Temas Militares

CRIPTOGRAFÍA

Por el Coronel MATA MANZANEDO
del Servicio de Estado Mayor

Recientemente se ha celebrado en el Museo Naval una exposición de documentos inéditos del archivo de la casa ducal de Veragua; entre ellos figura uno que se refiere al asunto que encabeza estas líneas.

Se trata de la clave del abecedario cifrado usado por el Almirante don Diego de Colón, primer virrey del Nuevo Mundo e hijo del glorioso descubridor, con el cartujano padre Gorricio.

El documento está fechado en Sevilla en 16 de marzo de 1509, y en su pie figura la siguiente recomendación: "En fin de la carta haga lo que mandare."

La clave emplea el sistema de perturbación o sustitución, y los signos que representan las distintas letras están constituídos por sencillas combinaciones de rectas y círculos o de ambas figuras.

La formación del alfabeto perturbado es bastante ingenua, ya que un mismo signo, variando su orientación, representa dos o más letras consecutivas. Así la T invertida es la equivalente a la *d*, y en su posición natural la *e;* el ángulo recto, según la región hacia la cual presenta su abertura, sustituye a la *f*, la *g* o la *h;* análoga ley sigue el resto del abecedario.

El autor del trabajo no debió de quedar muy satisfecho de la seguridad de la clave, pues agregó una segunda cifra para las cinco vocales, ya que una representación única para letras de tan frecuente repetición hubiera facilitado el descifrado de los escritos.

Hemos hecho mención de esta modesta manifestación criptográfica, solamente a título de curiosidad y por tratarse de un documento que, aunque de escaso valor intrínseco, desde el punto de vista de aquella ciencia, veía por vez primera la luz pública, y por su interés espiritual, así como por la utilidad que pudiera prestar para las investigaciones colombinas.

El empleo de la criptografía en el Ejército del Aire es continuo y no es preciso encarecer su importancia, ya que para toda acción aérea es imprescindible disponer de un Servicio de Transmisiones organizado en forma segura y completa. Estas, para el curso de sus despachos, emplean todos los medios de transmisión conocidos hasta el día; y esta circunstancia, unida a la creciente afición a la resolución de problemas de este género, como crucigramas, logogrifos y tableros más o menos complicados, nos induce a recordar algunas curiosidades de la ciencia criptográfica.

Esta es tan antigua como el hombre, ya que reducida en sus principios al arte de comunicarse veladamente por medio de la escritura velada o criptografía (*krytós*-oculto, *gráfoo*-escribir), tuvo sus primeras manifestaciones en el lenguaje simbólico o jeroglífico empleado por magos, sacerdotes e individuos de casta superior, con la finalidad de ocultar sus conocimientos a los más ignorantes, lo que les permitía aparecer ante sus ojos con una aureola sobrenatural y dominarlos más fácilmente.

Al constituirse los Estados, con sus ejércitos y embajadores se inicia la aplicación militar de la criptografía, que no tarda mucho tiempo en invadir otras actividades humanas, comerciales, financieras, en cuyas esferas su uso aumenta incesantemente.

Es probable que el primer pueblo que empleó las comunicaciones secretas fué el hebreo, y tenían el doble aspecto de dar al mensaje secreto la apariencia de uno corriente, empleando tintas invisibles o lenguajes convenidos, o de hacer ininteligible el mensaje para quien no fuese poseedor del secreto de su clave, pero sin perder el carácter de tal mensaje, es decir, cifrándolo.

Los griegos y romanos hicieron uso frecuente de ambos procedimientos, y así Histias, tirano de Susa, envió a Aristágoras la orden de sublevación que inició las guerras médicas, escrita mediante incisiones que practicó en el cuero cabelludo de un esclavo, con lo que el destinatario, simplemente afeitándole la cabeza, pudo leer cómodamente el mensaje. El adelanto de la criptografía en esta época lo prueba la aparición de aparatos para cifrar, tales como el escital o escítalo de los lacedemonios, la plancheta de Eneas y el alfabeto de Julio César, cuyos fundamentos, perfeccionados, son la base de muchos de los criptógrafos actuales.

En la Edad Media predominó el empleo del lenguaje convenido y alfabetos de perturbación sencilla, que no ofrecían gran seguridad en su secreto.

El siglo XV-XVI, con la aparición de los sistemas polialfabéticos, hizo destacar notablemente los trabajos del alemán Tritemio, italiano Porta y el francés Vignere, verdaderos padres de la criptografía, y sus métodos y procedimientos siguen actualmente en uso. La seguridad del cifrado que proporcionaban era tal, que documentos secretos de Luis XIV no ha sido posible descriptarlos hasta época muy reciente.

La evolución de la fortificación, que motivó prolongados asedios de las plazas fuertes, hizo cobrar gran importancia a la criptografía, que declina al aparecer la guerra de maniobra napoleónica, y la guerra 1914-1918 y la actual contienda elevan esta ciencia a los términos más brillantes.

En la Biblioteca Nacional existe un manuscrito atribuído, con poco fundamento, a Alfonso X el Sabio; está escrito en lenguaje cifrado para hurtar al público el conocimiento de la "piedra filosofal", y no ha podido ser descifrado. El Archivo Nacional de Simancas posee una notable colección de claves completas e incompletas y diccionarios para cifrado, que a partir de los Reyes Católicos y por Monarcas posteriores fue-

ron empleados en capitulaciones matrimoniales, embajadas y para las relaciones reservadas con personajes importantes.

En nuestra guerra de Liberación los dos bandos concedieron gran importancia al servicio de cifra: así lo atestiguan los datos que posteriormente se reseñan.

Como decíamos anteriormente, el mensaje transmitido puede tener apariencia normal; para este fin se usan tintas invisibles o simpáticas, así llamadas porque el empleo de un medio adecuado, calor, humedad o reactivos químicos revela la escritura

Se emplean líquidos comunes como zumos de frutas, leche, cerveza, o bien compuestos químicos en polvo que, fácilmente ocultables en lapiceros o sellos farmacéuticos, al diluirlos en agua permiten preparar rápidamente la tinta simpática; lógicamente, estos últimos ofrecen mucha más garantía, pues no siempre se cuenta con el reactivo especial que precisa el criptograma para su revelado. En la pasada guerra 1914-1918 todas las tintas invisibles empleadas acabaron por ser descubiertas en plazo más o menos largo, pues por la generalización de su empleo los Estados Mayores organizaron secciones de personal especializado que se dedicaban a esta actividad.

El lenguaje convenido logra dar apariencia inocente a los mensajes, modificando el sentido de frases o palabras. En la pasada campaña de Liberación la Radio Nacional usó mucho este sistema para notificar la llegada de evadidos de Zona roja, con vistas a evitar las represalias sobre los familiares de los mismos. La Prensa corriente, libros de devoción o científicos, y las partituras musicales se han utilizado mucho para transmitir mensajes convenidos. Su mayor aplicación es en los servicios especiales, ya que su empleo en los mensajes de carácter puramente militar tiene el inconveniente de alargar la transmisión por la mayor extensión del mensaje.

Por ello la criptografía militar en la última actividad citada emplea casi exclusivamente el lenguaje cifrado; los distintos métodos en uso pueden agruparse en tres sistemas: el de transposición, que valiéndose de las mismas letras del texto claro invierte o varía su colocación en forma más o menos complicada; el de perturbación o sustitución, que, como su nombre indica, sustituye las letras del texto claro por otras, guarismos o signos especiales; y el sistema vario, que comprende todos los métodos no incluídos en los dos grupos anteriores.

Sin entrar en su descripción, manejo y análisis de sus ventajas e inconvenientes (que figuran en todas las obras de esta materia), citaremos los más importantes.

El método de transposición más sencillo es el de inversión; cabe citar como curiosidad, que la única frase incifrable con este método es la tan conocida: "Dábale arroz a la zorra el abad"; desde la antigüedad se ha empleado mucho el método chino o bustrofedón, así llamado, pues el camino seguido para la lectura de las letras en el rectángulo formado con las del texto claro, es el de los bueyes que aran. En el método del paralelogramo la lectura del texto cifrado se hace siguiendo las diagonales del mismo o sus paralelas, y, finalmente, existen muchas variedades del conocido método de divisores.

Entre los aparatos más difundidos para cifrar con este sistema figura el antiguo escítalo antes aludido, consistente en dos bastones de madera o marfil rigurosamente idénticos, de los que cada corresponsal disponía de uno de ellos. El remitente escribía su mensaje en una banda de papiro arrollada con una inclinación cualquiera sobre el bastón, y la lectura del texto claro sólo era posible arrollando previamente la banda con la debida coincidencia de letras, cosa fácil para el corresponsal que se hallaba en posesión del bastón adecuado. También han sido y son muy empleados los aparatos de celosía o enrejado, en los que se vacía uno o más de los pequeños cuadrados del rectángulo total formado con las letras del texto claro; variando o invirtiendo la colocación del aparato sobre el texto en una forma convenida quedan al descubierto, sucesivamente, varias letras, cuyo orden determina el mensaje cifrado.

Los métodos de perturbación cabe agruparlos en los de perturbación sencilla y múltiple o variable. Los primeros emplean siempre el mismo signo para representar una letra determinada; entre los más antiguos figura el conocido con el nombre de alfabeto de Julio César (si bien parece fué empleado anteriormente por fenicios y cartagineses); sustituye cada letra por la que ocupa otra adelantada o retrasada un número determinado de lugares; y el inocente y difundido método de fuga de vocales, atribuido a los padres benedictinos. Tambien es muy conocido el llamado alfabeto masónico, basado en las figuras elementales en que puede descomponerse dos figuras origen: una cruz de San Andrés y otra formada por cuatro segmentos, paralelos dos a dos, que se cortan normalmente. Como al descomponerlas solamente pueden obtenerse trece figuras distintas, la representación de las trece letras restantes se consigue punteando las figuras anteriores. El alfabeto Mirabeau, tan en auge durante la revolucion francesa, representa cada letra por un quebrado, cuyos términos son, respectivamente, el numero de orden del grupo de cifras y el orden de estas dentro del mismo; existen muchas mas soluciones de alfabetos, inspirados en analogos principios.

Para la perturbación múltiple se emplean tablas especiales, como la de Trithemio, Porta y la de alfabetos perturbados irregularmente, la tabla numeral y el metodo de Saint-Cyr, y otra infinidad de variantes mas o menos ingeniosas. La invencion de estas claves, con vistas a aumentar su rendimiento, ha motivado la invencion de aparatos especiales o criptografos, como los tan conocidos de discos giratorios y de cinta correderiza.

El sistema vario emplea diccionarios para la sustitución de silabas o palabras por letras, silabas o grupos de cifras; los diccionarios pueden ser los normales, asignando a cada palabra como su equivalente la situada un numero determinado de lugares delante o detrás de la misma; o bien diccionarios o codigos especiales, que pueden tener aplicaciones muy varias, desde los internacionales de Marina y señales radiogoniométricas y meteorológicas, hasta los formados con fines particulares y reservados, como los militares y diplomáticos. Las condiciones teóricas de seguridad de una clave militar son en parte antagónicas, ya que es deseable que sea prácticamente indescifrable aun en el caso que el enemigo llegue a conocer el sistema porque resulte fácil cambiar rápidamente la clave o palabras base de la clave; que en su utilización se preste fácilmente al empleo de todos los medios de transmisión; que pueda emplearse de memoria sin exigir notas escritas, siempre propicias a indiscreciones; que su manejo resulte sencillo aun para el personal no especializado; que sea transportable cómodamente, y que su utilización no imponga el empleo de aparatos especiales.

Los progresos de la construcción electromecánica han permitido construir máquinas de cifrar de sustitución, que realizan el trabajo con gran rapidez y seguridad. La más sencilla es la máquina de escribir normal, en la que se cambian

las teclas de las distintas letras. Este cambio se hace en forma que resulte reversible; así, si al presionar la tecla B sale la T, en la máquina del corresponsal debe verificarse a la inversa.

En la máquina eléctrica, de forma análoga a las de escribir, al oprimir la tecla correspondiente a la letra del texto claro, ilumina o imprime la letra del texto cifrado. Su trabajo resulta prácticamente indescifrable, ya que los distintos circuitos eléctricos atraviesan cuatro discos, tres de los cuales son móviles, pudiendo ocupar, por tanto, seis posiciones relativas distintas; como cada disco tiene veintiséis contactos, correspondientes a las distintas letras del alfabeto, al asociarse los movimientos y posiciones de los discos el mensaje queda cifrado polialfabéticamente con veintiséis alfabetos distintos, lo que hace que pueda formarse un número de combinaciones superior a los doscientos trillones.

Finalmente, la televisión se presta a la transmisión de escritos o gráficos en forma velada, ya que la dificultad inicial de sorprender la debida sintonía es posible aumentarla guardando pausas irregulares en la emisión. Su continuo perfeccionamiento permite augurar sus grandes posibilidades en el futuro.

Descifrado.—La conservación del secreto de una clave, pese a los intentos del enemigo por descubrirla, reside principalmente en su construcción, la que, por tanto, ha de ser estudiada lenta y meticulosamente, según la aplicación posterior que de ella vaya a hacerse; está a cargo de personal idóneo en la materia, que dispone de los elementos necesarios y que no trabaja con gran agobio; por tanto, lógicamente cabe esperar que su labor vaya acompañada del éxito.

Pero el personal encargado del descifrado se encuentra en caso bien distinto. Con excepción del organismo central encargado de este servicio, o de los similares en los escalones de mando muy elevados que contaran con verdaderos "virtuosos" del descifrado y medios adecuados para el mismo fin, el personal en campaña de las grandes y pequeñas unidades aéreas o antiaéreas, aerodromos y red de acecho, trabajará más precariamente; por otra parte, ciertas claves exigirán un desciframiento inmediato que permita realizar una rápida explotación del informe captado, y la premura del tiempo viene a aumentar las dificultades.

Esto resalta la conveniencia de fomentar la afición del personal a estos problemas, a fin de que lleguen a poseer un verdadero *espíritu criptográfico*, ya que si esto tiene ventajas desde el punto de vista del descifrado, no serán menores las que reporte al lograr que los encargados de la redacción de los mensajes propios lo hagan en forma adecuada, pues la mayor proporción de claves descubiertas es motivada por una redacción rutinaria o indiscreta del mensaje.

No es posible dar reglas fijas para la formación de buenos descriptadores; deben seleccionarse entre aquellos que posean buenas cualidades congénitas, que una adecuada instrucción las perfeccionará por el complemento de las adquiridas. Condición preponderante entre las primeras debe ser poseer una paciencia tenaz y perseverante que supere el desaliento que origina el fracaso de las primeras tentativas. Asimismo es muy conveniente un aguzado espíritu de observación que permita percibir los indicios más insignificantes; discreción absoluta e intuición que le limite sus pesquisas a un número de hipótesis probables relativamente reducido.

Las cualidades adquiridas pueden resumirse en la posesión de una amplia base cultural, principalmente en Filología, Criptografía y táctica y técnica en relación con la actividad de que se ocupe, y fundamentalmente un conocimiento profundo del idioma empleado en la redacción de los mensajes propios y enemigos.

Todos los idiomas presentan leves y particularidades cuyo conocimiento puede resultar muy conveniente, y entre las muchísimas que contiene el castellano citaremos algunas.

Prescindiendo de las letras dobles *ch, ll, rr,* nuestro alfabeto tiene veintiséis letras; aunque la proporción en que entran en un escrito no es rigurosamente exacta, pues depende del asunto del mismo, cabe establecerla aproximadamente.

TANTO POR MIL DE VOCALES Y CONSONANTES

	Español	Francés	Italiano	Alemán	Inglés
Vocales.	460	440	477	384	385
Consonantes..	540	560	533	616	617

El cuadro adjunto refleja la proporcionalidad de las distintas letras comparativamente entre varios idiomas europeos; igualmente se indica la proporción entre vocales y consonantes.

TANTO POR MIL DE LETRAS EN DISTINTOS IDIOMAS

Español	E 146	A 119	O 91	N 72	S 72	I 71	R 66	L 55	D 50	C 48	T 40	U 33	P 31	M 28	G 13	B 11	Y 11	V 9	F 7	J 6	Q 5	Z 4	H 3	X 2	Ñ 1	K	W
Francés.	E 185	S 88	R 78	I 74	A 72	N 71	T 65	O 57	U 52	L 46	D 42	M 36	C 34	P 25	V 16	F 14	Q 10	G 9	X 7	J 6	B 5	H 4	Z 3	Y 1	Ñ	K	W
Italiano..	A 149	E 115	I 103	L 82	O 77	T 76	N 67	R 55	D 55	C 45	S 44	U 37	G 35	V 30	P 28	M 23	F 12	B 5	H 5	Q 3	Z 2	K 1	Y	J	X	Ñ	W
Alemán .	E 185	N 104	I 68	S 68	R 66	U 57	A 52	H 51	D 49	T 47	L 42	G 41	C 36	B 23	O 22	M 20	F 19	Z 12	W 11	K 10	V 9	P 5	J 3	Ñ	Q	X	Y
Inglés....	E 129	T 100	O 84	A 83	N 75	S 66	R 65	I 61	H 59	L 41	D 34	F 32	M 28	U 27	C 23	G 21	W 20	Y 19	P 16	B 15	V 6	K 6	Z 4	J 3	Q 1	Ñ	X

Concretándonos al castellano, citaremos algunas curiosidades: la *q* y la *u* son inseparables, así como la *e* y *x* en el prefijo *ex.*

Las letras duplicadas no son muy numerosas: la *a*, la *i* y la *u* solamente se doblan en las palabras *Saavedra, pisimo* y *duunviro;* la *cc*, por el contrario, abunda muchísimo, como lo hace en los términos que denotan acción: *atracción, proyección*, etc. La *oo* figura en algunos vocablos, como *cooperación, coordinación* y otros anticuados; la *r* en algunos casos se dobla en mitad de palabra, como en *amarrar.*

El único femenino terminado en *o* es *mano;* la palabra *maravedí* tiene tres plurales diferentes *(maravedíes, maravedís* y *maravedises)*, contrariamente a *régimen*, que carece de él.

No son frecuentes las oraciones que, teniendo sentido, todas sus letras sean distintas, como ocurre con las doce siguientes: "Un triple caso".

El conocimiento de la composición de gran número de palabras también facilita la labor de descifrado.

En nuestro idioma sólo existen cinco monogramas, que ordenados por orden de frecuencia, son: *a, y, o, e, u.*

La *f* sólo forma bigrama con la *e* y *u* en *fe* y *fu;* la *h*, con la *a* y *e*, en *ha* y *he;* la *i*, solamente con la *r* y *d;* la *l, m, n, o, t, u, v* e *y*, en las formas pronominales, artículos y preposiciones; además existen los bigramas de la escala musical y algunos otros de uso poco frecuente.

La mayor parte de las palabras de tres letras tienen la vocal en el centro; pero no son escasos los trigramas que tienen la primera y tercera letras vocales, y algunas las dos unidas, como *rey, aún* y *hoy.*

Naturalmente, en palabras de mayor número de letras las agrupaciones que cabe hacer son mucho más numerosas, según sus letras o sílabas estén repetidas o no, y prescindimos, por tanto, de su enumeración.

Por último, reseñaremos brevemente las actividades criptográficas en nuestra guerra de Liberación; como es lógico, por la forma en que se produjeron los hechos, ni uno ni otro bando pudieron utilizar el sistema vigente en los departamentos oficiales, y tuvieron que improvisar su cifra. En la zona nacional se empleó en mucha mayor proporción el sistema de transposición; el bando contrario dió preferencia al de sustitución; ambos tienen sus apologistas, pero parece ser que a igualdad de complicación y utilizados por personal que no tenga gran preparación, es más seguro el primero.

Un índice del entusiasmo con que trabajó el personal de descifrado, que en su mayor parte era voluntario, lo acusa el número de claves descubiertas, que ascendieron a 245, que unidas a las 156 cogidas al enemigo, suponen un total de 401 claves anuladas. En cantidad destacó la oficina de Baleares, y punto a calidad, probablemente Zaragoza, ya que descubrió claves verdaderamente difíciles. Un catedrático de la Universidad aragonesa se reveló como un criptógrafo de excepción.

La Criptografía es objeto de gran atención en muchos países, y así, en Italia el inspector general del servicio es un general; para asistir al curso que anualmente se organiza son seleccionados de 20 a 30 oficiales, no obstante lo cual el número de los que alcanzan el título de criptógrafo no suele pasar de tres, ya que se considera que para ello no es suficiente haber logrado con el trabajo del curso la adquisición de las condiciones antes citadas, sino haber evidenciado a lo largo de él unas condiciones de verdadera excepción.

INTENDENCIA TÉCNICA

POR **MARIANO LAHOZ RUPÉREZ**
Capitán de Intendencia del Aire

A principios de siglo podía decirse que la Intendencia era aquel Cuerpo castrense encargado de proporcionar al Ejército todo aquello que precisara para subsistir. Misión amplia, que tiene un carácter genérico a todas las Intendencias organizadas en los Ejércitos, si bien, específicamente, en algunos países esta misión era ampliada o reducida en funciones, según los casos y épocas de paz o guerra. Todo ello independientemente de la labor administrativa, que no vamos a referirnos en el presente trabajo.

La primera misión, es decir, la misión básica de la Intendencia (la de proporcionar o proveer) en circunstancias normales, la podía realizar con sus propios medios o buscando el libre concurso de los particulares. En circunstancias anormales o casos de guerra, le bastaba para cumplir su cometido, además de los procedimientos anteriores, hacer uso de las facultades que leyes y reglamentos daban a este Cuerpo, ya que el Ejército tenía efectivos limitados y siempre quedaba una retaguardia capaz de producir lo bastante para cubrir las necesidades de aquél. La Intendencia adquiría esta producción y la suministraba al soldado.

Eran aquéllos los tiempos en que la lucha era de Ejércitos, y estos Ejércitos se componían de soldados. Hoy las circunstancias han cambiado por completo; la guerra es integral, la Aviación hizo frente al puerto, al taller, la mina; destruir una fuente de producción del enemigo es ganar una batalla; la guerra ya no es de Ejércitos, la guerra es de naciones.

Por otra parte, siendo muy importante, como lo sigue siendo, el elemento soldado ya no es único; aparece la máquina, uno tiene que ir ligado a la otra, y la retaguardia ha de dar vida y movimiento a ambos.

Por tanto, habiendo pasado a ser la retaguardia lugar predilecto de ataque del enemigo y siendo la nación entera la que combate a éste, bien sea con las armas en la mano (Ejército), o bien incrementando la producción, o pretendiendo obtener un material superior al del contrario, etc. (población civil), es lógico y necesario que la persona que encarne la jefatura de ambos (población combatiente y población producto-