duda la clave Darhan y la clave telegráfica de Pelligero(25). La utilización de esta última, publicada en 1893, reportaba según el autor, las siguientes ventajas:

> 1ª Secreto perfectamente garantido con las sencillas é infinitas combinaciones que son aplicables á toda clase de correspondencia privada y á la telegráfica.
>
> 2ª Notable economía en el precio de cada uno de los telegramas que por esta CLAVE se transmitan.

La seguridad del método se basa en la utilización de una clave, de común acuerdo entre emisor y receptor, que junto con la utilización del libro, permite la confidencialidad en las comunicaciones entre ambos. El código está formado por un repertorio de tres columnas, que llamaremos columnas principales, cada una de las cuales se subdivide a su vez en cuatro columnas. En la primera columna de cada columna principal aparecen en orden alfabético 32160 palabras de uso común y frases usuales. La segunda columna contiene a su vez

palabras castellanas ordenadas alfabéticamente que se pueden transmitir en sustitución de las anteriores. De estas, no hay ninguna que contenga la letra *ñ* para evitar errores, ya que la *ñ* se transmite por telégrafo como *n*. La tercera columna está formada por combinaciones de letras, también ordenadas alfabéticamente, con la particularidad de que ninguna de ellas supera las cuatro letras y empiezan todas por vocal, no existiendo en ninguna palabra más de una vocal. Esto permite fácilmente separar las palabras ya que las letras que la forman estarán separadas por vocales. En la cuarta columna aparecen todos los números desde el 00001 al 32280, ya que el autor deja 120 combinaciones para que los dos comunicantes puedan añadir las palabras o frases más comunes que vayan a utilizar ambos y que no estén incluidas ya en la clave.

ABJ	ABA	ABB		ABO	ABO	ABD		ABR	ABO	ABG	
a	a	a	00001	abjurar	abatió	abcy	00041	abordo	abocar	abfy	00081
abacá	ab	ab	00002	ablandar	abatir	abcz	00042	aborrece	abocas	abfz	00082
abacería	ababa	abb	00003	abnegación	abazón	abd	00043	aborrecer	aboco	abg	00083
abajo	ababol	abbb	00004	abocada	abdica	abdb	00044	aborrecida	aboga	abgb	00084
abanderado	abacá	abbc	00005	abocado	abdico	abdc	00045	aborrecido	abogan	abgc	00085
abanderar	abaco	abbd	00006	abochornado	abecé	abdd	00046	abortar	abogar	abgd	00086
abandona	abad	abbf	00007	abofetear	abedul	abdf	00047	aborto	abogas	abgf	00087
abandonada	abada	abbg	00008	abogacía	abeja	abdg	00048	abrasado	abogo	abgg	00088
abandonado	abades	abbh	00009	abogado	abejar	abdh	00049	abrasador	abogue	abgh	00089
abandonar	abadía	abbk	00010	abogados	abejas	abdk	00050	abraza	abole	abgk	00090
abandono	abaja	abbl	00011	abogando	abejón	abdl	00051	abrazada	abolen	abgl	00091
abanico	abajar	abbm	00012	abogar	abenuz	abdm	00052	abrazado	aboles	abgm	00092
abarca	abajo	abbn	00013	abolengo	abetal	abdn	00053	abrazados	aboli	abgn	00093
abarcado	abajor	abbp	00014	abolición	abete	abdp	00054	abrazan	abolia	abgp	00094
abarcando	abala	abbq	00015	abolicionista	abetes	abdq	00055	abrazando	abolió	abgq	00095
abarcar	abalan	abbr	00016	abolida	abeto	abdr	00056	abrazar	abolir	abgr	00096
abastecedor	abalar	abbs	00017	abolidas	abetos	abds	00057	abrazo	abolo	abgs	00097
abastecer	abalas	abbt	00018	abolido	abey	abdt	00058	abre	abolla	abgt	00098
abastecido	abale	abbv	00019	abolidos	abeya	abdv	00059	abreviada	abolle	abgv	00099
abasto	abalen	abbx	00020	abolir	abiar	abdx	00060	abreviado	abollo	abgx	00100
abatida	abaleo	abby	00021	abominable	abigeo	abdy	00061	abreviados	abona	abgy	00101
abatido	abales	abbz	00022	abona	abisma	abdz	00062	abreviando	abonan	abgz	00102
abatidos	abalo	abc	00023	abonable	abisme	abf	00063	abrevien	abonar	abh	00103
abatimiento	abano	abcb	00024	abonada	abismo	abfb	00064	abrevio	abonas	abhb	00104
abdica	abanos	abcc	00025	abonadas	abita	abfc	00065	abriendo	abondo	abhc	00105
abdicación	abanto	abcd	00026	abonado	abitan	abfd	00066	abrieron	abone	abhd	00106
abdicar	abaos	abcf	00027	abonados	abitar	abff	00067	abriga	abonen	abhf	00107
abdico	abarca	abcg	00028	abonamos	abitas	abfg	00068	abrigado	abones	abhg	00108
aberración	abarco	abch	00029	abonan	abite	abfh	00069	abrigando	abono	abhh	00109
abertura	abasta	abck	00030	abonar	abiten	abfk	00070	abrigar	abonos	abhk	00110
abetunado	abaste	abcl	00031	abonara	abites	abfl	00071	abrigo	aborda	abhl	00111
abierta	abasto	abcm	00032	abonaran	abito	abfm	00072	abrigue	aborde	abhm	00112
abiertas	abata	abcn	00033	abonare	abjura	abfn	00073	Abril	abordo	abhn	00113
abierto	abatan	abcp	00034	abonares	abjure	abfp	00074	abrió	aborra	abhp	00114
abiertos	abatas	abcq	00035	abonaron	abjuro	abfq	00075	abrir	aborre	abhq	00115
ab-intestato	abate	abcr	00036	abonen	ablano	abfr	00076	abrirá	aborri	abhr	00116
Abisinia	abaten	abcs	00037	abono	abnega	abfs	00077	abro	aborro	abhs	00117
abismado	abates	abct	00038	abordable	abnego	abft	00078	abrumador	aborso	abht	00118
abismo	abati	abcv	00039	abordage	aboca	abfv	00079	abrumadora	aborta	abhv	00119
abjurado	abatia	abcx	00040	abordar	abocan	abfx	00080	abrumadores	aborte	abhx	00120

1

Clave de Pelligero

Pelligero enumera cinco maneras de asegurar el secreto en la transmisión.

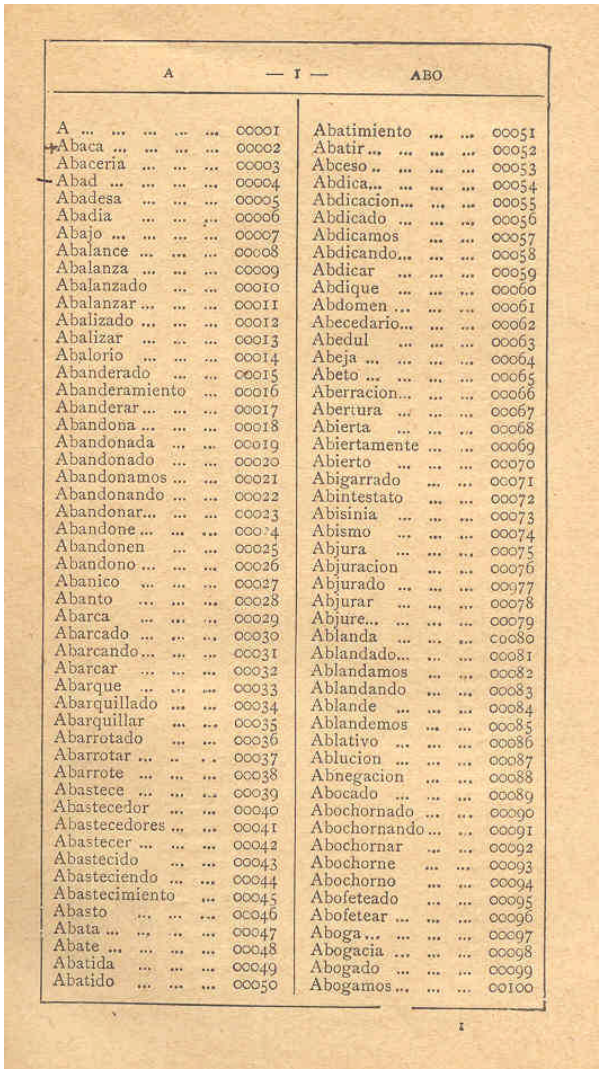
1) Aumentar o disminuir una cantidad fija al número que corresponda transmitir, esta cantidad, junto con la operación a realizar sería la clave. Por ejemplo, si queremos transmitir la palabra “aviso” que corresponde al número 03008, y utilizamos 20 y la adición como clave, el número resultante sería el 03028 que corresponde a la palabra ayudado. Para transmitir utilizamos luego la palabra correspondiente que aparece en la segunda o tercera columna, en este caso “avisar” o “ambf”.
2) Aumentar o disminuir una cantidad a cada una de las palabras que contenga el telegrama y luego operar como en el caso anterior. Por ejemplo sumar un múltiplo de diez a cada posición. Es decir a la primera palabra le sumamos diez, a la segunda veinte, a la tercera treinta y así sucesivamente.
3) Saltar un número de columnas base determinado y se escoge cualquiera de las dos columnas transmisibles.

4) Intercambiar la colocación de los números de la cuarta columna. Para ello los comunicantes se ponen de acuerdo en intercambiar dos números de la cuarta columna, por ejemplo se intercambia el valor del tercer y quinto dígitos. En este caso, si queremos poner en clave la palabra "deuda", su equivalente numérico es 10610. Intercambiando el tercer y quinto dígito tenemos que el número se convierte en 10016 que corresponde a la palabra en claro "desinfección". Luego se envía cualquiera de los valores transmisibles.
5) Cambiando la vocal con que empieza el grupo de letras asignado a cada palabra. Por ejemplo cambiando la vocal por la vocal siguiente, y si esta es la *u*, cambiándola por la *a*. si queremos cifrar la palabra "cañón", el equivalente de la tercera columna es "aqqc". Si cambiamos la vocal por la siguiente tenemos como resultado "eqqc" que corresponde a la palabra "ebanista". Se envía pues el valor de la primera columna transferible que es "guapote".

Como ya hemos comentado previamente, la seguridad del sistema es muy baja. Es muy susceptible, independientemente del modelo que se emplee para ocultar el contenido, a un ataque por palabra probable. Es sin embargo muy útil al reducir en muchos casos el coste del telegrama, pero a costa de perder legibilidad en el caso de que se produzca un error en la transmisión.

Otro de las claves utilizadas en España es la clave de Darhan, anterior incluso a la de Pelligero, se publicó en 1891, y que tiene varios puntos en común con ésta. La clave telegráfica de Darhan consta de 30000 palabras en orden alfabético numeradas del 00001 al 30000. Para cifrar se utiliza alguna de las siguientes combinaciones:

1) Sumar o restar una cantidad fija a los números que correspondan a las palabras a cifrar, al igual que hacíamos con el de Pelligero.
2) Alterar el orden de colocación de los tres dígitos de la derecha. Por ejemplo, el número 25327 se convierte en 25723.
3) Combinar los dos casos anteriores.
4) Añadir a la primera palabra el número de las que forman el texto, a la segunda el doble, a la tercera el triple, etc.



A — 1 — ABO

A	00001	Abatimiento	00051
Abaca	00002	Abatir	00052
Abaceria	00003	Abceso	00053
Abad	00004	Abdica	00054
Abadesa	00005	Abdicacion	00055
Abadia	00006	Abdicado	00056
Abajo	00007	Abdicamos	00057
Abalance	00008	Abdicando	00058
Abalanza	00009	Abdicar	00059
Abalanzado	00010	Abdique	00060
Abalanzar	00011	Abdomen	00061
Abalizado	00012	Abecedario	00062
Abalizar	00013	Abedul	00063
Abalorio	00014	Abeja	00064
Abanderado	00015	Abeto	00065
Abanderamiento	00016	Aberracion	00066
Abanderar	00017	Abertura	00067
Abandona	00018	Abierta	00068
Abandonada	00019	Abiertamente	00069
Abandonado	00020	Abierto	00070
Abandonamos	00021	Abigarrado	00071
Abandonando	00022	Abintestato	00072
Abandonar	00023	Abisinia	00073
Abandone	00024	Abismo	00074
Abandonen	00025	Abjura	00075
Abandono	00026	Abjuracion	00076
Abanico	00027	Abjurado	00077
Abanto	00028	Abjurar	00078
Abarca	00029	Abjure	00079
Abarcado	00030	Ablanda	00080
Abarcando	00031	Ablandado	00081
Abarcar	00032	Ablandamos	00082
Abarque	00033	Ablandando	00083
Abarquillado	00034	Ablande	00084
Abarquillar	00035	Ablandemos	00085
Abarrotado	00036	Ablativo	00086
Abarrotar	00037	Ablucion	00087
Abarrote	00038	Abnegacion	00088
Abastece	00039	Abocado	00089
Abastecedor	00040	Abochornado	00090
Abastecedores	00041	Abochornando	00091
Abastecer	00042	Abochornar	00092
Abastecido	00043	Abochorne	00093
Abasteciendo	00044	Abochorno	00094
Abastecimiento	00045	Abofeteado	00095
Abasto	00046	Abofetear	00096
Abata	00047	Aboga	00097
Abate	00048	Abogacia	00098
Abatida	00049	Abogado	00099
Abatido	00050	Abogamos	00100

Clave Darhan

El diccionario Stiller fue otro de los diccionarios telegráficos famosos de la época. Éste estaba formado por cien páginas sin numerar en cada una de las cuales había cien palabras numeradas del 00 al 99. En este sistema el primer paso para cifrar consiste en numerar las páginas y luego la cifra estaría formada por la combinación de página, dos cifras, y palabra dentro de la página, dos cifras más. Por ejemplo, si la palabra es la número 25 de la pagina 63 se enviaría el número 6325. La única variación que se permite al respecto es cambiar el orden de las cuatro cifras según un patrón determinado. En nuestro ejemplo podría enviarse cualquiera de las 24 combinaciones de los dígitos que forman el número.

Debemos reseñar, sin embargo, que la utilización de sistemas parecidos a los anteriores, códigos formados por repertorios de palabras ordenados alfabéticamente, con adición de cardinales y espacio para voces especiales se venían utilizando en España, con carácter criptográfico, desde mucho antes de que apareciesen los códigos telegráficos. En el Archivo General de la Administración existen varios de estos códigos. Los que consultamos, correspondían a las cifras para comunicaciones entre la Embajada de Berlín y la de Madrid entre los años 1867 y 1898.

A partir de finales del siglo XIX empezamos a ver el Método Oficial de Guerra, el criptógrafo de cinta móvil. La primera vez que vemos documentado el sistema es en el excelente libro de Carmona (1), poco tiempo después aparece en el texto de telegrafía militar

de Lossada(2) con el nombre de método español. Según Carmona el método era utilizado en la época de su publicación por todos los Ministerios exceptuando el de Estado, Lossada por su parte afirma que es el procedimiento adoptado en España para cifrar los escritos oficiales. Su utilización fue amplia abarcando más de medio siglo, ya que aparece incluso en el libro de Serrano García (3), un buen libro también pero sin llegar a las altas cotas del de Carmona, con el nombre de criptógrafo de cinta. Utilizaremos este nombre, añadiendo la palabra móvil, al parecernos más descriptivo del sistema.

El criptógrafo de cinta móvil consiste en una tabla de sustitución múltiple formada por una fila en la que figura el alfabeto en el orden normal, una cinta móvil con un alfabeto doble totalmente aleatorio que hemos colocado en la segunda fila, y todos los números que se pretende sustituyan a las letras del mensaje en claro. En la descripción dada por los autores anteriores se indica que en la tabla aparecen los números de dos dígitos del 10 al 99 totalmente desordenados y colocados al azar, sin embargo, en los sistemas utilizados en la guerra civil esta limitación se cambia en algunos casos y se elimina en otros llegándose a representar todos los números de dos dígitos. En el diseño original la cinta pasa a través de dos ranuras a ambos lados de la tarjeta donde está ubicada la clave y justo debajo del alfabeto en claro, tal como muestra el dibujo siguiente.

	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**Ñ**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	
B	*E*	*W*	*T*	*R*	*S*	*M*	*Q*	*Y*	*U*	*I*	*O*	*P*	*A*	*N*	*D*	*F*	*G*	*H*	*J*	*K*	*L*	*Ñ*	*Z*	*X*	*C*	*V*	*B*	*E*
	10		20		30		32		41		01		92		87		99		45		26		25		76		37	
		02		62		13		27		63		05		14		61		07		22		21		09		12		
	11		03		15		34		29		35		37		24		36		38		23		39		40		69	
		04		18		28		49		51		54		19		06		08		58		64		71		70		
	33		31		50		32		16		44		52		55		56		59		60		65		72		75	
		47		17		48		42		43		46		53		57		66		68		74		78		80		
	67		73		81		84		83		85		91		79		90		77		82		88		89		86	

El alfabeto doble solía generarse mediante la utilización de una palabra clave. Por ejemplo, si utilizamos la palabra revolución el alfabeto generado podría ser, utilizando el mismo esquema que el presentado en el libro de Carmona[5],

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

Con lo que el alfabeto en la cinta quedaría como,

RAPEBQVDSOFTLGVUHWCJXIKYNMZ

En la siguiente imagen podemos ver la clave de guerra número 3 utilizada en 1915.

[5] Curiosamente en el ejemplo de la descripción del método en los libros de Carmona, Nuñez y Lossada se utiliza la misma palabra, “murciélago”, y el mismo esquema de generación de clave.

Fuente: Archivo General de la Administración C. 2298.

Si bien parece chocante que un sistema con tan poca seguridad fuese tan ampliamente utilizado, lo es más cuando vemos que se utilizó en los niveles más altos de seguridad. Carmona ya avisaba de la poca seguridad del método y daba un ejemplo de cómo descifrar un mensaje sin conocer la clave.

Durante la Primera Guerra Mundial todas las potencias en conflicto se dedican a potenciar sus códigos y claves, así como a intentar obtener las del enemigo. Se vuelve a dotar de medios y personal a los gabinetes de criptoanálisis. En España sin embargo, al no haber entrado en el conflicto, parece que esa no fuera una de las preocupaciones. Los sistemas usados por España en esa época eran tremendamente flojos, el teniente Stützel, uno de los mejores expertos en cifras del ejercito alemán, aseguraba que sin saber nada de español era capaz de descifrar todos los mensajes entre el embajador español en Berlín y Madrid. En realidad prácticamente todos los contendientes eran capaces de romper nuestros códigos.

A nivel diplomático, sin embargo, se seguían utilizando los códigos, con un sistema bastante parecido a los códigos comerciales antes descritos, y con una baja seguridad (29).

Esta pauta siguió durante los años siguientes. Durante la guerra del Rif en 1925, el mariscal francés Lyautey, presentaba a su oficial de información a un grupo de oficiales españoles con estas palabras: "*He aquí quien me traduce sus telegramas*". Ni que decir tiene que los españoles cambiaron inmediatamente sus claves (22).

Por lo que vemos nuestras claves no eran precisamente excepcionales, pero ¿qué podemos decir de las normas de uso? Como en la mayoría delos casos en que la seguridad es baja, ésta es más debida a una pobre o inadecuada utilización de las herramientas, acompañada de un control administrativo deficiente. Para ello solo debemos fijarnos en las siguientes normas:

CRIPTÓGRAFO.- Las instrucciones de 21-08-1922 de la Guardia Civil previenen lo siguiente:

1º.- Poseen criptógrafo. El General Director, los Generales Inspectores, Coroneles subinspectores y Director de los Colegios, primeros jefes de comandancia y el de la de

guardias jóvenes, Capitanes de compañía y escuadrón, Jefes de línea y comandantes de puesto, los que se comunicarán entre sí con clave amarilla. Igualmente lo tienen el Ministro de la Gobernación, Director de orden público, Inspector general de orden público en Madrid, y Gobernadores civiles de las provincias. con los cuales se comunicará con clave de autoridades civiles.

2º.- El criptógrafo se reputa como documento secreto que se conservará en la carpeta de "Ordenes y antecedentes reservados" y no lo usarán otras personas que las que lo tienen a su cargo y las que con arreglo a ordenanza les sustituyan en el mando.

3º.- El uso del criptógrafo se limitará a los casos en que la prudencia lo aconseje, para evitar el peligro de la divulgación del contenido de un despacho en perjuicio del mejor servicio.

4º.- El extravío o pérdida del criptógrafo constituye falta grave.

5º.- Una copia de las presentes instrucciones para uso del criptógrafo se conservará unida a la misma.

Como vemos la seguridad teórica quedaba reflejada en un documento que de seguirse estrictamente, y siempre que las claves utilizadas fuesen de calidad, permitía garantizar una cierta seguridad. Pero, ¿y la forma de preparación y envío de los mensajes? En (6) se indica "*Prohíbe nuestro reglamento*[6] *el expedir despachos en parte cifrados y en parte en lenguaje corriente o condensado e igualmente el repetir íntegro, o en extracto, ya en lenguaje corriente o condensado, o ya cifrado de distinto modo, un mensaje anteriormente expedido o recibido, así como pedir o dar explicaciones acerca del mismo*.". Sin embargo tanto la expedición de documentos en parte cifrados, en parte en claro, como la repetición del mismo mensaje en diferentes claves fue una tónica habitual incluso en la guerra civil española.

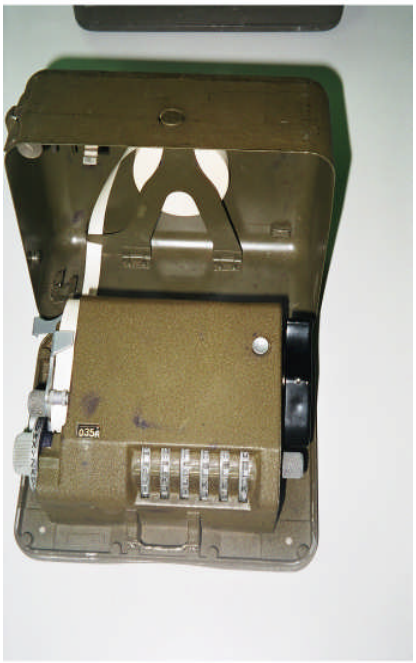
Máquinas de rotor.

La aparición de las maquinas de rotor puede considerarse el principio de una nueva era en la criptografía y el criptoanálisis. Los tiempos del criptoanalista que en un arranque de genialidad era capaz de romper un código pasaron en el momento en que estas se pusieron en funcionamiento. Estas máquinas fueron ampliamente utilizadas durante la II Guerra Mundial por todos los contendientes, cada uno con sus variantes, pero utilizando un esquema común, el concepto de rotor. Un rotor no es nada más que una pieza cilíndrica con una serie de contactos en su interior y un conjunto de letras y símbolos en su exterior. Los rotores podían ser de dos clases, cableados o con muescas. Estas muescas podían ser activas o inactivas. En realidad el rotor no es más que un conmutador que genera una sustitución monoalfabética al pasar la corriente de un conector de una de las caras a otro. Las máquinas de rotor lo que hacían era poner varios rotores en cascada y hacer que estos se movieran a diferente velocidad, de forma que se generase una sustitución poliafabética de gran complejidad y con un periodo de la clave fuera muy grande. Desde un punto de vista muy simplista podemos decir que las maquinas de rotor pueden considerarse como sistemas que generan cifrados de Vigenère con un periodo muy elevado. En particular si el rotor tiene 26 posiciones, una

[6] Reglamento para el Enlace y el Servicio de Transmisiones, aprobado por Real Orden Circular de 1 de agosto de 1925.

máquina de *n* rotores tendrá un periodo de 26^n. La imagen siguiente nos muestra un par de rotores de una máquina Enigma militar.

El concepto de las máquinas de rotor fue desarrollado casi simultáneamente por Arvid Damm en Suecia, Edward Hebern en Estados Unidos, Arthur Scherbius en Alemania y Hugo Alexander Koch en Holanda, aunque las ultimas investigaciones sobre el tema parecen apuntar a que la paternidad holandesa correspondería a Th. A. Van Hengel y R. P. C. Spengler, dos tenientes de la Armada holandesa. Todos ellos desarrollaron máquinas que utilizaban una combinación de movimientos mecánicos generados por los rotores e impulsos eléctricos que hacían muy difícil el descifrado. Las más famosas entre estas máquinas fueron la E*nigma* alemana y su diferentes versiones, la B-211 y la serie C de Hagelin, y la ECM Mark II o SIGABA americana. La B-21, una máquina electromecánica con representación del texto cifrado mediante un panel de luces, como en la máquina Enigma, fue presentada por Hagelin al ejército francés en 1934. Los franceses obligaron a realizar varios ajustes antes de adoptarla definitivamente. La nueva máquina, la B-211, era una máquina relativamente ligera, unos quince kilogramos de peso, siendo fabricada por Ericsson en Colombes. De esta máquina se llegaron a construir más de quinientas antes de la guerra y unas cien después. En 1936 Hagelin presenta sus modelos C-36 y C-37, con la particularidad de que permitían la impresión del texto cifrado. De estas máquinas se vendieron más de 50000 unidades a países como Francia, Italia, Japón, Finlandia y Alemania. Solo Francia llegó a comprar más de 5000. En 1940 Hagelin marcha a Estados Unidos donde logra convencer al Servicio de Inteligencia americano (el Signal Intelligence Service) de la utilidad de su máquina mejorada, la C-38, que se fabricaría en Estados Unidos por la empresa Smith Corona y que se conocería con el nombre de convertidor M-209 por parte del ejército, y CSP-1500 por parte de la marina. De esta máquina se fabricaron más de 140000 unidades durante la guerra mundial. La foto siguiente muestra una M-209B del Ejército español, lo que nos indica que éste las utilizó a finales de los 40 o al menos las estudió o evaluó su adquisición.



La máquina Enigma.

El proyecto de la máquina enigma fue concebido por Arthur Scherbius y E. Richard Ritter en 1918. En 1919 Hugo Alexander Koch había patentado su máquina de cifrar (Patente nº. 10700), pero debido a problemas con el diseño, decidió vender la patente al Dr. Alexander Scherbius en 1923. Scherbius y Ritter montaron una empresa con su nombre e intentaron vender, sin éxito, su máquina de cifrar a la Marina alemana. Posteriormente lo intentaron con el Ministerio de Asuntos Exteriores, que tampoco demostró ningún interés. En 1923 Scherbius y Ritter, que no disponían de capital para montar una empresa propia, se asociaron con Willie Korn, transfiriendo la patente a la empresa *Gewerkshaft Securitas* que crea una compañía llamada *Enigma Chiffiermaschinen AG* en Berlín para dedicarla a la venta de máquinas de cifra, quedando Scherbius y Ritter como directores de la nueva empresa. En junio de 1923, se empieza a producir la primera máquina Enigma, en la Sreglitzer Strasse nº 2 de Berlin W 35. A partir de los años treinta la fabricación pasa a la compañía *Chiffriermaschinen Geselschaft Heimpold un Rinke* aunque varias de las piezas de las máquinas son fabricadas por otras empresas. La primera versión comercial, la versión A, dotada de cuatro rotores y que también funcionaba como máquina de escribir, fue producida en 1923 y presentada en Berna, más tarde se presentó en la feria de Leipzig y en la Exhibición Postal Internacional en Estocolmo en agosto de 1924, como un sistema para garantizar el secreto de los datos comerciales. La máquina tenía un precio en el marcado de 350 reichmarks. A pesar del escaso éxito comercial obtenido, se fabricaron tres modelos más, conocidos como Enigma B, C y D respectivamente. Los japoneses, los británicos y los polacos copiaron la máquina comercial adaptándola para su propio uso.

El gobierno alemán, convencido de la seguridad del sistema, basándose en el gran número de posibilidades de codificación, adoptaron Enigma como el sistema oficial de cifrado. Se puede decir que a partir de 1926 el estado alemán adquiere todos los derechos sobre la máquina y esta desaparece del mercado comercial, vendiéndose únicamente a aquellos países considerados como amigos, o con alguna relación con el estado alemán, como era el caso de España o Suiza.

La primera en utilizar Enigma para cifrar sus comunicaciones fue la Kriegsmarine en 1926. El ejercito de tierra alemán, la Wehrmacht, empezó a utilizarla a partir del primero de julio de 1928, el ejercito del aire a partir del primero de agosto de 1935 y la policía y la GESTAPO a partir del primero de septiembre de 1937. En realidad el número de máquinas en funcionamiento llegó a ser muy elevado, se calcula que el ejército alemán tenía más de treinta mil en funcionamiento

La máquina militar básica rediseñada denominada Modelo G, empezó a probarse en 1928, entrando en servicio la versión definitiva de la máquina, denominada Enigma I, en Junio de 1930. Aunque tanto los alemanes como los japoneses consideraban sus máquinas como indescifrables, los códigos generados por ambas máquinas fueron rotos por criptoanalistas polacos e ingleses en el primer caso y americanos bajo la dirección de William Friedman en el segundo. Para romper el código de la máquina Enigma los criptoanalistas polacos diseñaron la primera *bomba*, un dispositivo mecánico utilizado para forzar las claves de Enigma, y, posteriormente con la información obtenida por los polacos, Alan Turing y su equipo crearon un ordenador de propósito especial capaz de descifrar las claves de Enigma.

Cifrar con la máquina Enigma era un proceso lento. Lo operadores trabajaban en grupos de dos, con una persona pulsando las teclas, operación muy lenta ya que las teclas debían pulsarse con mucha fuerza para hacer girar los rotores, y otro registrando la letra cifrada que se encendía en el panel superior de bombillas. Las primeras máquinas Enigma tenían tres rotores y unos doce kilos de peso. La mayoría de los países compraron maquinas para su evaluación y todos ellos hicieron sus versiones. La versión británica era conocida como TYPEX y de ella se construyeron unas 12000 unidades, siendo adoptada por el ejército

y la RAF. Incluso los polacos, que fueron de los primeros en romper el código generado por la máquina tuvieron su versión de la misma que llamaban LACIDA.

La criptografía en la Guerra Civil Española.

El inicio de la guerra civil provocó un hecho curioso, ambos bandos utilizaban las mismas claves y sus expertos habían sido preparados en los mismos lugares y con los mismos medios. Había pues que cambiar los métodos y claves de una manera rápida. Eso explica la precariedad e improvisación de los primeros meses utilizándose incluso diccionarios impresos comercialmente para generar los mensajes cifrados, tal como relata el almirante Pascual Cervera y Cervera en un artículo de la revista general de la Marina(30). Al este mismo método era utilizado por los espías italianos en los puertos republicanos. De todas maneras, la calidad de los sistemas criptográficos en ambos bandos era más bien baja. En el artículo antes comentado, el almirante Cervera afirma "Nada se nos resistía, ya que eran simples claves de trasposición, y en esta materia estábamos, tanto los nacionales como los rojos, en mantillas.

Al principio de la Guerra Civil, la provincia de Jaén se mantuvo fiel a la republica, sin embargo un grupo de guardias civiles favorables a los nacionalistas se refugiaron con sus familias en el santuario de Nuestra Señora de la Cabeza a las ordenes del capitán Santiago Cortés González, que se declaró rebelde a la Republica. La esperanza del capitán Cortés era que las fuerzas nacionalistas eligieran la ruta de Despeñaperros en su marcha hacia Madrid. Sin embargo, Despeñaperros fue ocupado por las fuerzas republicanas, quedando el santuario cercado por el ejercito republicano. La resistencia del Santuario fue aprovechada como elemento propagandístico por el bando nacionalista, que decidió finalmente lanzar una operación que liberase a los guardia civiles cercados. El 6 de Marzo Queipo de Llano lanzó una ofensiva con este propósito, pero llegó tarde. El primero de mayo de 1937, gravemente herido el capitán Cortés, los resistentes deciden rendirse.

Durante el asedio se utilizaron palomas para enviar mensajes al bando nacionalista. En uno de los mensajes, el guardia Pedro Gallego cifró un mensaje utilizando una sustitución numérica simple. Las primeras letras, del alfabeto quedaban cifradas de la siguiente manera:

Cifrado:	25	26	28	30	31	33	34	35
Texto en claro:	a	b	c	d	e	f	g	h

El general Antonio Cordón[7], en sus memorias, explica que cogieron una paloma con un mensaje cifrado, y que consiguieron descifrar el mensaje en pocas horas. En realidad el descifrado de mensajes enemigos era una cosa habitual al principio de la guerra, dada la baja calidad de los sistemas utilizados. El cifrado del mensaje se acostumbraba a realizarlo en la parte que correspondía a su interés militar dejando el resto en claro.

Otra de las claves que se utilizaron por la Guardia Civil es la siguiente, en la que se aprecia la utilización de dos cifras indistintamente en las letras de uso más frecuente y la utilización de las mismas cifras para letras que difícilmente puedan generar confusión (S, R).

[7] Antonio Cordón García (1895-1969). Capitán de Artillería retirado. Afiliado al Partido Comunista se reintegró en el ejército al estallar la guerra. Fue jefe de Estado Mayor en distintos frentes, incluyendo el de Belchite en agosto de 1937. Posteriormente fue nombrado jefe de Operaciones del Estado Mayor Central, puesto del que fue destituido por Prieto, y al que volvió en 1938, siendo nombrado posteriormente subsecretario del Ministerio de Defensa. Ascendió a general en febrero de 1939 y acabó la guerra como jefe del EM del Grupo de Ejércitos del Este. Se exilió en la URSS. Falleció en Praga el 1971. Escribió un libro de memorias muy interesante y ameno de título "Trayectoria. Recuerdos de un artillero".

A 53-91	B 12-70	C 40-86	D 31	E 27-43	F 24	G 16	H 11	y 40-59	J 22
L 13	m 15	N 96-66	0 84-39	P 75	Q 71	S 28-54	R 28-54	T 19	u 74-44

Una variante del cifrado de Polibio, utilizado por los comunistas en la guerra civil española consistía en generar una tabla con tres filas de diez columnas. La primera fila no tenía numeración y la segunda y tercera filas se numeraban respectivamente con dos de los números no utilizados en las columnas de la primera fila. Las columnas se numeraban con una permutación de los dígitos del cero al nueve.

El proceso de cifrado consistía en poner una palabra de ocho o menos letras diferentes en la primera fila. En esta palabra se eliminaban las letras repetidas y el resto, hasta completar el alfabeto, se disponían en las dos filas siguientes. El cifrado es similar al de Polibio, pero aquí las letras pueden codificarse como uno o dos números.

Por ejemplo si tenemos el mensaje "*Atacar al amanecer*", la clave *fusil* y las columnas generadas por el siguiente orden:

	8	**3**	**0**	**2**	**4**	**6**	**1**	**7**	**5**	**9**
	F	U	S	I	L					
5	A	B	C	D	E	G	H	J	K	M
1	N/Ñ	O	P	Q	R	T	V	X	Y	Z

El mensaje cifrado sería 581658505814584585958185450541 4. El descifrado es sencillo, ya que si el dígito inicial es un cinco o un uno sabemos que es el carácter viene representado por dos dígitos, en caso contrario, por uno solo.

Sin embargo, los métodos manuales de cifra más utilizados por ambos bandos fueron sin duda las tablas de sustitución, en general numéricas y con múltiples homófonos y nulos, como la clave Oviedo, pequeños nomenclátores como la clave Asturias y métodos de sustitución múltiple como el criptógrafo de cinta, que ya hemos descrito en el capítulo anterior. Una clave famosa fue sin la clave *Bocho*, utilizada para las comunicaciones cifradas entre José Antonio Aguirre, presidente del Gobierno vasco, Juan Ruiz Olazarán, Delegado del Gobierno de Santander, y el ministro Prieto. Su descriptado por parte del bando nacionalista permitió la captura el 8 de marzo de 1937 del buque "*Mar Cantábrico*" cargado de armas con destino al ejército de la República. El descriptado fue realizado por dos de los grupos más importantes de descriptado, el de la sección segunda del Estado Mayor de la Comandancia de Palma de Mallorca, y el de Zaragoza, adjunto a la segunda sección del V Cuerpo de Ejército. En ellos trabajaban dos excelentes criptoanalistas, que superaron sin duda alguna a sus maestros italianos y alemanes. Nos referimos al teniente Baltasar Nicolau Bordoy y al catedrático José María Iñiguez y Almech. Sus descriptados se enviaban directamente al Cuartel General de Franco, lugar donde se centralizaban todas las demandas de descifrado del ejército nacionalista. Éste fue uno de los grandes aciertos nacionalistas, la centralización de las claves obtenidas y de todo aquello relacionado con el almacenamiento y distribución de claves, tanto propias como enemigas. El artífice de este sistema fue D. Antonio Sarmiento León-Toyano, Jefe de los servicios de escucha y criptografía nacionalistas. La calidad de trabajo de los criptoanalistas españoles fue tal, que, en el caso de Iñiguez, los alemanes le enviaban por avión los telegramas captados que no habían conseguido descriptar ya que estaba especialmente dotado para ello. Sin embargo, no fueron los únicos, en la tabla

siguiente se presentan los descriptadores más destacados del bando nacional y los centros de descriptación en los que trabajaban:

V Cuerpo de Ejército	José María Iñiguez y Almech
	Federico Alzamora
Comandancia Militar de Baleares	Baltasar Nicolau Bordoy
CTV	Teniente coronel Francesco Dragone
	Comandante de Nacki
	Alférez Vuolo
SIPM	Antonio Espinosa San Martín
	Gonzalo de Erice
	Juan Solabre Lazcano
Gabinete del Cuartel General	Román Martínez de Velasco

De las secciones de criptoanálisis nacionalistas, aparte de las comentadas estaban el centro de criptoanálisis de la Marina ubicado en Cádiz a las ordenes, primero de D. Pascual Cervera y Cervera, y después del capitán de artillería de la Armada D. Francisco Liaño Pacheco, que posteriormente se encargaría de la sección de cifra de la Armada nacionalista y que, una vez acabada la guerra sería nombrado profesor de química y explosivos de la Escuela Naval Militar.

En el bando republicano el descriptado de las comunicaciones corrió a cargo prácticamente durante toda la guerra del gabinete de contracifra del Servicio de Información del Estado Mayor. Sus miembros, ayudados por asesores rusos que permanecieron en España hasta los últimos meses de la guerra, trabajaron siempre en condiciones precarias y con una falta alarmante de medios. Hacia el final de la contienda parece ser que el SIM republicano montó su propio servicio de contracifra, sin embargo no sabemos prácticamente nada de él. Los miembros que conocemos del gabinete de descriptado republicano, dirigido en esa época por Carmelo Estrada Manchón, son, aparte del propio Estrada:

- César Vigas Vigas.
- Fernando Baringué Millat.
- Manuel Inglada Díaz.
- José Medina Cantero.
- José Díaz Rodríguez.

Algunos de ellos, exceptuando Estrada, que marchó a México y Fernando Baringué, que volvió a España, debieron formar parte del grupo de españoles dirigidos por Faustino Antonio Camazón, que ayudaron a los franceses y polacos en los PC Bruno y Cadix durante la guerra mundial.

Volviendo a los métodos de cifrado, y en particular al método de cinta móvil, éste sufrió varias modificaciones durante la guerra civil. Una de las primeras variaciones fue el cambio del alfabeto de la primera fila. Originalmente dicha fila presentaba todas las letras en orden alfabético, siendo sustituida más adelante por un alfabeto en el que las letras aparecían en un orden aleatorio. Esta modificación ya la vemos en la clave general de 15 de abril de 1910, con lo que no podemos decir que se trate de una innovación aparecida en la guerra. Otra fue el añadir varias cintas móviles como en la clave aviación 1931 en la que las cintas eran una la típica del alfabeto móvil y dos correspondientes a dos de las filas de códigos. Esto hacia que un mismo número representase a varias letras en función de su colocación y

permitía, teóricamente, mejorar la resistencia del código. Además se solían incluir pequeños repertorios para las claves más comunes.

Si bien parece chocante que un sistema con tan poca seguridad fuese tan ampliamente empleado en la guerra civil española, lo es más cuando vemos que se utilizó en los niveles más altos de seguridad, al menos por parte republicana. Como ya hemos comentado, Carmona ya avisaba de la poca seguridad del método y daba un ejemplo de cómo descifrar un mensaje. Si añadimos la laxitud, por decirlo de alguna manera, con la que se tenía al principio de la guerra el tema del cifrado no hace falta decir que el descifrado por parte del enemigo era previsible cuando no habitual

En el ámbito diplomático, al menos en 1937, el sistema predominante en las embajadas de la España republicana era la utilización de libros de códigos, sistema de fácil manejo y fácil intercambio mediante valija diplomática. En las legaciones diplomáticas nacionalistas, aunque al principio se intentó dotarlas de máquinas Enigma, se seguían utilizando códigos, y solo pasaron a utilizar las Enigma una vez acabada la guerra y hasta su retirada pocos meses después de finalizar la guerra mundial. Sin embargo la utilización de códigos no fue exclusiva de las embajadas, el ejército y la marina también los utilizaron. Sin embargo, los códigos utilizados por los militares seguían un esquema como mínimo curioso, pero interesante y que elimina uno de los problemas inherentes a la utilización de los códigos, su difícil distribución. Un ejemplo de estos era el denominado código 17 que se utilizaba a mediados de 1938 por el Ejercito republicano. Este código estaba formado por mil valores de tres cifras divididos en diez columnas, cada uno de los valores era una letra, prefijo, sufijo o número. El número de código se obtenía juntando el de columna, de un dígito y que variaba cada semana, con el de fila que variaba cada día. El número de fila, de dos dígitos, era un número aleatorio que estaba en una cinta móvil que se posicionaba en función del número diario determinado.

Por último hablar de la amplia utilización de los “códigos de trinchera”, códigos muy reducidos y especializados al arma y función que se esperaba de ellos, entre ellos tenemos los códigos de avistamiento de la aviación republicana o el código de bous de la marina republicana.

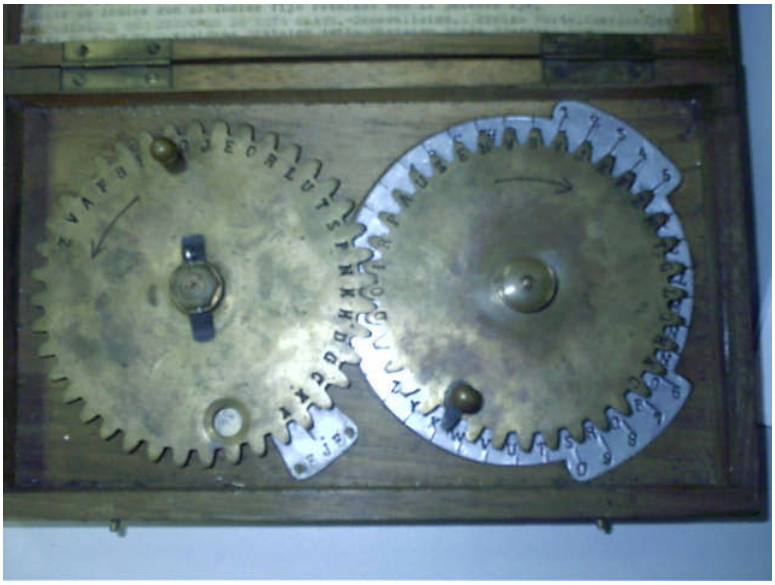
En cuanto a los servicios de contracifra republicanos fueron entrenados inicialmente por asesores soviéticos, y, entre ellos destacaron los miembros del servicio de criptografía del Servicio de Información del Estado Mayor que solo hace unos meses pudimos identificar(32). Su rendimiento parece haber sido muy bueno, dado que fueron inmediatamente reclutados por los franceses para ayudarles al poco de empezar la guerra mundial.

En cuanto a la utilización de métodos de cifrado más fuertes en la guerra civil española (31), aparte de la utilización de máquinas Enigma, de las que se adquirieron diez en noviembre de 1936 y cuyo número total en uso en la guerra civil rondó la cincuentena, y Kryha, de las que tenemos noticias de su utilización por parte del bando nacionalista, tenemos algunos dispositivos de cifrado más artesanales como la denominada “clave norte”. La clave Norte era un dispositivo de cifrado mecánico extremadamente simple. El dispositivo consistía en un sistema con dos ruedas dentadas que se encontraban encima de dos círculos, el de la izquierda de cartulina en el que se encontraba el alfabeto cifrado, y el de la derecha en el que se encontraba el alfabeto en claro, con algunas letras repetidas.

Las dos ruedas tenían diferente número de dientes, cuarenta la izquierda y treinta y siete la derecha, y diferente tamaño, 10,5 centímetros de diámetro exterior y diez centímetros de diámetro interior la izquierda por 9,7 y 9,2 respectivamente la derecha. La rueda izquierda tiene un agujero a continuación de las letras, en la parte inferior, que es por donde se puede ver el resultado del cifrado.

Los componentes fijos de la clave norte son, las dos ruedas y la plancheta metálica de la derecha, la cartulina se cambiaba, aunque no puedo precisar la frecuencia. En la que pudimos ver ponía la siguiente leyenda ”*Servirá desde el 20 de agosto de 1937 hasta nuevo aviso y ver T.P. 9 de agosto de 1937*”.

En la fotografía siguiente podemos ver un ejemplar de clave Norte.



Una vez acabada la guerra España, dada su precariedad de medios, mantuvo junto con las máquinas Enigma, cifrados manuales tales como las claves R y cifradores como el “Eolus”. Ya en los años cincuenta, con las máquinas Enigma ya retiradas, el Ejército español empezó a dotarse con máquinas Hagelin para asegurar sus comunicaciones.

Podemos concluir este breve estudio indicando que en la Criptología española hay luces de una enorme intensidad, así como épocas de sombra profunda, pero que en su conjunto es una historia que merece y debe estudiarse por su riqueza, variedad, y, sobre todo, por que forma parte de nuestro patrimonio histórico.

(1) Joaquín García Carmona. 1894.Tratado de criptografía con aplicación especial al ejército. Sucesores de Rivadeneyra.
(2) Fernando de Lossada y Sada. 1898. Manual militar de telegrafía. Librería de Hernando y Compañía.
(3) Pedro Serrano García. 1953. Criptografía y perlustración. Ed. La Xilográfica.
(4) El Servicio de Información en la Guerra de la Independencia. Fernando Mazarro Ciarán.
(5) Nuevos métodos criptográficos. D. Manuel Núñez y Muñoz. Librería e imprenta de Izquierdo y Compañía 1897.
(6) Teniente coronel de ingenieros Fernando de la Peña. 1937. El enlace y las transmisiones en campaña. Los medios de enlace. Papelería Plácido Gómez.
(7) Orgánica Naval. Capitán de corbeta D. Pascual Diez de Rivera y Casares. Madrid 1934.
(8) Analysis of criminal codes and ciphers. Daniel Olson. Forensic Science Communications. Enero del 2000. Volumen 2, Número1.
(9) Los nueve libros de la historia. Heródoto. ORBIS 1987.
(10) Historia del Perú. Diego Fernández. Ed. Atlas 1963.
(11) Les chiffres secrets dévoilés. Commandant Bazeries. Librairie Charpentier et Fasquelle 1901.
(12) AENEAS TACTICUS. Textos completos. LOEB CLASSICAL LIBRARY 1928.
(13) Tratado de Criptografía con aplicación especial al ejercito. Primer teniente de infantería Carmona. Est. Tip. Sucesores de Rivadeneyra 1894.
(14) The myth of the skytale. Thomas Kelly. Cryptologia vol. XXII, nº 3, Julio 1998.
(15) La criptografía en anécdotas. José Luis Muñoz. Ediciones ejercito 1955.
(16) Criptografía moderna: curioso cifrario entre el obispo Diego de Muros y los reyes católicos. Juan Carlos Galende Diaz. Boletín del Real Instituto de Estudios Asturianos.
(17) Cifras y claves indianas. Capítulos provisionales de un estudio sobre criptografía indiana. Guillermo Liman Villena. Anuario de Estudios Americanos, XI. Sevilla, 1954.
(18) La escritura cifrada durante el reinado de los Reyes católicos y Carlos V. Juan Carlos Galende Díaz. Separata de los cuadernos de estudios medievales y ciencias y técnicas historiográficas nº 18-19. Universidad de Granada 1993-1994.
(19) Criptografía española. Mariano Alcocer. Tipografía de Archivos 1934.
(20) Los códigos secretos. Simon Singh. Editorial Debate 2000.
(21) Les cahiers secrets de la cryptographie. Editions du rocher 1972.
(22) Histoire des services secrets français. Douglas Porch. Albi Michel 1997.
(23) La cryptographie militaire. Auguste Kerckhoffs. Journal des sciences militaires 1883. Disponible en http://www.el.cam.ac.uk/~fapp2/.
(24) The man who broke the Napoleon´s codes. Mark Urban. Faber & Faber 2001.
(25) CLAVE para obtener secreto y economía en toda clase de correspondencia y singularmente en la telegráfica. G. Pelligero. Establecimiento tipográfico de Ricardo Fé. 1893.
(26) Poligrafía o arte de escribir en cifra. Francisco Paula Martí. Imprenta de Sancha 1808.
(27) Claves cifradas Carlistas. César Alcalá Gimenéz.
(28) Una clau criptográfica del segle XV. A. M. Aragó Cabañas. Cuadernos de Arqueología e Historia de la Ciudad, Barcelona, 12, 1968, 171-176.
(29) The American Black Chamber. Herbert O. Yardley. Amereon House 1997.
(30) Criptografía rudimentaria. Almirante Cervera y Cervera. Revista General de Marina. Julio 1973.
(31) Mechanical cipher systems in the spanish civil war. José Ramón Soler Fuensanta. Cryptologia vol. XXVIII, nº. 3. Julio 2004.

(32) Los Hombres que nunca existieron. José Ramón Soler Fuensanta y Javier López-Brea Espiau. Revista Española de Historia Militar 64. Octubre de 2005.