DE LOS PRIMEROS MENSAJES CIFRADOS A LA CIBERSEGURIDAD

Autora: Marina Pérez Valverde

Tutor: Ignacio Sánchez Blanco

Departamento: Matemáticas

IES Gerardo Diego, Curso 2023-2025

AGRADECIMIENTOS:

A mi tutor, Nacho, por cada pregunta respondida cada vez que estaba perdida y no sabía cómo continuar, gracias por tu paciencia y dedicación.

Agradecerle también a toda mi familia por darme ánimos durante todas las fases del proyecto. Y a mis amigos que me acompañan desde siempre.

ÍNDICE

1. Resumen

A lo largo de la historia, la criptografía ha sido utilizada para proteger mensajes en tiempos de guerra y en contextos confidenciales.

Uno de los primeros métodos de cifrado fue el Atbash, mencionado en la Biblia. En Esparta se utilizó la escítala lacedemonia. Otro avance importante lo llevó a cabo Julio César, que empleó un cifrado simple de desplazamiento, conocido como cifrado César, cuya base es la aritmética modular (fundamental también en la criptografía actual). En la Alta Edad Media ya había tres métodos fundamentales de encriptación: transposición, sustitución y ocultación. Más adelante, durante el Renacimiento, la criptografía evolucionó con métodos como el cifrado Alberti o la tabla de Vigenère. En el siglo XVIII, durante la guerra de la independencia de los Estados Unidos, se desarrolló el cilindro de Jefferson y, más tarde, durante la segunda guerra mundial, la criptografía jugó un papel crucial con la creación de la máquina enigma.

Actualmente, con la aparición de ordenadores y los avances tecnológicos, la criptografía ha pasado a estar presente en todos los ámbitos relacionados con la información, las redes sociales o la banca electrónica.

Todavía queda mucho por explorar e investigar en este campo ya que la criptografía cuántica supondrá un avance significativo.

2. Abstract

Throughout history, cryptography has been used to protect messages in times of war and in confidential contexts.

One of the first encryption methods was Atbash, mentioned in the Bible. In Sparta the Lacedaemonian Scythal was used. Another important advance was carried out by Julius Caesar, who used a simple displacement cipher, known as the Caesar cipher, whose basis is modular arithmetic (also fundamental in current cryptography). In the Early Middle Ages there were already three fundamental methods of encryption: transposition, substitution and concealment. Later, during the Renaissance, cryptography evolved with methods such as the Alberti cipher or the Vigenère table. In the 18th century, during the

American War of Independence, the Jefferson cylinder was developed and later, during World War II, cryptography played a crucial role with the creation of the enigma machine.

Currently, with the appearance of computers and technological advances, cryptography has become present in all areas related to information, social networks, electronic banking, etc.

There is still much to explore and research in this field as quantum cryptography will be a significant advance.

3. Introducción

La criptografía es una disciplina fundamental para proteger la información mediante códigos y cifras. A lo largo de la historia, ha sido una herramienta clave para asegurar la confidencialidad y la privacidad de los mensajes. Desde las primeras civilizaciones, que utilizaban métodos rudimentarios de cifrado, principalmente para asegurar las comunicaciones en las guerras, hasta los avanzados algoritmos criptográficos modernos, que son cruciales para garantizar la privacidad y seguridad de los datos, esta disciplina ha evolucionado significativamente, y, en gran medida, su desarrollo ha estado profundamente vinculado a las matemáticas.

Este proyecto explora la historia de la criptografía, desde sus orígenes hasta su papel en el mundo digital actual, haciendo hincapié en las matemáticas que sustentan los sistemas criptográficos más relevantes. Desde la utilización de técnicas como el cifrado de sustitución en la antigua Roma, pasando por el cifrado de Enigma en la Segunda Guerra Mundial, hasta los modernos esquemas de cifrado asimétrico basados en la teoría de números, la criptografía ha dependido de principios matemáticos clave como la aritmética modular y la complejidad computacional.

A lo largo de este proyecto, se hará un recorrido por los distintos hitos históricos relacionados con la criptografía y se analizará el papel de las matemáticas en alguno de los métodos de cifrado más relevantes.

4. Estado de la cuestión

La información es uno de los recursos más valiosos hoy en día, mientras que la desinformación puede ser una de las peores armas. Por esa razón, en la sociedad actual, la seguridad en las comunicaciones y en internet es fundamental. Sin embargo, esta necesidad de estar protegido o de ocultar información a otras personas no es nada nuevo. A lo largo de nuestra historia, se ha hecho un amplio uso de la criptografía. Figuras históricas como Thomas Jefferson, quien ideó un sistema de cifrado en 1795, y la creación del "Cabinet Noir" en Francia, demuestran la importancia de la criptografía en la política y la guerra.

Numerosos expertos e investigadores colaboran en redes y comunidades invisibles de publicaciones para desarrollar nuevas líneas de investigación en el ámbito de la criptografía. Dentro de este amplio conjunto, destacan especialmente:

- **David Khan** es escritor, periodista e historiador estadounidense, especializado en criptografía. Su obra más importante, "The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet", publicada por primera vez en 1967, es una referencia fundamental en el campo de la criptografía. Este libro ofrece una visión detallada de la historia y evolución de la criptografía a lo largo de los siglos.

  Dentro de los principales temas de estudio de Khan encontramos la historia antigua de la criptografía, su desarrollo en la Edad Media y el Renacimiento, la era de los grandes cifrados, la revolución industrial y el siglo XIX, la criptografía en el siglo XX y finalmente, la era de la información.

  Además de su obra más conocida, "The Codebreakers", Kahn ha escrito otras obras importantes sobre criptografía e inteligencia militar. Algunas de sus obras más destacadas incluyen:
  - “Seizing the Enigma: The race to break the german U-boats codes, 1939-1943” (1991).
  - "Hitler's Spies: German Military Intelligence in World War II" (1978).
  - "The Reader of Gentlemen’s Mail: Herbert O. Yardley and the Birth of American Codebreaking" (2004).
  - "Kahn on Codes: Secrets of the New Cryptology" (1983).

- **Dr. Jorge Ramió Aguirre**, experto en criptografía y seguridad de la información, conocido por su contribución significativa en la educación, investigación y divulgación de estos campos. Es el coordinador de la Red Telemática Iberoamericana de Criptografía y Seguridad de la Información (CriptoRed), además de profesor en la Universidad Politécnica de Madrid. El objetivo de CriptoRed es que el conjunto de países Iberoamericanos (Latinoamérica, España y Portugal) estén integrados en ella con representantes de sus universidades, centros de investigación, instituciones y empresas. El fin, una comunidad científica virtual que difunde en su sitio Web sus conocimientos sobre seguridad informática.

  Además, ha publicado numerosos libros y artículos científicos sobre criptografía y seguridad de la información. La mayoría de sus escritos son electrónicos y recientemente ha actualizado su último libro electrónico "*Seguridad Informática y Criptografía en Diapositivas*". También ha desarrollado y enseñado cursos en línea masivos y abiertos (MOOC) sobre criptografía, llegando a miles de estudiantes a nivel global y es el fundador de la plataforma educativa Crypt4you, que ofrece cursos gratuitos sobre criptografía.

  En pocas palabras, Jorge Ramió Aguirre ha sido ampliamente reconocido por su capacidad para hacer accesibles los complejos temas de la criptografía y la seguridad de la información. Su trabajo ha inspirado a nuevas generaciones de criptógrafos y profesionales de la seguridad y ha contribuido significativamente a la educación y divulgación de estos temas a nivel global.

- **Luis Hernández Encinas**, es licenciado y doctor en matemáticas por la universidad de Salamanca y profesor de investigación en el Grupo de investigación en Criptología y Seguridad de la Información (GiCSI) del Consejo Superior de Investigaciones Científicas (CSIC), en Madrid. Sus áreas de investigación abarcan la criptología pre y post-cuántica, los protocolos de firma digital, autenticación e identificación, la criptobiometría y la teoría de números. Ha participado en más de 50 proyectos de investigación, tanto a nivel nacional como internacional. Es autor de varios libros y patentes, además de haber publicado más de 200 artículos en revistas especializadas y realizado más de 150 contribuciones en congresos. Ha dirigido múltiples tesis doctorales y forma parte de varios comités nacionales e internacionales en temas de seguridad y ciberseguridad, actuando como asesor criptológico para organismos de

seguridad del Estado. Dentro de sus libros destacamos "La criptografía", publicado en 2016 por la editorial Catarata y CSIC. Trata desde la criptografía clásica hasta los usos actuales y tendencias futuras de este campo.

En la actualidad, son las grandes potencias mundiales las que realizan una mayor investigación en el campo de la criptografía, puesto que donde más se investiga y se necesita es en el sector militar. Aun así, hoy en día se utilizan los criptosistemas para proteger información civil, pues en esta era en la que la información es dinero y poder, es necesario evitar la intercepción y desciframiento de esta.

5. Objetivos

El propósito principal de este trabajo es explorar la evolución histórica de la criptografía y estudiar los fundamentos matemáticos de alguno de los métodos criptográficos más relevantes.

Para ello, haremos un recorrido a lo largo de los hitos clave en la historia de este campo, desde sus orígenes en las civilizaciones antiguas hasta las técnicas avanzadas en la era digital y profundizando en algunos conceptos matemáticos como la aritmética modular, el algoritmo de Euclides o el Teorema de Euler. De esta forma, se ve la clara relación entre los avances matemáticos y los criptográficos.

Además, muestra cómo muchos de los conceptos tratados en el proyecto han impactado en la actualidad, siendo fundamentales en multitud de procesos cotidianos como firmas electrónicas, certificados digitales o el DNI electrónico, entre otros.

En definitiva, este estudio tiene como objetivo acercarnos al interesante y complejo mundo de la criptografía. Además, ofrece la oportunidad de explorar métodos y herramientas diseñados para garantizar la seguridad y confidencialidad en la transmisión de mensajes, a la vez que se analizan los métodos utilizados para asegurar la privacidad en estas comunicaciones.

6. Introducción a la criptografía, criptología y criptoanálisis

La criptología (del griego kryptós, "escondido" y logos, "estudio") es la disciplina que se dedica al estudio de la escritura secreta, es decir, estudia los mensajes que, procesados de cierta manera, se convierten en difíciles o imposibles de leer por personas no autorizadas.

Como disciplina fundamental en el ámbito de la seguridad de la información, desempeña un papel crucial en la protección de datos sensibles y en la garantía de la confidencialidad en las comunicaciones. Es decir, se enfoca en 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 comunicaciones. Esta disciplina se divide en dos principales ramas: la criptografía (del griego kryptós, “escondido” y graphos, “escritura”), encargada del proceso de cifrado de mensajes en clave y del diseño de sistemas criptográficos (de los cuales hablaremos más adelante), y el criptoanálisis (del griego kryptós, “escondido” y analyein, “desatar”), que se dedica a descifrar los mensajes en clave, con el objetivo de vulnerar el criptosistema.

Definir qué es la criptografía es realmente difícil puesto que, al haber tenido tantas aplicaciones a lo largo de la historia, una definición podría contradecir a otra, siendo ambas correctas. Según la Real Academia Española, la criptografía es “el arte de escribir con clave secreta o de un modo enigmático”.

Esta definición nos da una idea general de que la criptografía es una disciplina que se ocupa de la protección de información a la hora de transmitir un mensaje, el cual es un “enigma”, puesto que se utilizan códigos únicamente conocidos por el emisor y el receptor. No obstante, debemos añadir que en la actualidad su principal uso no está tan orientado a la transmisión de mensajes secretos sino más bien a la protección de la información.

Podemos dividir la criptografía en:

- Criptografía simétrica: aquella en la que se usa la misma clave para el cifrado y descifrado de un texto. Esta clave es compartida con los interlocutores de manera segura antes de comenzar la comunicación.
- Criptografía asimétrica: se usan dos claves diferentes para cifrar y descifrar el mensaje. Normalmente, la clave pública se usa para encriptar el mensaje y la privada para descifrarlo.

- Criptografía hash: se genera un solo valor que simboliza un texto o conjunto de datos. Son claves únicas, generadas con un algoritmo. Estas claves generadas no son reversibles: simplemente se emplean para verificar que los archivos y mensajes no han sufrido alteraciones, asegurando así su integridad.
- Criptografía de ofuscación: esta metodología es más directa en comparación con la anterior, ya que implica ocultar el texto sin la generación explícita de una clave. Se logra alterando el lenguaje original del mensaje para volverlo ininteligible. Aunque esta técnica no previene completamente los ataques, los ralentiza, por lo que puede resultar útil en ciertos contextos.

Por otro lado, el criptoanálisis es la ciencia opuesta a la criptografía (aunque podría ser más apropiado considerarlas complementarias en vez de opuestas), ya que trata de resolver los sistemas de cifrado, revelando su vulnerabilidad. En otras palabras, trata de descifrar los criptogramas. El concepto de descifrar típicamente desencadena debates técnicos, aunque en este contexto asumiremos que se refiere a obtener el texto claro a partir de un criptograma, evitando entrar en controversias sobre la reversibilidad y la solidez de los criptosistemas.

Para evaluar posibles debilidades en un sistema de cifrado, se deben tener en cuenta las condiciones del peor caso, esto es: si el criptoanalista tiene acceso total al algoritmo de cifrado, si tiene una considerable cantidad de texto cifrado, o si conoce el texto claro de parte de ese texto cifrado, es muy probable que el sistema sea de fácil ataque y, por lo tanto, no sea seguro.

También se deben tener en cuenta los Principios de Kerckhoffs. Como veremos más adelante, estos principios establecen que la seguridad del cifrado depende exclusivamente de la clave secreta y no del algoritmo.

Si bien los criptosistemas suelen ser evaluados bajo estas condiciones del peor caso, existen también ataques más específicos donde no se cumplen todas estas condiciones. El ataque de fuerza bruta, donde se prueban todas las posibles claves hasta encontrar la correcta, es uno de ellos.

7. Historia

Como ha sido mencionado anteriormente, la criptografía no es una disciplina moderna, sino que ha sido usada desde tiempos muy antiguos. Hagamos un recorrido a lo largo de su historia.

7.1. Primera transformación de un texto

La evidencia más antigua conocida del uso de alguna forma de la criptografía se descubrió en una inscripción tallada alrededor del año 1900 a.C., ubicada en la cámara principal de la tumba del noble Khnumhotep II en Egipto. En esta inscripción, el escriba empleó símbolos jeroglíficos inusuales en lugares específicos en vez de los más comúnmente utilizados. El propósito no era ocultar el mensaje, sino posiblemente alterarlo de manera que resultara más decoroso. Aunque la inscripción no constituía una escritura secreta, transformó el texto original, siendo el ejemplo más antiguo conocido de este tipo de práctica.

Ciertamente no lo podemos considerar como el inicio de la criptografía, pero sí es cierto que es un hito importante pues, a partir de este momento, ya se pueden encontrar claros ejemplos del uso de mensajes cifrados.

7.2. La Biblia- Atbash

La Biblia hace referencias al Atbash, un método de codificación del alfabeto hebreo, utilizado entre el 600 y 500 a.C. Este sistema reemplaza las letras aplicando la siguiente regla a modo de clave: en un alfabeto de n letras, se sustituye la que ocupa la posición i por la que se encuentra en la posición n-i+1 en el mismo alfabeto. Por lo tanto, este método aplicado a nuestro alfabeto sería así:

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

Tabla 1- Cifrado Atbash.

Lo sorprendente del Atbash es que lo podemos encontrar en la biblia hebrea, concretamente en el Libro de Jeremías, capítulo 25, versículo 26 (Jr 25, 26): *"y todos los reyes del norte que están cerca y lejos, uno tras otro, y todos los [demás] reinos de la*

tierra que están sobre la superficie del suelo; y el mismo rey de ***Sesac*** *beberá después de ellos."* Se menciona a **Sesac** que es en realidad el nombre encriptado por el método mencionado anteriormente de Babel (Babilonia). Además, se repite más tarde en el capítulo 51, versículo 41 de este mismo libro.

Normal:	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
Inverso:	ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

Figura 1- Atbash, alfabeto hebreo invertido.

La razón por la que se tuvo que encriptar el mensaje fue porque el Libro de Jeremías fue redactado tanto en Judá como en Egipto, en el año 625 a.C. Ese mismo año, Nabucodonosor derrotó al faraón egipcio Nekó, asegurando el control sobre Judá. Jehoiaquin fue designado como rey por Nabucodonosor, pero tres años después fue derrocado al rebelarse.

En este contexto, cuando Jeremías escribió la profecía acerca de Babilonia, cuyo rey era Nabucodonosor, este último tenía autoridad sobre Judá. En consecuencia, Jeremías estaba expuesto a represalias por parte del rey si se enteraba de que profetizaba su caída.

7.3. La escítala

En Esparta, alrededor del siglo V a.C. se vivían periodos de guerras y surgió la necesidad de comunicarse de forma segura. Los espartanos usaban la criptografía para proteger sus mensajes. Crearon un método que consistía en enrollar una cinta a lo largo de una vara de madera. Así inventaron la escítala lacedemonia, con un propósito únicamente militar. El emisor escribía el mensaje horizontalmente sobre la vara y al desenrollarla se creaba un mensaje oculto. En este caso, la clave para descifrar el mensaje es tener una escítala del mismo diámetro, de tal forma que, una vez enrollada la cinta por parte del receptor, se pudiera leer el mensaje. En caso contrario, el mensaje continuaría siendo ilegible. Así pues, la escítala es un método criptográfico de transposición o permutación, que consiste en cambiar de lugar los elementos del texto claro.

La escítala fue el primer sistema criptográfico militar de la historia, que aparte de por los espartanos, fue utilizado por Alejandro Magno (356-323 a.C.)

Figura 2- Escítala espartana.

7.4. Cifrado de Polibio

Muchos autores no consideran el método de Polibio como verdadera criptografía puesto que no pretende ocultar información sino transmitirla de manera más eficaz. Aun así, su estudio es interesante pues sus ideas se utilizan en criptografía.

La cifra de Polibio es históricamente la primera que emplea el sistema de sustitución. En este caso, se asigna a cada letra una pareja de números, tal y como se indica en la tabla 2. En este cifrado, con tan solo 5 números, se puede escribir cualquier mensaje, pero tiene un problema: el mensaje cifrado es el doble de largo que el texto original.

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i/j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Tabla 2- Cuadrado de Polibio 1.

A modo de ejemplo, con el alfabeto español, vamos a coger el mensaje “mariposa”, que correspondería al siguiente criptograma (como solo se pueden utilizar 25 letras, la *i* y la *j* se sustituyen por la *j*): “32 11 42 24 35 34 43 11”

Por otra parte, para establecer una clave en este sistema, basta con elegir una palabra cualquiera y colocar sus letras al principio de la tabla; después se escriben las letras restantes del alfabeto en orden. Si cogemos la palabra “bosque” como clave, el mensaje anterior pasaría a ser: “41 22 44 33 43 12 13 22”

	1	2	3	4	5
1	b	o	s	q	u
2	e	a	c	d	f
3	g	h	j	k	l
4	m	n	p	r	t
5	v	w	x	y	z

Tabla 3- Cuadrado de Polibio 2.

7.5. Cifrado César

Otro de los métodos más antiguos es el cifrado César o cifrado por desplazamiento. Es un método simple de cifrado simétrico basado en la sustitución. Julio César (100 a.C. - 44 a.C.) empleó un método de cifrado bastante sencillo para comunicaciones confidenciales con sus generales.

En su origen, en el cifrado César se reemplazaba cada letra del alfabeto con la letra que se encuentra tres posiciones adelante. Se podría decir que la clave es el número tres. Actualmente se considera cifrado César cualquier método de sustitución por desplazamiento y la clave puede variar desde el 0 hasta el 26.

De forma matemática, el método de Julio César funciona de la siguiente manera:

1. Se le asignan números del 0 al 26 al abecedario:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Tabla 4- Alfabeto cifrado César.

2. Se sustituye cada letra de nuestro mensaje con su número correspondiente:

v	e	n	i	v	i	d	i	v	i	c	i
22	4	13	8	22	8	3	8	22	8	2	8

Tabla 5- Mensaje sin cifrar.

3. Aplicamos la regla de Julio César sumando 3 a cada número:

22	4	13	8	22	8	3	8	22	8	2	8
+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3	+3
25	7	16	11	25	11	6	11	25	11	5	11

Tabla 6- Cifrando mensaje.

4. Sustituimos los números obtenidos por las letras correspondientes:

25	7	16	11	25	11	6	11	25	11	5	11
y	h	p	l	y	l	g	l	y	l	f	l

Tabla 7- Mensaje cifrado.

5. Se envía el mensaje: YHPLYLGLYLFL.

Para que el receptor pueda descifrar el mensaje, debe conocer la clave y aplicar lo explicado anteriormente, pero de forma inversa, de tal manera que en vez de sumar habría que restar 3 y por último sustituir cada número por su letra correspondiente. De esta forma, se obtendría el mensaje descodificado.

Teóricamente, una persona no autorizada no podía descifrar el mensaje sin la clave, pero con tan solo 27 intentos (con el alfabeto español) se podría descifrar, por lo que el método resulta poco seguro. Los ordenadores tardarían actualmente menos de un segundo en hacerlo.

Existe una clara correspondencia entre el cifrado César y la aritmética modular, también conocida como "aritmética del reloj". Estamos acostumbrados a operar con las horas de un reloj: si son las 7 de la mañana y pasan 6 horas, será la 1 de la tarde: $7\text{am} + 6 = 1\text{pm}$. De la misma manera, si son las 10 de la noche y pasan 4 horas, serán las dos de la

madrugada: $10\text{pm} + 4 = 2a\text{m}$. Esto conecta con el concepto matemático de congruencia:

Definición: $a \equiv b(mod\ n) \Leftrightarrow a - b = k \cdot n\ (k \in \mathbb{Z})$

Un número entero a es congruente a b módulo n sí y solo sí $a - b = k \cdot n$, siendo k un número entero.

Si tomamos por ejemplo $a = 53$ y $n = 14$

$$\begin{array}{r|l} 53 & 14 \\ \cline{2-2} 11 & 3 \end{array} \qquad 53 \equiv 11\ (mod\ 14), \text{ ya que } 53 - 11 = 3 \cdot 14$$

En el caso del cifrado César, el módulo es 27 ($n = 27$) ya que hay 27 letras en el abecedario. De esta manera: $27 \equiv 0\ (mod\ 27)$, $28 \equiv 1\ (mod\ 27)$ y $29 \equiv 2\ (mod\ 27)$. Además, es importante observar que cada número entero es congruente solamente a un número del conjunto $\mathbb{Z}_{27} = \{0, 1, 2, \ldots, 26\}$, esto es, el conjunto de posibles restos al dividir el número entre 27.

En el cifrado anterior la clave es "sumar 3" y es evidente que -3 descifra a +3. Es decir, toda clave de cifrado tiene clave de descifrado y además podemos cifrar todos los elementos del conjunto inicial. En lugar de esta clave se podría haber usado la clave "sumar n" para cada n perteneciente a $\mathbb{Z}_{27}$, excluyendo el 0.

Como una forma de modificar el cifrado César, podríamos intentar reemplazar operación "sumar" por "multiplicar". Para explorar esta variante veamos dos ejemplos:

Ejemplo 1: seleccionamos la clave "multiplicar por 5":

Letra	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
Código numérico	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Multiplicar por 5 (mod 27)	0	5	10	15	20	25	3	8	13	18	23	1	6	11	16	21	26	4	9	14	19	24	2	7	12	17	22
Letra cifrada	A	F	K	O	T	Y	D	I	N	R	W	B	G	L	P	U	Z	E	J	Ñ	S	X	C	H	M	Q	V

Tabla 8- Multiplicación cifrado César 1.

Aparentemente, multiplicando por 5, este cifrado funcionaría: todas las letras quedan cifradas de forma única.

Ejemplo 2: seleccionamos la clave "multiplicar por 9":

Letra	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
Código numérico	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Multiplicar por 9 (mod 27)	0	9	18	0	9	18	0	9	18	0	9	18	0	9	18	0	9	18	0	9	18	0	9	18	0	9	18
Letra cifrada	A	J	R	A	J	R	A	J	R	A	J	R	A	J	R	A	J	R	A	J	R	A	J	R	A	J	R

Tabla 9- Multiplicación cifrado César 2.

En este caso, hay un problema: al multiplicar por 9, las letras cifradas se repiten. Esto no puede pasar: varias letras quedarían cifradas de la misma forma, lo que haría imposible descifrar un mensaje a pesar de conocer la clave.

¿Por qué funcionan unos números y otros no? Si comprobamos con todos los números entre el 1 y 26, nos damos cuenta de que la multiplicación funciona con todos ellos excepto con el 3, 9, 12, 15, 18, 21 y 24. Todos estos números tienen factores comunes con el 27, por lo que aparentemente el sistema funciona con todos aquellos números que son primos relativos con el 27. Veamos por qué:

- **Proposición**: si MCD $(a, n) = 1$, los siguientes restos son todos distintos módulo n: $a, 2a, 3a, \dots, (n-1)a$. Es decir, barremos todos los posibles restos.

  Demostración:

Supongamos que hay dos iguales y veamos que llegamos a una conclusión absurda. Es decir, supongamos que existen x, y con $0 < x < y < n$ tales que:

$$ay \equiv ax\ (mod\ n) \Rightarrow ay - ax = kn\ ;\ \mathrm{k} \in \mathbb{Z} \Rightarrow a(y-x) = kn\ ;\ \mathrm{k} \in \mathbb{Z}$$

Como MCD $(a, n) = 1 \Rightarrow n$ es divisor de $y - x$, lo cual es imposible ya que

$0 < y - x < n$, por lo que quedaría demostrada la proposición.

- **Algoritmo de Euclides**: El algoritmo de Euclides es una forma alternativa de calcular el MCD de dos números. Si consideramos la división:

$$\begin{array}{c|c} a & b \\ \hline r & q \end{array} \quad \Rightarrow \quad \mathrm{MCD}\ (a, b) = \mathrm{MCD}\ (b, r)$$

  Como b y r son a su vez enteros, también existen q_1 y r_1 tales que $b = rq_1 + r_1$ y podremos repetir el proceso hasta obtener un resto 0. Lo que nos dice el algoritmo de Euclides es que el último resto obtenido distinto de 0 es el máximo común divisor de a y b.

Este procedimiento no solo es útil y rápido cuando *a* y *b* son números muy grandes, sino que nos permite escribir el MCD (*a, b*) como una combinación lineal de *a* y *b*. Para ello, basta invertir los pasos realizados, como podemos ver en el siguiente ejemplo:

Ejemplo: vamos a calcular el MCD de $a = 14$ y $n = 9$ y a expresarlo como combinación lineal de 14 y 9:

$$\begin{array}{r|l} 14 & 9 \\ \hline 5 & 1 \end{array} \qquad 14 = 9 \cdot 1 + 5$$

$$\begin{array}{r|l} 9 & 5 \\ \hline 4 & 1 \end{array} \qquad 9 = 5 \cdot 1 + 4$$

$$\begin{array}{r|l} 5 & 4 \\ \hline 1 & 1 \end{array} \qquad 5 = 4 \cdot 1 + 1$$

Por tanto, el MCD $(14, 9) = 1$ ya que en la siguiente división el resto sería 0.

Vamos a expresar este MCD como combinación lineal de 14 y 9. De las expresiones anteriores se deduce lo siguiente:

- $5 = 14 \cdot 1 + 9 \cdot (-1)$
- $4 = 9 \cdot 1 + 5 \cdot (-1) = 9 \cdot 1 + \big(14 \cdot 1 + 9 \cdot (-1)\big) \cdot (-1) = 14 \cdot (-1) + 9 \cdot 2$
- $1 = 5 \cdot 1 + 4 \cdot (-1) = \big(14 \cdot 1 + 9 \cdot (-1)\big) + \big(14 \cdot (-1) + 9 \cdot (2)\big) \cdot (-1) =$

$$= 14 \cdot 2 + 9 \cdot (-3)$$

Con lo que el MCD queda expresado como combinación lineal de 14 y 9. Este resultado se conoce como Identidad de Bézout: MCD $(a, b) = xa + yb;\ \text{con}\ x, y \in \mathbb{Z}$

- **Corolario** (existencia y cálculo del inverso multiplicativo):

Hemos visto que si MCD $(a, n) = 1$, podemos hallar dos números x, y tales que:

$$xa + yn = 1$$

Esta expresión nos permite además calcular el inverso de a módulo n ya que:

$$xa + yn = 1 \Rightarrow xa - 1 = kn\ (k \in \mathbb{Z}) \Rightarrow xa \equiv 1\ (mod\ n)$$

Es decir, x es el inverso de a módulo n (el número que al multiplicarlo por *a* da 1 módulo *n*). Por lo tanto, el algoritmo de Euclides permite hallar dicho inverso. Volviendo al

ejemplo anterior, si $1 = 2 \cdot 14 + 9 \cdot (-3)$, deducimos que 2 es el inverso de 14 módulo 9 y que -3 es el inverso de 9 módulo 14. Efectivamente:

$$2 \cdot 14 = 28 \equiv 1 \ (mod\ 9)$$

$$-3 \equiv 11 \ (mod\ 14); 11 \cdot 9 = 99 \equiv 1 \ (mod\ 14)$$

Por tanto, no solo hemos demostrado que si MCD $(a, n) = 1$ existe inverso, sino que lo hemos calculado.

7.6. Edad Media

La criptografía en la Edad Media se desarrolló en un contexto en el que la comunicación segura era de gran importancia, especialmente en ámbitos militares y diplomáticos. Aunque no se encontraban tecnologías avanzadas como las de hoy en día, la necesidad de proteger la información confidencial llevó al desarrollo de métodos criptográficos rudimentarios pero efectivos.

Durante esta época, se produjo una significativa revolución en el ámbito de la criptografía en el mundo árabe. En el siglo IX, Al-Kindi sentó las bases esenciales del criptoanálisis mediante el estudio del Corán, específicamente la técnica del análisis de frecuencias. Este método se basa en la observación de que, en cualquier idioma, algunas letras aparecen con mayor frecuencia que otras. Al estudiar la frecuencia de las letras en un mensaje cifrado, es posible hacer conjeturas sobre las sustituciones y, finalmente, descifrar el mensaje sin contar con la clave correspondiente. Ibn al-Durayhim y Ahmad al-Qalqashandi también se adentraron en los análisis de frecuencias, contribuyendo al desarrollo de códigos más resistentes al aplicar múltiples sustituciones posibles a cada letra de un mensaje, lo que quebrantaba los patrones aprovechados en este tipo de cifrados. Sin embargo, es en el siglo XIII cuando la criptografía empezó a tomar forma y a desarrollarse, principalmente bajo la influencia del Papado en las ciudades italianas.

Durante la Alta Edad Media, se empleaban tres métodos fundamentales de encriptación:

1. Transposición: este sistema ya había sido usado anteriormente por los espartanos con la escítala. Consiste en colocar el soporte físico donde se encuentra el texto cifrado en un lugar conocido por el destinatario del mensaje (como la cinta de la escítala). Este cifrado podía implicar alterar el orden natural de letras, sílabas o

palabras, a veces creando anagramas con ellas. Es decir, en lugar de reemplazar letras, en este método, se cambia el orden de las letras en el mensaje. Para revertir el orden y poder leer el mensaje correctamente hace falta una clave conocida por el receptor.

2. Sustitución: se trata de reemplazar ciertas letras del alfabeto con otros símbolos previamente acordados entre el emisor y el receptor, ya fueran números, otras letras o símbolos de otros alfabetos. Un ejemplo de este método es el cifrado César, mencionado previamente.
3. Ocultación: se basa en transmitir un mensaje de manera escondida o disfrazada dentro de un texto, por ejemplo, mediante el uso de tinta invisible.

En los reinos europeos altomedievales, el método predominante fue la sustitución, y existen numerosos ejemplos de su aplicación. Un caso destacado es el de Carlomagno. Carlomagno utilizaba estas técnicas principalmente para proteger correspondencia diplomática, instrucciones militares y documentos oficiales que requerían un alto nivel de confidencialidad. Dado que la alfabetización estaba restringida y los métodos de criptografía eran básicos, incluso una simple tabla de sustitución podía ser efectiva para mantener la seguridad de la información.

La cancillería carolingia empleó varios métodos de cifrado. Uno de ellos, ya mencionado anteriormente, es el cifrado César. También desarrollaron un método donde cada letra del alfabeto se sustituye por otra según una tabla predeterminada. Por ejemplo, la letra “A” podría sustituirse por cualquier otra letra establecida en la tabla, pero una vez establecido el alfabeto, este se mantenía fijo. Es decir, si la “A” se sustituía por la “M”, sería así durante todo el cifrado hasta que se cambiara la tabla.

Es posible que la cancillería carolingia tuviera sus propias tablas de sustitución personalizadas, donde las correspondencias entre las letras del alfabeto fueran acordadas de manera específica y conocidas solo por los escribas y funcionarios autorizados. Estas tablas podrían haber sido diseñadas para no seguir un patrón obvio (como en el cifrado César) para dificultar su ruptura por terceros. Además, estas tablas incluían otros símbolos específicos para representar ciertas letras o palabras comunes, haciendo que el cifrado fuera un poco más complejo y menos predecible.

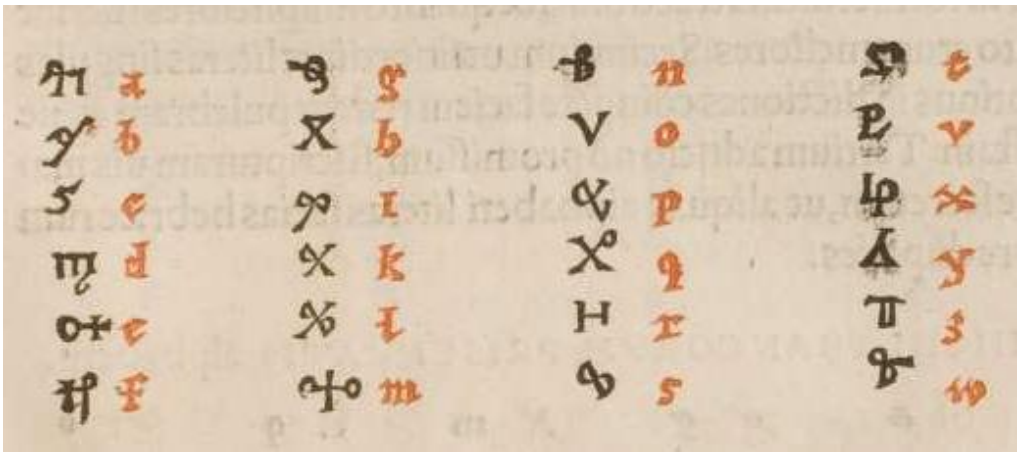

Figura 3-Tabla sustitución cancillería carolingia.

7.7. Criptografía en la escritura visigótica

En la península Ibérica, durante la Alta Edad Media, la escritura predominante en los documentos oficiales era la escritura visigótica, originada en el reino visigodo. Se encuentran ejemplos de métodos criptográficos en esta escritura, especialmente mediante el uso del sistema de sustitución. El método más conocido consiste simplemente en escribir las letras de forma diferente, utilizando una tabla, de manera similar al código de Carlomagno.

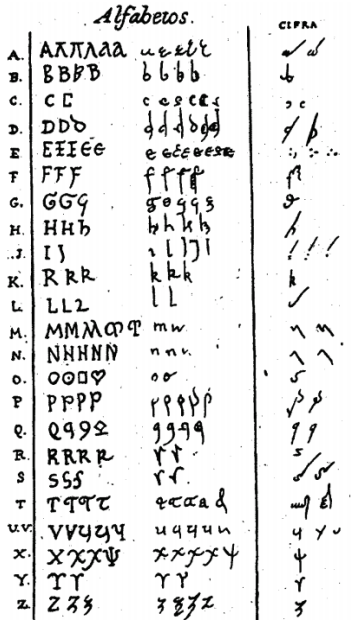

Figura 4- Tabla sustitución visigoda.

Aparte de esta tabla, existen otros métodos bastante imaginativos como el de sustituir las vocales por su numeral romano en decenas. (la vocal ***a*** se sustituye por *X* (10 en números romanos), la ***e*** por *XX* (20) y así sucesivamente. También reemplazaban las vocales por

grafías de puntos, sustituían las letras latinas por griegas o escribían al revés ciertas sílabas, palabras, oraciones o párrafos completos.

Es importante destacar que, aunque estos métodos eran relativamente simples en comparación con la criptografía moderna, cumplían su propósito en un contexto donde la mayoría de las personas no estaban familiarizadas con las técnicas de descifrado y la comunicación era principalmente oral o escrita a mano. La criptografía en la Edad Media jugó un papel crucial en la protección de la información en un mundo donde la seguridad de las comunicaciones era esencial para el éxito en diversos ámbitos.

7.8. El Renacimiento

Durante el Renacimiento, los Estados Pontificios destacaron por su intensivo uso de la criptografía. Leon Battista Alberti, quien ejerció como secretario personal de tres Papas, se erigió como una figura clave de la época en esta disciplina. Alberti, al igual que destacados criptógrafos como Ibn al-Durayhim y Ahmad al-Qalqashandi, se dedicó al desarrollo del cifrado polialfabético y creó un sistema de codificación mecánica basado en discos, conocido como el cifrado de Alberti. También en esta época destaca Johannes Trithemius con su tratado Polygraphia y Blaise de Vigenère con su cuadro de cifrado.

7.8.1. Cifrado Alberti

Este cifrado consiste en dos discos concéntricos, uno más grande que el otro, montados sobre un eje común, de tal forma que ambos pueden girar de manera independiente.

El disco externo es el más grande, está fijo y tiene grabado el alfabeto latino en mayúsculas, ordenado de forma convencional, junto con las cifras 1, 2, 3 y 4 al final. Mientras que el disco interno, es más pequeño y móvil, tiente también grabado el mismo alfabeto en minúsculas, pero de forma desordenada y al final, en vez de cuatro números, tiene el símbolo '&' y las letras 'h', 'k' e 'y'.

De esta manera, el usuario puede alinear, mediante la rotación del anillo móvil, el alfabeto del círculo superior con tantos alfabetos del círculo inferior como giros específicos del anillo realice, con un límite máximo igual al número de caracteres del alfabeto utilizado. Por lo tanto, el número de alfabetos diferentes utilizables en un disco de Alberti es de 24.

Figura 5- Disco de Alberti.

La clave del sistema está definida por el orden de los símbolos del anillo móvil y por la posición inicial de ambos anillos. Por eso las operaciones que realiza el receptor son inversas a las del emisor.

Para cifrar un mensaje, el usuario primero debe alinear los discos de acuerdo con una clave inicial. Por ejemplo, la letra "A" del disco externo podría alinearse con la letra "g" del disco interno. Una vez que los discos están alineados, el usuario selecciona una letra del mensaje original (texto claro) en el disco externo y encuentra la letra correspondiente en el disco interno. Esta letra es la que se escribe como parte del mensaje cifrado.

Por ejemplo, con la clave inicial mencionada anteriormente, si el mensaje que se quiere enviar es “VIGILAR”, el mensaje que se enviaría sería “hvtvzgm” como se puede observar en la figura 6.

Después de cifrar una o varias letras, el usuario puede girar el disco interno para cambiar la correspondencia entre las letras, haciendo que el cifrado sea aún más complicado. Esto significa que una misma letra del texto claro puede cifrarse como diferentes letras en el texto cifrado, dependiendo de la alineación en ese momento.

Tanto el remitente como el destinatario deben compartir un "libro de códigos" que especifique el significado de cada código utilizado. Este libro de códigos contendría

palabras o frases de gran importancia dentro del contexto de uso del cifrado y que requieren una mayor seguridad.

Para el desencriptado, el receptor, que conoce la clave inicial y el método de rotación de los discos, puede revertir el proceso alineando los discos de la misma manera y descifrando cada letra.

Figura 6- Disco de Alberti cifrado.

Este cifrado representa un avance significativo porque introduce por primera vez en la historia la idea de cambiar los alfabetos de cifrado a lo largo del mensaje. Como resultado aumenta la seguridad y complejidad del cifrado en comparación con métodos anteriores.

7.8.2. Johannes Trithemius

Otra de las figuras clave de la criptografía de este periodo fue Johannes Trithemius, un monje alemán, conocido principalmente por sus contribuciones en los campos de la criptografía, el ocultismo y el misticismo cristiano.

Trithemius ganó reconocimiento por sus obras sobre criptografía, en particular con su tratado "Polygraphia", publicado en 1518. En esta obra, Trithemius ofrece una amplia gama de métodos para escribir y comunicarse de manera secreta. Estos métodos incluyen cifrados simples, como la sustitución de letras por símbolos o números, así como técnicas más avanzadas, como el uso de tablas y cuadrículas para codificar mensajes. También aborda el uso de códigos y símbolos ocultos en la comunicación escrita.

Lo que hace que "Polygraphia" sea particularmente interesante es que no solo se centra en la criptografía, sino que también explora la relación entre el conocimiento secreto y el poder. Argumenta que aquellos que dominan el arte de la escritura secreta tienen una ventaja sobre los demás, ya que pueden comunicarse de manera segura y discreta. Este trabajo sentó las bases para el estudio de la criptografía y la esteganografía (práctica de ocultar información dentro de otro mensaje u objeto físico para evitar su detección) y le valió a Trithemius un lugar en la historia como uno de los pioneros de los métodos de comunicación secreta.

7.8.3. Tabla Vigenère

En este mismo siglo, en Francia, nace otra de las figuras clave de la criptografía, Blaise de Vigenère. Su contribución al campo de la criptografía fue la "Tabla Vigenère" o "Cuadro de Vigenère".

La "Tabla Vigenère" es un método de cifrado polialfabético que mejora el cifrado de César al permitir que una palabra clave determine qué cifrado César se usa en cada letra del mensaje. Esto hizo que fuera mucho más difícil de romper que los métodos de cifrado anteriores.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	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	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S
U	V	W	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	W	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
W	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
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	W
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	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y

Figura 7- Tabla de Vigenère

Para cifrar un mensaje con el cifrado de Vigenère se utiliza la tabla de Vigenère (Figura 7) con una palabra clave. Cada letra del texto claro se cifra utilizando la fila de la tabla correspondiente a la letra de la palabra clave. El resultado es un texto cifrado más difícil de romper gracias al uso de múltiples alfabetos.

Supongamos que queremos cifrar el texto “CRIPTO” con la clave “KEY”:

1. Repetimos la palabra clave hasta llegar al mismo número de letras que las del texto claro:

   Texto claro: “C R I P T O”, tiene 6 letras.

   Clave: “K E Y K E Y”, repetimos hasta tener 6 letras.

2. Utilizar la tabla de Vigenère. Para cada letra del texto claro, utilizamos la correspondiente de la palabra clave para determinar que fila de la tabla usar.
   - Primera letra:

     Texto claro: “C”; buscamos esta letra en la segunda fila de la tabla.

     Clave: “K”; buscamos esta letra en la primera columna de la tabla.

     Letra cifrada: “M”

Para el resto de letras:

- Segunda letra: texto claro: “R”; clave: “E”; letra cifrada: “V”
- Tercera letra: texto claro: “I”; clave: “Y”; letra cifrada: “G”
- Cuarta letra: texto claro: “P”; clave: “K”; letra cifrada: “Z”
- Quinta letra: texto claro: “T”; clave: “E”; letra cifrada: “X”
- Sexta letra: texto claro: “O”; clave: “Y”; letra cifrada: “N”

Texto cifrado: MVGZXN

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	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	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S
U	V	W	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	W	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
W	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
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	W
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	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y

Tabla 10- Tabla de Vigenère, ejemplo.

A pesar de que su método original fue descifrado, el trabajo de Vigenère sentó las bases para futuras investigaciones en criptografía y su método sigue siendo estudiado como un hito importante en la historia de este campo.

7.8.4. Homófonos y nulos

El uso de homófonos y nulos en los sistemas criptográficos de sustitución se originó alrededor del Renacimiento, en los siglos XV y XVI, y se desarrolló en los siglos posteriores, especialmente en el ámbito militar y diplomático. Estas técnicas mejoraron la seguridad de los cifrados al hacerlos más resistentes al análisis de frecuencias.

Un homófono consiste en asignar múltiples símbolos a una sola letra. Por ejemplo, en un cifrado homofónico, la letra "E" (que es muy común en muchos idiomas) podría estar representada por varios símbolos diferentes en el mensaje cifrado, de modo que el análisis de frecuencias no pueda identificar fácilmente las letras más comunes.

Los nulos son símbolos que se insertan en el mensaje cifrado pero que no corresponden a ninguna letra o significado en el texto claro. Estos símbolos confunden aún más a los criptoanalistas al aumentar la cantidad de caracteres que deben descifrar sin aportar ninguna información útil.

7.9. Guerras de religión de Francia

Durante las guerras, surge la necesidad de una comunicación segura entre cada bando. Por eso la criptografía se convierte en una pieza esencial para los ejércitos de todo el mundo y los métodos de encriptado van evolucionando, buscando cada vez más seguridad. Este es el caso de las Guerras de religión francesas, una serie de conflictos entre partidos protestantes y católicos (1562-1598).

Durante estas guerras, descifrar los mensajes enemigos pasó a ser un objeto táctico, y en 1628, Antoine Rossignol se convertiría en uno de los criptógrafos más importantes del país.

Durante el asedio del Príncipe Condé a Realmont (un asentamiento protestante), se interceptaron mensajes cifrados enemigos. Para descifrarlos, Condé llamó a Rossignol, un matemático local aficionado a los cifrados. En tres horas, Rossignol descubrió que los hugonotes estaban sin municiones y pedían refuerzos. Condé utilizó esta información para invitarles a rendirse, lo cual hicieron inmediatamente. Tiempo después, Richelieu lo integró en la política estatal, donde siguió cifrando y descifrando mensajes, convirtiéndose en uno de los mejores criptoanalistas del siglo XVII.

Rossignol fue el creador de “La Gran Cifra”, un código que utilizaba un nomenclátor compuesto por dos tomos, uno para cifrar y otro para descifrar. Consistía en la correspondencia ente números y palabras de manera aleatoria, aunque constante para cada palabra, sílaba o forma gramatical. Por eso se necesitaba un libro para cifrar, donde las palabras estaban ordenadas alfabéticamente junto con su respectivo código numérico, y otro libro para descifrar, donde los números se correspondían con las palabras.

Por ejemplo:

1012 La
1013 Dejar
1014 Lorena
1013 1012 1014 = Dejar La Lorena.

En este sistema, 'La' siempre será 1012 y 'Dejar' será 1013, en cualquier mensaje. Otros ejemplos fueron: “Trampa” -4367-, “Piedra” -1025- y “Saquear” -6884-.

Tanto el hijo de Rossignol como su nieto continuaron su legado trabajando en el primer centro de criptología de Francia, conocido como el "Cabinet Noir" (“cámara negra”). Allí se abrían y leían de manera sofisticada las cartas de personas influyentes. La cámara fue tan criticada como usada durante la revolución francesa, tanto por los líderes revolucionarios como por Napoleón Bonaparte.

El secreto del código de Rossignol y los dos diccionarios se perdieron con la muerte de su nieto. No fue hasta finales del siglo XIX que el código fue descifrado. Gendron fue el primero en intentarlo sobre cinco documentos de Luis XIV, sin éxito. Luego recurrió al Mariscal Bazeries, un experto criptoanalista, quien tardó tres años en descifrarlo. Sus intentos iniciales, basados en criptografía homofónica y bigramas, no dieron resultado. Finalmente, observó secuencias repetidas de números, como 124 22 125 46 345, que identificó como algo común en los documentos militares, lo que relacionó con "les-en-ne-mi-es", en español “los enemigos”. Así, poco a poco, logró descifrar más palabras del rompecabezas de Rossignol.

7.10. El complot de Babington

El fallido complot de Babington es otro ejemplo del uso de mensajes cifrados. Dicho complot tuvo lugar en 1586 con el objetivo de asesinar a la reina Isabel I de Inglaterra y colocar en el trono a su prisionera María I de Escocia. En esta conspiración participó incluso el rey Felipe II de España con la intención de invadir Inglaterra.

El principal conspirador fue Anthony Babington, cuya mala suerte residió en enviar una carta codificada mediante una combinación de cifrado César y símbolos que representaban palabras a la prisionera María I de Escocia. Esta carta fue interceptada y

descifrada por Thomas Phelippes. Astutamente, Phelippes no intervino de inmediato; esperó a que María I respondiera con una nueva carta cifrada, a la cual añadió unas líneas cifradas por él mismo que decían: *"Me alegraría conocer los nombres y las cualidades de los seis caballeros que llevarán a cabo el plan; porque puede que, conociendo a los participantes, yo pueda daros algún consejo necesario para seguirlo en eso, así como de vez en cuando los particulares de cómo proceder: y en cuanto podáis, con el mismo propósito, quienes conocen ya, y en qué medida los detalles de esta cuestión."*

Babington cayó en la trampa, lo que provocó la ejecución de María I y de los seis caballeros involucrados y el fracaso de Felipe II.

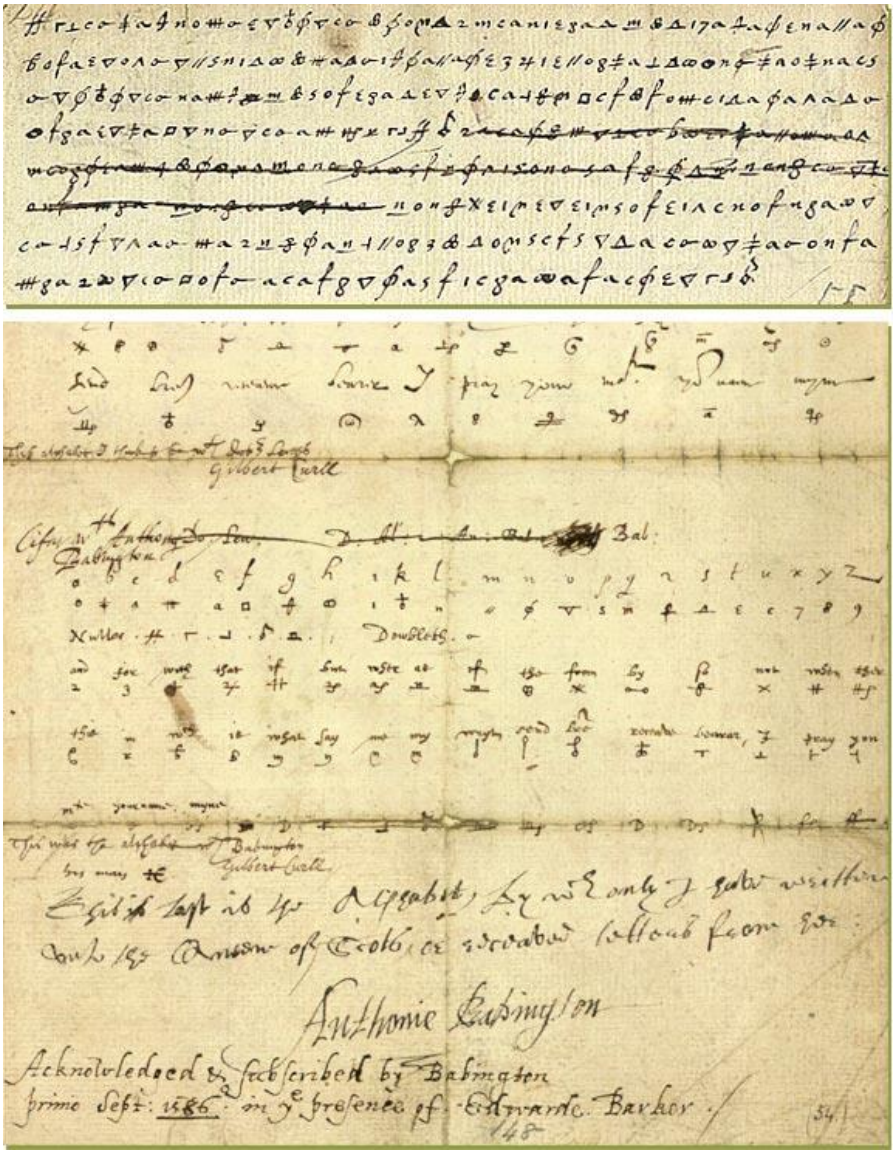

Figura 8- Carta de Maria I a Anthony Babington.

7.11. Independencia de Estados Unidos de América

La criptografía fue utilizada en la mayoría de los conflictos armados de la época, pero en concreto tuvo una gran importancia en la Guerra de Independencia de las colonias británicas en América (1775-1783) al interceptar los mensajes del ejército británico y al desarrollar nuevos métodos de cifrado como la "rueda de cifrado" de Jefferson.

Thomas Jefferson (1743-1826) fue el tercer presidente de los Estados Unidos y autor de la Declaración de Independencia de los EE. UU. En 1795 elaboró un sistema de cifrado que consistía en un cilindro compuesto por 36 discos de madera, cada uno con las 26 letras del alfabeto impresas y dispuestas en diferentes órdenes, que giraban alrededor de un eje metálico. Al girar los discos, se podía componer el mensaje en cualquier línea. El primero en fabricarlo en serie fue Étienne Bazeries en 1891.

El mensaje claro se formaba moviendo los discos de madera hasta que este aparecía en una de las líneas del cilindro. Una vez hecho esto, el emisor enviaba como criptograma cualquier otra línea con la formación de los discos fijada. Para que el receptor pudiera descodificar el mensaje, debía poseer un cilindro con los discos colocados en el mismo orden, de tal manera que cuando recibía el mensaje, formaba la línea recibida moviendo los discos y buscaba entre las líneas restantes la que tenía sentido.

La seguridad de este sistema reside en que, aunque algún atacante interceptara el criptograma y poseyera los discos, tendría que encontrar la posición de estos. Teniendo en cuenta que cada disco puede situarse de 36 maneras distintas, el número de formas de colocar los discos sería: $P_{36} = 36! \approx 3.72 \cdot 10^{41}$.

Figura 9- Cilindro de Jefferson.

7.12. Los principios de Kerckhoffs

Auguste Kerckhoffs fue un filólogo holandés que durante la segunda mitad del siglo XIX se dedicó a la enseñanza del alemán en la Escuela Superior de Estudios Comerciales de París. Sin embargo, lo que le ha hecho destacar hasta el día de hoy son unos ensayos que publicó en la Revista de Ciencias Militares francesa en 1833. Estos consisten en seis principios básicos para el diseño correcto de sistemas criptográficos:

1. Si el sistema no es teóricamente irrompible, al menos debe serlo en la práctica.
2. La efectividad del sistema no debe depender de que su diseño permanezca en secreto.
3. Poder comunicar y mantener segura la clave sin necesidad de notas escritas y poder cambiar la clave de forma discreta ante los periodistas.
4. El sistema debe ser compatible con la comunicación telegráfica. Los criptogramas deberán dar resultados alfanuméricos.
5. El sistema debe ser portátil y su uso no debe requerir más de una persona.
6. Por último, dadas las circunstancias en las que se aplica dicho sistema, tiene que ser fácil de usar y no debe provocar demasiado estrés, ni tampoco exigir unos amplios conocimientos sobre una serie de reglas.

Más de un siglo después de su publicación, los seis principios siguen plenamente vigentes.

El primer principio sostiene que los sistemas criptográficos modernos deben depender de espacios de claves lo suficientemente largos para que sea imposible reunir la potencia de cálculo necesaria para descifrarlos. Cuando la tecnología avanza y las claves actuales pueden ser "rotas", se incrementa la longitud de las claves para mantener la seguridad.

El segundo principio, conocido como la Doctrina de Kerckhoffs, establece que la seguridad de un criptosistema debe depender solo del secreto de la clave, no del diseño del sistema. Durante años, se ignoró este principio, confiando en la "seguridad por oscuridad". La Guerra Fría demostró que mantener en secreto el diseño era costoso e inviable. Desde entonces, se han hecho públicos los diseños de los criptosistemas, permitiendo su análisis y mejora por parte de la comunidad, confirmando la validez de la Doctrina de Kerckhoffs.

El tercer principio se observa en situaciones cotidianas, donde políticas de seguridad demasiado estrictas llevan a los usuarios a escribir contraseñas complejas en post-its pegados a sus ordenadores, comprometiendo así la seguridad.

Los principios cuarto, quinto y sexto subrayan la necesidad de que los sistemas criptográficos reconozcan las limitaciones humanas para ser efectivos. Si un sistema es demasiado complejo, los usuarios tienden a simplificarlo, reduciendo su seguridad. Un ejemplo histórico es el incorrecto uso de la máquina Enigma por parte de los alemanes en la Segunda Guerra Mundial, lo que facilitó el trabajo de los criptoanalistas británicos.

7.13. Primera Guerra Mundial

7.13.1. El telegrama de Zimmerman

Como ya se ha mencionado anteriormente, la criptografía fue crucial durante las guerras. El telegrama de Zimmerman es uno de los episodios más significativos de La Gran Guerra en el ámbito de la inteligencia militar y criptografía. Este mensaje cifrado fue enviado el 16 de enero de 1917 por el ministro de Asuntos Exteriores alemán, Arthur Zimmerman, al embajador de Alemania en Estados Unidos, Johann Heinrich von Bernstorff. A su vez, este debía enviar el mensaje al embajador alemán en México.

El telegrama proponía una alianza entre el Reich y México en caso de que Estados Unidos entrara en la guerra contra el Imperio alemán. Además, Berlín ofrecía a México ayuda para reconquistar Texas, Arizona y Nuevo México.

Al día siguiente de que los alemanes mandaran el telegrama, la inteligencia británica lo interceptó. Los británicos lograron descifrar el mensaje gracias a la ayuda de la unidad "Habitación 40", llamada así porque ocupaba la dependencia número 40 de su cuartel general y que estaba especializada en el desciframiento de códigos y cifrados enemigos.

El dos de abril de 1917, Estados Unidos declaró formalmente la guerra al imperio alemán. Por primera vez en la historia, el criptoanálisis llevó a una nación entera a entrar en guerra.

7.13.2. La rejilla de Cardano

La “Rejilla de Cardano” fue inventada por el italiano Gerolamo Cardano en el siglo XVI. A pesar de ser un método de cifrado inventado en el Renacimiento, fue principalmente utilizado durante la Primera Guerra Mundial.

La rejilla de Cardano consiste en una plantilla con varios huecos en su superficie, de tal manera que cuando se coloca sobre un papel se escribe el mensaje sobre los huecos de izquierda a derecha y de arriba abajo. En el siguiente ejemplo podemos ver el mensaje “Tomad la cuidad”.

	T		O		
M			A		D
		L		A	
C					I
	U			D	
A		D			

Tabla 11- Rejilla Cardano 1.

Una vez escrito el mensaje, se retira la plantilla y se rellenan los huecos libres con letras aleatorias que dificulten la lectura del mensaje.

I	T	E	O	S	B
M	A	H	A	L	D
C	X	L	D	A	E
C	A	F	V	N	I
M	U	E	R	D	J
A	I	D	E	U	S

Tabla 12- Rejilla Cardano 2.

Para que el receptor pueda leer el mensaje cifrado debe colocar una plantilla igual a la utilizada por el emisor.

A pesar de no ser un sistema muy seguro fue empleado por el ejército alemán durante esta guerra. Sin embargo, el barón Eduard von Fleissner von Wostrowitz, ideó una variante más segura. En la rejilla que proponía Fleissner, el mensaje se escribe girando la plantilla

noventa grados una vez están completos los huecos. La rejilla debe estar diseñada cuidadosamente para que los huecos no se solapen al girarla. Esto asegura que todas las letras se escriban y descifren de manera única.

Por ejemplo, si se quiere enviar el mensaje “Hemos llegado a la capital sin bajas”.

Posición inicial

			H	E
	M		O	S
L				L
	E			
			G	

Tabla 13- Rejilla Cardano 3.

Primer giro de 90º

	A			
D		O		
			A	
L			A	C
	A			P

Tabla 14- Rejilla Cardano 4.

Segundo giro de 90º

	I			
			T	
A				L
	S	I		N
B	A			

Tabla 15- Rejilla Cardano 5.

Tercer giro de 90º

J			A		
S					

Tabla 16- Rejilla Cardano 6.

Se rellenan los huecos libres (sombreados en verde).

J	I	A	A	H	E
S	D	C	O	T	B
A	M	A	O	S	L
L	S	I	A	N	L
L	E	M	A	E	C
B	A	A	U	G	P

Tabla 17- Rejilla Cardano 7.

7.13.3. Cifrado ADFGX

Los alemanes enseguida se dieron cuenta de las desventajas de la rejilla, ya que a pesar de las mejoras de Fleissner, los aliados la conseguían desencriptar. De esta manera el cifrado ADFGX fue introducido en 1918 por el oficial de inteligencia del ejército alemán Fritz Nebel.

En el cifrado ADFGX se realiza primero un cuadrado de Polibio de 5·5 que contiene las letras del alfabeto. Cada letra del mensaje original se reemplaza por un par de letras de la matriz ADFGX. Por ejemplo, si la letra “B” está en la primera fila y columna, se codifica como “AA”.

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

Tabla 18- Cifrado ADFGX 1..

Si se quiere transmitir el mensaje “Nos atacan”, se cifra convirtiéndolo en pares de letras según la tabla 18:

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

Tabla 19- Cifrado ADFGX 2.

Para la letra N tendríamos FX, para la O sería DF, de tal manera que el mensaje cifrado será: FX DF FG AF AD AF GF AF FX

Para complicar más este sistema, se mezclaba posteriormente con una palabra clave que debía ser conocida por el emisor y el receptor. En este caso se usará la palabra “GUERRA”.

G	U	E	R	R	A
F	X	D	F	F	G
A	F	A	D	A	F
G	F	A	F	F	X

Tabla 20- Cifrado ADFGX 3.

Después se ordenaban las letras de cada columna en orden alfabético.

A	E	G	R	R	U
D	F	F	F	G	X
A	A	A	D	F	F
A	F	F	F	G	X

Tabla 21- Cifrado ADFGX 4.

Hecho esto se obtiene el mensaje cifrado leyendo verticalmente las letras de cada columna: ADAA EFAF GFAF RFDF RGFG UXFX.

Sin duda, este cifrado era más seguro que los anteriores usados durante la guerra a pesar de que fue descifrado en junio de 1918 por un criptoanalista francés.

7.14. Segunda Guerra Mundial

La criptografía jugó un papel crucial en la Segunda Guerra Mundial, siendo un factor decisivo en el desenlace del conflicto. Durante esta guerra, tanto las potencias del eje (Alemania, Italia y Japón) como los Aliados (Reino Unido, EE. UU., y la URSS), invirtieron grandes esfuerzos en desarrollar y romper códigos secretos que protegían las comunicaciones militares, diplomáticas y estratégicas. Dos de los aspectos más destacados de la criptografía en este periodo fueron el uso de la máquina Enigma por parte de Alemania y la labor de los descifradores en Bletchley Park en el Reino Unido.

Figura 10- Máquina Enigma.

La máquina Enigma fue el principal dispositivo criptográfico utilizado por las fuerzas armadas alemanas. Inicialmente fue diseñada para uso comercial en la década de 1920 por el ingeniero alemán Arthur Scherbius y fue luego adaptada por el ejército alemán para desarrollar un sistema de cifrado extremadamente complejo.

El componente clave de la máquina Enigma era su conjunto de rotores, unos discos móviles con circuitos eléctricos internos, puesto que su estructura externa era muy similar a una máquina de escribir portátil. En la versión militar, Enigma utilizaba generalmente tres rotores, aunque algunas versiones posteriores usaron cuatro o más.

Los rotores se colocaban en un eje común dentro de la máquina y podían ser intercambiados y configurados en diferentes posiciones antes de cada sesión de cifrado. Cada rotor tenía 26 posiciones posibles, correspondientes a las 26 letras del alfabeto, y al girarse, cambiaba las conexiones eléctricas internas que determinaban la sustitución de las letras. Cada vez que se pulsaba una tecla, el primer rotor giraba una posición. Cuando se completaba una vuelta, el siguiente rotor se desplazaba una posición. Este movimiento continuo de los rotores significaba que la sustitución de las letras cambiaba con cada pulsación de tecla.

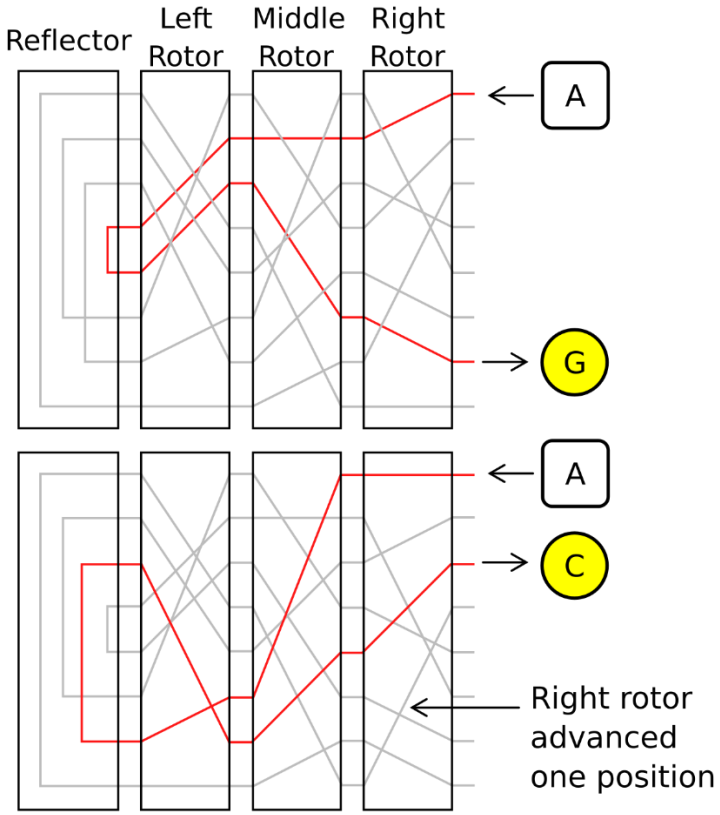

Figura 11- Rotores máquina Enigma.

Detrás de los rotores se encontraba otro componente, el reflector, que enviaba la señal eléctrica de vuelta a través de los rotores por un camino diferente, de tal forma que el proceso de cifrado fuera bidireccional, así Enigma podía cifrar y descifrar con el mismo ajuste. Aun así, estaba la debilidad de que ninguna letra podía cifrarse como ella misma.

En la parte frontal, debajo del teclado, había un panel de conexiones llamado Steckbrett. Con este panel, el operador podía conectar cables entre pares de letras, intercambiando sus valores antes de que el mensaje pasara por los rotores, esto aumentaba exponencialmente el número de conexiones posibles.

Encima del teclado, Enigma tenía un panel con 26 lámparas, una para cada letra del alfabeto. Cuando se presionaba una tecla en el teclado, la corriente eléctrica pasaba a través de los rotores y el reflector, y finalmente encendía una de las lámparas para indicar la letra cifrada correspondiente. El operador leía la letra iluminada y la anotaba como parte del mensaje cifrado. Para descifrar, el proceso era inverso: el mensaje cifrado se introducía letra por letra, y la máquina indicaba las letras del mensaje original.

El funcionamiento del cifrado con Enigma consistía en tres pasos:

1. **Configuración Inicial:** Antes de cifrar o descifrar un mensaje, se configuraban los rotores en una posición inicial específica, se seleccionaba el orden de los rotores, y se establecían las conexiones en el Steckerbrett. Estas configuraciones eran parte de la clave diaria, que debía ser conocida por ambos, el remitente y el receptor.
2. **Cifrado:** Al ingresar un texto en la máquina Enigma, las letras del mensaje original eran sustituidas por otras letras de acuerdo con la compleja interacción entre los rotores y el Steckerbrett. El operador anotaba el resultado que aparecía en las luces indicadoras, produciendo así el mensaje cifrado.
3. **Descifrado:** El receptor del mensaje cifrado configuraba su máquina Enigma con la misma clave inicial y simplemente ingresaba el texto cifrado. La máquina revertía el proceso, devolviendo el texto claro original.

Aunque Enigma se consideraba irrompible, varios factores contribuyeron a su descifrado por los Aliados. En el Reino Unido, un equipo de matemáticos, ingenieros y lingüistas, trabajando en Bletchley Park, logró descifrar los mensajes codificados con Enigma. Entre ellos, el matemático Alan Turing fue una figura clave. Utilizando una combinación de análisis matemático y máquinas especiales llamadas bombas

criptográficas, desarrolladas para probar miles de combinaciones de Enigma rápidamente, el equipo de Bletchley Park pudo leer los mensajes alemanes. El desciframiento de Enigma fue uno de los secretos mejor guardados de la guerra y se estima que acortó el conflicto en varios años, salvando millones de vidas.

7.15. Criptografía en la actualidad

Con la aparición de ordenadores y los avances tecnológicos del siglo XX la criptografía pasó de ser usada durante las guerras (con fines únicamente militares o diplomáticos) a estar presente en todos los ámbitos relacionados con la información (tarjetas de crédito, DNI electrónico, correos electrónicos, redes sociales…).

La criptografía se utiliza para proteger la información, tanto en el ámbito personal como empresarial, ya sea cuando está en tránsito o almacenada. Se basa en técnicas y algoritmos matemáticos que transforman un mensaje o información en texto claro en algo ilegible (cifrado), accesible solo para quienes poseen las claves necesarias.

Aunque una desventaja de la criptografía es que el proceso de encriptación y desencriptación requiere procesamiento adicional en los dispositivos involucrados en la transmisión, lo que puede reducir la velocidad de transmisión de la información, una de sus grandes ventajas es que permite que nuestros datos e información valiosa viajen de manera segura a través del mundo digital, garantizando que solo las personas autorizadas puedan acceder a ellos.

Muchos de los principios fundamentales utilizados a lo largo de la historia siguen jugando un papel esencial en la criptografía moderna, como el ya comentado “principio de Kerckhoffs”.

La criptografía moderna se basa en dos grandes ramas: la criptografía simétrica y la asimétrica. Ambas cumplen funciones críticas en la protección de información, pero lo hacen a través de métodos y aplicaciones diferentes.

7.15.1. Criptografía simétrica

Es uno de los métodos más antiguos y fundamentales para cifrar datos en el cual, tanto el emisor como el receptor comparten la misma clave para cifrar y descifrar la información. Además, la clave es única y debe ser conocida por ambas partes de manera confidencial.

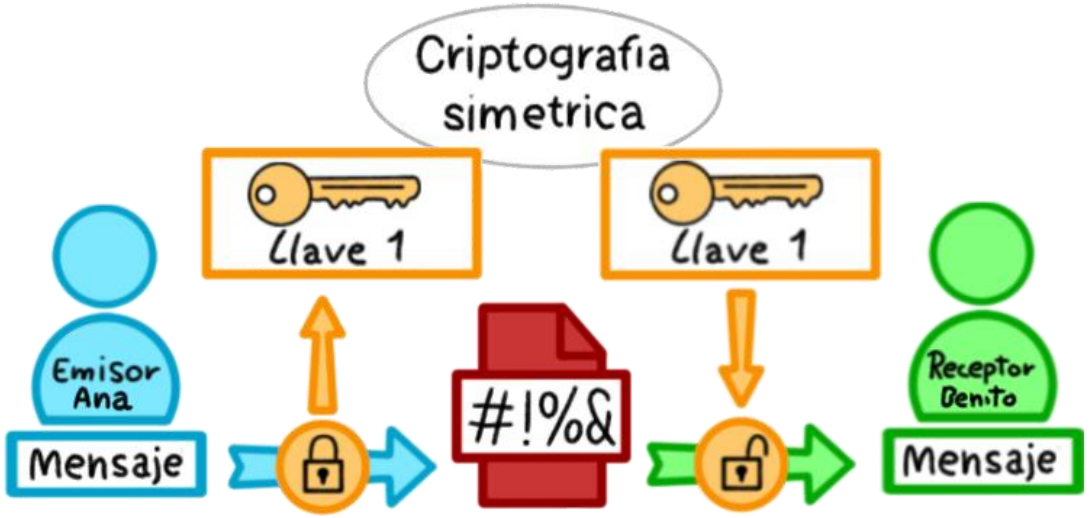

Figura 12- Criptografía simétrica.

Los algoritmos de criptografía simétrica actuales son rápidos y eficientes. Ejemplos comunes de algoritmos simétricos incluyen DES (Data Encryption Standard) y su sucesor 3DES y AES (Advanced Encryption Standard).

Cifrado DES: Es un método muy usado en los años 70 ya obsoleto porque utiliza una clave de 56 bits que lo hace menos seguro. Esta clave de 56 bits genera 2^{56} posibles combinaciones (72.000 billones de claves).

Aunque este número es muy grande, en unos días un ordenador común podría probar todas las claves posibles, y una máquina especializada podría hacerlo en solo cuestión de horas.

Cifrado 3DES: a medida que la informática avanzaba, DES resultó ineficaz contra ciertos ataques, por lo que se introdujo este algoritmo de cifrado, el cual permite lograr una longitud de clave más segura.

Al utilizar 3DES pasamos de claves de 56 bits a otras de 128 bits, lo que genera 2^{128} combinaciones posibles (340 mil millones de billones de billones de billones de claves). Este número es significativamente mayor, y aunque se usaran un gran número de máquinas trabajando en conjunto, llevaría un tiempo considerable encontrar la clave correcta.

Cifrado AES: es un cifrado simétrico en bloques. La principal diferencia entre AES y otros métodos es que utiliza varias fases de rotación, sustitución y mezcla en lugar de una sola fase de sustitución. AES puede utilizar una longitud de clave de 128, 129 y 256 bits, consiguiendo claves más difíciles de descifrar si se aplican métodos de fuerza bruta.

El principal problema de esta rama es que la confidencialidad depende totalmente de la clave, es decir, si un atacante obtiene la clave ya puede descifrar todo el contenido protegido por la misma. Además, en un entorno de comunicaciones amplias, compartir claves de manera segura puede ser complejo y arriesgado.

7.15.2. Criptografía asimétrica

También conocida como criptografía de clave pública, fue un avance revolucionario en el campo de la criptografía. Introducida en la década de 1970, este método utiliza dos claves diferentes, una para cifrar y otra para descifrar, eliminando así la necesidad de compartir una clave secreta entre las partes. Además, no se basa tanto en operaciones lógicas sino matemáticas. Por eso los mensajes son normalmente números con los que se llevan a cabo operaciones.

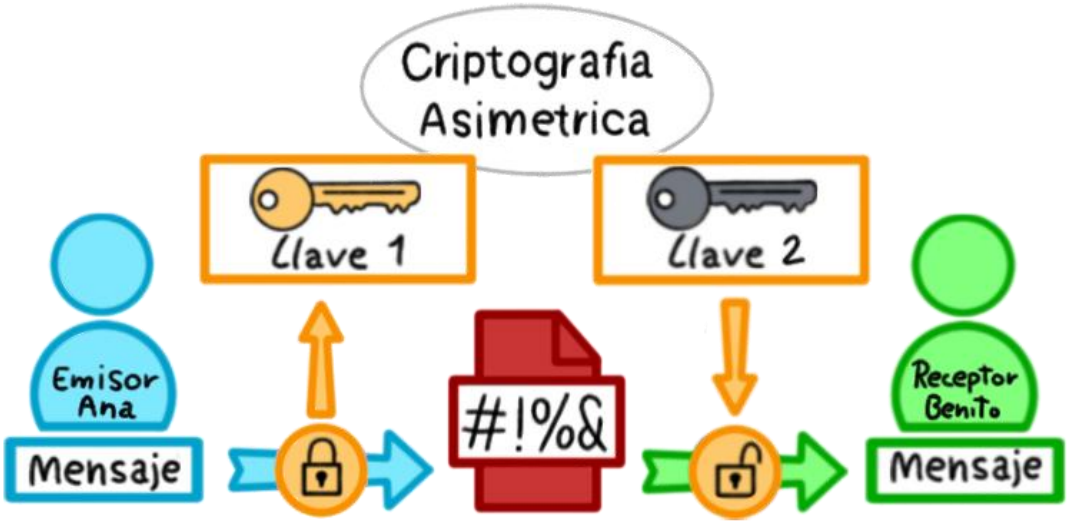

Figura 13- Criptografía asimétrica.

En este método cada usuario tiene dos claves, una privada y otra pública, que puede compartir abiertamente. Un mensaje cifrado con la clave pública solo puede ser descifrado con la clave privada correspondiente y viceversa. Esto no solo permite cifrar datos sino también comprobar la identidad de los usuarios. Por ejemplo, si un mensaje es

cifrado con la clave privada del emisor, cualquier persona con acceso a la clave pública del emisor puede verificar que el mensaje proviene de quien dice ser.

La principal ventaja de esta rama es que, al utilizar una clave pública para el cifrado, no es necesario que las partes compartan una clave secreta de antemano, lo que simplifica la distribución de claves. Sin embargo, los algoritmos tienden a ir más despacio por lo que son menos adecuados para grandes cantidades de datos.

Algunos de los algoritmos más conocidos de criptografía asimétrica son RSA (Rivest-Shamir-Adleman), ElGamal y el algoritmo de Diffie-Hellman para el intercambio seguro de claves.

El criptosistema RSA es uno de los más utilizados en la actualidad. Su seguridad se basa en la dificultad de factorizar números enteros grandes. Más concretamente si $n = pq$ con p, q primos muy grandes, encontrar p y q a partir de n le llevaría mucho tiempo a cualquier ordenador, por muy potente que sea. Investiguemos un poco más en qué consiste este sistema de cifrado. El cifrado RSA consta de tres partes: generación de claves, cifrado y descifrado:

1. Generación de claves: este protocolo lo lleva a cabo cada usuario eligiendo dos números primos, p y q (cuanto más grandes sean los números mayor es la seguridad). A continuación, se calcula $n = pq$ y la función de Euler $\varphi(n)$ o función totiente. Expliquemos brevemente las principales características de esta función:

Definición: Sea $n \in N$, se define $\varphi(n)$ como el número de enteros positivos menores que n y coprimos con n.

Ejemplo: $\varphi(9) = 6$, ya que $\{1,2,4,5,7,8\}$ son coprimos con 9.

$\varphi(5) = 4$, ya que $\{1,2,3,4\}$ son coprimos con 5.

La función de Euler tiene numerosas propiedades. Dos de las más importantes son las siguientes:

- Si p es primo, $\varphi(p) = p - 1$ (trivial)
- Si m y n son coprimos, $\varphi(mn) = \varphi(m) \cdot \varphi(n)$

Por lo tanto, en nuestro caso $\varphi(n) = \varphi(pq) = \varphi(p) \cdot \varphi(q) = (\mathrm{p} - 1) \cdot (\mathrm{q} - 1)$

Para completar el proceso de generación de claves, se elige *A*, que junto a *n* es el par de números que forman la clave pública. *A* debe ser un número entero positivo mayor que 1, menor que $\varphi(n)$ y que sea coprimo con él, es decir, el MCD de $(\varphi(n), A) = 1$

Por último, se calcula el número entero *a* que al multiplicarlo por *A* módulo $\varphi(n)$ da como resultado 1, es decir, su inverso módulo $\varphi(n)$.

Veamos un ejemplo para comprender mejor este sistema. Benito va a enviar un menaje encriptado a Ana. Previamente Ana tiene que generar sus claves públicas (*n* y *A*) y privada (*a*). Como se ha explicado antes, elegimos dos números primos. Por ejemplo $p = 23$ y $q = 29$ y calculamos n y $\varphi(n)$:

$$p = 23;\ q = 29;\ n = pq = 23 \cdot 29 = 667$$

$$\varphi(n) = (p-1)(q-1) \Rightarrow \varphi(667) = (23-1)(29-1) = 22 \cdot 28 = 616$$

Escogemos el valor de *A*, por ejemplo 3, que es coprimo con 616.

La clave pública de Ana es el par de números $(A, n) = (3, 667)$. Hallamos el inverso de A módulo $\varphi(n)$, esto es, hallamos a tal que:

$$A \cdot a \equiv 1 \left(mod\ \varphi(n)\right) \Rightarrow 3a \equiv 1\ (mod\ 616)$$

Aunque esto lo hace rápidamente un ordenador, se puede hallar 3^{-1} fácilmente mediante el algoritmo de Euclides (explicado en el apartado 8.5 del cifrado César).

$$\begin{array}{r|l} 616 & 3 \\ \hline 1 & 205 \end{array}$$

$$1 = 616 - 3 \cdot 205$$

$$1 = 616 + 3 \cdot (-205)$$

$$3 \cdot (-205) \equiv 1\ (mod\ 616)$$

$$-205 \equiv 3^{-1}\ (mod\ 616)$$

Como $-205 + 616 = 411$, entonces $-205 \equiv 411\ (mod\ 616)$. Por lo que

$$3^{-1} \equiv 411\ (mod\ 616)$$

Por lo tanto, la clave privada de Ana será $a = 411$.

2. Cifrado: Si otro usuario, por ejemplo Benito, desea mandar un mensaje secreto a Ana, lo primero que debe hacer es pedir las claves públicas (667, 3) a Ana. Supongamos que Benito quiere mandar el mensaje m a Ana. Previamente debemos convertir este mensaje en un número que llamaremos M. Una posibilidad es usar la tabla de códigos ASCII ya que permite transformar todas las letras y los principales símbolos en números.

Caracteres ASCII imprimibles

DEC	HEX	Simbolo	DEC	HEX	Simbolo	DEC	HEX	Simbolo
32	20h	espacio	64	40h	@	96	60h	`
33	21h	!	65	41h	A	97	61h	a
34	22h	"	66	42h	B	98	62h	b
35	23h	#	67	43h	C	99	63h	c
36	24h	$	68	44h	D	100	64h	d
37	25h	%	69	45h	E	101	65h	e
38	26h	&	70	46h	F	102	66h	f
39	27h	'	71	47h	G	103	67h	g
40	28h	(	72	48h	H	104	68h	h
41	29h	)	73	49h	I	105	69h	i
42	2Ah	*	74	4Ah	J	106	6Ah	j
43	2Bh	+	75	4Bh	K	107	6Bh	k
44	2Ch	,	76	4Ch	L	108	6Ch	l
45	2Dh	-	77	4Dh	M	109	6Dh	m
46	2Eh	.	78	4Eh	N	110	6Eh	n
47	2Fh	/	79	4Fh	O	111	6Fh	o
48	30h	0	80	50h	P	112	70h	p
49	31h	1	81	51h	Q	113	71h	q
50	32h	2	82	52h	R	114	72h	r
51	33h	3	83	53h	S	115	73h	s
52	34h	4	84	54h	T	116	74h	t
53	35h	5	85	55h	U	117	75h	u
54	36h	6	86	56h	V	118	76h	v
55	37h	7	87	57h	W	119	77h	w
56	38h	8	88	58h	X	120	78h	x
57	39h	9	89	59h	Y	121	79h	y
58	3Ah	:	90	5Ah	Z	122	7Ah	z
59	3Bh	;	91	5Bh	[	123	7Bh	{
60	3Ch	<	92	5Ch	\	124	7Ch	|
61	3Dh	=	93	5Dh	]	125	7Dh	}
62	3Eh	>	94	5Eh	^	126	7Eh	~
63	3Fh	?	95	5Fh	_	elCodigoASCII.com.ar		

ASCII extendido

DEC	HEX	Simbolo	DEC	HEX	Simbolo	DEC	HEX	Simbolo	DEC	HEX	Simbolo
128	80h	Ç	160	A0h	á	192	C0h	└	224	E0h	Ó
129	81h	ü	161	A1h	í	193	C1h	┴	225	E1h	ß
130	82h	é	162	A2h	ó	194	C2h	┬	226	E2h	Ô
131	83h	â	163	A3h	ú	195	C3h	├	227	E3h	Ò
132	84h	ä	164	A4h	ñ	196	C4h	─	228	E4h	õ
133	85h	à	165	A5h	Ñ	197	C5h	┼	229	E5h	Õ
134	86h	å	166	A6h	ª	198	C6h	ã	230	E6h	µ
135	87h	ç	167	A7h	º	199	C7h	Ã	231	E7h	þ
136	88h	ê	168	A8h	¿	200	C8h	╚	232	E8h	Þ
137	89h	ë	169	A9h	®	201	C9h	╔	233	E9h	Ú
138	8Ah	è	170	AAh	¬	202	CAh	╩	234	EAh	Û
139	8Bh	ï	171	ABh	½	203	CBh	╦	235	EBh	Ù
140	8Ch	î	172	ACh	¼	204	CCh	╠	236	ECh	ý
141	8Dh	ì	173	ADh	¡	205	CDh	═	237	EDh	Ý
142	8Eh	Ä	174	AEh	«	206	CEh	╬	238	EEh	¯
143	8Fh	Å	175	AFh	»	207	CFh	¤	239	EFh	´
144	90h	É	176	B0h	░	208	D0h	ð	240	F0h	
145	91h	æ	177	B1h	▒	209	D1h	Ð	241	F1h	±
146	92h	Æ	178	B2h	▓	210	D2h	Ê	242	F2h	‗
147	93h	ô	179	B3h	│	211	D3h	Ë	243	F3h	¾
148	94h	ö	180	B4h	┤	212	D4h	È	244	F4h	¶
149	95h	ò	181	B5h	Á	213	D5h	ı	245	F5h	§
150	96h	û	182	B6h	Â	214	D6h	Í	246	F6h	÷
151	97h	ù	183	B7h	À	215	D7h	Î	247	F7h	¸
152	98h	ÿ	184	B8h	©	216	D8h	Ï	248	F8h	°
153	99h	Ö	185	B9h	╣	217	D9h	┘	249	F9h	¨
154	9Ah	Ü	186	BAh	║	218	DAh	┌	250	FAh	·
155	9Bh	ø	187	BBh	╗	219	DBh	█	251	FBh	¹
156	9Ch	£	188	BCh	╝	220	DCh	▄	252	FCh	³
157	9Dh	Ø	189	BDh	¢	221	DDh	¦	253	FDh	²
158	9Eh	×	190	BEh	¥	222	DEh	Ì	254	FEh	■
159	9Fh	ƒ	191	BFh	┐	223	DFh	▀	255	FFh	

Figura 14- Código ASCII.

Por tanto, Benito quiere enviar el mensaje 109 ya que es el número que corresponde a la letra m en ASCII. Para ello, Benito realizará la siguiente operación:

$c = M^A \ (mod\ n) \Rightarrow c = 109^3 \ (mod\ 667)$, donde c es el mensaje ya cifrado.

Como $109^3 = 1295029$, hallamos el resto de dividir 1295029 entre 667:

$$\begin{array}{rrrrrrr|rrrr} 1 & 2 & 9 & 5 & 0 & 2 & 9 & 6 & 6 & 7 \\ \cline{8-11} & 6 & 2 & 8 & 0 & & & 1 & 9 & 4 & 1 \\ & & 2 & 7 & 7 & 2 & & & & & \\ & & & 1 & 0 & 4 & 9 & & & & \\ & & & & 3 & 8 & 2 & & & & \end{array}$$

Por lo que $c = 382 \ (mod\ 667)$ y es el código que le mandará a Ana.

3. Descifrado: Una vez que Ana recibe en mensaje cifrado *c*, llevará a cabo el descifrado para comprender el mensaje, procediendo de la siguiente manera: Ana elevará este mensaje cifrado *c* a su clave secreta *a*, obteniendo el mensaje original M:

$$c^a \ (mod\ n) = 382^{411} \ (mod\ 667) \equiv 109 \ (mod\ 667) = M \ (mod\ 667)$$

¿Por qué obtenemos el mensaje original M? La explicación se basa en el Teorema de Euler, que dice lo siguiente:

Si a y n son coprimos, $a^{\varphi(n)} \equiv 1 \ (mod\ n)$

Por tanto $c^a \ (mod\ n) = \ (M^A)^a \ (mod\ n) = M^{Aa} \ (mod\ n)$

Pero como $A \cdot a \equiv 1 \ \big(mod\ \varphi(n)\big) \Rightarrow A \cdot a = k\varphi(n) + 1$

Entonces $M^{Aa} \ (mod\ n) = M^{k\varphi(n)+1} \ (mod\ n) = (M^{\varphi(n)})^k \cdot M \ (mod\ n) \equiv M(mod\ n)$, ya que, por el Teorema de Euler, $\big(M^{\varphi(n)}\big) \equiv 1 \ (mod\ n)$, si M es coprimo con $\varphi(n)$.

Observación: $c^a \ (mod\ n) = 382^{411} \ (mod\ 667)$. Al ser una operación tan compleja, se suele usar la exponenciación binaria (o método de elevar al cuadrado y multiplicar) Aunque una explicación detallada llevaría mucho tiempo, se hace, por ejemplo:

$a^8 = ((a^2)^2)^2 \rightarrow$ 3 operaciones en vez de 7

$a^{10} = ((a^2)^2 \cdot a)^2 \rightarrow$ 4 operaciones en vez de 9

$a^{13} = ((a^2 \cdot a)^2)^2 \cdot a^{\square} \rightarrow$ 5 operaciones en vez de 12

Para números muy grandes, el número de operaciones es significativamente menor que haciéndolo por la definición de potencia.

En los ejemplos anteriores, se puede observar que, a veces, solo elevamos al cuadrado y, a veces, elevamos al cuadrado y multiplicamos por *a*. Cuál de los caminos tomar depende de la expresión en binario del exponente:

$(8)_{10} = (1000)_2 \rightarrow$ elevo – elevo – elevo (la primera cifra siempre es 1 y no interviene)

$(10)_{10} = (1010)_2 \rightarrow$ elevo – elevo y multiplico – elevo.

$(13)_{10} = (1101)_2 \rightarrow$ elevo y multiplico – elevo – elevo y multiplico.

En nuestro caso, debemos realizar la operación 382^{411}. En primer lugar, escribimos 411 en binario: $(411)_{10} = (110011011)_2$

1	1	0	0	1	1	0	1	1
K_8	K_7	K_6	K_5	K_4	K_3	K_2	K_1	K_0

Tabla 22- Expresión binaria de 411.

Con la primera cifra K_8 no trabajamos, comenzamos el desencriptado con K_7.

K_7. El mensaje recibido $c = 382$ lo elevamos al cuadrado módulo $n = 667$. Para calcular ese valor seguimos el procedimiento explicado en el apartado anterior y obtenemos como resultado 518 módulo 667.

$$382^2 \ (mod\ 667) \equiv 518 \ (mod\ 667)$$

Como K_7 se corresponde con el valor 1 en la expresión binaria de 411, se hace una operación adicional multiplicando el resultado obtenido por $c = 382$ en el mismo módulo. El resultado obtenido es 444 módulo 667.

$$518 \cdot 382 \ (mod\ 667) \equiv 444 \ (mod\ 667)$$

K_6. Se repite el mismo procedimiento, teniendo en cuenta que ahora K_6 se corresponde con el valor 0 en la expresión binaria de 411. Por lo tanto, no se hace ninguna operación más.

$$444^2 \ (mod\ 667) \equiv 371 \ (mod\ 667)$$

Siguiendo el mismo proceso para el resto de cifras de la expresión binaria de 411:

K_5.

$$371^2 \ (mod\ 667) \equiv 239 \ (mod\ 667)$$

K_4.

$$239^2 \ (mod\ 667) \equiv 426 \ (mod\ 667)$$

Como K_4 corresponde al valor 1 se multiplica de nuevo por 382.

$$426 \cdot 382 \ (mod\ 667) \equiv 651 \ (mod\ 667)$$

K_3.

$$651^2 \ (mod\ 667) \equiv 256 \ (mod\ 667)$$

$$256 \cdot 382 \ (mod\ 667) \equiv 410 \ (mod\ 667)$$

K_2.

$$410^2 \ (mod\ 667) \equiv 16 \ (mod\ 667)$$

K_1.

$$16^2 \ (mod\ 667) \equiv 256 \ (mod\ 667)$$

$$256 \cdot 382 \ (mod\ 667) \equiv 410 \ (mod\ 667)$$

K_0.

$$410^2 \ (mod\ 667) \equiv 16 \ (mod\ 667)$$

$$16 \cdot 382 \ (mod\ 667) \equiv 109 \ (mod\ 667)$$

Ya no quedan valores de la expresión binaria y, por lo tanto, el resultado obtenido por Ana es el mensaje original M, que volviendo a la tabla ASCII, comprobamos que es una "m".

Conviene recordar una vez más que hemos elegido números primos pequeños para facilitar la explicación. En la realidad, n tiene cientos de cifras.

7.15.3. Criptografía híbrida

Debido a las limitaciones que mostraban la criptografía simétrica y la asimétrica surge la criptografía híbrida, que combina las fortalezas de ambos sistemas para ofrecer un método seguro y eficiente de protección de datos: la seguridad del intercambio de claves de la criptografía asimétrica y la rapidez y eficacia del cifrado simétrico.

7.15.4. Criptografía cuántica

Hemos visto que la seguridad de métodos como el cifrado RSA se basa en la dificultad de factorizar números enteros grandes, que requieren miles de años de cálculo con los ordenadores actuales. Sin embargo, con la llegada de los ordenadores cuánticos, estos problemas podrían resolverse en cuestión de minutos u horas debido a su gran velocidad de cálculo (por ejemplo, con el algoritmo de Shor)

Los ordenadores cuánticos podrían resolver problemas que las computadoras tradicionales no pueden, incluyendo romper los sistemas de cifrado actuales. Sin

embargo, es previsible que se desarrollen nuevos métodos de encriptado aprovechando esta misma tecnología.

8. Literatura

Como hemos visto a lo largo del proyecto, la criptografía ha sido un hito importante y necesario en nuestra historia, por lo que es de esperar que también esté presente en la literatura. Dos de los ejemplos más importantes y que mejor representan los sistemas criptográficos son el cuento El escarabajo de oro (1843) de Edgar Allan Poe y a la aventura de Sherlock Holmes titulada El misterio de los bailarines (1903) de sir Arthur Conan Doyle.

8.1. El escarabajo de oro

El protagonista de este relato corto es William Legrand, un hombre de familia adinerada que, tras una serie de infortunios, cae en la miseria. Para evitar la humillación se traslada a la pequeña y solitaria isla de Sullivan, cerca de Charleston, en Carolina del Sur, donde se desarrolla la trama.

En la isla, Legrand encuentra un escarabajo de oro y un trozo de pergamino viejo. En este, al acercarlo por accidente a la chimenea, aparece la firma del capitán pirata Kidd y un criptograma que indicaría dónde había escondido el pirata su tesoro. Por lo tanto, si Legrand hallaba el tesoro, recuperaría su posición y fortuna perdidas.

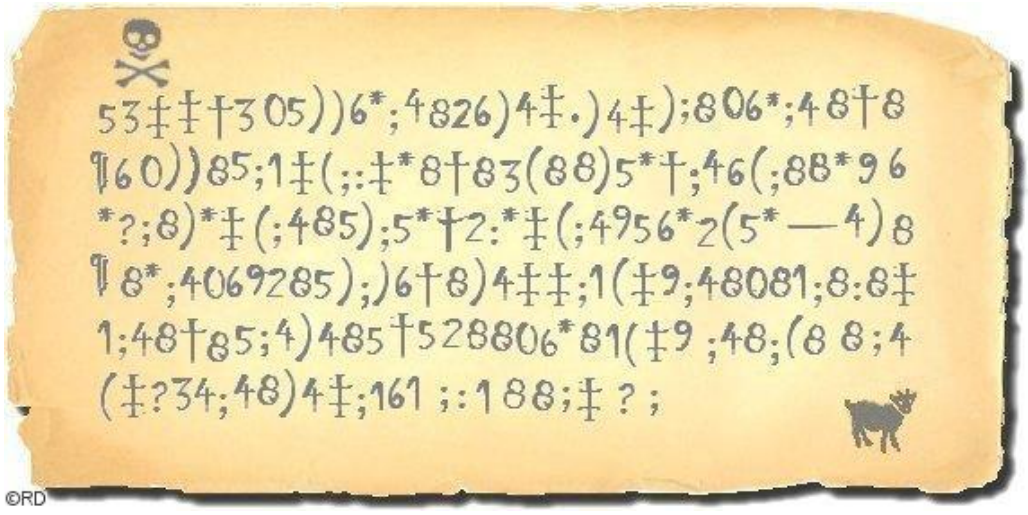

Figura 15- Pergamino encontrado por Legrand dentro del escarabajo de oro.

En primer lugar, es importante destacar que Edgar Allan Poe combina en este cuento la esteganografía (oculta el mensaje en un pergamino mediante tinta invisible) con la criptografía (el mensaje está cifrado).

El mensaje que encuentra es el que aparece en la figura 15. El protagonista descifra el código porque va sustituyendo cada símbolo por una letra del abecedario, considerando que los signos que más se repiten deben corresponder a las letras que más se repiten en inglés (idioma en el que se escribió el cuento). El siguiente listado muestra las letras en orden de frecuencia: de más frecuentes, a la izquierda a menos frecuentes, a la derecha como ya se ha explicado en el análisis de frecuencias del apartado 6.6 de la edad media.

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

Si creamos una tabla en la que aparezca cada símbolo relacionado con el número de veces que se repite, podremos asignar a cada uno una letra del listado anterior en orden de frecuencia.

Símbolo	Frecuencia	Sustitución
0	6	L
1	8	F
2	5	B
3	4	G
4	19	H
5	12	A
6	11	I
8	33	E
9	5	M
-	1	C
(	10	R
)	16	S
*	13	N
.	1	P
:	4	Y
;	26	T
?	3	U
¶	2	V
†	8	D
‡	16	0

Tabla 23- Análisis de frecuencias.

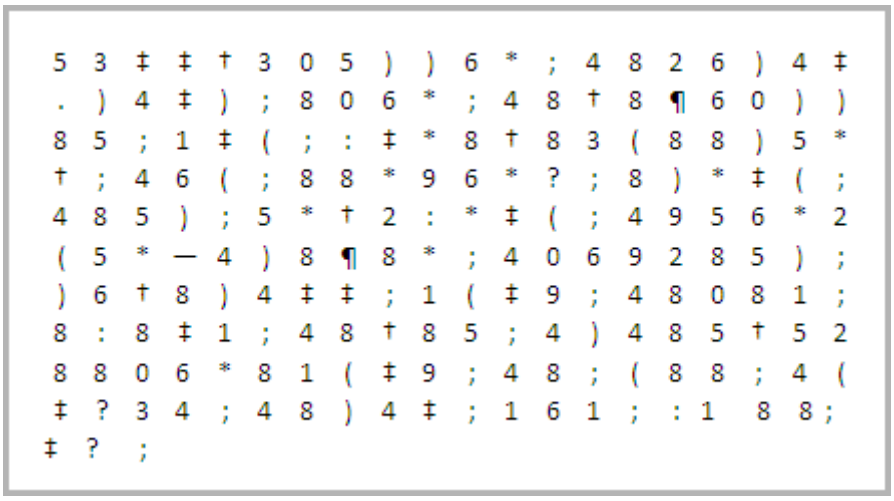

Figura 16- Mensaje cifrado de El escarabajo de oro.

53‡‡†305))6*;4826)4‡.)4‡);80
agoodglassinthebishopshostel

6*;48†8¶60))85;1‡(;:‡*8†83(8
inthedevilsseatfortyonedegre

8)5*†;46(;88*96*?;8)*‡(;485)
esandthirteenminutesnortheas

;5*†2:*‡(;4956*2(5*—4)8¶8*;4
tandbynorthmainbranchseventh

069285);)6†8)4‡‡;1(‡9;48081;
limbeastsideshootfromtheleft

8:8‡1;48†85;4)485†528806*81(
eyeofthedeathsheadabeelinefr

‡9;48;(88;4(‡?34;48)4‡;161;:
omthetreethroughtheshotfifty

188;‡?;
feetout

Se trata de un simple cifrado por sustitución, en español, dice: *"Un buen vaso en el hostal del obispo en el asiento del diablo cuarenta y un grados y trece minutos noreste y por la rama principal norte siete lados de la bestia ululan desde el ojo izquierdo de la calavera una línea recta desde el árbol a través del disparo cincuenta pies de distancia"*.

El desenlace ocurre cuando el grupo sigue las instrucciones del mensaje descifrado, que los conduce a un árbol en una colina. Allí, Legrand ordena a su compañero que trepe al árbol y deje caer el escarabajo dorado por una rama específica. Este acto parece extraño, pero resulta ser crucial para marcar el lugar donde deben excavar. Al cavar en el lugar indicado, encuentran un enorme tesoro compuesto de monedas, joyas y otros objetos de valor.

El compañero, sorprendido, le pregunta a Legrand cómo fue capaz de descifrar el criptograma y localizar el tesoro. Legrand explica el proceso en detalle, revelando su método para descifrar el código y el razonamiento que lo llevó a identificar su ubicación. Todo el enigma del escarabajo de oro se resuelve como una serie de acertijos y lógica que culminan en la fortuna enterrada.

8.2. Los bailarines- Sherlock Holmes

En esta aventura, Holmes y Watson reciben la visita de Hilton Cubitt, un hidalgo campesino. Durante su visita, Cubitt expresa su preocupación por el estado de su joven esposa, muy alterada tras recibir unos extraños jeroglíficos en su residencia:

Figura 17- Mensaje con jeroglíficos de bailarines.

A medida que llegan más mensajes con los dibujos, Holmes va descifrando las palabras ocultas en ellos y descubre la clave; se trata de un cifrado por sustitución. Los bailarines mencionados en el título, resultan ser las letras de un nuevo abecedario.

Antes de que Holmes pueda resolver el caso por completo, ocurre una tragedia: Hilton es asesinado en su casa, y Elsie queda gravemente herida en un aparente intento de suicidio. Holmes, al descifrar los últimos mensajes, descubre que un hombre llamado Abe Slaney, un antiguo pretendiente de Elsie y miembro de una peligrosa banda criminal en Estados Unidos, es el culpable. Slaney había estado usando los dibujos para comunicarse con Elsie, intentando forzarla a volver con él.

Holmes organiza una trampa para atraer a Slaney y lo captura. Finalmente, Slaney confiesa, y Elsie sobrevive. Aunque devastada por la muerte de su esposo, queda libre de las amenazas de su pasado.

Holmes consigue descifrar los mensajes empleando un análisis de frecuencias y sustituyendo cada figura por la letra correspondiente, al igual que Legrand en El escarabajo de oro.

9. Anexos:

9.1. Glosario.

- Aritmética modular: relación de congruencia entre enteros, que es compatible con las operaciones en el anillo de enteros: suma y multiplicación. Para un determinado módulo n: *a* y *b* se encuentran en la misma "clase de congruencia" módulo *n*, si ambos dejan el mismo resto si los dividimos entre *n*, o, equivalentemente, si $a - b$ es un múltiplo de *n*.

- Ataque por fuerza bruta: método de ataque que consiste en probar todas las combinaciones posibles de claves o contraseñas hasta encontrar la correcta.

- Bit (*binary digit*): corresponde a un dígito del sistema de numeración binaria y representa la unidad mínima de información.

- Cifrado asimétrico: método criptográfico que utiliza un par de claves, una clave pública para cifrar el mensaje y una clave privada, única y secreta, para descifrarlo.

- Cifrado simétrico: método criptográfico en el que la misma clave se utiliza tanto para cifrar como para descifrar un mensaje.

- Criptoanálisis: rama de la criptología que trata de vulnerar los métodos de cifrado establecidos por la criptografía.

- Criptografía: ciencia que trata de cómo intercambiar información de forma segura, haciendo el mensaje ilegible, sin ocultar la existencia de dicho mensaje.

- Criptología: ciencia resultante de la unión de la criptografía y el criptoanálisis.

- Criptosistema: conjunto de algoritmos criptográficos necesarios para implementar un servicio de seguridad particular, generalmente para conseguir confidencialidad.

- Esteganografía: ciencia que trata de la escritura de un mensaje, de modo que este quede encubierto u oculto.

- Indicador de Euler: función que proporciona la cantidad de números coprimos con un número dado y menores que tal número.

- Inverso (multiplicativo): elemento que al ser multiplicado por el primero da como resultado el neutro de la multiplicación, es decir, el 1. El inverso de a es a^{-1}.

- Máximo común divisor: mayor divisor que tienen en común dos números a y b: MCD (a, b).

- Número primo: todo número entero positivo cuyos únicos divisores son la unidad y él mismo.

- Números primos entre sí (coprimos): números enteros positivos, primos o no, que no tienen divisores comunes salvo el 1, es decir, cuyo máximo común divisor es el 1.

- Romper (el mensaje): descifrar o descubrir el contenido de un mensaje cifrado sin conocer la clave, generalmente mediante técnicas de ataque o análisis criptográfico.

- Sustitución: técnica de cifrado que reemplaza cada carácter o grupo de caracteres del texto claro por otros según una regla o clave específica.

- Texto claro: mensaje original que no ha sido cifrado.

- Transposición: técnica de cifrado que reorganiza el orden de los caracteres del texto claro según una regla específica, sin alterar los caracteres en sí, para ocultar el contenido del mensaje.

9.2. Índice de imágenes

9.3. Índice de tablas

Bibliografía

Álvarez, J. (1 de Marzo de 2019). *LBV*. Obtenido de Giovanni della Porta, el sabio renacentista que encriptaba mensajes dentro de huevos para eludir el control de la inquisición: https://www.labrujulaverde.com/2019/03/giovanni-della-porta-el-sabio-renacentista-que-encriptaba-mensajes-dentro-de-huevos-para-eludir-el-control-de-la-inquisicion

Biblioteca Nacional de España. (29 de Febrero de 2024). *Datos BNE*. Obtenido de Polygraphiae libri sex Ioannis Trithemii: https://datos.bne.es/edicion/a5669871.html

Calcular Áreas. (19 de Junio de 2023). Obtenido de Congruencias y criptografía en la teoría de los números: https://www.calcularareas.com/congruencias-y-criptografia-en-la-teoria-de-los-numeros/

Central Intelligence Agency. (s.f.). *Central Intelligence Agency*. Obtenido de We are the Nation's first line of defence: https://www.cia.gov/

Cobb, M. (9 de Enero de 2023). *TechTarget*. Obtenido de What is Triple DES and why is it being disallowed?: https://www.techtarget.com/searchsecurity/tip/Expert-advice-Encryption-101-Triple-DES-explained

Corral, J. L. (1 de Febrero de 2018). *Historia, National Geographic*. Obtenido de El códice Voynich, el manuscrito más extraño del mundo: https://historia.nationalgeographic.com.es/a/codice-voynich-manuscrito-mas-extrano-mundo_12344

Cypher Research Laboratories. (2013). *Cypher Research Laboratories*. Obtenido de A Brief History of Cryptography: https://www.cypher.com.au/crypto_history.htm

Dante's Lab. (19 de Diciembre de 2008). *Dante's Lab*. Obtenido de La Doctrina de Kerckhoffs: https://esblog.dlab.ninja/2008/12/la-doctrina-de-kerckhoffs.html

David Kahn, L. K. (1977-2024). *Taylor & Francis Online.* Obtenido de Cryptologia: https://www.tandfonline.com/journals/ucry20

Díaz, J. C. (2009). Elementos y sistemas criptográficos en la escritura visigótica. *Universidad Complutense de Madrid*, 173-183.

Electicomania. (7 de Noviembre de 2010). *Electicomania*. Obtenido de El cifrado Vigenère y como lo rompió Charles Babbage: https://eclecticomania.net/2010/11/07/el-cifrado-vigenere-y-como-lo-rompio-charles-babbage/

Emilio. (1 de marzo de 2015). *GeoGebra*. Obtenido de El escarabajo de oro: https://www.geogebra.org/m/t7PzcgFk#:~:text=El%20se%C3%B1or%20Legrand%20consigue%20descifrar,A%2C%20la%20O...

Encinas, L. H. (2016). *La Criptografía.* Madrid: Los Libros de la Catarata.

Europa Press Ciencia. (5 de Febrero de 2016). *Cienciaplus*. Obtenido de El código secreto soviético de la Guerra Fría no es impenetrable: https://www.europapress.es/ciencia/laboratorio/noticia-codigo-secreto-sovietico-guerra-fria-no-impenetrable-20160205140412.html

Fundamental objectives of cryptography. (6 de Septiembre de 2022). *Ideas worth translating*. Obtenido de Los principios de Kerckhoffs de "La cryptographie militaire": https://www.ibidem-translations.com/edu/principios-kerckhoffs-criptografia-militar/

García, J. V. (2020). *Guerras olvidadas: de Crimea a la crisis balcánica. 1853-1913.* La Coruña: Galland Books S.l.n.e.

Gobierno Buenos Aires. (18 de Abril de 2023). *Buenos Aires, centro de ciberseguridad*. Obtenido de Criptografía en la vida cotidiana: https://buenosaires.gob.ar/noticias/criptografia-en-la-vida-cotidiana

Gutiérrez, Á. (s.f.). *Criptografía y Criptoanálisis en las dos guerras mundiales.* Recuperado el 19 de Julio de 2024, de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.acta.es/medios/articulos/comunicacion_e_informacion/052063.pdf

Hinsley, A. S. (2001). *Codebreakers: The Inside Story of Bletchley Park.* Oxford University Press.

Immune Institute. (29 de Marzo de 2023). *Immune Technology Institute*. Obtenido de Tipos de criptografía ¿Cuáles son los más comunes para la privacidad de las

comunicaciones?: https://immune.institute/blog/tipos-de-criptografia-seguridad-online/

Interactive College of Technology. (s.f.). *Interactive College of Technology*. Obtenido de Letras más y menos utilizadas en el inglés para principiantes: https://es.ict.edu/es/letras-mas-y-menos-utilizadas-en-el-ingles-para-principiantes/#:~:text=Por%20lo%20a%20ella%20se,texto%20de%20aproximadamente%20300.000%20palabras.

Juana Contreras, C. d. (2001). Aritmética modular y códigos secretos . *Revista del Instituto de Matemática y Física*, 1-10.

Keepcoding. (27 de Febrero de 2024). *Tech School*. Obtenido de ¿Qué es la criptografía? (3 tipos): https://keepcoding.io/blog/que-es-la-criptografia-3-tipos/

Larragán, M. G. (11 de Agosto de 2016). *El blog de García Larragan y Cía*. Obtenido de Criptografía (XXVIII): ¿Sabías que...?: https://mikelgarcialarragan.blogspot.com/2016/08/criptografia-xxviii-sabias-que-iv.html

Macho, M. (11 de Enero de 2014). *ZTFNews*. Obtenido de Jefferson, el criptógrafo: https://ztfnews.wordpress.com/2014/01/11/jefferson-el-criptografo/

Macho, M. (16 de Junio de 2014). *ZTFNews*. Obtenido de 'Los bailarines', un criptograma resuelto por Sherlock Holmes: https://ztfnews.wordpress.com/2014/06/16/los-bailarines-un-criptograma-resuelto-por-sherlock-holmes/

Mark, J. J. (6 de Mayo de 2022). *World History Encyclopedia*. Obtenido de French Wars of Religion: https://www.worldhistory.org/French_Wars_of_Religion/

Morales, G. (25 de 12 de 2021). *El Debate*. Recuperado el 25 de julio de 2024, de https://www.eldebate.com/historia/20211225/telegrama-llevo-estados-unidos-guerra.html#:~:text=El%20%C2%ABtelegrama%20Zimmermann%C2%BB%20fue%20un,Mundial%20contra%20el%20Imperio%20alem%C3%A1n.

Nuño, A. (19 de Mayo de 2019). El académico que asegura haber descifrado por fin el manuscrito Voynich. *El Confidencial*. Obtenido de El académico que asegura haber descifrado por fin el manuscrito Voynich.

Oyarzún, J. (18 de Diciembre de 2019). *Matemáticas y ciencias*. Obtenido de Álgebra y Geometría: https://www.matematicas.ciencias.uchile.cl/juaco/section-10.html

Panda mediacenter. (27 de Julio de 2023). *Panda security*. Obtenido de ¿Qué es el cifrado AES? Una guía sobre el Advanced Encryption Standard: https://www.pandasecurity.com/es/mediacenter/cifrado-aes-guia/

Poe, E. A. (1843). *The Gold Bug.* Philadelphia: Dollar Newspaper.

Prieto, M. J. (s.f.). *Curistoria*. Obtenido de Los principios de Kerckhoffs y la criptografía moderna: https://www.curistoria.com/2020/01/los-principios-de-kerckhoffs.html

Real Academia Española. (23.a). *Real Academia Española*. Obtenido de Diccionario de la lengua española: https://dle.rae.es/criptolog%C3%ADa

Real Academia Española. (s.f.). *Diccionario de la lengua española*. Obtenido de RAE-Criptología: https://dle.rae.es/criptolog%C3%ADa

RedIRIS. (15 de Julio de 2002). *Red IRIS*. Obtenido de Criptología: https://www.rediris.es/cert/doc/unixsec/node29.html

Ruperto. (5 de Agosto de 2014). *Koranet*. Obtenido de Criptografía en la biblia: https://koranets.net/criptografia-en-la-biblia/

Sadurní, J. M. (17 de Junio de 2024). *Historia National Geographic*. Obtenido de Alan Turing, el arma secreta de los aliados: https://historia.nationalgeographic.com.es/a/alan-turing-arma-secreta-aliados_16352

Sidhpurwala, H. (12 de Noviembre de 2023). *Red Hat*. Obtenido de Una breve historia de la criptografía: https://www.redhat.com/es/blog/brief-history-cryptography

Talens-Oliag, S. (Abril de 2003). *Universidad de Valencia*. Obtenido de Introducción a la Criptología: https://www.uv.es/~sto/articulos/BEI-2003-04/criptologia.html

Tomás Fernández, E. T. (2004). *Biografías y Vidas*. Obtenido de Resumen de El escarabajo de oro, de Edgar Allan Poe: https://www.biografiasyvidas.com/obra/escarabajo_oro.htm

Velasco, J. J. (20 de mayo de 2014). *Breve historia de la criptografía*. Obtenido de elDiario.es: https://www.eldiario.es/turing/criptografia/breve-historia-criptografia_1_4878763.html

Victoria Ruiz Parrado, J. A. (2022). Matemáticas Discreta y Álgebra. *Teoría y práctica por y para la computación y la ciberseguridad*, 17-47.

Imágenes

- Figura 1: (*Atbash, alfabeto hebreo invertido*). Recuperado de https://koranets.net/criptografia-en-la-biblia/
- Figura 2: *(Escítala espartana)*. Recuperado de https://museo.inf.upv.es/blog/2021/05/14/escitala-espartana/
- Figura 3: *(Tabla sustitución cancillería carolingia)*. Recuperado de https://www.condadodecastilla.es/blog/criptografia-en-la-alta-edad-media/
- Figura 4: *(Tabla sustitución visigoda)*. Recuperado de https://www.condadodecastilla.es/blog/criptografia-en-la-alta-edad-media/
- Figura 5: *(Disco de Alberti)*. Recuperado de https://criptografia20162.wordpress.com/alberti/
- Figura 7: *(Tabla de Vigenère)*. Recuperado de https://www.kaspersky.es/blog/vigenere-cipher-history/6804/
- Figura 8: *(Carta de María I a Anthony Babington)* Recuperado de: https://es.wikipedia.org/wiki/Complot_de_Babington
- Figura 9:*(Cilindro de Jefferson)*. Recuperado de: https://ztfnews.wordpress.com/2014/01/11/jefferson-el-criptografo/
- Figura 10: *(Máquina Enigma)*. Recuperado de: https://es.wikipedia.org/wiki/Enigma_%28m%C3%A1quina%29
- Figura 11*: (Rotores máquina Enigma)*. Recuperado de https://ca.wikipedia.org/wiki/M%C3%A0quina_Enigma
- Figura 14: *(Código ASCII)* Recuperado de: https://elcodigoascii.com.ar/
- Figura 15: *(Pergamino encontrado por Legrand dentro del escarabajo de oro)* Recuperado de https://hugonorwood.com/codigos
- Figura 16: *(Mensaje cifrado de El escarabajo de oro)* Recuperado de https://mikelgarcialarragan.blogspot.com/2016/08/criptografia-xxviii-sabias-que-iv.html
- Figura 17: *(Mensaje con jeroglíficos de bailarines)* Recuperado de https://ztfnews.wordpress.com/2014/06/16/los-bailarines-un-criptograma-resuelto-por-sherlock-holmes/