CRIPTOGRAFÍA HISPANOAMERICANA DURANTE EL SIGLO XVI

María PALLÁS FERNÁNDEZ

1. QUÉ ES LA CRIPTOGRAFÍA.

La palabra criptografía proviene de los términos griegos κρυπτος, que significa 'secreto', y γραφος, 'escritura', por lo que podría interpretarse etimológicamente como el estudio de lo oculto, de lo escondido. Su definición contemporánea la considera una ciencia cuyo objeto de estudio son los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en clave entre un emisor y un receptor a través de un canal de comunicación.

Se divide en dos grandes ramas: la criptografía propiamente dicha, ocupada del cifrado de mensajes en clave y del diseño de criptosistemas, y el criptoanálisis, que trata de descifrar los mensajes en clave, rompiendo así su criptosistema.

Es una disciplina muy antigua, sus orígenes se remontan al nacimiento de nuestra civilización. Los chinos, indios, 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 los períodos bélicos.

En origen su único objetivo era proteger la confidencialidad de informaciones militares y políticas, mantener en secreto un mensaje. Sin embargo, en la actualidad es una ciencia que no sólo persigue la privacidad de los datos, sino que busca además garantizar su autenticación.

No se trata sólo de ocultar la existencia de un mensaje, sino sobre todo de ocultar su significado, un proceso que se conoce como codificación. La criptografía tuvo también un uso personal cuando a algún particular le interesaba que la información del documento sólo llegase a la persona a quien iba destinado.

Comúnmente los textos codificados se adaptan a los formularios propios de la correspondencia privada o de las notas empleadas en la administración. Sin embargo, se eluden muchas veces los tratamientos protocolarios, los saludos, la intitulación, la dirección y la data. En función de esta particularidad, su descifrado o extracción del texto claro, que solía correr a cargo de un oficial bien capacitado, se podía presentar al receptor en una hoja aparte o bien sobre el propio papel original.

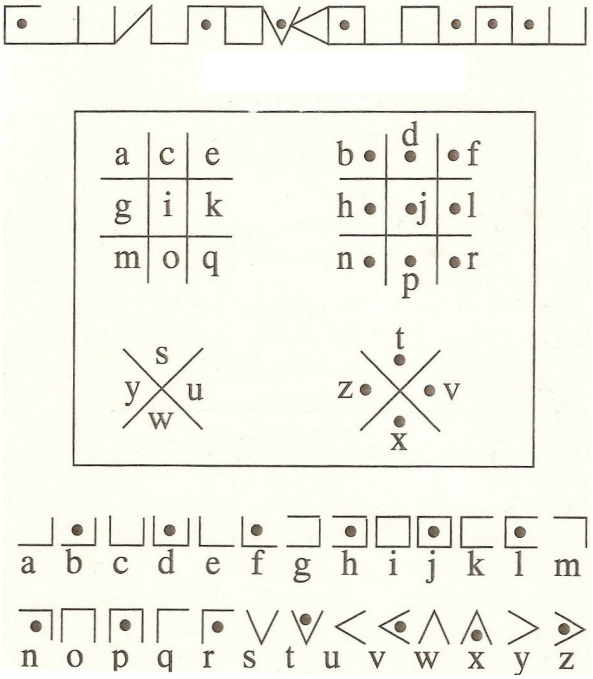
Los tres tipos de sistemas de cifrado desarrollados a lo largo de la historia son:

–El de **sustitución o perturbación**, que consiste en cambiar alguna letra del texto original por otro carácter o por determinado signo según una clave conocida por emisor y receptor. Puede ser simple o múltiple (es decir, con varias claves).

Es posible realizar la *sustitución simple* por desplazamiento (cada letra se reemplaza por otra del mismo alfabeto), como en el método de Julio César[1], o bien por signos (cada letra es representada mediante un signo ajeno al abecedario original), como ocurre con el sistema masónico.

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

Método de Julio César.



Método masónico.

La *sustitución múltiple* combina muchísimas variables, es decir, varios mecanismos de sustitución, en especial alfabéticos. Esto hace que sea mucho más complicado descifrarlo.

[1] El método de Julio Cesar consistía en dos alfabetos, uno de ellos doble, que se acoplaba convenientemente a otro sencillo.

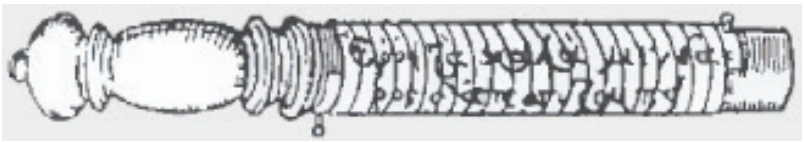
Un ejemplo es el método de la tabla llana de Tritemio[2].

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	X	Y	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	ñ	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	ñ	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
Ñ	ñ	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
O	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ
P	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o
Q	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p
R	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q
S	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r
T	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s
U	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t
V	v	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	x
Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	x	y

–El segundo mecanismo es la **transposición**, que consistía en alterar el orden de las letras, sílabas o palabras de un texto con arreglo a una clave que el emisor y el receptor conocían. Pueden emplearse claves sencillas o muy complicadas.

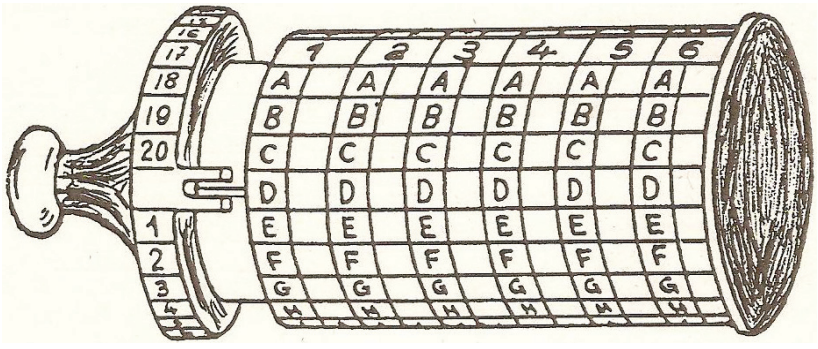
Para poder descifrar estos códigos se necesita una tabla con la distribución de las letras ocultas del documento que se quiere cifrar, en forma de líneas horizontales y columnas. Según como estén distribuidas las letras, las tablas se clasifican en normales, inversas, alternas o inversas alternas.

Hay muchos ejemplos, como el del escítalo[3].



O el de Richelieu, en el que el texto se codifica con una clave numérica adjudicando un número a cada letra; una vez terminada la cifra, se le añadirá otro número, y así sucesivamente. Por último, el mensaje se distribuye según el orden de los números, con lo que el destinatario deberá estar al corriente de la clave numérica para poder descifrarlo.

Entre los sistemas de trasposición múltiple podemos citar el de Soudart.



Método de Soudart.

–Y por último, los sistemas de **ocultación**, que esconden cierta información dentro del documento sin que sea visible aparentemente, como ocurre con las tintas invisibles. En la antigüedad se empleaba el método

[2] La tabla llana de Tritemio consta de varios alfabetos diferentes dispuestos tal y como aparece en la figura.

[3] El escítalo estaba formado por dos varas idénticas, una para el emisor y otra para el receptor. Se colocaba en la varilla una tira, normalmente papiro o de cuero, y se escribía a lo largo de ella. Luego se quitaba y se enviaba al receptor quien, para su descifrado, lo colocaba en su propia varilla. Se uso en las Guerras del Peloponeso.

llamado *del mensajero*: se rapaba la cabeza de una persona, se escribía sobre el cuero cabelludo y, cuando le crecía de nuevo el pelo, partía en busca del destinatario.

2. CRIPTOGRAFÍA MODERNA.

Persiguió componer algoritmos de cifrado extremadamente complejos, pues las claves más sencillas y susceptibles de ser resueltas mediante un análisis estadístico de frecuencias, eran fácilmente descifrables. Para solventar este problema, utilizaron los homófonos y las nulas.

Los cifrados homofónicos[4] emplean alfabetos con más grafías que el normal de 26 letras. Para ello se añaden algunas más, que corresponden a los caracteres con mayor frecuencia de aparición en una determinada lengua.

En la Edad Moderna la mayoría de las veces se utilizaban cifrarios monoalfabéticos: la clave, una vez elegida, no se modificaba a lo largo de toda la operación.

Ejemplo:

Alfabeto original	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	P	q	r	s	t	u	v	w	x	y	z
Alfabeto cifrado	H	R	J	O	Y	D	I	Q	T	Z	S	L	M	E	U	N	B	K	W	A	F	P	C	X	G	V

Se empezó a utilizar además el cifrado mediante dos o más alfabetos, alternándolos, para aumentar la dificultad de desciframiento en caso de interceptación del mensaje: se pasa así de cifrarios monoalfabéticos a cifrarios polialfabéticos[5]. En el siglo XVI el francés Blaise de Vigenère desarrolló la teoría de la criptología polialfabética, lo que hoy se denomina tablero de Vigenère.

Una ventaja de este segundo sistema es que una misma letra puede cifrarse de varias formas posibles. El inconveniente es que hay que tener en cuenta en la clave cómo se distribuyen los distintos alfabetos empleados.

En el siglo XVI, en particular durante el reinado de Felipe II, España atravesó un período de expansión a nivel internacional, con la apertura de embajadas y legaciones diplomáticas en multitud de lugares. Este hecho, unido a las continuas guerras y a la inestabilidad política, provocó un enorme incremento en el uso de la criptografía, que se convirtió en una ciencia muy necesaria. A lo largo del siglo XVII, con el retroceso político y militar de la monarquía hispánica, decayó también el empleo de mensajes cifrados.

3. SITUACIÓN POLÍTICA. LA RELACIÓN ENTRE ESPAÑA E HISPANOAMÉRICA.

Desde finales del siglo XV y durante todo el Quinientos, la Corona española constituyó un imperio de dimensión universal cuyos acontecimientos clave fueron: la conquista del Caribe (durante la década de 1490 y primeros de 1500), la conquista de México (en la década de 1520), la conquista de Perú (en 1530), las Filipinas (1560), y la anexión de Portugal con la consiguiente anexión del África, el lejano Oriente y Brasil (1580). La dispersión por todo el globo terráqueo de los territorios incorporados a la monarquía hispánica dio origen a la conocida frase "el imperio donde nunca se pone el sol".

Los castellanos del siglo XVI se veían a sí mismos como un pueblo elegido, y por tanto superior, que tenía como misión de evangelizar, las nuevas tierras de América: el mayor deber y la mayor responsabilidad de Castilla era la difusión y defensa de la cristiandad.

La conquista y colonización de América durante el siglo XVI permitió que Castilla se convirtiera en una gran potencia, pero también trajo consecuencias económicas, administrativas y psicológicas no siempre positivas. Cuando llegó la hora de hacer frente a los pagos, resultó muy difícil, desembocando en una situación de malestar general, incluso podría decirse que de fracaso.

4. SISTEMAS CRIPTOGRÁFICOS USADOS EN HISPANOAMÉRICA.

En relación a Hispanoamérica, los métodos de cifrado guardan un gran paralelismo con los utilizados en la Península, y es que la génesis de la pasigrafía[6] indiana, como es lógico, se encuentra en suelo hispano. Con el fin de impedir que ciertos despachos importantes cayesen en manos enemigas se tomaron diversas prevenciones y así, además de remitir el documento por triplicado o cuadruplicado, se codificaba. Es más, como afirma Guillermo Lohmann, la dificultad en la elaboración de las claves aumentaba si se quería encubrir información a potencias extranjeras.

Los descubridores, conquistadores, colonizadores o libertadores de América emplearon diferentes mecanismos de cifrado para asegurar el secreto de sus mensajes, con particular incidencia en el período de la emancipación. Fue el caso, por ejemplo, de Hernán Cortés (de quién luego analizaré con más detalle un documento) o de Simón Bolívar, Cristóbal Colón, Pedro de la Gasca, el virrey Francisco de Toledo...

Los métodos más utilizados fueron los basados en sustituir los elementos del texto (letras, sílabas, palabras o frases) por un determinado signo ajeno al alfabeto original; dichos signos podían ser literales, numéricos o esteganográficos (uso de imágenes o dibujos), es decir, métodos de sustitución. También se emplearon

---

[4] En los cifrados de sustitución tradicionales cada letra del texto plano era sustituída por un símbolo diferente. Al hacerlo así, la frecuencia de los caracteres del original se mantiene en el criptograma, por lo que, conociendo la frecuencia en la que aparecen las letras en esa lengua, podemos obtener algunas pistas que nos permitirán resolver el criptograma. El objetivo de este nuevo sistema es disminuir el efecto de las frecuencias en el criptograma resultante. Así pues, si sabemos que la letra *a* es la más frecuente, podemos sustituirla por símbolos diferentes.

[5] Los sistemas polialfabéticos cambian letras del texto por otros símbolos para formar el texto cifrado. La diferencia con los sistemas monoalfabéticos es que no siempre se cambia un símbolo del texto por el mismo símbolo en el texto cifrado, sino que dependerá del signo que se va a sustituir y de la posición que ocupe. Los cifrados polialfabéticos aplican varias sustituciones.

[6] La pasigrafía es un tipo de representación gráfica que busca hacer inteligible un texto a cualquier persona que lo lea (la partícula παϛ en griego significa 'todo'), independientemente de la lengua que éste hable.

claves de sustitución que, según algunos autores, se presentan de forma independiente, como son los diccionarios y las tablas cifradoras[7].

Ya desde el siglo XV se empezaron a tomar medidas para que la información no cayera en manos de los enemigos de la Corona. Por eso la documentación comenzó a cifrarse a fin de dificultar su comprensión, y la Casa de la Contratación puso en práctica distintos procedimientos criptográficos. De esta forma se conseguía ocultar información a otras potencias: fechas de navegación de las flotas que traían las riquezas ultramarinas, diversas noticias que afectaban a la Corona...

Se fueron así confeccionando claves oficiales cada vez más complejas para evitar su interceptación e interpretación. Las emplearon tanto los virreyes americanos como los funcionarios peninsulares, así como los miembros de órdenes religiosas (jesuitas) e incluso personas particulares. También se conoce algún caso de utilización de mensajes cifrados por parte de los corsarios para comunicarse entre sí.

Durante toda esta etapa, el sistema que triunfó en la documentación cifrada indiana, al igual que en Europa, fue el de sustitución, tanto en su modalidad sencilla, como múltiple.

En 1561 la capital se traslada de Valladolid a Madrid y, desde esta villa, la Secretaría del Despacho Universal repartía los mensajes cifrados a cualquier destino, tanto en la propia España como los dirigidos a Hispanoamérica o a los países europeos con los que se mantenían relaciones diplomáticas. Luego la oficina de reparto se instaló en el propio alcázar, correspondiendo su dirección al Secretario del Exterior. Cada Corte solía tener un especialista en claves para poder descifrar los mensajes que llegaban.

Fue también en el siglo XVI cuando se llevó a cabo el primer estudio teórico sobre criptografía: Diego Fernández de Palencia dedicó el capítulo LII de su Historia del Perú, publicada en Sevilla en 1571, a describir y analizar diversos mecanismos de cifrado.

Durante la emancipación americana se usaron claves correspondientes a los tres sistemas de cifrado. En el caso de los métodos por transposición destacó el de rejilla simple[8], y en los de sustitución las claves simples con un solo alfabeto, en especial el diccionario[9] y el nomenclátor[10]. También se utilizó con mucha frecuencia el sistema de ocultación, disimulando informes debajo de dibujos o mediante la escritura invisible.

5. UN EJEMPLO DE DOCUMENTO CIFRADO: UNA MISIVA DE HERNÁN CORTES.

La carta que voy a analizar[11] fue descifrada por Francisco Monterde. Las tablas elaboradas por este autor fueron utilizadas después por Lohmann para descifrar otro documento de Cortés.

El contenido de la carta trata distintos asuntos: la explicación a Francisco Núñez (primo y abogado de Cortés) de los motivos por los cuales debería seguir encargándose de todos sus asuntos jurídicos ante la Corona; la orden a Núñez de que se desplazara a cualquier lugar que fuera preciso con el fin de mantenerse siempre próximo al emperador y a los asuntos de la Corte, y la recomendación de que le tuviera informado de los movimientos de los principales cortesanos y de los acontecimientos políticos de mayor trascendencia. Fija además las cantidades de dinero que habría que gastar en salarios, comenzando por el del propio Núñez, y en sobornos y regalos. Además, instruye jurídicamente a su procurador para obrar de modo que la Corte acepte compensarle por los perjuicios causados al instalar población española en las tierras concedidas a Cortés en Oaxaca.

La carta de Cortés está redactada en escritura humanística cursiva. El sistema de cifrado empleado es el nomenclátor.

Todos los signos cifrados están escritos de corrido, sin ningún espacio entre ellos que nos indique dónde empiezan y acaban las palabras, lo que hace más difícil su interpretación. Su desciframiento fue muy dificultoso ya que se usaron diferentes caracteres para una misma letra, mezclando los de tipo matemático con los alfabéticos. Sin embargo, no se utilizaron los nulos[12]. Cortés empleó deliberadamente ciertos métodos para esconder el significado literal de los caracteres, usando un sistema criptográfico que mezcla cifras y códigos, un sistema basado en la sustitución homofónica.

Se llegan a usar cincuenta signos para representar las letras: la “a” aparece escrita de tres maneras diferentes, la “b” de dos, la “c” de dos, la “d” de dos... Las letras mas repetidas en el idioma español son las vocales, por lo que son precisamente éstas las que se dotaron de más signos distintos en la cifra.

En el diccionario de nombres en código y en las tablas que fijan la correspondencia homofónica o alfabética de los signos, se incluyeron no sólo caracteres aislados, sino grupos de hasta cuatro o cinco letras como “are”, “aca”, “beril”, “adan”..., utilizados en particular para esconder nombres propios. De esta forma, nadie salvo Cortés y su procurador, podría descodificar la correspondencia. Así, “are” se refería a dos términos “emperador” o “rey”; “aca” era el nombre en clave de “Francisco de los Cobos”, secretario real desde 1517 y de Indias desde 1518...

Las imágenes (figura 1 y figura 2) corresponden a la carta cifrada del 25 de junio 1532 de Hernán Cortés a Núñez.

---

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

[8] O 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 según la extensión del texto.

[9] El diccionario es un método para el que han de prepararse dos volúmenes: uno destinado a cifrar y otro a descifrar.

[10] Los nomenclátores o tablas cifradoras se componen de un alfabeto, por lo general homofónico, y un conjunto de palabras o frases adecuadas al uso que se destinen, las cuales pueden estar representadas por uno o más símbolos.

[11] Tomada de R. NARVAÉZ, Roberto, “Historia y Criptología: reflexiones a propósito de dos cartas Cortesianas”, *Anales del Museo Nacional de Arqueología, Historia y Etnografía*, 3 (1925), pp. 436-443.

[12] Son signos inútiles que se usan a propósito para el ocultamiento.

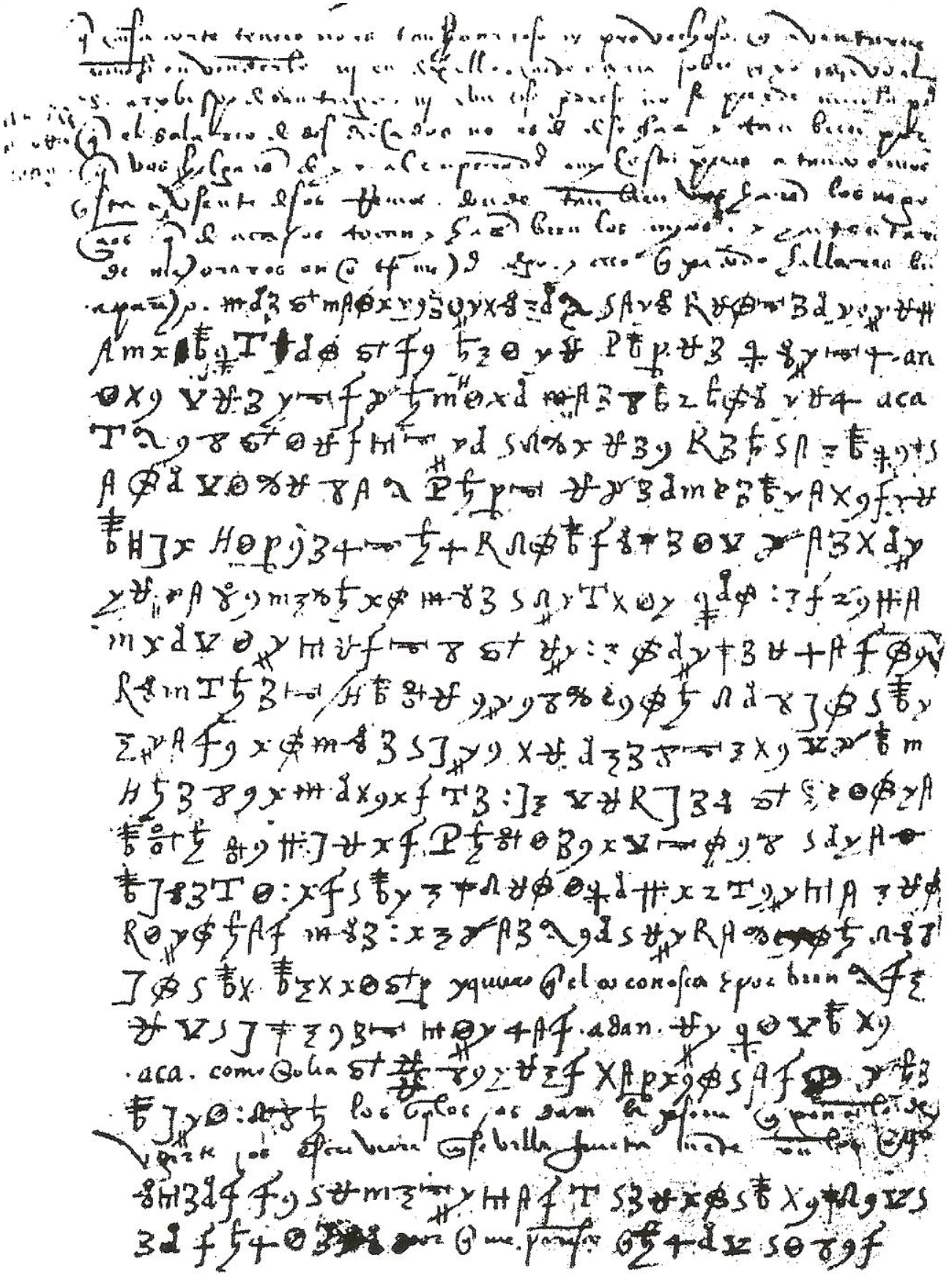


Figura 1.

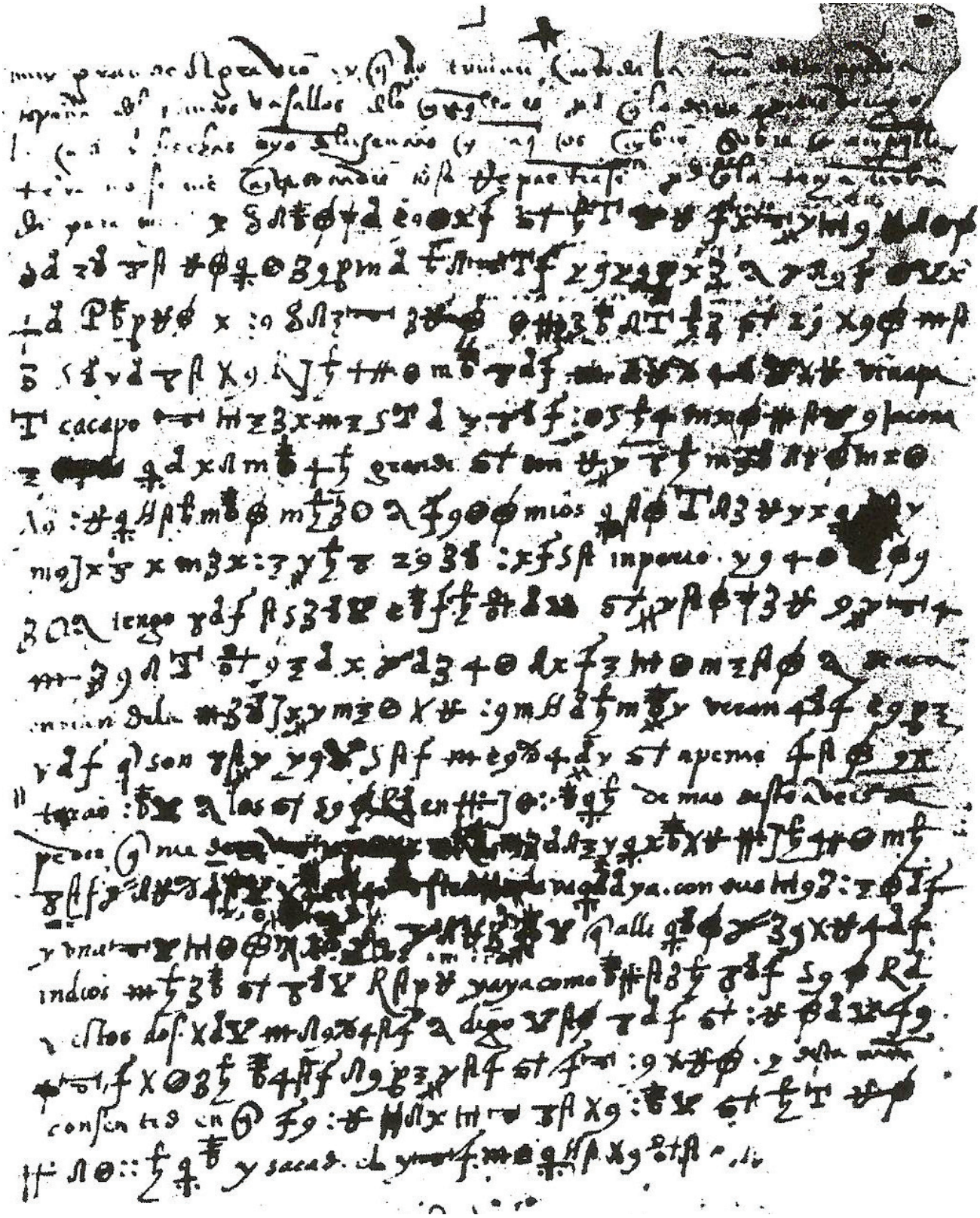


Figura 2.

En la última imagen (figura 3) aparece representada la tabla de correspondencia usada por Cortés, restituida por Francisco Monteverde[13]:

[13] "La carta cifrada de don Hernán Cortés", en *Anales del Museo Nacional de Arqueología, Historia y Etnografía*, 3 (1925), p. 438.

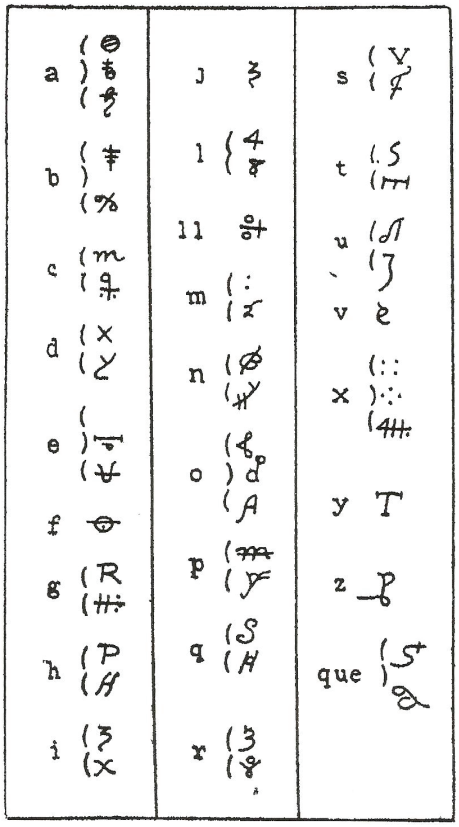


Figura 3.

CONCLUSIÓN.

Tras analizar las cartas cifradas de Cortés, queda claro que la información puede que sea uno de los bienes más importantes, pues permite, en una situación de conflicto como la que vivía por entonces el conquistador, actuar con ventaja.

En la actualidad la criptografia tiene un lugar importante en la actividad diplomática, no sólo a nivel interno de un determinado país, sino también a escala internacional entre los diferentes gobiernos y estados, siendo empleada preferentemente por militares y diplomáticos.

Pero además, en la sociedad moderna ha surgido la necesidad de una criptografia civil para proteger la información que se almacena en bancos de datos y se transmite a través de redes. Las llamadas telefónicas, el correo electrónico, las redes sociales, los mensajes, pueden ser interceptados con facilidad, poniendo en peligro la privacidad. Asimismo, cada vez más negocios se llevan a cabo por Internet, plataforma en la que hay que extremar el cuidado y crear sistemas de mayor seguridad para proteger a las empresas y a sus clientes.

BIBLIOGRAFÍA.

P. CABALLERO GIL, *Introducción a la criptografía*, Madrid, 2002.

R. DE MIGUEL GÁRCIA, *Criptografía clásica y moderna*, Oviedo, 2008.

S. FERNÁNDEZ, "La criptografia clásica", *Revista SIGMA*, 24 (2004).

J. C. GALENDE DÍAZ, Juan Carlos, "La escritura cifrada durante el reinado de los Reyes Católicos y Carlos V", *Cuadernos de Estudios Medievales y Ciencias y Técnicas Historiográficas*, 18-19 (1993-1994), pp. 159-178.

J. C. GALENDE DÍAZ, *Criptografía. Historia de la escritura cifrada*, Madrid, 1995.

J. C. GALENDE DÍAZ, "Recorrido histórico por la criptografia militar", *Revista de Historia Militar*, 88 (2000), pp. 11-34.

J. C. GALENDE DÍAZ, "Sistemas criptográficos empleados en Hispanoamérica", *Revista Complutense de Historia de América*, 26 (2000), pp.57-71.

J. C. GALENDE DÍAZ, "El calígrafo Luis de Olod y su aportación a la criptografia española", *Cuaderno de investigación histórica*, 20 (2003), pp. 133-154.

J. GÓMEZ, *Matemáticas, espías y piratas informáticos. Codificación y criptografía*, Barcelona, 2010.

J. HUXTABLE ELLIOTT, *España y su imperio en los siglos XVI y XVII*, en http://www.ignaciodarnaude.com/textos_diversos/Elliott,Espanya%20y%20su%20Imperio%20en%20los%20siglos%20XVI%20y%20XVII.pdf [consultado el 20 de junio de 2013].

G. LOHMANN, Guillermo, "Documentos cifrados indianos", *Revista de Indias*, 15 (1995), pp. 225-282.

R. NARVAÉZ, Roberto, "Historia y Criptología: reflexiones a propósito de dos cartas Cortesianas", *Anales del Museo Nacional de Arqueología, Historia y Etnografía*, 3 (1925), pp. 436-443.

J. ORTEGA TRIGUERO, M. Á. LÓPEZ GUERRERO y E. GARCÍA DEL CASTILLO, *Introducción a la criptografía historia y actualidad*, Cuenca, 2006.