ELEMENTOS Y SISTEMAS CRIPTOGRÁFICOS EN LA ESCRITURA VISIGÓTICA

Dr. D. Juan Carlos Galende Díaz
Profesor Titular de "Paleografía y Diplomática"
Universidad Complutense de Madrid

Introducción

Etimológicamente, se puede conceptuar la criptografía como la ciencia que estudia la escritura escondida u oculta.

Además de esta nomenclatura, también se ha denominado a este sistema de escribir mediante signos convencionales "poligrafía", "estenografía", "pasigrafía" y "esteganografía", amén de escritura "cifrada", "diplomática" o "en clave", por emplearse de manera común por los gobiernos y sus representantes diplomáticos.

Su finalidad no es otra que ocultar a terceros el contenido de textos que por su naturaleza y trascendencia sólo los deben conocer los interesados. De ahí que se trate de una disciplina que enseñe a diseñar cifrarios o códigos secretos, es decir, a escribir en un lenguaje pactado mediante el empleo de claves o cifras[1].

Por ende, a la labor inversa, interpretar mediante análisis los cifrarios construidos por los criptógrafos, es mejor denominarla "criptoanalizar"; a su vez, este examen se puede verificar conociendo la clave o ignorándola, por lo que conviene distinguir entre el "descifrado" o "decodificado"[2] y el "descriptado" o "perlustrado", respectivamente.

[1] La voz "cifra" proviene del vocablo hebreo "saphar", que significa "numerar".

[2] Incluso se pueden matizar estos dos términos, "descifrar" y "decodificar", prefiriendo el primero cuando se realice la labor de resolver un mensaje en cifra, es decir, sustitución al nivel de letras, y el segundo cuando se lleve a efecto la operación de

No es necesario precisar que la formación de una clave no es complicada, puesto que no se sujeta a normas fijas, dependiendo en exclusiva de la pericia personal en la disposición de los signos. Lo problemático es dar solución a un texto codificado o criptograma, más aún si se ignora la clave. Es en este caso cuando la tarea es dificilísima, pues requiere determinados conocimientos: la lengua en que está el texto cifrado, el sistema empleado en su confección, la frecuencia en la aparición de las grafías o el empleo de los caracteres repetidos, inertes, dobles, etc.

A tenor de lo expuesto, de una manera más genérica, se puede definir la criptografía como todo el conjunto de normas, técnicas, métodos y procedimientos que incumben tanto al cifrado como al descifrado de la información[3].

Noticia histórica

Bien es verdad que la cifra es tan antigua como la escritura y, en cierto modo, se considera como escritura esos signos de las hogueras que se encendían a larga distancia, telégrafos de banderas y luces de Marina. Pero la verdad es que ninguna de las civilizaciones antiguas hizo uso común de la criptografía, salvo en contadas ocasiones. Su empleo normalizado comienza durante el periodo medieval, con los árabes, y en Europa, a partir del Renacimiento[4].

La Historia está llena de códigos. Se tienen noticias de su empleo desde, aproximadamente, el año 1900 a.C. En la civilización egipcia, de forma esporádica, se alteraban los signos literales por otros simbólicos. Semejante procedimiento se utilizó cuatrocientos años después en la cultura mesopotámica. Otros ejemplos criptográficos de la antigüedad se pueden encontrar en algunos textos bíblicos hebreos (siglo VI a.C.) o en métodos ocultistas chinos y griegos (s. V a.C.). Sin embargo, tradicionalmente, está considerado como primer empleo de escritura cifrada, en el ámbito militar, el conocido método del "escítalo" espartano, utilizado en la quinta centuria

transformar en claro un criptograma codificado al nivel de las palabras o las frases. Simon SINGH: *Los códigos secretos*, Madrid, Debate, 2000, pp. 41-42.

[3] Juan Carlos GALENDE DÍAZ: "La criptografía medieval: El libro del Tesoro", en *II Jornadas Científicas sobre Documentación de la Corona de Castilla (siglos XIII-XV),* Madrid, Cema, 2003, pp. 41-42.

[4] Jesús J. ORTEGA TRIGUERO, Miguel Ángel LÓPEZ GUERRERO y Eugenio C. GARCÍA DEL CASTILLO CRESPO: *Introducción a la criptografía: Historia y actualidad*, Ediciones de la Universidad de Castilla-La Mancha, Cuenca, 2006, p.19.

anterior a Cristo, y del que Plutarco, en su *Vida de Lisandro*, efectúa una descripción[5].

Unos siglos después, en la segunda centuria antes de Cristo, el escritor griego Polibio también empleó un código cifrador para sus comunicaciones, en el que diversas letras eran sustituidas por un número de dos cifras, los cuales podrían transmitirse por medio de señales luminosas procedentes de hachones.

Otro de los primeros episodios en que se utilizó un método para transmitir información con carácter secreto data de la época romana. La comunicación se efectuaba sustituyendo unos símbolos por otros en el conjunto de los que componían el mensaje, obedeciendo a una cierta regla permanente.

Hasta el siglo decimotercero no se tiene mucho conocimiento de la evolución de la criptografía, aunque es presumible que se utilizase, sobre todo, por motivos bélicos o diplomáticos. Las cancillerías carolingia o irlandesa, durante la Alta Edad Media, emplearon procedimientos muy simples, consistentes en la permuta de letras del texto claro, en especial las vocales, por elementos simbólicos[6]. Del mismo modo, los copistas de códices, en ocasiones, escondían sus nombres usando técnicas criptográficas tales como el

[5] "Cuando un general parte para una expedición de tierra o mar, los éforos toman dos bastones redondos, perfectamente iguales en longitud y grosor, de manera que se correspondan exactamente uno con otro en todas sus dimensiones. Ellos guardan uno de estos bastones, dando el otro al general, y llaman a estos bastones escítalos. Cuando quieren enviar al general un secreto de importancia, cortan una tira de pergamino, larga y estrecha como una correa, arrollándola alrededor del escítalo que guardaron, sin dejar el menor intervalo entre los bordes de la banda, de tal suerte que el pergamino cubra enteramente la superficie del bastón. Sobre este pergamino así arrollado alrededor del escítalo, escriben lo que desean y después quitan la cinta y la envían al general sin el bastón. El general que la recibe no sabría leerla, porque las letras, perdida la alineación y dispersas, no tendrían continuidad; pero él toma el escítalo que llevó consigo, y arrollando alrededor la banda del pergamino, se reunirán las vueltas, volviendo las letras a tomar el primitivo orden en que fueron escritas. Esta misiva se llama escítalo, del nombre mismo del bastón, como aquello que se mide toma el nombre de aquello que le sirve de medida". Pedro SERRANO GARCÍA: *Criptografía y perlustración*, Madrid, La Xilográfica, 1953, p. 22.

[6] Muchos de estos elementos eran tomados de alfabetos foráneos, tales como el celta, el griego, el hebreo, el árabe o el siriaco. Luis NÚÑEZ CONTRERAS, *Manual de Paleografía. Fundamentos de historia de la escritura latina hasta el siglo VIII*, Madrid, Cátedra, 1994, p. 180.

anagrama, la fuga de vocales o la alteración e inversión de las grafías componentes de sus nombres[7].

Más tarde, a partir del siglo XIII, en algunas repúblicas italianas y en la curia papal, la escritura oculta comenzó a practicarse de manera más frecuente, antesala del período moderno y de la consolidación del "nomenclátor" o tabla cifradora[8] como método preferido, gracias a la seguridad que proporcionaba.

Luego, desde la centuria dieciochesca, poco a poco comienza el declive de la escritura secreta, desapareciendo la elegancia y la uniformidad antes empleada en la construcción de criptogramas. Será el momento en el que empiecen a emplear ingenios mecánicos, en detrimento "del lápiz y el papel"[9], es decir, el tránsito de la criptografía "histórica" a la "mecánica". Durante esta etapa contemporánea, y más todavía desde la comercialización de los primeros ordenadores, surgió la necesidad de una criptografía civil, la cual se ha introducido en actos cotidianos, pues su difusión le ha otorgado una función notable en la sociedad.

Criptografía visigótica

En la anterior reseña histórica se han mencionado los tres principales sistemas criptográficos: "transposición", "sustitución" y "ocultación". El primero, consiste en colocar un fragmento cifrado en un lugar previamente conocido por el otro corresponsal, comprendiendo los métodos que alteran el orden natural de las letras, sílabas o palabras de un texto, trastocándolas o formando anagramas con ellas. El segundo, también llamado de "perturbación", consiste en reemplazar alguna letra del alfabeto por uno o varios signos convenidos de antemano por ambas partes, abarcando aquellos procedimientos basados en relevar las grafías de un escrito por otras distintas, por guarismos o por signos; es decir, los elementos del texto claro son sustituidos por una representación distinta a la original, bien literal, numérica o esteganográfica. Por último, el sistema de ocultación incluye aquellos métodos en los que el remitente transmite de forma escondida o disfrazada el mensaje auténtico.

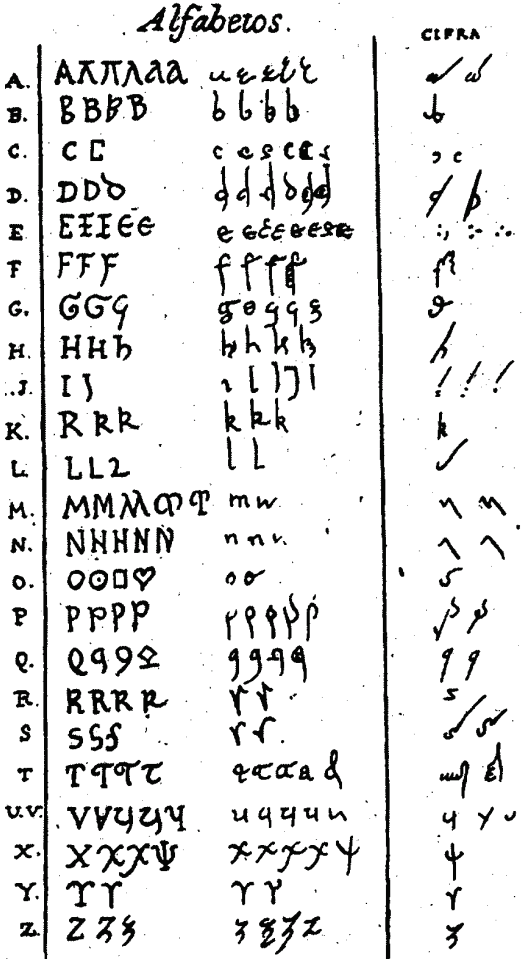
[7] Juan Carlos GALENDE DÍAZ: *Criptografía. Historia de la escritura cifrada*, Madrid, Complutense, 1995, pp. 75-77.

[8] El primer cifrario homofónico conocido es el empleado en el año 1401 en la correspondencia mantenida entre la corte mantuana y Simeón de Crema.

[9] Denominación empleada por Andrea SGARRO en su obra *Códigos secretos* (Madrid, Pirámide, 1990), p. 83.

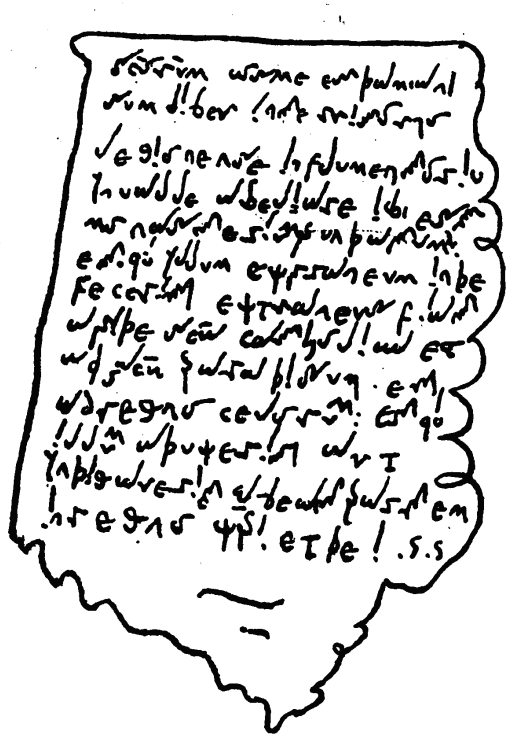
La principal característica de los métodos poligráficos desarrollados durante esta época es la sencillez a la hora de confeccionar las claves. En la escritura visigótica, preferentemente se utilizó el sistema de sustitución, siendo los métodos aplicados los siguientes.

Empleo de un alfabeto convencional, derivado de las grafías cursivas y taquigráficas, que se usó a partir del siglo X para las suscripciones y signaturas de algunos documentos y para algunas notas de códices.



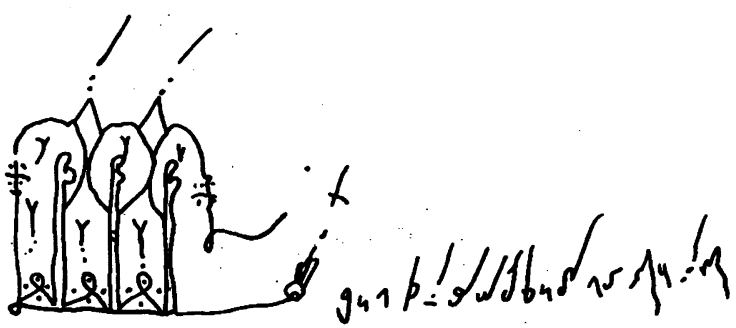
Alfabetos y cifra visigótica

En este alfabeto criptográfico se combinan elementos literales y estenográficos o figurativos, faltando los de naturaleza numérica. De este modo, la letra "a" es semejante a la realizada en la escritura visigótica cursiva, salvo que el trazo final se desarrolla desproporcionadamente en dirección diagonal ascendente; la "b" no guarda diferencias con la visigótica, a excepción de un corto apéndice horizontal en su zona izquierda; la "c" presenta dos formas, una igual que la minúscula y otra de hechura invertida; la "d" tiene la peculiaridad de su notable inclinación y la prolongación de su trazo recto por debajo de la caja del renglón, a la vez que el lazo lo puede tener a uno u otro lado; la "e" se realiza por la combinación de tres elementos: bien tres puntos dispuestos de forma piramidal, bien por dos y una coma o por dos y un guión; la "f" guarda semejanzas con la trazada en la escritura visigótica cursiva, aunque muestra un trazo final manierístico; la "g" tiene forma de bucle volteado; la "h", al igual que la "d", se caracteriza por su destacada inclinación; la "i" puede presentar en la parte inferior de su rasgo vertical, que habitualmente se sesga, un punto, dos puntos o dos guiones; la "k" es prácticamente idéntica a la minúscula cursiva; la "l" revela la forma de un semicírculo tangente a la línea del renglón que prolonga oblicuamente en dirección ascendente su último trazo; la "m" recuerda a la actual "n", pero desarrollando su trazo final hacia abajo; la "n" simplifica los elementos de la "m" a uno sólo, el último; la "o" cifrada, proveniente de las notas tironianas romanas, se traza de forma parecida a la "l", pero una vez terminado el semicírculo tangente se extiende hacia la derecha el rasgo final; la "p" suele tener la cabeza separada del caído, aunque también puede presentar otra forma peculiar, trazada de un único golpe de pluma, en el que ambos elementos están unidos; la "q" no tiene problemas de identificación, pues su configuración es como la actual; la "r" recuerda en su hechura a la "z" corta, pero invirtiendo su figura; la "s" está compuesta de dos elementos, uno que es la forma uncial de esta letra y otro que es un trazo oblicuo prolongado que arranca de su extremidad superior; la "t" revela una forma muy peculiar, con un primer componente configurado por el ensamble de varias curvas en disposición vertical u horizontal, y un rasgo anguloso unido a uno de sus extremos; la "u", bien puede presentar su forma vocálica, con rasgo final descendente o sin él, o consonántica de "v", con el mismo remate inferior de manera oblicua; la "x" recuerda la letra "psi" griega; la "y" exhibe un perfil cursivo y simplificado de su forma original; por último, la "z" tiene un contorno idéntico al de la minúscula común visigótica en su silueta baja.



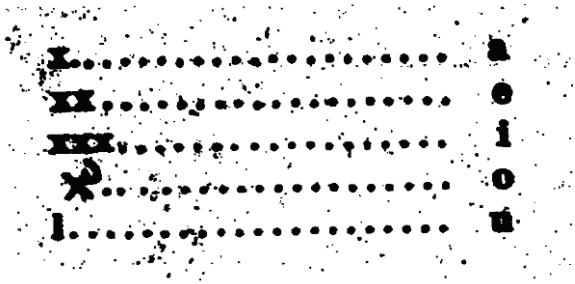
Fragmento códice cifrado[10]

[10] Esta ilustración, recogida del libro de Jesús MUÑOZ Y RIVERO: *Paleografía visigoda. Método teórico-práctico para aprender a leer los códices y documentos españoles de los siglos V al XII* (Madrid, Daniel Jorro, 1919, p. 134), representa un fragmento cifrado de un códice conservado en San Isidoro de Léon (signatura 22). Su decodificado es el siguiente: *Sanctorum Cosme et Damiani sum liber in territorio Legionense in flumen Torio in valle Abeliare ibi est monasterium fundatum et que illum extraneum inde fecerit extraneus fiat a fide sancta catholica et ab sanctum paradisum et ad regno celorum et qui illum aduxerit aut indigaverit abeat partem in regno Christi et Dei*.



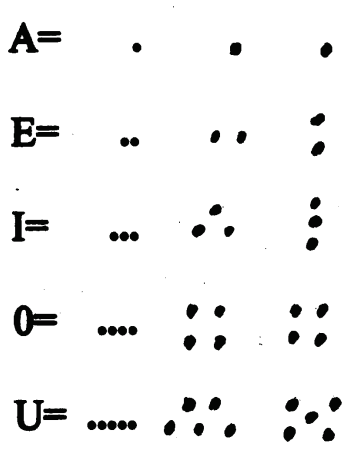
Suscripción notarial de carta de venta[11]

Sustitución de las vocales por los numerales romanos representativos de las cinco primeras decenas, con la salvedad de que para simbolizar la "o" se emplea el episemon, con valor de cuarenta, cuya figura está configurada por una "x" aspada y una "l" cursiva que cuelga, en forma de vírgula, de su extremo superior derecho.



Permuta de las vocales por puntos y líneas, a modo de alfabeto Morse, es decir, como el anterior, se trata de un método de sustitución parcial, sin problemas a la hora de su descriptado.

[11] Se trata de la suscripción notarial, con caracteres cifrados, de una carta de venta, fechada el 18 de septiembre de 1082 (*Gundisalbus notuit*). Archivo Histórico Nacional, sección Clero, carpeta 884, número 21.



Perturbación de las grafías latinas por sus correspondientes griegas. No obstante, este hábito utilizado durante la centuria décima y la siguiente, no fue exclusivo de la documentación hispana, pues también se puede encontrar en originales franceses e italianos[12].

Escritura de donación[13]

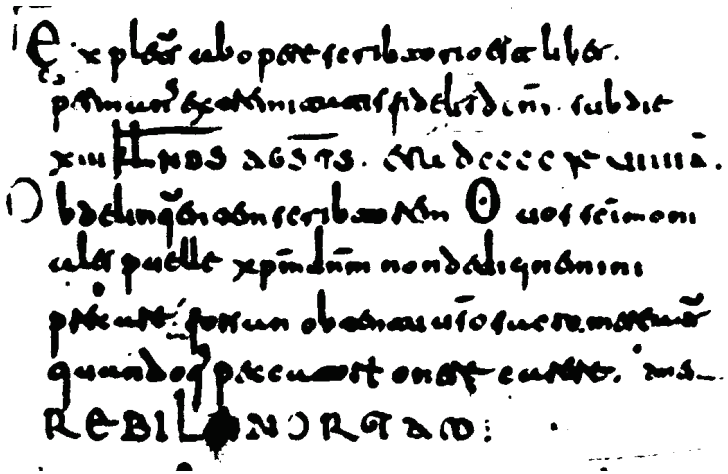
Además del sistema de sustitución, también se empleó, aunque con menos asiduidad, el procedimiento de transposición. Concretamente el método de inversión o alteración, consistente en escribir al revés las sílabas, palabras, oraciones o mensajes enteros[14]. Entre los códices visigóticos que ofre-

[12] Agustín MILLARES CARLO: *Tratado de paleografía Española*, vol. I, Madrid, Espasa Calpe, 1982, pp. 290-294.

[13] Fragmento de una escritura de donación de diversas heredades en Bascuñuelos, otorgada por el presbítero Sonna en favor del monasterio de Oña el año 1045. Su descifrado es: *Sonna supradictas exaravit et confirmavit*.
Jesús MUÑOZ Y RIVERO: *Paleografía visigoda*, p. 88.

[14] Una palabra de seis letras puede perturbarse de seis maneras distintas, mientras que un grupo de veinte grafías darían lugar a 2.432.902.007.246.400.000 combina-

cen muestras de este procedimiento es característico uno del año 911, escrito por el diácono Fidel. Se trata de la obra de Taio, *Sententiae*; en la suscripción del copista se puede leer: REBIL ENORTAM, es decir, LIBER MATRONE[15].



Asimismo, durante esta etapa, también se utilizó, como en cualquier otro momento histórico, el sistema de ocultación, por el que cualquier artimaña era buena si se quería transmitir un mensaje de manera disfrazada. Tretas existieron desde tiempos arcaicos, baste recordar algunas: afeitar la cabeza de un emisario y escribir en su cuero cabelludo, con caracteres endebles, el mensaje del que era portador[16]; tragarse objetos pequeños que contenían criptogramas[17]; utilizar tintas simpáticas, para lo que se emplearon

ciones posibles. John LAFFIN: *Códigos y cifras. Los mensajes secretos y su historia*, La Coruña, Adara, 1976, pp. 22-23.

[15] Archivo de la Corona de Aragón, Ripoll 49. La transcripción de la suscripción y de la data es: *Expletus ab opere scribtorio est liber per manus extremitatis Fidelis diaconi, sub die XIII kalendas agustas, era DCCCCXLVIIII^a^.*

[16] Este método críptico fue utilizado, por ejemplo, en el siglo VI a.C. por el griego Histiaeo, quien, precisando remitir un mensaje a su yerno Aristágoras de Mileto para que capitaneara una revuelta, se valió de él. Vicente GARCÍA ORGA: *La ocultación de mensajes y el ordenador*, Madrid, Siglo Cultural, 1986, p. 8.

[17] En la antigua China se escribían mensajes sobre seda, la cual, una vez comprimida y recubierta de cera, era ingerida por el portador.

productos caseros[18]; enmascarar el texto original[19]; o esconder la cifra de manera más o menos estratégica, de tal manera que, en ocasiones, se conformaban con guardar en receptáculos cerrados el mensaje privado, pero bastaba con capturar al portador para obtener la información.

Por último, cabe significar que desde que el hombre dispuso de la escritura como vehículo de comunicación mostró un empeño especial en impedir la lectura de información particular. No obstante, aunque Francis Bacon, vizconde de St. Albans y lord canciller de Inglaterra, sentenciaba que "una cifra perfecta no debe ser trabajosa de escribir ni de leer, debe ser imposible de descifrar", siempre han existido expertos criptólogos, por lo que "el triunfo del criptógrafo constituye el fracaso del criptoanalista, y viceversa", según reza el axioma.

[18] En el siglo I, Plinio el Viejo experimentaba con el jugo de la planta "thythymallus", el cual, una vez seco, se transparentaba, pero al calentarlo suavemente volvía a revelarse, pues adquiría una tonalidad pardusca.

[19] A comienzos del siglo V a.C. Damarato, un exiliado griego en Persia, para informar a los lacedemonios del proyecto de Jerjes de invadir Grecia, escribió un mensaje inciso en unas tablillas y las recubrió después de cera; de este modo, según nos relata Herodoto en sus *Historiae*, "las tablillas, al estar aparentemente en blanco, no ocasionarían problemas con los guardas del camino".