Los orígenes de la Criptografía y su desarrollo hasta el Siglo XIX

Por
Jaime ROJAS Brugués
Capitán de Corbeta
Armada de Chile

PRIMERA PARTE

La palabra Criptografía viene del griego "kryptos" = oculto y "graphein" = escribir. De acuerdo a esto, muchos autores han abarcado en esta acepción todo el extenso campo de la "escritura oculta", lo que indudablemente conduce a confusiones. Debemos reconocer la diferencia al respecto entre "Esteganografía", que consiste en escribir de manera que los elementos del texto no se visualicen y "Criptografía" que consiste en escribir de manera que los elementos del texto se puedan visualizar, pero no se puedan entender.

La Esteganografía se aplicó mucho antes del siglo V A. de C. Los reyes sirios, cuando querían enviar un mensaje cuyo contenido deseaban mantener en secreto, rapaban a sus esclavos, escribían en sus cueros cabelludos el mensaje y luego, dejándoles crecer el pelo, los enviaban a destino donde el corresponsal al raparlos nuevamente podía leer la información. Indudablemente que este método no parece ser suficientemente rápido ni lógico para nosotros. El empleo de tintas simpáticas, diminutas cámaras fotográficas para reproducir documentos, etc. dejan totalmente obsoletos este sistema tan primitivo. Quizás lo más sorprendente en este campo en la actualidad es el llamado "procedimiento de micropunto": El mensaje o documento se fotografía con un film "MIKRAT", el que se posa sobre el punto de una "i", con cuyo tamaño coincide, de manera que una revista o cualquiera otra publicación de aspecto inofensivo puede contener un importante mensaje, completamente oculto al

ojo desnudo. Los microscopios necesarios para la lectura de semejantes documentos pueden estar escondidos, por ejemplo, dentro de una pluma fuente.

La "Criptografía" sin embargo comienza a ser utilizada con posterioridad y con procedimientos un poco más refinados. Como dijimos anteriormente, consiste en ocultar la información, pero de tal manera que los elementos del mensaje se pueden ver, pero no así "entender" por quien no posea la clave o artificio que se empleó. De otra manera, para leer el mensaje aún sin estar en posesión de la clave, debemos recurrir al estudio de un campo de aún mucho mayores proyecciones: el Criptoanálisis.

Para diferenciar a su vez estos dos conceptos podemos decir que por lo general los que confeccionan las claves, los criptógrafos, son personas que no necesariamente deben poseer una preparación especial. En cambio los que tienen por misión descriptar o "romper" el secreto de las claves, los criptoanalistas, generalmente son personas dotadas de habilidad innata, con una preparación completa y que disponen de todo el tiempo y los medios necesarios para concentrarse en su labor de investigación. Lo único que puede dificultar la acción de estos peritos es el empleo de claves muy complicadas; pero la complicación es fatal, porque puede producir errores que conviertan el mensaje en algo ininteligible, aún para el que posea la clave.

Hoy en día, sin embargo, no se acepta un divorcio entre ambas especialidades. No se concibe un criptógrafo sin que necesariamente deba poseer los conocimientos aunque sean básicos de criptoanálisis, para que al confeccionar las claves pueda él mismo ponderar el grado de confiabilidad y seguridad que ella ofrecerá.

A la luz de esta acotación entra en escena lo que podríamos llamar la quintaesencia de la problemática criptográfica: "Las características propias de los idiomas".

Las particularidades de cada lengua constituyen el principal recurso para la acción de criptoanalizar; en cambio, para el que confecciona las claves se transforman en el peor enemigo.

En cada idioma encontramos una determinada frecuencia de empleo de las letras y que ellas siguen a su vez un determinado orden para formar las palabras que componen la expresión de un pensamiento. Encontraremos además en cada pensamiento la infaltable presencia del verbo, de palabras cortas de ligazón como los artículos y preposiciones, y por último, entre otros innumerables aspectos, encontraremos que dentro de cada idioma existen palabras más usadas que otras, como son las de cortesía.

El criptoanalista se fija precisamente en este tipo de cosas para lograr su objetivo, mientras que el criptógrafo trata a toda costa de que su clave haga desaparecer estas características. Para ello se vale de dos grandes sistemas: las transposiciones y las substituciones.

La transposición consiste en desordenar los elementos de un texto sin cambiarlos por otros, mientras que la substitución consiste en reemplazar los elementos del texto por otros diferentes. En términos generales se puede decir que las substituciones ofrecen un mayor margen de seguridad que las transposiciones y por esta razón siempre han monopolizado la atención de los estudiosos de la criptografía, a través de la historia.

Tal vez se piense que debido al alto grado de desarrollo que la tecnología ha alcanzado en nuestra era, un análisis histórico de la criptografía sería un esfuerzo inoficioso; pero es increíble la importancia que reviste un análisis de tal naturaleza si consideramos que muchos de los principios criptográficos estipulados, digamos hace 400 años, constituyen la piedra angular de los sistemas modernos de escritura secreta.

Los griegos al parecer fueron los primeros cultores de uno de estos dos grandes sistemas criptográficos: las transposiciones. Efectivamente, los monarcas griegos enviaban instrucciones a sus generales haciendo uso de una escítala. La escítala no era más que un cilindro de madera sobre el cual se enrollaba una tira de pergamino y luego sobre ella, si-

guiendo la generatriz, se escribía el mensaje. Una vez escrito, se enviaba el pergamino al corresponsal de destino, el que volvía a enrollar la tira en una escítala de exactamente las mismas medidas, con lo cual podía leer el texto.

El otro gran sistema criptográfico, el de las substituciones, fue copiosamente aplicado por los romanos y según Suetonio y Aylio Gelio fue Julio César su inventor y de allí que a la forma más elemental de substituir se le conoce hoy en día con el nombre de "Sistema de Julio César". Este consistía en usar un alfabeto ordenado (que comenzara con la "A") para ubicar las letras del texto claro que se querían substituir y un alfabeto también ordenado, pero desplazado con respecto al anterior, de donde se obtendrían las letras que reemplazarían a las originales. A pesar de la simplicidad e inseguridad de este sistema (puesto que las letras del texto claro eran reemplazadas por otras pero siempre por las mismas), él se mantuvo en vigencia por mucho tiempo con algunas variaciones que sólo obedecían a distintos desplazamientos del alfabeto cifrador.

Tanto las transposiciones como las substituciones no tuvieron ningún progreso notable sino hasta promediar la Edad Media. Tanto la curia romana como algunas de las pequeñas repúblicas italianas, en especial Venecia, comenzaron a utilizar intensivamente estos sistemas dando lugar a que hombres notables de la época se interesaran por la criptografía e introdujeran en ella progresos por cierto categóricos. León Alberti, el florentino que por lo universal de sus conocimientos fuera destacado por los escritores contemporáneos como el mejor representante del espíritu del siglo XV, aparece precisamente también como el más destacado en el campo de la criptografía. Un manuscrito suyo de sólo 26 páginas constituye el tratado más antiguo de criptoanálisis occidental. En el tratado, Alberti presenta un estudio bastante completo de las características del Latín, y luego, basándose en ellas, expone algunos métodos para solucionar las substituciones monoalfabéticas que se habían estado empleando hasta ese entonces. Estas mismas investigaciones son la causa de que Alberti se dedicara a buscar un sistema que, en reemplazo de las substituciones monoalfabéticas, sirviera efectivamente para ocultar las particularidades del Latín, llegando por este camino a proponer el primer paso hacia las substituciones "polialfabéticas". Diseña entonces un par de discos concéntricos, uno fijo con un alfabeto normalmente ordenado y otro móvil con un alfabeto desordenado. Ambos corresponsales por supuesto que debían tener discos idénticos. Se acordaba una letra del disco móvil como índice y ella se fijaba sobre una letra del disco fijo. Estando en dicha posición los discos, se seguía el mismo procedimiento de una substitución monoalfabética, reemplazando las letras del texto claro, ubicadas en el disco fijo, por las que había en el disco móvil. Hasta aquí en nada se había mejorado las claves usadas hasta la fecha. Pero Alberti, al seguir explicando su método, hacía variar la concordancia del índice a otro lugar del disco fijo cada vez que se hubieran cifrado 4 ó 5 letras por ejemplo, de manera que desde ese momento las letras del disco fijo tomaban otro significado con respecto a las letras del disco móvil. Con esto, cada cambio de la posición relativa de los discos significaba un nuevo alfabeto cifrador. Por esta razón, Alberti pasó a la historia como el "Padre de la criptología occidental", reconociéndole con el término "Criptología" sus méritos como criptógrafo y criptoanalista.

En los albores del siglo XVI, uno de los más célebres intelectuales del Renacimiento comienza a distinguirse en criptografía. Se trata del alemán Johannes de Trittenheim, más conocido en la posteridad como el "Abate Tritemio". En su inagotable sed de dejar escritos sus conocimientos, Tritemio, estando en el monasterio de Spanheim, dio término a un tratado voluminoso al que da el título de "Esteganografía", en que desgraciadamente, queriendo dar explicación a una serie de fenómenos esotéricos, se sumerge en el mundo de los espíritus, Kábalas y algo que en nuestros días vendría a ser algo como telepatía, conceptos que para él no significaban una contraposición de sus principios re-

ligiosos. El tratado constaba de seis tomos, los dos primeros de los cuales, muy breves, hablaban de la escritura oculta o criptografía.

La mentalidad de su época sindicó a Tritemio como "brujo" y fue obligado a abjurar de dichos temas. En 1508 estando en el monasterio de San Jacobo insiste en su obra, pero ahora, tocando sólo el tema de las cifras, escribe un tratado muy completo, compuesto de seis tomos nuevamente, al que da el nombre de "Tratado de Poligrafía". La mayor parte de su voluminoso contenido establece diferentes códigos (que es una forma de substitución monoalfabética), en los que se destaca su famoso "Ave María", un libro con 384 columnas de palabras latinas de corte religioso, dos columnas por página, y en que cada palabra representa a una letra que está frente a ella. Pero el mayor valor de la obra de Tritemio que estamos comentando reside en su contribución para mejorar los sistemas polialfabéticos y ello se encuentra en el tomo sexto, donde expone y luego discute un sistema que en líneas generales podemos presentarlo de la siguiente manera: Un cuadrado de 26 líneas de 26 letras cada una. La primera línea es un alfabeto normalmente ordenado y que empieza con la letra "A". La segunda línea es otro alfabeto ordenado pero que empieza con la letra "B" y así sucesivamente los 26 alfabetos, cada uno desplazado una letra con respecto al otro anterior, hasta llegar a la línea 26 con un alfabeto encabezado con la letra "Z". A este cuadrado Tritemio le llamó "Tabla recta". El primer alfabeto (el de la letra "A") se podía usar para indicar bien las letras del claro y también como alfabeto cifrador.

Tritemio usó la tabla de la manera más simple posible. La primera letra del texto claro era cifrada en el primer alfabeto cifrador, la segunda letra en el segundo alfabeto y así sucesivamente, de manera que después de 26 letras volvían a usarse los mismos alfabetos. A pesar que esto constituía una ventaja sobre el sistema de Alberti, aún dejaba abiertas las puertas para la labor de los criptoanalistas, Sin embargo, el método de Tritemio fue la primera tentativa que se conoce para la formación de claves progresivas en el cifrado letra a letra, y por esta sola razón muchos autores han coincidido en llamarle el "Padre de la Criptografía".

Con una extraordinaria capacidad de síntesis y habilidad para instruir, un cientista y literato italiano, Giovanni Battista Porta, en el año 1563, tuvo el mérito de resumir todos los intentos aislados y desordenados que sus antecesores habían empeñado al tratar el campo de la criptografía. Porta fue la primera persona que presentó una perspectiva clara sobre la materia, en un tratado de sólo cuatro tomos. En ellos hace un estudio de las claves antiguas, de las contemporáneas, del criptoanálisis y en el último libro detalla una lista de características lingüísticas como una poderosa ayuda para la solución de los diferentes tipos de claves. De esta manera, su obra abarca una visión de conjunto de los conocimientos criptográficos de la época. Es interesante resaltar que Porta en su obra aborda con éxito temas tan interesantes como la solución integral de las substituciones monoalfabéticas y la solución de éstas incluso cuando el criptograma no presentaba separaciones entre las palabras, lo que indudablemente presentaba más problemas al criptoanalista. Asimismo, diseña los primeros sistemas de substitución múltiple en base a Tablas de conversión. Una de ellas empleaba las mismas letras del alfabeto para reemplazar las del texto claro, consiguiendo una representación en el criptograma de dos letras por cada letra del texto claro. En otro tipo de tabla presentaba dos letras del texto por un solo signo especial convenido, con lo que lograba el doble objetivo de acortar el texto y complicar la labor del criptoanálisis.

En el campo de las substituciones polialfabéticas, Porta expone métodos muy eficientes para descriptar los mensajes cifrados con los sistemas de Alberti y de Tritemio y esto le permite proponer un procedimiento más seguro para formar la serie progresiva de alfabetos cifradores, en base a la elección de palabras o frases convenidas entre los corresponsales. En su obra escribió: "Mientras mayor sea el largo de estas

palabras o frases y mientras más desusadas ellas sean, mayor será la categoría polialfabética que revista la clave y mayores problemas dará al criptoanalista". Esta sentencia lleva implícito el principio de "aperiodicidad", término fundamental en la concepción moderna de la criptografía, y de allí precisamente la importancia de la obra de Giovanni Battista Porta.

Es increíble que a pesar de haber sido tan valederos los postulados de Alberti, Tritemio y Porta, y a pesar de haber estado ellos tan cerca del establecimiento definitivo de una clave de tipo aperiódico, esto no ocurrió sino hasta el advenimiento del físico y luego diplomático francés Blas de Vigenére que decididamente colocó a Francia como la nación priora en el campo de la criptografía, prestigio que aún mantiene con orgullo. Vigenére tomó contacto con los criptólogos de la curia papal mientras servía el cargo de secretario de la Embajada de Francia en Roma y fue allí donde comenzó su interés por la criptografía. Años más tarde, después de haber leído todas las obras de sus antecesores y haber obtenido con ello un excelente respaldo de conocimientos, los suma a su interés y habilidad personal para comenzar a escribir sus monumentales obras. No es de extrañar el término "monumental", puesto que Vigenére incluso se sale de los moldes clásicos para profundizar en otros aspectos muy interesantes relacionados con el tema. Al anotar en uno de sus libros "Todas las cosas en el mundo constituyen una cifra y la naturaleza no es más que una clave, una escritura oculta", liga la criptografía, entre otras cosas, al estudio del verdadero contenido de las obras cuyos autores emplean un lenguaje simbólico; por ejemplo, la interpretación de las Sagradas Escrituras.

Vigenére tiene también a su haber el hecho de presentar la primera representación de los ideogramas japoneses; pero, donde brilla con mayor claridad su genio criptográfico es en su aporte a la idealización de un sistema aperiódico de substitución polialfabética. A este respecto, diseña una tabla parecida a la de Tritemio, pero con las letras que actualmente tiene el alfabeto latino y en base a ella propone cifrar los mensajes utilizando como alfabetos cifradores las mismas letras del texto claro, con una o dos letras claves iniciales, con lo que la repetición secuencial de dichos alfabetos no se produciría jamás. Paralelamente, como alternativa, propone que los alfabetos cifradores sean las mismas letras cifradas que se vayan obteniendo después de la operación de cifrar la primera o las dos primeras letras en los dos alfabetos claves iniciales o de partida. El sistema de Vigenére se convirtió en la clave indescifrable por excelencia, lo que le valió el honroso apelativo de "arquetipo de las substituciones polialfabéticas" que le dieron sus contemporáneos... Se dice que el sistema Vigenére permaneció indescifrable durante tres siglos. Aquí empero hay algo que discutir. Primero: el hecho de que un criptoanalista rompa una clave no es para que lo publique a los cuatro vientos puesto que él sabe que una clave es fácil de reemplazar por otra, no así los códigos que obligan a un enorme trabajo de recopilación y clasificación cada vez que se deban cambiar. Por lo tanto, era de esperar que si algún criptoanalista de la época resolvió la clave de Vigenére, mantuvo en buen secreto su éxito con el objeto de seguir usufructuando de ella. Seguidamente, quedaría establecer el hecho de que los secretarios de cifra de la época, o bien desconocían la verdadera seguridad que ofrecía este tipo de clave, o bien eran reacios a su empleo debido a lo complicado de su operación, lo cierto es que preferencialmente usaron los códigos, los que son de operación más fácil y rápidos que las claves. Más aún, actualmente ningún criptoanalista claudicaría con una clave como la de Vigenére. Sin embargo debemos reconocerle. una vez más a este diplomático francés el mérito indiscutible de "orientar decididamente la criptografía moderna".

Durante los siglos XVI y XVII es cuando se aplican con mayor intensidad los métodos de Porta y Vigenére. En esa misma época aparecen criptógrafos y criptoanalistas de menor envergadura que no aportan a la criptografía sino pequeñas variaciones a los métodos fundamentales ya establecidos por sus antece-

sores. Entre ellos es posible destacar a Viéte, que logró descriptar diversos mensajes que se cursaban entre la Liga y el rey de España. La República de Venecia tenía organizado un servicio de claves colocado bajo las órdenes directas del Consejo de los Diez, donde alguno de sus secretarios de cifras eran muy hábiles, figurando entre ellos Pietro Partemio, al que se encargó de renovar todas las claves de las embajadas de la república cuando, a causa de una indiscreción de Viéte, se supo que eran descifrados los mensajes que enviaba Venecia. Las claves que confeccionó, a pesar de que fueron una modificación de las de Porta, alcanzaron una alta calidad debido en gran parte a que Partemio tenía también grandes dotes como criptoanalista. De más está decir que el Consejo de los Diez, al ejercer el control total de la marcha política, económica y administrativa del país, asignaba a su servicio de claves una importancia extraordinaria.

Otro de los célebres en esta materia en el siglo XVII fue Bacon, creador también de una variante de los métodos de Porta, consistente en un sistema de dos alfabetos de tipografía ligeramente diferente, imperceptible para quienes no estuvieran en antecedentes del asunto. El método de Bacon, sin embargo, siendo todo lo seguro que pueda sugerir el hecho de que algunos de sus manuscritos aún no han podido ser descriptados, no tendría aplicación práctica en nuestros días por ser demasiado lento, complicado e inadaptado para las transmisiones de radiotelegrafía.

Indiscutiblemente que en esta época que estamos analizando, el lugar prominente lo ocupa el francés Rossignol, quien sirviera durante 56 años a su país en las técnicas de descriptación, siendo en el período de Richelieu cuando su labor fue más intensa. Uno de sus mayores triunfos en esta materia fue aquel en que estando sitiada la plaza de Réalmont en poder de los Hugonotes y cuando a causa de la tenaz resistencia Enrique II Príncipe de Condé estaba dispuesto a levantar el sitio, se logró interceptar un mensaje que fue descriptado por Rossignol. En este mensaje los sitiados daban cuenta de su escasez de municiones y víveres y de que si no los recibían pronto tendrían que rendirse. Bastó que la traducción fuese enviada a los sitiados, para que estos renunciaran a continuar la resistencia. A partir de ese momento Richelieu, que tomó conocimiento de lo sucedido, tuvo a Rossignol a su lado confirmando su gran habilidad para descriptar. Rossignol creó un verdadero servicio de claves y criptoanálisis que funcionó con gran eficiencia.

Durante el siglo XVIII la criptografía languidece considerablemente y es utilizada sólo en muy poca correspondencia particular y oficial. Se hacen algunos intentos infructuosos por mejorar los métodos de cifrado conocidos y las más de las veces estos esfuerzos tienen un resultado desastroso. Durante la Convención, por ejemplo, los emigrados hicieron uso de un sistema de substitución monoalfabética al estilo Julio César con la variante de aplicar algunos bigramas previamente establecidos para los nombres propios, pero que no ofrecían ninguna dificultad para ser descriptados.

Durante el siglo XIX tampoco salió la criptografía de su letargo. Tanto las claves militares y diplomáticas de la época napoleónica, las de las sociedades secretas y aún las usadas en la guerra de 1870 eran sumamente débiles sin contar con que abundaron los mensajes sin cifras o en claro, total o parcialmente, con las consecuencias consiguientes. En todo caso merece destacarse en este siglo al mayor Kasiski del Ejército alemán que expuso un método completísimo, paso a paso, para descriptar los sistemas de substitución polialfabéticas con empleo de palabras claves convenidas (sistema Porta). Introduce asimismo por primera vez el análisis matemático para estas soluciones. Gracias a Kasiski y también a que algunos literatos como Edgar A. Poe y Balzac logran interesar al público en sus principios y problemas, la criptografía vuelve a tomar gran auge y a partir de 1880 comienza a ser enseñada en todas las Academias Militares e incluso en algunas Academias Diplomáticas. Es así como vemos distinguirse en Alemania a Bartels y al Coronel Wostrowitz, en Inglaterra al Almirante Beaufort y en Francia a Valerio y Kerckchoft, todos los cuales nos legaron sus investigaciones, conocimientos y ex-

periencias en tratados que revisten el más alto interés.

Antes de dar término a la exposición del desarrollo criptográfico ocurrido hasta el siglo XIX, es conveniente relatar uno de los acontecimientos más sensacionales que conmovieron a la opinión pública francesa y mundial a fines del año 1894. Me refiero al proceso instruido en contra del Capitán Dreyfus del Ejército francés, acusado de alta traición, proceso que merece figurar como un caso maestro de espionaje, intriga y labor criptoanalítica y que nos demostrará también hasta dónde las autoridades de ese tiempo, teniendo ya claves de excelente calidad, las despreciaron, eligiendo códigos y otros procedimientos débiles para proteger sus informaciones.

El Servicio de Inteligencia del Ejército francés había interceptado un memorándum sin firma en que se ofrecía información militar secreta a Alemania. Este tipo de informaciones eran conocidas solamente en el seno del Estado Mayor General. Las sospechas recayeron sobre la persona del Capitán Alfred Dreyfus, un oficial de origen judío que tenía acceso directo a estos secretos y que diariamente se quedaba trabajando hasta altas horas de la noche. El día 15 de octubre, repentinamente se le llamó a presentarse ante un comité de altos Jefes del Estado Mayor y se le hizo tomar nota de un dictado que tenía por objeto confrontar su caligrafía con la del memorándum ya señalado. Cuando Dreyfus, ignorante de las sospechas, terminó el dictado, recibió atónito la siguiente sentencia: "Usted está arrestado a partir de este momento y se le acusa de alta traición a la patria". Las caligrafías, por simple coincidencia, habían mostrado alguna similitud y a falta de expertos calígrafos en esa época, bastó al Estado Mayor para que esto constituyera una prueba de culpabilidad y se iniciara el sumario correspondiente.

Al principio el arresto se mantuvo en gran secreto, pero algunos días después debido a una infidencia, un periódico antisemita lanzó la primera noticia con grandes titulares en primera página: ¡Alta traición! ¡Arresto del oficial de origen judío Alfred Dreyfus! . . . ¡Dreyfus estaría siendo pagado por Alemania o Italia! Ese mismo día el Agregado Militar italiano en París, Coronel Alejandro Panizzardi, viendo que su país estaba siendo involucrado en este hecho, escribió a sus superiores en Roma una carta urgente en que comunicaba que ni él ni su colega alemán tenía conocimiento alguno sobre el prisionero ni relación con los hechos, pero que tal vez este oficial francés pudiera estar trabajando directamente con el Estado Mayor en Roma, de lo cual no tenía informaciones.

Como en los días siguientes toda la prensa de París se hizo eco de este acontecimiento, dándole caracteres de escándalo y creando un clima contrario a las relaciones de Francia con sus vecinos, "las que ya estaban bastante deterioradas", Panizzardi se vio obligado a telegrafiar a Roma una reiteración de su carta anterior, en el sentido de que si el Capitán Dreyfus no hubiese tenido contacto directo con Roma debiera publicarse un desmentido oficial a fin de evitar los comentarios adversos de la prensa.

El telegrama, cifrado, salió el día 2 de noviembre y como de costumbre la oficina de censura del Ministerio de Correos y Telégrafos francés envió una copia de él a la oficina de claves del Ministerio de Relaciones Exteriores. Su texto cifrado era el siguiente:

Comando Stato Maggiore Roma

913 44 7836 527 3 88 706
6458 71 18 0288 5715 3716
7567 7943 2107 0018 7606 4891
6165 Panizzardi

Los criptoanalistas del Ministerio de Asuntos Exteriores relacionaron inmediatamente la estructura de los grupos de código del mensaje (agrupaciones de 1, 2, 3 ó 4 dígitos) con la misma que presentaba un código comercial italiano publicado hacía poco tiempo en Turín, Italia, llamado "Diccionario para correspondencia en clave", de Baravelli.

Este código había llegado a poder de los criptoanalistas hacía 4 meses, en junio, cuando el Jefe del Servicio de Inteligencia del Ejército, Coronel Sandherr, llegó con él hasta la oficina de claves del Ministerio. Cómo obtuvo Sandherr este libro, no tiene importan-

cia. Lo que sí interesa es ver cómo estaba constituido el código para establecer sus relaciones con el telegrama de Panizzardi.

El código de Baravelli constaba de cuatro secciones: La tabla I, en la que las cinco vocales y cinco signos de puntuación aparecían representados por los dígitos del 0 al 9; esta tabla no tenía numeración de páginas y los diez dígitos estaban precedidos de una línea de puntos con la intención de permitir al usuario sobrecifrarlos cuando estimara conveniente. La Tabla II estaba dividida en diez grupos de diez elementos cada uno consistentes en consonantes, verbos irregulares y formas gramaticales. Cada grupo estaba representado por un dígito (de 0 a 9) y cada elemento dentro de cada grupo por otro dígito (de 0 a 9); por lo tanto, cada consonante o forma gramatical era representada por un conjunto de dos dígitos; el primero, indicador de grupo, se podía sobrecifar, pero el segundo, indicador del elemento dentro del grupo, siempre permanecía fijo. La Tabla III consistía de diez páginas numeradas de 0 a 9 dentro de las cuales estaban vertidas todas las sílabas más usuales, identificadas cada una por un conjunto de dos dígitos, los que sumados al número indicador de la página formaba una representación de tres dígitos para cada sílaba a usar; el número de la página podía sobrecifrarse debiendo permanecer fija la numeración correlativa de cada sílaba dentro de la página. La Tabla IV constaba de cien páginas numeradas de 00 a 99 conteniendo cada una cien palabras numeradas también de 00 a 99, con lo que se formaba un conjunto de cuatro dígitos para identificar cada palabra. Los números de las páginas se podían sobrecifrar, pero los números correlativos de cada palabra debían permanecer fijos. Una vez asegurada la relación estructural existente entre el código Baravelli y el telegrama de Panizzardi, los criptoanalistas trataron de obtener el texto claro directamente sin suponer sobrecifrado de las partes permitidas. Este primer intento les entregó un texto totalmente incoherente con lo cual llegaron a la conclusión de que Panizzardi había hecho uso del sobrecifrado, por lo que se dieron a la tarea de descriptar el mensaje, tarea ardua desde que era la primera vez que Panizzardi ocupaba este código. Sin embargo los criptoanalistas pensaron, y con sobrada razón, que el mensaje debía contener los términos "arresto", "Capitán" y el apellido "Dreyfus" y más aún, examinando el código llegaron a concluir que había un solo camino para deletrear este apellido en la forma más breve y esto mediante la sílaba "DR", la vocal "E", la consonante "Y" y la sílaba "FUS", las que sacadas directamente del código formarían las representaciones numéricas "227" (tabla III página 2 línea 27, para "DR"), "98" (Tabla II, grupo 9 línea 8, para la "Y"), "1" (Tabla I, línea 1, para la "E") y "306" (Tabla III, página 3 línea 06 para "FUS), lo que daba en conjunto: 227 1 98 306.

Ahora bien; el telegrama Panizzardi incluía en una de sus partes una secuencia igual de grupos de códigos de tres, uno, dos y tres dígitos: 527 3 88 706. Más aún, los números que en esta secuencia presumiblemente representaban las líneas —27, 8 y 06 (omitiendo el dígito de la tabla I)— eran idénticos con aquellos que formaban el apellido Dreyfus. Obviamente, entonces la secuencia 527 3 88 706 representaba la codificación que Panizzardi había dado para el apellido Dreyfus. De aquí que pudieron deducir que los dígitos representativos de líneas se mantenían fijos, sin substituir, tal como lo sugería el diseño del código. Con esto como base, los criptoanalistas, después de hacer varias combinaciones de texto utilizando las partes fijas de los grupos de código del telegrama, lograron una primera aproximación del texto completo descriptado que consideraron una posibilidad exacta a excepción de las cuatro últimas palabras, las que dejaron subrayadas y con signos de interrogación, en señal de dudosas, puesto que su traducción literal no daba un significado muy cuerdo: "Se capitano Dreyfus non ha avuto relacione costá sarebbe conveniente incaricare ambasciatore smentire **uffiziale? rimane? prevenuto? emisario?**". Lo anterior, traducido al castellano podría ser: "Si el capitán Dreyfus no ha

tenido relación con uds. sería conveniente encargar al embajador desmentir **oficial? queda? prevenido? espía?".**

Una copia de esta traducción, tal cual, fue presentada al Jefe del Servicio de Inteligencia Coronel Sandherr con las salvedades del caso, quien, haciendo caso omiso de las conjeturas, las entregó al Jefe del Estado Mayor diciéndole: "He aquí otra prueba de la culpabilidad de Dreyfus". Pero en el intertanto, los criptoanalistas del Ministerio de Relaciones habían insistido en ubicar la codificación exacta de todo el mensaje incluyendo las cuatro últimas palabras que confusamente inculpaban a Dreyfus, hasta que después de dos días lograron reconstituir completamente el "sistema" seguido por Panizzardi para cifrar las partes no fijas de los grupos de código y establecieron el texto real definitivo (Se muestra el texto completo con los grupos de código cifrados en primera plana y luego sin cifrar en segunda):

De esta manera el grupo de código (sin cifrar) para "Capitano" 1336 se convirtió en 7836 y el grupo 3306 de "evitare" se convirtió en 7606. El segundo de los alfabetos numéricos citados servía asimismo para cifrar el número de página, grupo y línea de las tablas III, II, y I, respectivamente.

La nueva versión del telegrama de Panizzardi que se había descriptado y que de ninguna manera relacionaba a Dreyfus con el escándalo que hemos mencionado, fue entregada nuevamente al Coronel Sandherr; pero éste, que estaba obsesionado con la idea de que Dreyfus era un traidor, no quedó muy complacido con dicha versión y la presentó a sus jefes con el siguiente comentario: "Tratándose de asuntos extranjeros, no se puede estar siempre seguro de estas cosas. Ellas carecen de precisión". Sin embargo, se concibió una hábil maniobra para despejar las dudas. Ellos inducirían a Panizzardi días más tarde a

913	44	7836	527	3	88	706	6458	71	18
913	44	7836	227	1	98	306	5858	31	08
Nº de serie	Se	Capitano	DR	E	Y	FUS	non	ha	avuto

0288	5715	3716	7567	7943
7588	2215	2116	4367	0343
relacione	costá	sarebbe-conveniente	incaricare	ambasciatore

2107	0018	7606	4891	6165
8607	9518	3306	1791	8865
smentire	ufficialmente	evitare	comenti	stampa

Traducido al castellano, el mensaje decía:

"Si el capitán Dreyfus no ha tenido relación con Uds. sería conveniente encargar al Embajador desmentir oficialmente para evitar comentarios prensa".

Panizzardi en consecuencia había usado dos alfabetos numéricos para substituir y al mismo tiempo transponer los números de páginas del código:

1er. dígito del Nro. página, sin cifrar	0	1	2	3	4	5	6	7	8	9
2do. dígito del Nro. página, cifrado	9	8	7	6	5	4	3	2	1	0
2do. dígito del Nro. página, sin cifrar	0	1	2	3	4	5	6	7	8	9
1er. dígito del Nro. página, cifrado	1	3	5	7	9	0	2	4	6	8

enviar un telegrama codificado a Roma cuyo contenido les fuera conocido. Esta solución serviría para confirmar o refutar el criptoanálisis del mensaje que hablaba sobre Dreyfus. Simularon entonces un mensaje con palabras escogidas desde las páginas del código Baravelli cuya numeración aún ofrecía dudas (especialmente para la parte final del mensaje) y cuyo texto revistiera real importan-

cia de manera que Panizzardi no pudiera ignorarlo y de carácter tan urgente que tuviera que enviarlo por telegrama. El mensaje artificialmente confeccionado decía más o menos lo siguiente: "Un espía francés, señor x, que está actualmente en xx, saldrá próximamente hacia París llevando documentos relativos al Plan de Movilización del Ejército italiano, documentos conseguidos en las oficinas del Estado Mayor en Roma. Esta persona se domicilia en la calle xxx". El mensaje fue inteligentemente presentado a Panizzardi en la forma de un aviso, verbal, a través de uno de sus espías, que sin su conocimiento trabajaba como "doble" para el servicio francés de contraespionaje. Panizzardi cayó en la trampa y envió el mensaje a Roma casi textualmente, el día 13 de noviembre. La copia que recibió el Ministerio de Relaciones (que no tenía conocimiento de esta jugada) fue descriptada íntegramente y enviada al Estado Mayor del Ejército por cuanto revestía interés militar. De acuerdo con este segundo mensaje, cuyo contenido era exactamente igual al texto preparado por los oficiales del servicio de Inteligencia, se confirmó la validez del criptoanálisis al primer mensaje y se despejaron todas las dudas acerca de la inocencia de Dreyfus. Sin embargo el ejército se vio obligado a mantener la alteración del verdadero significado del primer telegrama de Panizzardi, el que había pasado a los archivos del sumario con el siguiente contexto oficial: Estado Mayor Roma "Capitán Dreyfus arrestado; el Ministerio de Defensa tiene pruebas de sus relaciones con Alemania. Las informaciones entregadas son altamente secretas. Nuestro agente está prevenido". Panizzardi.

La razón de esta obcecada actitud del Ejército no tenía por objeto injuriar y condenar en forma injusta a un distinguido oficial, sino más bien era debido al temor de que se divulgaran dos hechos importantes: Primero, que el código usado por el Agregado Militar italiano era conocido por los franceses y segundo, que había espías pertenecientes al contraespionaje francés en las Embajadas de Alemania e Italia. Se necesitaron varios años para que el Parlamento y la opinión pública francesa lograran romper la obstinada resistencia del Estado Mayor y tomaran conocimiento del verdadero contenido del telegrama Panizzardi y del desarrollo de los hechos. El análisis moral de este acontecimiento histórico no es materia que concierna al campo de la criptografía.