Revista Complutense de Historia de América ISSN: 1132-8312
2000, 26: 57-71

Sistemas criptográficos empleados en Hispanoamérica

Juan Carlos GALENDE DÍAZ
Departamento de Ciencias y Técnicas Historiográficas
Facultad de Geografía e Historia de la Universidad Complutense

RESUMEN

Tras una breve introducción, en la que se explican los fundamentos de los sistemas utilizados en la composición de criptogramas, el autor se centra en la evolución histórica de la criptografía en Hispanoamérica, analizando los principales métodos que emplearon diversos personajes, tan conocidos como Hernán Cortés, Pedro de La Gasca, Antonio José de Sucre, Simón Bolivar, etc., para cifrar sus comunicaciones, tanto en la Edad Moderna como en la Contemporánea, ya que, si bien la génesis de la criptografía indiana se encuentra en tierras hispanas, la época de mayor esplendor se sitúa durante la Emancipación.

Palabras claves: criptografía, documentación, edad moderna, edad contemporánea, escritura, historia, historia de América, paleografía.

ABSTRACT

Following a brief introduction, where the fundamentals of the various cryptogram composition methods are explained, the author elaborates on the historical evolution of cryptography in Latin America, analysing the chief methods used by several famous personages as Hernán Cortés, Pedro de la Gasca, José de Sucre, Simón Bolivar, etc., from Modern and Contemporary Ages, given that despite the fact. That the genesis of Spanish-American cryptography occurs on Spanish soil its most splendorous period takes place during Emancipation.

Key words: cryptography, documentation, modern age, contemporary age, write, history, americans history, paleography.

Atendiendo al étimo del término «criptografía» («kryptos» y «graphein»), se entiende por tal la ciencia que estudia la escritura oculta. Más precisa, sin embargo, es la siguiente definición: el arte de escribir en un lenguaje convenido mediante el empleo de claves o cifras[1]; cifras que, como bien expone Alain Buquet, son las piezas maestras de todas las escrituras secretas[2]. La operación inversa se denomina «criptoanalizar»: interpretar mediante análisis los cifrarios construidos por los criptógrafos.

Por su parte, la labor de transformar un texto cifrado o criptograma en el mensaje original, si se conoce la clave, se llama «descifrar» o «decodificar»[3], pero si ésta es ignorada es más adecuado denominarla «perlustrar» o «descriptar».

En atención a lo expuesto, se puede deducir que para criptoanalizar un documento codificado, hay que saber la clave del significado de los signos, es decir, el sistema o el código seguido. La formación de una clave no es complicada, ya que no se sujeta a reglas fijas y sólo depende de la pericia en la combinación de los signos; lo difícil es, como apunta Mariano Alcocer, el descifrado del criptograma cuando falta la clave[4]. A su vez, la criptografía puede dividirse en «estratégica» y «práctica»; la primera consiste en garantizar el secreto de los mensajes cifrados por un largo período de tiempo, mientras que la segunda se conforma con el tiempo imprescindible para llevar a buen término una acción establecida[5]. Pero en un caso o en otro, bien se trate de descifrar y más aún de perlustrar, la tarea es penosa y enrevesada. No sólo requiere determinar el sistema empleado, saber la lengua y buscar la frecuencia en la aparición de las letras, sino también reconocer los signos repetidos, cuñas, ele-

---

[1] El profesor brasileño Ricardo Román Blanco ofrece el siguiente concepto: *«A criptografia consiste em comunicar por meio de letras, signos ou números, as informaçoes conseguidas pela espionagem, dispostas de tal maneira que, mesmo que o inimigo consiga interceptá-las, nao consiga descobrir seu significado»*. ROMAN, Ricardo: *Estudos paleográficos*. Sao Paulo, Lasermint, 1987, p. 110.

[2] BUQUET, Alain: *L'expertise des ecritures*. París, Presses du CNRS, 1991, p. 69.

[3] Incluso algunos autores matizan estas expresiones, proponiendo que se emplee el término «descifrar» cuando se lleve a efecto la labor de resolver un mensaje en cifra, es decir, sustitución al nivel de letras, y «decodificar» cuando se verifique la operación de transformar en claro un criptograma codificado, es decir, al nivel de las palabras o las frases. SINGH, Simon: *Los códigos secretos*. Madrid, Debate, 2000, pp. 41-42.

[4] ALCOCER, Mariano: «Criptografía española». *Revista de Archivos, Bibliotecas y Museos*, 42, 1921, pp. 629-631.

[5] SGARRO, Andrea: *Códigos secretos*. Madrid, Pirámide, 1990, p. 73.

mentos inertes, etc., toda una serie de trabas que dificultan la labor descriptadora.

Entendida en sentido amplio, la criptografía se utiliza desde la más remota antigüedad. Chinos, indios[6], persas, babilonios y egipcios, entre otros pueblos, poseían ya signos convencionales, que eran equivalentes a las grafías de sus alfabetos, con los que transmitían órdenes a sus emisarios, en especial durante períodos bélicos[7]. Desde tiempos pretéritos se utilizaron ya ciertas señales que consistían en luminarias sobre determinadas alturas, agrupadas o esparcidas de un modo convenido, para avisar bien de la presencia del enemigo bien de cualquier otro acontecimiento previsto de antemano. Después se utilizaron antorchas encendidas o estandartes desde torres construidas al efecto, con los que se comunicaban haciéndolos aparecer y desaparecer[8].

A lo largo de la historia se han empleado distintos sistemas de cifrado, siendo los tres principales: el de *transposición*, el de *sustitución* y el de *ocultación.*

El primero de ellos consiste en colocar un fragmento cifrado en un lugar previamente conocido por el destinatario. Comprende todos los métodos que modifican el orden natural bien de las letras, de las sílabas o de las palabras en un texto, trastrocándolas o formando anagramas con ellas. Entre otros métodos de transposición, se pueden citar: «escítalo», «alteración», «Richelieu», «telégrafo», «enrejado», «tabla», «Soudart», etc. Por lo general, se emplea cuando los textos a cifrar no son muy extensos.

---

[6] Una de las descripciones más antiguas de codificación por sustitución aparece en el *Kamasutra*, obra compuesta en el siglo IV por el erudito brahmín Vatsyayana, pero que se basa en textos escritos ocho centurias antes. En ella se recomienda a las mujeres estudiar 64 artes: cocinar, dar masajes, preparación de perfumes, encuadernación de libros, prestidigitación, etc.; el número 45 de esta relación es el arte de la escritura secreta, preconizado para ayudar a la féminas a ocultar detalles de sus relaciones amorosas. Una de las técnicas recomendadas es reunir al azar las letras del alfabeto y luego reemplazar cada grafía del mensaje original por su pareja. SINGH, 2000, p. 22.

[7] El prof. Luis Núñez Contreras expone que uno de los medios criptográficos más primitivos fue el que empleó el rey espartano Damarato en el siglo VI a.C., quien, según relata Herodoto en sus *Historiae,* escribía los mensajes incisos en una tablilla y luego los recubría de cera, y así informaba a los lacedemonios del proyecto de Jerjes —el «Rey de Reyes»— sobre la invasión de Grecia. NÚÑEZ CONTRERAS, Luis: *Manual de paleografía*. Madrid, Cátedra, 1994, p. 179.

[8] Se sabe, por ejemplo, que los romanos emplearon la telegrafía óptica, cuyas torres se ven todavía entre los vestigios que quedan de los denominados campos romanos. CARMONA, Juan Carlos: *Tratado de criptografía con aplicación especial al ejército*. Madrid, Sucesores de Rivadeneyra, 1894, p. 155.

El segundo sistema —sustitución o perturbación— estriba en reemplazar alguna letra del alfabeto por uno o más signos convenidos por los corresponsales. Engloba los métodos basados en sustituir los elementos del texto normal —letras, sílabas, palabras o frases— por una representación distinta a la original, que puede ser literal, numérica o esteganográfica, es decir, figurativa. Son ejemplos de métodos de sustitución: «alfabeto Morse», «masónico», «Julio César», «Guyot», «Porta», «Cechetti», «benedictino», «Tritemio», «Hirsch», «Jean», «Collange», «Beaufort», «Jefferson», «Lord Bacon», «silábico», «Ivry», «tabla numeral», «Fleissner», «Bazeries»...[9]. También pertenecen a este sistema una serie de métodos que, en ocasiones, se presentan de forma independiente, v. gr.: «impresos», «diccionarios» y «tablas cifradoras»[10], «lenguaje convenido»[11] y «máquinas cifradoras».

Finalmente, en el sistema de ocultación se incluyen aquellos procedimientos en los que el remitente transmite el contenido del mensaje de forma oculta o disfrazada. En consecuencia, este sistema abarca todas las argucias y artimañas empleadas a lo largo de la historia para conseguir que un criptograma sea leído únicamente por el destinatario, impidiendo su comprensión a quien no le ha sido enviado.

Como ya advertía en mi estudio: *Criptografía. Historia de la escritura cifrada*[12], los métodos de cifrado empleados en Hispanoamérica guardan

---

[9] Son varios los estudios centrados en analizar detenidamente tanto este sistema como el de transposición. Entre ellos, cabe destacar los siguientes: CALABUIG, Vicente: *Elementos de criptología*. Valencia, Fundación Universitaria San Pablo CEU, 1999; GIVIERGE, Marcel: *Cours de cryptographie*. París, Berger et Levrault, 1925; KAHN, David: *The codebrakers*. New York, Macmillan, 1967; LANGE, André: *Traité de Cryptographie*. París, Alcan, 1925; MILLIKIN, Donald: *Elementary cryptography*. New York, University Bookstore, 1943; MULLER, André: *Les écritures secrétes. Le chiffre*. París, Presses Universitaires de France, 1971; POPE, Maurice: *The story of decipherment*. Londres, Thames & Hudson, 1975; PRATT, Fletcher: *Histoire de la cryptographie*. París, Payot, 1940; SERRANO GARCÍA, Pedro: *Criptografía y perlustración.* Madrid, La Xilográfica, 1953; SMITH, Lawrence Dwight: *Cryptography. The science of secret writing*. New York, Dover, 1943; WOLFE, James Raymond: *Secret writing*. McGraw-Hill, 1970; y ZANOTTI, Mario: *Crittografia. La scrittura segrete*. Milán, Ulrico Hoepli, 1928.

[10] Este método de cifrado, también llamado «nomenclátor», fue usado con mucha asiduidad durante toda la Edad Moderna, especialmente por la seguridad que ofrecía en la correspondencia diplomática.

[11] Es decir, aquel a cuyo texto se da, convencionalmente, un significado distinto del verdadero o gramatical. Su empleo ha sido constante y, por su formulismo personal, suele ser complicado de interpretar.

[12] GALENDE, Juan Carlos: *Criptografía. Historia de la escritura cifrada*. Madrid, Complutense, 1995, p. 109.

un paralelismo evidente con los utilizados en la Península, y es que la génesis de la criptografía indiana, obviamente, se encuentra en tierras hispanas[13].

Desde la centuria decimosexta[14], para evitar que ciertos despachos importantes cayeran en manos enemigas, fue necesario tomar precauciones. De ahí que, en múltiples ocasiones, la documentación estuvo confeccionada mediante claves, tanto esteganográficas, como literales y numéricas, siendo éstas últimas las que terminan por imponerse. No era suficiente enviar el documento por triplicado o cuadruplicado, si no que había que codificarlo[15]. La propia Casa de la Contratación, desde mediados del siglo XVI, puso en práctica procedimientos criptográficos[16].

Es más, como afirma Guillermo Lohmann Villena[17], la complicación en la elaboración de las claves aumentaba si se trataba de ocultar información a potencias foráneas, como por ejemplo: las fechas de navegación de las flotas que porteaban riquezas ultramarinas[18], las noticias alarmantes sobre inquietudes y motines en las Indias y la existencia de problemas económicos que afectaban indispensablemente a la Monarquía. Por lo tanto, el empleo de procedimientos más o menos confidenciales en la

---

[13] A nivel general, puede consultarse la obra de MARTANS FARRO, Héctor: *Tratado de criptografía*. Lima, CIP, 1958.

[14] La etapa prehispánica es examinada, entre otros, en los siguientes trabajos: CALDERÓN, Héctor: *Clave fonética de los jeroglíficos mayas*. México, Orión, 1966; CORDÁN, Wolfang: *Introducción a los glifos mayas. La clave de los glifos mayas. La fiesta de las abejas*. México, El Manual Moderno, 1969; GARCÍA MONTERO, Eduardo: *El código de los Piratas*. Lima, Imprenta Domingo Miranda, 1951; LACOMBE, Charles y D'OBRENOVIC, Michel: «Project «xoc». Some keys to maya hieroglyphics». *Journal of Inter-American Studies*, 3, 1968, pp. 406-430; y RADICATI, Carlos: «La «seriación» como posible clave para descifrar los quipus extranumerales». *Documenta*, IV, 1965, pp. 112-215.

[15] En el sevillano Archivo de Indias se conserva una más que notable masa documental con estas características, que por la irregularidad de su origen no es posible adscribirlas a una serie documental determinada. MILLARES CARLO, Agustín: *Tratado de Paleografía Española*. Madrid, Espasa Calpe, 1983, vol. I, pp. 293-294.

[16] Es conocida, entre otras muchas, la cifra que este organismo hace llegar en 1566 al general Juan de Velasco de Barrio, basada en un sistema de sustitución simple. *Archivo General de Indias, Contratación, 5101*.

[17] LOHMANN, Guillermo: «Cifras y claves indianas. Capítulos provisionales de un estudio sobre criptografía indiana». *Anuario de Estudios Americanos*, XI, 1954, pp. 299-300.

[18] Los corsarios también emplearon diversos métodos criptográficos para comunicarse entre sí. Un ejemplo elocuente son los criptogramas que el pirata Jorge Anson dejó en la isla de Juan Fernández en 1743. *Archivo General de Indias, Chile, 98*.

transcripción de las noticias era imprescindible. Períodicamente se fueron confeccionando claves «oficiales», para de este modo evitar su interceptación e interpretación, como por ejemplo las compuestas en 1632, 1658 o 1675 entre el Consejo de Estado y los virreyes de Nueva España y Perú o la seguida en 1770, que pertenecía al grupo de las aritmológicas, no sólo con los virreyes citados, sino también con el de Nueva Granada y el gobernador de Buenos Aires.

Pero no sólo utilizaron este sistema los virreyes[19] y otras altas jerarquías de la Corona, sino que también lo usaron miembros de órdenes religiosas[20] y simples particulares[21], tanto para comunicarse entre sí desde distintos enclaves indianos como de la Península. Entre otros personajes, se sabe que emplearon métodos criptográficos: Cristóbal Colón[22], Hernán Cortés[23],

---

[19] Por lo general, todos los virreyes americanos emplearon métodos cifradores para criptografiar su correspondencia, tanto a nivel privado como oficial. Entre ellos, por ser uno de los más aficionados y experimentados, hay que destacar la figura del conde de Chinchón, Luis Jerónimo Fernández de Cabrera, quien entorno a 1630 aplica diversos códigos en su correspondencia con la Corona. Sirva de ejemplo la misiva, fechada el 9 de septiembre de 1630, referente a las incursiones enemigas en el Pacífico (Archivo General de Indias, Lima, 572, libro 20, folio 233v.). Guillermo Lohmann, en su estudio citado, ofrece un repertorio de las claves empleadas por este virrey. LOHMANN, 1954, pp. 326-339.

[20] Se tiene constancia de que desde los primeros años del establecimiento de los jesuitas en tierras peruanas hicieron uso de métodos criptográficos para comunicarse con Roma. Además de diversa documentación que así lo demuestra, se conserva su cifra, consistente en una tabla alfanumérica. LOHMANN, 1954, pp. 37-39.

[21] Resulta curiosa la clave ideada por el arbitrista José de Orozco y Gamarra en 1604, quien envió a su hijo Bartolomé Inga de Orozco desde El Callao, con destino a la metrópoli, para que portara un memorial suyo, a servicio de la Corona, en el que ofrecía medidas conducentes al mejor beneficio y explotación de las minas y tratamiento del mineral. Receloso de que esta memoria pudiera extraviarse y ser localizada, lo que conllevaría su remedo y plagio, José de Orozco la criptografió utilizando unos complicados signos esteganográficos.

[22] Véase los estudios de: BLUM, André: «Les chiffres de Colomb». *Studi Colombiani*, II, 1928, pp. 207-210; y A. TONNEAU: «L'enigme des chiffres de Christophe Colomb». *Studi Colombiani*, II, 1928, pp. 137-180. Consta que en el año 1500, el gobernador Francisco de Bobadilla remitió a los Reyes Católicos diversas misivas que habían sido escritas *«con caracteres ignotos»* por Cristóbal Colón a su hijo Diego, en las que le recomendaba como debía ser su conducta en caso de que el comisionado regio le encarcelase.

[23] Es conocida la misiva cifrada que Hernán Cortés remite desde Cuernavaca el 25 de junio de 1532 y que en la actualidad se conserva en el Museo Nacional de Arqueología, Historia y Etnografía de México. Fue publicada en la revista *Anales*, III, 1925, pp. 123-130 y 436-443. En la confección de este criptograma, considerado como uno de los más antiguos del Nuevo Mundo, Cortés emplea un nomenclátor, consistente en sustitu-

Pedro de La Gasca[24], el contador Rodrigo de Albornoz[25], Luis de Velasco[26], el almirante Flores de Valdés[27], Cristóbal de Eraso[28], el almirante Antonio de Aguayo[29], el virrey Francisco de Toledo[30], fray Fran-

---

ciones homofónicas monoalfabéticas, mediante las cuales cada letra era representada por dos o tres símbolos, tanto literales como numéricos y convencionales. Idéntico método aplica en la carta que escribe desde el Puerto de Santiago el 20 de junio del año siguiente, y cuyo original obra en los autos seguidos en 1546 por el licenciado Francisco Núñez contra el marqués del Valle, por pago de devengados (*Archivo General de Indias, Justicia, 1009, número 3*).

Aunque ya habían sido publicadas, entre otros autores por el padre Mariano CUEVAS: *Cartas y otros documentos de Hernán Cortés, novísimamente descubiertos en el Archivo General de Indias de la ciudad de Sevilla* (Sevilla, F. Díaz y Compañía, 1915), no fue hasta 1925 cuando se desveló la clave utilizada por Hernán Cortés, labor que llevó a efecto Francisco Monterde García-Icazbalceta.

[24] En el virreinato peruano, las primeras noticias relativas a la existencia de una cifra de carácter oficil datan de la época de este virrey. Se sabe que utilizaba una clave, consistente en un sistema de sustitución simple de las letras por signos convencionales, para su correspondencia privada, de la que son prueba diversas misivas que remite en 1545 al Consejo de Indias solicitando la atribución de una serie de facultades que consideraba imprescindibles para llevar a feliz puerto su misión como virrey, conservadas en la *Biblioteca de Palacio* (*manuscrito 1960, número 11*), y otra similar para su correspondencia oficial, la cual, por ejemplo, emplea en un despacho que remite el 21 de mayo de 1547, relativo a la unión matrimonial de Gonzalo Pizarro con su sobrina Francisca (*Archivo General de Indias, Lima, 566, libro 6, folio 49*).

[25] Este secretario de Carlos V, valiéndose de un código que le entregó el presidente del Consejo de Indias —Rodríguez de Fonseca— cuando partió hacia Nueva España, comunicaba desde México informes sobre los proyectos, aspiraciones y andanzas de Hernán Cortés.

[26] Se conoce, entre otra correspondencia, la misiva que el virrey de Nueva España Luis de Velasco remite desde Cholula al monarca el 18 de octubre de 1550, la cual contiene caracteres cifrados en diversos fragmentos de la misma. *Archivo General de Indias, México, 19*.

[27] Flores de Valdés utilizaba un sistema de sustitución simple, en el que cada letra era reemplazada por una representación esteganográfica. Por ejemplo, la aplicó en la epístola escrita desde Nombre de Dios el 6 de agosto de 1567. *Archivo General de Indias, Panamá, 39*.

[28] Este almirante usa también el sistema de sustitución simple. Puede verse en la carta que remite desde San Juan de Ulúa el 20 de febrero de 1568. *Archivo General de Indias, México, 168*.

[29] Empleaba el sistema de sustitución de primer grado, reemplazando las letras del abecedario por signos caprichosos. Se puede comprobar en la misiva que remite desde Nombre de Dios el 1 de agosto de 1563. *Archivo General de Indias, Indiferente General, 2004*.

[30] El llamado «Legislador de Perú» mantuvo, en la década de 1570, correspondencia cifrada con otros coetáneos suyos, como Mateo Vázquez —secretario de Felipe II— y Ovando —presidente del Consejo de Indias—.

cisco de la Cruz[31], el gobernador y capitán general de la isla de Cuba Juan de Tejada[32], etc.[33].

Durante toda esta etapa, sin duda, el sistema que triunfó en la documentación cifrada indiana, al igual que en Europa, fue el de sustitución, tanto en su modalidad de «simple» o «sencillo» —en el que cada letra del mensaje es sustituida por otra letra, cifra o signo— como de «doble», «múltiple» o de «varias claves» —en el que cada grafía del texto claro se puede reemplazar por diversas letras, cifras o signos—[34]. Hasta tal punto se empleaba la criptografía que, con el fin de mejorar el gobierno del Perú, el oidor de la audiencia limeña, Diego González Altamirano, en un memorial de 1555 recomienda imponer su prohibición argumentando que mediante este método *«se entienden los alterados y se conmueven unos a otros a levantarse y como no se entiende no se puede proveer»*[35].

Es también durante el siglo XVI, cuando aparece el primer acercamiento de un autor hispano-americano sobre esta materia. Se trata de la obra impresa en Sevilla en 1571 por Diego Fernández Palencia que se

---

[31] Este dominico fue procesado por el Santo Oficio en 1572. Durante su causa, uno de los delatores —fray Pedro de Toro—, le acusa de haber mantenido con él y con otro religioso —fray Alonso Gasco— correspondencia en clave. El propio fray Francisco de la Cruz reconoce haberse valido del lenguaje convencional para explicar sus errores dogmáticos.

[32] Se conserva, entre otra documentación cifrada del gobernador Juan de Tejada, una carta fechada en La Habana el 7 de octubre de 1591, confeccionada por el sistema de sustitución simple. *Archivo General de Indias, Santo Domingo, 99*.

[33] De estos personajes históricos, y de otros no tan conocidos —v. gr. el capitán Pedro de Roelas en 1558; el general de la flota Pedro Menéndez Márquez en 1591; el gobernador del Río de la Plata Bruno Mauricio de Zabala en 1717; y los hermanos Illán y Benito Suárez de Carbajal, quienes mantenían correspondencia cifrada con Francisco Pizarro y su hermano Gonzalo—, Guillermo LOHMANN ofrece diversas muestras en su artículo: «Documentos cifrados indianos». *Revista de Indias*, 15, 1955, pp. 255-282. Este mismo autor publicó y analizó otra serie de originales criptografiados en su estudio: «Documentos cifrados relativos al Perú en la época del Virreinato». *Revista Histórica*, XX 1955-1956, pp. 222-253, así como en una «Primera adición» a su artículo «Cifras y claves indianas», en *Anuario de Estudios Americanos*, XIV, 1957, pp. 351-359.

[34] Métodos, por otra parte, que partiendo del *«principio de máxima verosimilitud»* —análisis estadístico de las frecuencias en la aparición de cada letra—, pasando por el habitual *«ataque con texto evidente»* —descifrado disponiendo de la clave— y empleando las *«debilidades y degeneraciones criptográficas»*, pueden ser criptoanalizados con éxito. RODRÍGUEZ LIAÑEZ, Laureano; ROMERO TALLAFIGO, Manuel y SÁNCHEZ GONZÁLEZ, Antonio: *Arte de leer escrituras antiguas*. Huelva, Publicaciones de la Universidad de Huelva, 1995, p. 84.

[35] *Archivo General de Indias, Patronato, 192, número 2-18*.

titula: *Historia del Perú*. En su capítulo 52 —libro 2.º, segunda parte— describe la composición de diferentes tintas simpáticas y explica diversos métodos criptográficos empleados en la configuración de textos cifrados[36].

A diferencia de la evolución histórica en la península Ibérica, en donde la edad de oro de esta ciencia se sitúa en el siglo XVI —y más concretamente durante el reinado de Felipe II—, en Hispanoamérica será durante la etapa emancipadora cuando alcance su mayor esplendor[37]. Resulta interesante comprobar que el empleo de los sistemas criptográficos estaba bastante difundido, aunque eran en cierto modo arcaicos y elementales, tanto en el bando realista[38] como en el de patriotas americanos. A lo largo de la historia, los ejércitos en combate, siempre han utilizado y precisado de algún sistema criptográfico, tanto para sus comunicaciones como informaciones. En este período se emplearon numerosas cifras, claves que han sido analizadas por el historiador Juan Miguel Bákula[39], quien ha estudiado y descrito las usadas por Antonio José de Sucre[40], Simón Bolívar[41], José Francisco de San Martín[42], Bernardo

---

[36] FERNÁNDEZ PALENCIA, Diego: *Historia del Perú*. Sevilla, 1571, p. 105.

[37] Hasta el año 1561, fecha en que la capitalidad se traslada a Madrid, España centralizaba su criptografía «oficialista» en la Secretaría de Despacho Universal, desde donde era repartida por los correos a todos aquellos lugares, no sólo hispanos, sino también europeos y americanos, con los que se mantenían estrechas relaciones diplomáticas. Luego, este Despacho fue instalado en el Alcázar de Madrid, correspondiendo su dirección al Secretario del Exterior, por entonces Gonzálo Pérez.

Era costumbre que cada corte contara con un especialista en cifra. Entre los más conocidos departamentos de criptoanálisis —«cámaras negras», en un lenguaje más coloquial»— descuellan la Geheime Kabinet-Kanzlei vienesa y el Cabinet Noir parisino, tan eficientes, que al estudiar la historia de la criptografía durante esta época, se tiene la sensación de que el intercambio de criptogramas era únicamente un pasamiento social, debido a que su interceptación conllevaba su inmediata resolución.

[38] Una muestra elocuente la constituye la figura de Ruíz de Apodaca. A modo de ejemplo, se pueden citar sendas cartas remitidas a la Corona por este virrey de Nueva España en 1818. *Archivo General de Simancas, México, 1322, documento 34, y 1496, documento 2*.

[39] BAKULA, Juan Miguel: *Apuntes de historia, criptografía y diplomacia de la emancipación.* Lima, Imprenta Torres Aguirre, 1949.

[40] El vencedor de Pichincha dificultó la clave de sustitución simple por medio de letras muertas, números, separación de palabras e intercalaciones.

[41] La clave de Bolívar, revelada por O'Leary, es muy parecida a la de Sucre, pero más sencilla, pues sólo dificultaba su descriptación la separación de palabras.

[42] No sólo empleó el método de las «tintas simpáticas», sino también los de rejilla simple, nomenclátor y diccionario.

O'Higgins[43] (conocida gracias a Vicuña Mackenna), José Miguel Carrera[44], Francisco de Paula Santander[45], el general Ricafort, etc. Asimismo, este docto autor presenta, entre otras: la de la Misión García del Río-Paroissien[46], la de la primera legación en Chile[47] y la del Consejo de Estado (también revelada por el historiador chileno Benjamín Vicuña en 1860)[48].

Los tres sistemas criptográficos citados con anterioridad fueron empleados durante la emancipación americana[49]. De esta manera, se asiste a la utilización del sistema de transposición —sistema que se consolida a nivel internacional en el siglo XIX—, fundamentalmente el método de

---

[43] También era el sistema de sustitución simple el preferido por este Director Supremo, quien lo utilizó, fundamentalmente, durante su destierro en Montalván.

[44] La cifra del general José Miguel Carrera, empleada en la correspondencia privada con su hermano Luis en 1816, fue divulgada por Vicuña Mackenna. Se trata de una clave basada en el sistema de sustitución simple que contiene representaciones tanto numéricas como literales, pero sin orden establecido.

[45] Utilizaba una clave de perturbación sencilla, a un solo alfabeto, en el que cada letra está reemplazada por otra. Para conseguirlo, usaba dos medios alfabetos que siguen un orden normal pero intercalados entre sí.

[46] Esta clave, del año 1822, estaba configurada por un doble procedimiento: un sistema de sustitución simple y un código de 409 palabras, en el que cada una estaba representada por un signo, que podía ser una nota musical, una letra mayúscula, una figura geométrica, un símbolo caprichoso, etc.

[47] Al igual que la anterior, también es del año 1822 y con un sistema de cifrado muy similar. No obstante, esta clave permuta cada letra por una equivalencia de carácter numérico.

[48] Los métodos criptográficos empleados unos años después por el escritor y político cubano José Julián Martí son analizados por Rebeca ROSELL en su obra: *Las claves de Martí y el plan de alzamiento para Cuba*. La Habana, Cleveland Public Library, 1948.

[49] En relación a la independencia de Filipinas respecto a España (año 1898), se atesora una relevante colección de documentos en el madrileño Instituto de Historia y Cultura Militar (antiguo «Servicio Histórico Militar»). Concretamente resulta de enorme interés, la correspondencia —sobre todo telegramas, de contenido militar y económico— que mantienen el Gobernador General de Filipinas y el Ministro de Ultramar del Gobierno español entre 1893 y 1898, quienes utilizan como método de cifrado un amplísimo nomenclátor de carácter numérico (cuatro dígitos), compuesto por varios cientos de voces y sus oportunas correspondencias, v. gr.: 9084= apresar, 9125= archipiélago, 9132= armas, 9257= autor, 9371= batallón, 9953= cónsul, 9975= contrabando, 3022= cuenta, 3209= desfalco, 3671= enero, 4010= familiares, 4033= fecha, 4190= funcionarios, 4424= hacienda, 5021= islas, 5549= Méjico, 5607= militares, 5615= ministerio, 6002= operación, 6104= país, 6239= península, 6344= plata, 6906= religiosas y 7047= rey. *Instituto de Historia y Cultura Militar, sec. Ultramar, signs. 5.321.10, 5.322.06, 5.332.08, 5.322.12, 5.324.23 y 5.324.56*.

«rejilla simple»[50]. A modo de ejemplo, sirvan las figuras del virrey peruano Pezuela, quien emplea este método en la correspondencia directa con la Secretaría de Estado y del Despacho de la Gobernación de Ultramar[51], y de su sucesor, La Serna, quien recibió el criptógrafo y lo aprovechó en sus comunicaciones.

Igualmente, se utiliza el sistema de sustitución. En especial, se emplean claves de sustitución simple a un solo alfabeto[52] y, de forma más profusa, el método de «diccionario» y de «nomenclátor», debido a la garantía que suele proporcionar, como ya he apuntado anteriormente. El primero de estos métodos consiste en preparar dos volúmenes: uno destinado a cifrar —que contiene las palabras y frases convenientes, dispuestas alfabéticamente— y otro para descifrar —cuyas páginas están encabezadas por los grupos de letras o cifras, también ordenadas, que representan la traducción del texto enigmático—. Una subvariedad de este método es el de los «nomenclatores» —también llamados «códigos», «repertorios» o «tablas cifradoras»—, que se componen de

---

[50] En esencia, este método (también llamado de «rejilla fija») consiste en un rectángulo —de metal, cartón u otro material—, regularmente cuadriculado, en el que se vacían todas sus casillas y se numeran de forma arbitraria. La cantidad de casillas o ventanas es convencional y, generalmente, se adapta a la extensión de los mensajes que se van a codificar. Terminada la labor de cifrado, se levanta la rejilla y se rellenan los espacios vacios con letras nulas. Para cifrar se distribuyen, por orden correlativo desde la primera, todas las letras que configuran el texto claro en cada una de las casillas a partir del número uno y siguiendo su orden normal. Para descifrar, se disponen las letras de forma que al aplicar la rejilla aparezcan visibles por las ventanas; más tarde será suficiente tomarlas de acuerdo a lo que indique la numeración de las casillas.

Parecido es el método de «rejilla móvil», de «celosía» o de «Cardano» —en honor a su autor (siglo XVI), aunque perfeccionado en 1881 por el coronel austríaco Fleissner—. Consiste en un cuadro de lados iguales —que se puede emplear cuantas veces sea preciso—, dividido en tantas cuadrículas como se quiera, y de las cuales se vacían el 25%. De ahí, que al girarlo y colocarlo en cada una de las cuatro posiciones posibles vayan dejando al descubierto espacios distintos.

[51] Una muestra de su uso es la carta que remite desde Lima el 11 de septiembre de 1820. *Archivo General de Indias, Indiferente General, 313*.

[52] Por su sencillez y simplicidad, en grado sumo, ya que recuerda el método «benedictino» y el de «Cecheti», el capitán general de Cuba, José Cienfuegos Jovellanos, propuso en 1817 al ministerio de Guerra una cifra basada en la fuga de vocales, las cuales serían reemplazadas por representaciones numéricas, de la siguiente forma: *A=5*; *E=3*; *I=1*; *O=2*; *U=4*, mientras que las consonantes mantenían su valor. Una muestra del empleo de este método lo constituye el criptograma que remite desde La Habana, el 25 de mayo de 1819, al marqués de Casa-Irujo. *Archivo General de Indias, Estado, 12, documento 14*.

un alfabeto, por lo general homofónico[53], y un conjunto de palabras o frases adecuadas al uso que se destinen, las cuales pueden estar representadas por uno o más símbolos. Por consiguiente, la diferencia esencial entre el «nomenclátor» y el «diccionario» estriba en que éste procura abarcar todas las palabras, en tanto que aquél recoge un número limitado de ellas.

Por último, también es empleado —con mucha frecuencia— el sistema de ocultación. Son numerosas, y muy curiosas en ocasiones, las tretas seguidas para conseguir que la información llegue a buen término. Entre ellas, además de disimular informes bajo inocentes diseños, se utilizó la escritura invisible[54], por empleo de tintas simpáticas en la configuración de los mensajes, las cuales, una vez descubiertas e interpretadas por el receptor, pueden volver a borrarse o permanecer ya perennes[55].

Posteriormente, supondrá un importante avance en la criptografía, la invención de máquinas con dispositivos expresamente diseñados para cifrar y descifrar de forma automática toda clase de mensajes, los cuales resultan prácticamente ininteligibles para quienes no posean sus

---

[53] En la actualidad se considera como primer cifrario homofónico el empleado en el año 1401 en la correspondencia mantenida entre la corte mantuana y Simeón de Crema.

[54] Aunque en múltiples ocasiones se emplearon productos caseros, tales como la leche, jugos de uvas y zumos de cítricos (naranja, pomelo o limón), las tintas «simpáticas» suelen estar elaboradas a base de sustancias químicas: sulfato de hierro, carbonato de sodio, sulfato de cobre, etc., mientras que se revelan por el uso de otro producto químico, llamado el «reactivo», como por ejemplo el carbonato de sodio, el amoniaco y el cianato de potasio. Esta materia está tratada ampliamente por Charles BREMOND en su estudio: *Les écritures secrètes et les encres mystérieuses dites sympathiques*. París, Albin Michel, 1919; también se pueden consultar las obras que se citan a continuación: PAULA MARTI, Francisco de: *Poligrafía o arte de escribir en cifra de diferentes modos, arreglado a los métodos de varios autores antiguos y modernos; con una colección de tintas simpáticas y comunes, el modo de hacer revivir la escritura en los manuscritos antiguos y de borrar lo escrito cuando convenga*. Madrid, Imprenta de Sancha, 1808 (reed. en Valencia, 1993); *Recetario para tintas negras, de colores y simpáticas con un apéndice de un sistema de escritura cifrada por S. H. A*. Palma, 1876; y RIOLS, J. de: *La correspondance secrète devoilée*. París, A. L. Guyot, 1881.

[55] Mientras tanto, en España —año 1854—, a petición de Francisco Val, se intentó establecer una cátedra de poligrafía dependiente de la Sociedad Económica Matritense de Amigos del País, pero la comisión encargada de examinar la solicitud, tras sesiones maratonianas y no exentas de enfrentamientos, dictaminó finalmente un juicio contrario a la proposición formulada. *Archivo de la Real Sociedad Económica Matritense, leg. 436/24*.

claves y los correspondientes instrumentos. Suelen consistir en ingenios con teclados, que imprimen directamente el texto enigmático al pulsar sobre ellos el texto claro. Es decir, sus teclas llevan grabadas las representaciones normales y sus tipos imprimen los caracteres codificados.

Más tarde, a comienzo de la década de los 50, se produce un cambio fundamental en la práctica criptográfica. La comercialización de los primeros ordenadores y la potencia de cálculo que aportaron hizo surgir métodos de cifrado que se basan en la dificultad computacional de su vulneración. El ordenador ha revolucionado las técnicas criptográficas en razón de su enorme capacidad y de la gran celeridad con que trata la información. De este modo, se puede recurrir a claves de complejidad ilimitada, creándose infinitos criptosistemas[56].

En este siglo la criptografía ha avanzado con pasos de gigante: emplea ya instrumentos matemáticos de enorme sofisticación[57]. En vista de que las matemáticas han hecho su entrada triunfal en la criptografía, no debe

---

[56] Son numerosas las obras que han sido publicadas en los últimos años sobre este tema. Entre ellas, pueden citarse las siguientes: BLACK, Uyless: *Redes de ordenadores: protocolos, normas e interfaces*. Madrid, Ra-Ma, 1989; COBB, Stephen: *Manual de seguridad para PC y redes locales*. Madrid, McGraw-Hill, 1994; CRYPTO 83: *Advances in cryptology: proceedings of Crypto 83*. New York, Plenum Press, 1983; DOMINGO I FERRER, Josep: *Criptografia per als serveis telemàtics i el comerç electrònic*. Barcelona, Universitat Oberta de Catalunya, 1999; DEAVOURS, C. y KAHN, David: *Cryptology: machines, history and methods*. Nex York, Artech House, 1989; GREENWOOD, Gareth: *Códigos y claves secretas: criptografía en Basic*. Madrid, Anaya, 1986; KONHEIM, Alan G.: *Cryptography: a primer*. New York, A Wiley-Inter Science Publication, 1981; MARTÍNEZ ORGA, Vicente: *Criptografía: la ocultación de mensajes y el ordenador*. Madrid, Siglo Cultural, 1986; MASSEY, John L.: *Cryptography: fundamentals and applications*. Zurich, ATS Seminar, 1994; MORANT, José Luis, RIBAGORDA, Arturo y SANCHO, Justo: *Seguridad y protección de la información.* Madrid, Centro de Estudios Ramón Areces, 1994; PASTOR, José y SARASA, Miguel Angel: *Criptografía digital: fundamentos y aplicaciones*. Zaragoza, Prensas Universitarias de Zaragoza, 1998; RAMIO, Jorge: *Aplicaciones criptográficas*, Madrid, Publicaciones de la Escuela Universitaria de Informática de Madrid, 1999; ROBLING, E.D.: *Cryptography and data security*. Massachusetts, Addison Wesley, 1982; RODRÍGUEZ, Amador: *Protección de la información: diseño de criptosistemas informáticos*. Madrid, Paraninfo, 1986; y WELSH, Donald: *Codes and cryptography*. Oxford, Oxford Science Publications, 1988.

[57] Se considera el padre de la criptografía teórica moderna a Claude Shannon, nacido en 1916 y autor de un artículo básico y fundamental sobre esta materia: «Communication theory of secrecy systems». *Bell System Technical Journal*, 27, 1949, pp. 379-423 y 623-656.

resultar sorprendente que, al igual que existen teoremas algebraicos o geométricos, también los haya criptológicos[58].

Por último, no se puede concluir sin recordar, aunque sea brevemente, el procedimiento de la «criptofonía» (criptografía + telefonía) o «sacrofonía», empleado en la actualidad a nivel internacional. Esta práctica consiste en proteger las conversaciones telefónicas enmascarando las voces de los interlocutores. Un mecanismo de cifrar, el «modulador» o «mezclador», transforma las señales de origen convirtiéndolas en un sonido incoherente y confuso. Luego, otro aparato, el «demulador», se encarga de rectificarlas de salida, donde se halla el receptor autorizado. De este modo, cualquiera que pretenda escuchar a través de la línea telefónica sólo oirá el sonido inconexo, quedando garantizada la privacidad de la conversación[59].

Como resultado, la criptografía ha adquirido en la actualidad un lugar relevante y fundamental en la actividad diplomática, no sólo a nivel interno o nacional sino también internacional, de los diferentes gobiernos y estados. De estar en manos de militares y diplomáticos, en la sociedad moderna ha surgido la necesidad de la criptografía civil, debido al empleo de información diversa que se almacena en bancos de datos y se transmite a través de redes de ordenadores[60]. Tanto las llamadas telefónicas, que pasan por satélites, como el correo electrónico, a través de ordenadores, pueden ser interceptados con facilidad, poniendo en peligro la privacidad. Asimismo, cada vez más negocios se efectúan por Internet, motivo por el

---

[58] Consúltese las siguientes obras: *Actas de la IV reunión española sobre criptología*. Valladolid, Servicio de publicaciones de la Universidad, 1996; *Actas de la V reunión española de criptología y seguridad de la información.* Málaga, Servicio de publicaciones de la Universidad, 1998; AKRITAS, A.G.: *Elements of computer algebra*. New York, John Wiley & Sons, 1989; BEUTELSPACHER, Albrecht: *Cryptology*. Washington, Mathematical Association of America, 1994; CABALLERO, Pino: *Introducción a la criptografía*. Madrid, Ra-Ma, 1996; GELBAUM, Bernard R.: *Linear algebra*. Washington, North-Holland, 1989; JAKUBOWICZ, Daniel y LEHNING, Herve: *Matemáticas para la información personal*. Barcelona, Masson, 1985; LONGO, G. y MARCHI, M.: *Geometries, codes and cryptography*. Springer-Verlag, 1990; LOXTON, John: *Number theory and cryptography*. Cambridge, University Press, 1990; PATTERSON, N.J.: *Mathematical cryptology*. Londres, Rowman & Littlefield, 1987; ROSEN, Kenneth: *Elementary number theory and its applications.* Massachusets, Addison Wesley Publishing Company, 1988; y SÁNCHEZ ÁVILA, Carmen y SÁNCHEZ REILLO, Raul: *Apuntes de criptografía aplicada*. Madrid, ETSI Telecomunicación, 1999.

[59] SGARRO, 1990, p. 77.

[60] CABALLERO, 1996, p. X.

que hay que tener un cuidado mayor y crear más salvaguardias para proteger a las empresas y a sus clientes. La codificación es, supuestamente, la única manera de asegurar la privacidad y garantizar el éxito del mercado digital. De ahí, como precisa el profesor Simon Singh, que el arte de la comunicación secreta será el encargado de suministrar *«las cerraduras y las llaves de la Era de la Información»*[61].

[61] SINGH, 2000, p. 10.