TFG

CRÓNICA DE LA CRIPTOGRAFÍA. MENSAJES OCULTOS DE LA CAPILLA SIXTINA Y LA ÚLTIMA CENA.

Presentado por Miguel Mínguez Calvo
Tutor: D. Vicente Barón Linares

Facultat de Belles Arts de Sant Carles
Grado en Bellas Artes
Curso 2019-2020

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNIVERSITAT POLITECNICA DE VALENCIA
FACULTAT DE BELLES ARTS DE SANT CARLES

RESUMEN Y PALABRAS CLAVE.

El presente Trabajo Fin de Grado (TFG) es una investigación sobre el origen y evolución de la criptografía: ese mundo de mensajes secretos, codificados, que también se traslada al arte, del cual destacaremos dos obras maestras muy singulares por su gran contenido de mensajes ocultos.
El momento social de inmediatez y de rápida gestión de todo tipo de información me lleva a reflexionar sobre la herramienta tan valiosa que es la escritura. Las formas escritas del lenguaje evolucionaron lentamente durante siglos desde las pinturas a los símbolos, hasta llegar a un complejo sistema en el que signos abstractos representaron sonidos articulados. En los primeros tiempos del desarrollo humano, se suponía que las pinturas estampadas en las cavernas ejercían una magia que mejoraba las condiciones de vida. Con el tiempo, también las palabras adquirieron un significado mágico. Y con el avance de las civilizaciones, la instrucción y el conocimiento quedaban al poder de las clases dominantes, hasta la llegada de la Época Moderna.
La comunicación verbal y después escrita supuso un gran paso de la humanidad para el entendimiento y esa evolución tuvo lugar por el principio de supervivencia, por motivos de trabajo e incluso por esa necesidad social de intercambio de conocimientos en todos los ámbitos del saber mediante la transmisión de cultura.
Quizás lo más sencillo de este trabajo haya sido seleccionar dos obras que representan la quintaesencia de los mensajes ocultos en el arte: La Capilla Sixtina y la Última Cena, tan excepcionales como sus creadores Miguel Ángel y Leonardo.
Más adelante con la proliferación de la comunicación escrita, también se iniciaba un proceso para cifrar mensajes ocultos y guardar secretos que fuesen ininteligibles al resto, con la finalidad de dar órdenes o para manipular o bien para protegerse uno mismo de las circunstancias sociales, políticas y/o religiosas.
El saber es poder y saberlo ocultar es ingenio, talento y también creatividad. ¿Qué hubiese pasado si no hubiera estado cifrada la comunicación entre los seres humanos en ciertos momentos de la historia? No lo podemos saber pero lo que sí sabemos es que el control total del conocimiento y de la realidad es el verdadero PODER.

PALABRAS CLAVE.

Criptografía, escritura, mensajes secretos, ingenio.

RESUM I PARAULES CLAU.

El present Treball Fi de Grau (TFG) és una investigació sobre l'origen i evolució de la criptografia: aqueix món de missatges secrets, codificats, que també es trasllada a l'art, del qual destacarem dues obres mestres molt singulars pel seu gran contingut de missatges ocults.
El moment social d'immediatesa i de ràpida gestió de tota mena d'informació em porta a reflexionar sobre l'eina tan valuosa que és l'escriptura. Les formes escrites del llenguatge van evolucionar lentament durant segles des de les pintures als símbols, fins a arribar a un complex sistema en el qual signes abstractes van representar sons articulats. En els primers temps del desenvolupament humà, se suposava que les pintures estampades en les cavernes exercien una màgia que millorava les condicions de vida. Amb el temps, també les paraules van adquirir un significat màgic. I amb l'avanç de les civilitzacions, la instrucció i el coneixement quedaven al poder de les classes dominants, fins a l'arribada de l'Època Moderna.
La comunicació verbal i després escrita va suposar un gran pas de la humanitat per a l'enteniment i aqueixa evolució va tindre lloc pel principi de supervivència, per motius de treball i fins i tot per aqueixa necessitat social d'intercanvi de coneixements en tots els àmbits del saber mitjançant la transmissió de cultura.
Potser el més senzill d'aquest treball haja sigut seleccionar dues obres que representen la quinta essència dels missatges ocults en l'art: La Capella Sixtina i l'Últim Sopar, tan excepcionals com els seus creadors Miguel Ángel i Leonardo.
Més endavant amb la proliferació de la comunicació escrita, també s'iniciava un procés per a xifrar missatges ocults i guardar secrets que foren inintel·ligibles a la resta, amb la finalitat de donar ordres o per a manipular o bé per a protegir-se un mateix de les circumstàncies socials, polítiques i/o religioses.
El saber és poder i saber-ho ocultar és enginy, talent i també creativitat. Què hauria passat si no haguera estat xifrada la comunicació entre els éssers humans en uns certs moments de la història? No ho podem saber però el que sí que sabem és que el control total del coneixement i de la realitat és el vertader PODER.

PARAULES CLAU.

Criptografia, escriptura, missatges secrets, enginy

SUMMARY AND KEYWORDS.

The present Final Degree Paper (TFG) is an investigation about the origin and evolution of cryptography: that world of secret, coded messages, which also moves to art, of which we will highlight two very singular masterpieces for their great content of hidden messages.
The social moment of immediacy and rapid management of all kinds of information leads me to reflect on the very valuable tool that is writing. The written forms of language evolved slowly over centuries from paintings to symbols, until reaching a complex system in which abstract signs represented articulated sounds. In the early days of human development, paintings printed on caves were supposed to exert a magic that improved living conditions. Over time, words also acquired a magical meaning. And with the advance of civilizations, education and knowledge remained in the power of the ruling classes, until the arrival of the Modern Era.
Verbal and then written communication was a great step of humanity towards understanding and this evolution took place because of the principle of survival, because of work and even because of this social need to exchange knowledge in all areas of knowledge through the transmission of culture.
Perhaps the simplest part of this work was to select two works that represent the quintessence of the hidden messages in art: The Sistine Chapel and the Last Supper, as exceptional as their creators Michelangelo and Leonardo.
Later on, with the proliferation of written communication, a process was also started to encrypt hidden messages and keep secrets that were unintelligible to the rest, with the purpose of giving orders or manipulating or protecting oneself from social, political and/or religious circumstances.
Knowledge is power and knowing how to hide it is ingenuity, talent and also creativity. What would have happened if communication between human beings had not been encrypted at certain moments in history? We cannot know, but what we do know is that total control of knowledge and reality is the true POWER.

KEYWORDS.

Cryptography, writing, secret messages, ingenuity

AGRADECIMIENTOS.

A todos los docentes vocacionales y con pasión de enseñar que he conocido y he tenido el placer de asistir a sus clases, en especial a:
D. José Palomar Aparisi. (Pintura).
D. José Esteve Edo. (Dibujo y escultura).
D. Salvador Artemi Mollá Alcañiz. (Historia Medieval).
D. Manuel Micó Catalán. (Dibujo y pintura).
Dña. María del Carmen Marcos Martínez. (Fundición artística).
D. Raúl León Mendoza. (Fundición artística).
D. Fernando Evangelio Rodríguez. (Grabado).
D. Raúl Durá Grimalt. (Fotografía).
D. Pablo Ramírez Pérez. (Historia del Arte).
Dña. Isabel Doménech Ibáñez. (Proyectos).
Dña. Carmen Lucía Navarrete Tudela. (VACC).
D. José A. Sienra Lizcano. (Dibujo).
D. Carlos Plasencia Climent. (Anatomía).
A mi Tutor, D. Vicente Barón Linares, (Escultura) como profesor e instructor, por su profesionalidad y apoyo.
A Casilda Bulá Ejochi, Clara Bernat Peransi, José Olmedo Ruzafa y David Pfriem, compañeros de BB.AA.
A mis cuñadas, Carmen y Milagros.
A mis amigas, Emilia, Ana y Desampararados.
A mi amigo Pedro Vizcaíno y a la mujer de mis sueños, Montserrat Diez.
A mi familia.

ÍNDICE

2. INTRODUCCIÓN.

Este trabajo comienza con el misterio de las letras, talladas en el Monumento al Pastor del siglo XVIII en los terrenos de Shugborough Hall, Inglaterra. “D O-U-O-S-V-A-V-V M” ¿Qué misterio entraña? ¿Hay un secreto? ¿Hay un mensaje oculto o está a simple vista y no lo sabemos interpretar? Un misterio para un comienzo en un tema lleno de imaginación, que ha progresado conforme la humanidad y su saber han avanzado. El ser humano ha ido dejándonos petrogramas y petroglifos, vivencias, dibujos, pinturas, conocimientos. Unos de forma sencilla y otros de forma compleja, para que alguien los descifre. Así, todo tiene su sentido; desde una simple mano impresa, una talla, un dibujo, una pintura o una constelación.

La sabiduría se ha ido forjando poco a poco, en etapas donde unas culturas predominaban sobre otras, con inquietudes del saber, en edades doradas para cada civilización, en cualquier lugar del mundo y sin ir a la par se han nutrido, creando lenguajes y escrituras. Al mismo tiempo se trataba de ocultar información, por diversos motivos. “El conocimiento es poder” frase de Thomas Hobbes, era antes y será siempre. La criptografía es el arte de ocultar en un mensaje la información que se desea sea confidencial y que no cobrará sentido si se desconoce la clave o la cifra.

El objetivo principal de este TFG, es un análisis, un estudio, una exposición en la cual trato de forma cronológica la evolución de la criptografía, tanto redactada como la visual, dando información gráfica en cada momento de la historia, desde los primeros mensajes hasta la era digital. Son momentos clave para la humanidad, la escritura, el lenguaje, todo el avance del ser humano y en especial, la gran fascinación por el saber en todas las disciplinas del mundo árabe, sus aportaciones, todo el enriquecimiento que supuso para las sociedades humanas. Desde la tablilla mesopotámica (1500 a.C.), descifrar la Piedra de Rosetta por Jean-François Champollion, o el Lineal B por Ventris y Chadwick, logros importantísimos en la arqueología, hasta pensar que el invento de origen civil de Scherbius, máquina Enigma, se convertiría en el más temible sistema militar de codificación de la historia, superados por los criptógrafos polacos en cuanto a la creciente complejidad estructural y operativa del Enigma. Por ello “este fue el mayor avance del criptoanálisis en más de mil años” y el gran cerebro inglés que permitió el descifrado de Enigma Alan Turing, precursor, como Babbage, de los ordenadores modernos.

En los mensajes ocultos en el arte, me he centrado en dos obras grandiosas en si mismas, en las inquietudes de sus autores y en el mensaje que nos han querido dejar.

La relación con Bellas artes la podemos apreciar por la creatividad, la originalidad, innovación de la comunicación, a la hora de transmitir mensajes, la forma de expresión visual con diferentes medios, con talento.

3. OBJETIVOS Y METODOLOGÍA.

3.1. Objetivos generales.

El objetivo principal del presente trabajo fin de grado es:
- Conocer los métodos criptográficos utilizados a lo largo de la historia, centrándome en los más significativos.
- Estudiar la evolución de la criptografía.
- Descubrir las circunstancias que propician la necesidad de ocultar mensajes en el ser humano. ¿Qué motivos subyacen en la necesidad de cifrar mensajes? y ¿qué naturaleza tienen dichos motivos? ¿Son motivos personales, sociales, bélicos, religiosos, económicos…?

3.2. Objetivos específicos.

- Poner en práctica los conocimientos de arte adquiridos durante la carrera.
- Obtener nuevos conocimientos sobre la criptografía, haciendo hincapié en el talento artístico e ingenio en la creación de los sistemas criptográficos.
- Analizar dos grandes obras de arte, bajo el prisma de la criptografía, descifrando su mensaje oculto y la forma en que los artistas, con su talento, se las ingeniaron para realizarlo, en una etapa de tanta presión; jugándose la vida en ello.

3.3. Metodología.

En la metodología empleada podemos apreciar dos partes. La primera, gráfica, mediante fotos, desde las primeras representaciones humanas transmitiendo mensajes y a lo largo de la historia hasta la era digital, una cronología visual. La segunda de carácter teórico, enunciando el desarrollo de la escritura, el lenguaje e historia de la criptografía, como tema principal de la investigación y para concluir, con el análisis, de los mensajes secretos de dos obras maestras del Renacimiento, todo ello basado en:
- La documentación: mediante la recopilación y enumeración, clasificando la mayoría de los sistemas de criptografía que han existido y enunciar los sistemas más importantes.
- La investigación: mediante distintos soportes a mi alcance, libros, reportajes, revistas y bibliografía digital.

4. REFERENTES.

4.1. Referentes criptógrafos islámicos.

- Aryabhata. (hacia 476-550).
- Brahmagupta. (590-670).
- Abū Yūsuf Ya´ qūb ibn Isḥāq al- Kindī. (801-873).
- Ibrahim ibn Mohammad ibn Dunainir. (1187-1268).
- Abraham ben Samuel Abulafia. (1240-1291).
- Abdul 'aziz ibn ad-Duraihim. (1312-1361).

4. 2. Referentes criptográficos.

- León Battista Alberti. (1404-1472).
- Johannes Trithemius. (1462- 1516).
- Charles Babbage. (1791-1871).
- Hugo Alexander Koch. (1870- 1928).
- Sigfried Giedion. (1888-1968).
- Agnes Meyer Driscoll. (1889-1971).
- Faustino Antonio Camazón Valentín. (1901-1982).
- Margaret Rock. (1903-1983).
- Marian Adam Rejewski. (1905-1945).
- Ignace Jay Gelb. (1907-1985).
- Alan Mathison Turing (1912-1954)
- Elisabeth Lowther Murray (1917-1996)
- Mavis Lilian Batey. (1921-2013).

5. CRONOLOGÍA DE LA CRIPTOGRAFÍA.

5.1. Prehistoria.

5.1.1. Imágenes.

Fig.1 Panel de manos de la Cueva El Castillo, Cantabria, España, aprox. 48000 años de antigüedad.

Fig. 2 Signo en trazo rojo, Cueva de Altamira, Cantabria, España, 35500 - 13000 años de antigüedad.

Fig. 3 Cuerno de marfil, 27000 - 25000 años de antigüedad.

Los símbolos o ideas abstractas de cuyo significado aún no tenemos gran idea, tratan de evidenciar el desarrollo de nuestra mente en el pasado, aún por descifrar. Constituyen maravillas artísticas realizadas hace miles de años, algunas de las cuales superan los 40.000 años de antigüedad en el caso de las manos fig.1 *Sus dedos esbeltos, de delicada factura, se abren sobre la roca como si estuvieran arrojando un encantamiento. La curva entre el pulgar y el índice es bellísima. La forma de esta mano ya no es resultado de una simple impresión; parece haber sido refinada y perfeccionada con ayuda de un pincel. Esta mano revela algo del refinamiento espiritual que debió haber existido en las comunidades del Homo sapiens cuando quiso proyectar su ser interior a través de un medio de expresión supraindividual: el Arte.*[1]

Caracteres propios de nuestra especie son el sentimiento estético y su tendencia a la creación gráfica, entendiendo el arte desde la recreación visual-estética.Fig.3

Los hombres del Paleolítico Superior son los primeros autores de auténticas obras de arte. Con el hombre de Neardental asistíamos a sus balbuceos, con objetos naturales recogidos por curiosidad para ser utilizados como adorno, y las primeras marcas no figurativas sobre hueso.Fig.3-4 Ahora hace entre 30.000 y 10.000 años se extienden por Europa y parte de Asia las primeras manifestaciones artísticas, que tal vez estén en relación con el desarrollo de determinadas facultades cerebrales del Homo sapiens.[2]

En cuanto a los dibujos abstractos, fig.2 su interpretación es aún más compleja. Podemos afirmar es que de aquel pensamiento simbólico surgió algo fundamental para lo que somos hoy en día. Se trata de la capacidad que subyace en fenómenos tan nuestros como el lenguaje, el arte y hasta la religión. Sin él, serían imposibles estos fenómenos que nos identifican como especie.Fig.4

¿Quién sabe si algún día encontraremos la "piedra de Rosetta de la Prehistoria"? Entonces podríamos descifrar qué tenían en esas mentes tan creativas aquellos hombres y mujeres del Paleolítico, cuyo arte sigue maravillándonos miles de años después y son el antecedente de los símbolos previos a la escritura con una simbología compleja y difícil de interpretar.

---

[1]GIEDION, SIGFRIED. *El presente eterno: Los comienzos del arte,* p.131
[2]MOURE, ALFONSO. *El Origen del Hombre,* p. 99.

Fig. 4 Talla en marfil con caballos, La Madeleine, Dordogne, Francia. 14000 - 11500 años de antigüedad.

Una primera y larga etapa sería la del paso de un rudimentario lenguaje inarticulado, que los animales poseen en mayor o menor grado.[3]

En las ruinas de Göbekli Tepe, Turquía, de 11.600 años de antigüedad, se pueden ver esculturas y quizás la primera forma de escritura que muestran esa necesidad de comunicarse por medios a su alcance.Fig. 5

Los símbolos, como tipos especiales de signos, tienen un carácter peculiar. El símbolo es un fenómeno externo que convencionalmente, aunque en relación con la imagen intuitiva que se encierra en él, y a través de ésta, se utiliza para expresar un cierto contenido, a menudo bastante significativo y abstracto.[4]

Fig. 6 El hombre de Urfa o el gigante de Balıklıgöl, 9.500 años de antigüedad.

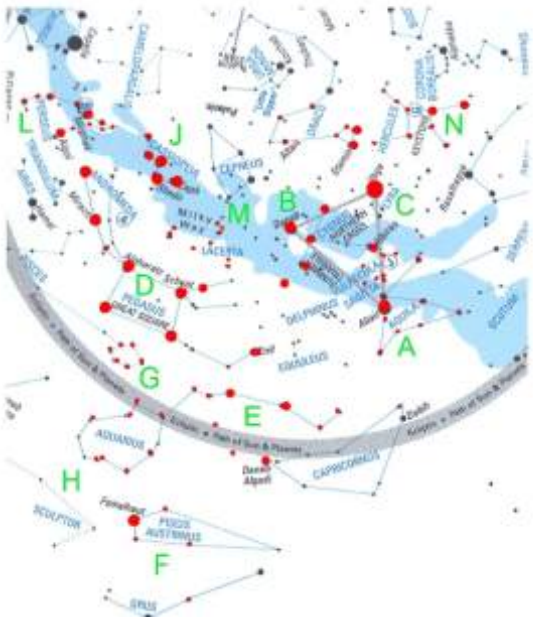


Fig. 5 Göbekli Tepe, 11.000 años de antigüedad.

La disposición de los animales que aparecen en los pilares de Göbekli Tepe, nos están diciendo según el ciclo de precesión, que la construcción se remontaría al año 12.000 a.C., cuando el sol estaba entrando en Virgo.Fig. 5

Este lugar, dobla la antigüedad de la historia de la humanidad, la época donde pensábamos que comenzaron las civilizaciones. Este complejo es miles de años más antiguo que las pirámides y Stonehenge.

Aún no se ha encontrado ninguna herramienta con la que cortaron la piedra, la pulieran… nada. Al igual que ocurriera con las pirámides de Egipto, se desconoce qué utensilios y herramientas se utilizaron para tal obra de ingeniería.

Fig. 7 Astrolabio sumerio, aprox. 3300 a. C.

---

[3]ENCICLOPEDIA UNIVERSAL, EL PAIS. *Historia Universal. Los Orígenes,* p. 182.

[4]REZNIKOV OSIPOVICH, LAZAR´. *Semiótica y teoría del conocimiento,* p.165

Fig. 8 Tablilla pictográfica de Uruk, aprox. 3100 a. C.

Fig. 9 Jeroglífico egipcio, aprox. 3000 a. C.

Fig. 10 Tablilla de Ur, aprox. 2900 - 2600 a. C.

Fig. 11 Tablilla de Shuruppak, aprox. 2600 a. C.

El lugar común al etnólogo y a aquellos de los que habla es un lugar, precisamente: el que ocupan los nativos que en él viven, lo definen, marcan sus puntos fuertes, cuidan las fronteras pero señalan también la huella de las potencias infernales o celestes, la de los antepasados o de los espíritus que pueblan y animan la geografía íntima, como si el pequeño trozo de humanidad que les dirige en ese lugar ofrendas y sacrificios fuera también la quintaesencia de la humanidad, como si no hubiera humanidad digna de ese nombre más que en el lugar mismo del culto que les consagra.[5]

Según Ezequiel 28:14, el Jardín del Edén estaba emplazado en un Monte Sagrado, como el de Göbekli Tepe. También la Biblia hace mención a que la gruta del nacimiento de Abraham, se encuentra en la ciudad de Urfa, apenas a 2 km de distancia de Göbekli Tepe. Esta gruta es conocida como el yacimiento de Balikligöl, y en su interior se encontró una escultura que incrementa el misterio de todo lo que rodea a Göbekli Tepe.Fig.6

Çatalhöyük, que se encuentra en Turquía, una de las aldeas más antiguas del mundo, por supuesto que estas cuevas no aparecieron por la oscuridad de estos lugares. Los espacios habitables más confortables se convirtieron primero en campamentos nómadas y luego en aldeas pequeñas. La humanidad, en su búsqueda de la comodidad para alojar a más población y proporcionar seguridad, comida y convivencia, formó los primeros asentamientos como lo ocurrido en Çatalhöyük hace 9.400 años.

En los precedentes de la historia, se incluyen todos los variados recursos con los que el hombre intentó primeramente transmitir sus ideas y sentimientos, semasiografía, es la fase en la que las pinturas pueden expresar el sentido general que quiere transmitir el que escribe. En esta etapa, la forma dibujada de modo visible - igual que el lenguaje mimético- puede expresar directamente el significado sin que intervenga una forma lingüística.[6]

5.2. Edad Antigua.

5.2.1. Escritura.

Sus orígenes se encuentran en Asia occidental, donde están situadas las ciudades más antiguas, una es Jericó en Palestina y la otra Jarmo en Mesopotamia, sobre 4000 a. C. Las mujeres y hombres del Paleolítico fueron los primeros pintores y arquitectos de la humanidad. En el Neolítico se realizaron las primeras instrucciones en forma de ¿monumentos religiosos? ¿astronómicos o funcionales por sus circunstancias?. Si algo nos querían transmitir, lo tenemos que averiguar.

---

[5]AUGÉ, MARC. *Los no lugares. Espacios del anonimato,* p.49
[6]JAY GELD, IGNACE. *Historia de la escritura,* p.248

Fig. 12 Ladrillo de Ur-Nammu, aprox. 2100 a. C.

Fig. 13 Tablilla sumeria, dimensiones 8 cm x 5 cm, aprox. 1500 a. C.

Fig. 14 Una tablilla del lineal B, aprox. 1400 a. C.

Los sistemas completos de escritura se originaron por primera vez en Oriente, por razones tanto históricas como prácticas, Egipto y las regiones adyacentes de Africa y por lo menos, en el periodo pre-helénico, los paises en torno al Mar Egeo, deben ser incluidas también en el ámbito de las civilizaciones orientales.
*En la amplia zona así delimitada encontramos siete sistemas de escritura, originales y completamente desarrollados, todos los cuales pueden a priori pretender un origen independiente: 1.- Sumerio, en Mesopotamia, 3100 a.C.-75 d.C.*fig.10 *2.- Proto - Elamita, en Elam, 3000 -2200 a.C. 3.- Proto - Indico, en el valle del Indo, 2200 a.C. 4.- Chino, en China, 1300 a.C. al presente. 5.- Egipto, en Egipto, 3000 a.C. - 400 d.C. 6.- En Creta y Grecia, 2000-1200 a.C. 7.- En Anatolia y Siria, 1500-700 a.C.*[7]
La hermosa tableta es un astrolabio, fig.7 un instrumento astronómico, el más antiguo conocido. Se trata de un mapa de las estrellas segmentado, en forma de disco. Las secciones intactas muestran texto cuneiforme de nombres de las estrellas y constelaciones, así como los puntos y diagramas, como flechas, triángulos , líneas de intersección y de una elipse, que comprenden dibujos esquemáticos de seis estrellas y constelaciones.
Según los casos, por consiguiente, la creación artística consistirá , dentro del marco inmutable de una confrontación de la estructura y del accidente, en buscar el diálogo, ya sea con el modelo, ya sea con la materia, ya sea co el utilizador, habida cuenta de aquél o de aquélla, de las que el artista que está trabajando anticipa, sobre todo, el mensaje.[8]
Estas constelaciones se dibujan como puntos que representan estrellas conectadas por líneas. "Así, el mapa de las estrellas circular divide el cielo nocturno en ocho sectores e ilustra las constelaciones más prominentes y su dirección de movimiento".
"Se vive en el mundo visible y se goza de su encanto, y al mismo tiempo se es consciente del mundo invisible, lo mismo que se es consciente de la presión atmosférica, en la que no se piensa cuando no perturba las propias funciones corporales, pero que se torna opresiva e o excitante cuando el equilibrio normal se altera. El mundo invisible está cargado de vida".[9]
Dos textos en etrusco y uno en fenicio que hacen referencia a la consagración del templo. En las Láminas de Pirgi, fig.15 accedemos de una manera parcial a la lengua y a la información sobre la relación entre etruscos y cartagineses, en una época en que ambos pueblos buscaban escapar a la presión ejercida por la cultura helénica en sus áreas de influencia.

---

[7]JAY GELD, IGNACE. *Historia de la escritura,* p.90
[8]LEVI-SRAUSS, CLAUDE. *El Pensamiento Salvaje,* p.51
[9]GIEDION, SIGFRIED. *El presente eterno: Los comienzos del arte,* p.312

Fig. 15 Láminas de Pirgi, siglo IX a, C.

Fig. 16 Alfabeto hebreo, 500 - 600 a. C.

Fig. 17 Escitala Griega, 486 a. C.

Fig. 18 Versión en bambú de el arte de la guerra, 475 a. C.

La ausencia de documentos escritos sobre el significado de las pirámides ha dado origen a fantásticas teorías de su situación central en el globo, a que se lean en ellas misteriosas profecías y a la suposición de que no eran tumbas sino la cristalización del conocimiento científico de la época. Estas teorías se han basado frecuentemente en mediciones inexactas o incluso falsas. Fantásticos mensajes astronómicos se han leído también en las dimensiones de la gran pirámide: la afirmación de que la distancia del sol a la tierra es mil millones de veces la altura de la pirámide, o que, desde otra de sus dimensiones, puede descifrarse el radio de la tierra e incluso los cambios climáticos del periodo glaciar.[10]

La escritura es puramente pictográfica,fig.8 y representa una etapa de transición entre la protoescritura y la emergencia de un silabario. Los escritos sumerios más antiguos que se conocen aparecieron en la antigua ciudad de Uruk.

En "la historia de las artes como disciplina humanística" se examina la relación entre disciplinas humanísticas y científicas, y se buscan las diferencias, pero sobretodo los puntos de contacto en particular, la denominación de métodos exactos para la historia del arte. En "iconografía e iconología" se echan las bases teóricas del método panofskiano: el estudio del significado de las obras de arte contrapuesto al estudio de sus valores formales. Panofsky distingue tres niveles de significado en la obra de arte: "el sujeto primario y natural" (dividido a su vez en "factual" y "expresivo"), que consiste en el reconocimiento sólo de formas; el "sujeto secundario o convencional" que consiste en la determinación de los temas de una obra y de su combinación.[11]

O la escritura en muros de los egipcios, aunque este pueblo también escribía en los lienzos y realizaban inscripciones sobre las momias.

La fuente fundamental de información sobre las matemáticas del antiguo Egipto es el papiro Rhind. Constituye el libro de texto sobre matemáticas más antiguo. Escrito alrededor del año 1650 a.C. por un escribano llamado Ahmes, la obra la copió de un texto más antiguo datado en el 1800 a.C. Lo más probable es que se tratase de un manual para escribas reales, la secta que ejercía todas las tareas de lectura, escritura y aritmética. Y esta cita corrobora la precisión, en la ambiciosa afirmación del Papiro Rhind. *"Cálculo exacto para entrar en conocimiento de todas las cosas existentes y de todos los oscuros secretos y misterios".*

Lineal B es el sistema de escritura usado para escribir el griego micénico, consiste en signos silábicos.fig.14 La traducción del Lineal B, considerada como la forma arcaica de la lengua griega, se debe a dos filólogos británicos, Michael Ventris y John Chadwick, quienes lograron descifrarla en 1952, se conoció como «el Everest de la arqueología griega».

---

[10]GIEDION, SIGFRIED. *El presente eterno: Los comienzos de la arquitectura,* p.449

[11]CALABRESE, OMAR. *El Lenguaje del Arte,* p.38

Fig. 19 Teléfono hidráulico, 360 a. C.

Fig. 20 Escritura ibérica, siglo IV a. C.

5.2.2. Lenguaje.

Las dos características externas más importantes de la conducta humana son la expresión y la comunicación. La primera se refiere a lo que podemos llamar conducta personal; la segunda, a la conducta social. El hombre posee muchas formas, naturales y artificiales, de expresar sus ideas y setimientos. Puede dar expresión, de forma natural, a su alegría, riendo o canturreando, y a su dolor con el llanto o la queja; puede expresarse con ayuda de medios artificiales en un poema, una pintura u otra obra de arte cualquiera.[12]

Parece difícil que lleguemos a saber cómo y cuándo se originó el lenguaje, en cómo empezaron a hablar nuestros antepasados. Hace 400.000 años el homo erectus ya habría desarrollado las áreas cerebrales, relacionadas con la producción y la comprensión del lenguaje; o un posible protolenguaje. La lingüística trata de explicar sus causas y su origen y las lenguas del mundo pueden ser clasificadas en una única genealogía, porque, de acuerdo con el estado de la investigación actual, el género humano tiene un único origen en un solo lugar, África oriental, en torno a 100.000 años a. P. Teorías hay sitúan el origen del lenguaje simultáneamente con el del homo sapiens, que parece que comenzó su andadura hace 50.000 años en África, tras una severa glaciación.

"La invención de la escritura y de un sistema eficaz de indicaciones sobre papel, ha influido más en elevar la raza humana que ninguna otra proeza intelectual en el progreso del hombre".[13]

Cada civilización, a su manera, ha desarrollado y utilizado códigos secretos para mantener incomprensibles textos que, de alguna manera, comprometían su permanencia. Los primeros mensajes que se conocen estaban escritos en caracteres logográficos, es decir, que empleaban dibujos para representar cosas concretas. Volviendo 3.000 años atrás hay que señalar a la ciudad de Uruk, que tiene un papel básico en el origen de la escritura cuneiforme. Fig.8 Hasta la llegada del alfabeto, el uso de la escritura se limitaba a poblaciones de las cuencas del Nilo, el Indo, Tigris y Eúfrates. Escritura: jeroglífica, hierática y demótica. No todo el mundo en el Antiguo Egipto podía leer y escribir jeroglíficos, fig.9 la mayoría de los egipcios utilizaban la lengua demótica y los sacerdotes la escritura hierática, haciendo así su significado incomprensible para el ciudadano común. Las instrucciones de Shuruppak fig11 son una pieza clave de la literatura sumeria, siendo probablemente el tratado de sabiduría más antiguo que existe. Es a su vez, una de las obras escritas más antiguas de la historia de la humanidad. El Código de Ur-Nammu es un código de leyes fechado entre los años 2100 y 2050 a. C.Fig.12

---

[12]JAY GELD, IGNACE. *Historia de la escritura,* p.17
[13]JAY GELD, IGNACE. *Historia de la escritura,* p.285

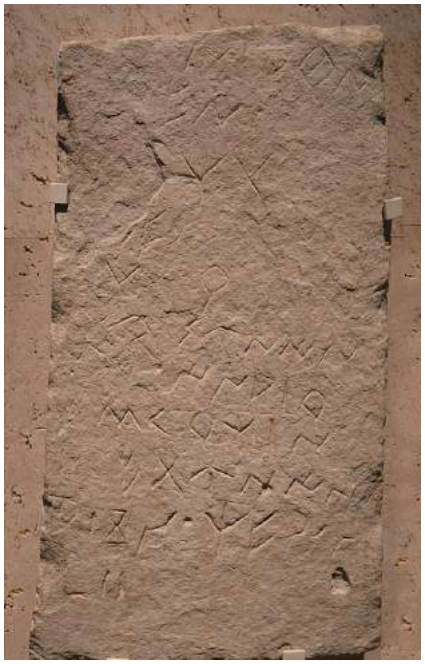


Fig. 21 Cultura ibérica, siglo III a. C.

Fig. 22 Bustrofedon, siglo lll a. C.

Fig. 23 Texto griego escrito en bustrofedon.

El barro cocido, principal y clásica materia de escritura de las civilizaciones caldea y asiria, también se extendió por la mayoría de las culturas y se trasladó a los trabajos de cerámica como azulejos, jarrones y platos.
Una tableta de 8 cm x 5 cm mesopotámica contenía una formula encriptada para construir piezas de cerámica, fig.13 demostración del nivel alcanzado en la antigüedad y de los primeros datos criptográficos.
La escritura comenzó al aprender el hombre a comunicar sus pensamientos y sentimientos mediante signos visibles, comprensibles también para las demás personas con cierta idea del determinado sistema. Al comienzo, las pinturas sirvieron para la expresión visual de las ideas en forma muy distinta del idioma, que expresaba sus ideas de modo auditivo. La relación entre escritura y lengua en los primeros estadios de la escritura fue muy vaga, ya que el mensaje escrito no correspondía a formas exactas de la lengua.[14]
Se estima que desde el siglo X a. C, el idioma hebreo fig.16 se escribía utilizando el llamado alfabeto paleohebreo, una variante del alfabeto fenicio. Más adelante el pueblo hebreo adoptó el alfabeto arameo. Los fenicios no tuvieron una civilización original; fue el resultado de influencias exteriores, griegas, egipcias y mesopotámicas y ante las dificultades de dichas escrituras, crearon el alfabeto, más útil de lo que eran estas escrituras, en lugar de representar sílabas o palabras. Eran letras que representaban ya sonidos y los griegos lo adoptaron para crear su alfabeto, incluyendo vocales; y a su vez éste fue usado por romanos para crear el suyo propio. Esta escritura mejorada retornaría a Fenicia que la expandió por el Mediterráneo, llevándola a todos los pueblos con los que comerciaba. La mayoría de los alfabetos recibieron la influencia de éste, inclusive puede decirse que el actual tiene bases en el fenicio. Se aprecia dicha escritura en la muestra de plomo ibérico de Ullastret con seis líneas.Fig.20
El alfabeto fenicio fig.21 era mucho más simple que los existentes hasta el momento, contaba con puntos para las vocales y 20 signos para las consonantes, así la escritura fue más accesible que la jeroglífica y la cuneiforme que contaban con cientos de signos y solo podían usar los escribas sino que fue accesible a mayor cantidad de personas.

5.2.3. Orígenes de la criptografía.

La definición correcta de criptografía es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

---

[14]JAY GELD, IGNACE. *Historia de la escritura*, p.31

	A	B	C	D	E
A	a	b	c	d	e
B	f	g	h	i	j
C	k	l	m	n	o
D	p	r	s	t	u
E	v	w	x	y	z

Fig. 24 Método de Polibio, 150 a. C.

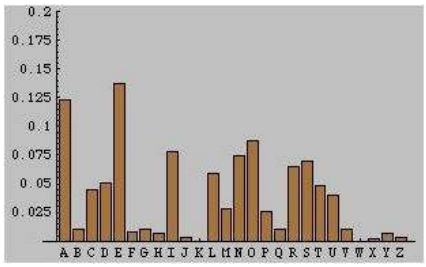


Fig. 25 Análisis de frecuencia, aprox. año 840.

Fig. 26 Alfabeto Orden del Temple, año 1119

En un principio el método fue esconder el mensaje, de forma física, "Esteganografía", es decir, un objeto guardado dentro de otro.

La clasificación de métodos de cifrado son tres:

- Sistema de Códigos, divididos en libros de códigos y nomenclatores.
- Sistema de trasposición, divididos en simple, que a su vez se subdivide en geométrica y columnar y doble.
- Sistema de sustitución, divididos en monoalfabética y polialfabética. La monoalfabética se subdivide en monográfica y poligráfica y ésta en digráfica, trigráfica y poligráfica.

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entes y, en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito.

La Escítala espartana fig.17 fue el primer instrumento criptográfico militar de la historia, usado en varias ciudades griegas hacia el siglo V a.C. El descifrado se producía enrollando la tira alrededor de otro palo que, para poder transformar el galimatías en un mensaje legible. Debía tener el mismo diámetro. Ese dato, el grosor del basón, era la clave.

El arte de la guerra de Sun Tzu fig.18 es el primer tratado castrense del mundo y su influencia ha superado las fronteras militares llegando a la política, la diplomacia, la cultura y la economía. Tiene la importancia de la escritura y la filosofía, un curso de acción conscientemente deseado y determinado de forma anticipada, con la finalidad de asegurar el logro de los objetivos de la empresa, el mismo objetivo que la criptografía. La cábala judía asocia a cada letra del alfabeto hebreo un número, manipulando dichos números con reglas matemáticas. Se pretende descubrir importantes secretos, estudiando cabalísticamente el texto sagrado judío por excelencia: la Torá.

Empleaban también en sus escritos distintos métodos criptográficos, pero más como un medio de dar un aura de misticismo, que con el proposito de ocultar información. El método ATBASH fue utilizado ya entre el 600 y 500 a.C. Existen otros métodos de codificación, pero todos ellos, se basan en la misma idea: sustituir unas letras por otras, o sustutuir letras por símbolos. La mayoría de las lenguas paleohispánicas desaparecieron sin dejar rastro, pero afortunadamente de algunas se han conservado inscripciones en escrituras paleohispánicas y en alfabeto latino que datan desde como mínimo el siglo V a.C. distintas escrituras que fueron naciendo de la misma raíz en la Hispania prerromana, desde el tartésico. Esto coincide con la llegada del imperio Romano a Hispania. Y a partir de la variante levantina, la última transformación se produjo, en torno a mediados del siglo II antes de Cristo, con el idioma celtíbérico y a la larga tendría como consecuencia la desaparición de estas formas de escritura paleohispánica, que en un principio significó una explosión del uso de esas antiguas escrituras.

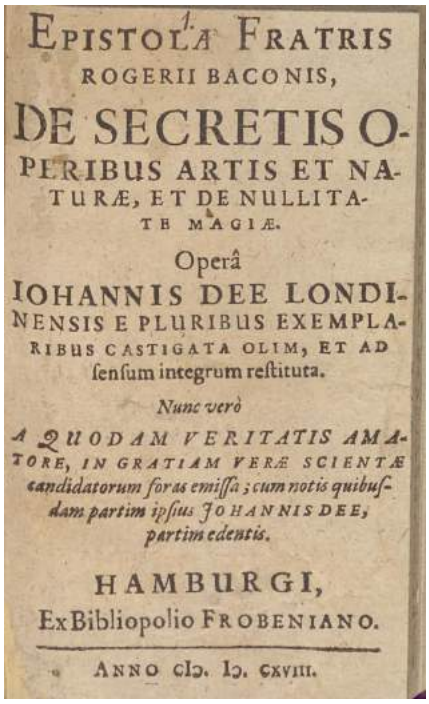

EPISTOLA FRATRIS
ROGERII BACONIS,
DE SECRETIS O-
PERIBUS ARTIS ET NA-
TURÆ, ET DE NULLITA-
TE MAGIÆ.
Operâ
IOHANNIS DEE LONDI-
NENSIS E PLURIBUS EXEMPLA-
RIBUS CASTIGATA OLIM, ET AD
sensum integrum restituta.
Nunc verò
A QUODAM VERITATIS AMA-
TORE, IN GRATIAM VERÆ SCIENTÆ
candidatorum foras emissa; cum notis quibus-
dam partim ipsius JOHANNIS DEE,
partim edentis.
HAMBURGI,
Ex Bibliopolio FROBENIANO.
ANNO CIↃ. IↃ. CXVIII.

Fig. 27 Roger Bacon. La Epístola sobre las obras de arte secretas y la nulidad de la magia, año 1250.

Fig. 28 Nomenclator de Gabriel di Lavinde, año 1379.

Fig. 29 Máquina de cifrar, año 1466.

Hacia los años 360 a.C. fueron creados los telégrafos de agua Fig.19 que almacenaban información detallada y luego se transmitía por señales de humo o fuego. La idea era poder almacenar las señales de los telégrafos de antorcha para que pudieran ser leídas posteriormente, esto se llamo telégrafo hidro-óptico y tenían telégrafos de humo por una longitud total de 4500 kilómetros, estos se usaban ampliamente para señalización militar, en los años 150 a.C. habían cerca de 3000 redes de telégrafos de agua alrededor del imperio Romano.

Bustrofedon fig.22 se trata de la forma en la que leían y escribían los etruscos y los griegos. Esta palabra quiere decir "el buey que da vueltas" y significa que se empezaba a leer de derecha a izquierda cambiando el sentido de la lectura en cada nueva linea.Fig23 El método de Polibio fig.24 no es considerado por muchos autores como verdadera criptografía, pues su interés no reside en ocultar la información, sino en trasmitirla de un modo más eficaz, la cifra de Polibio es históricamente la primera que emplea métodos de sustitución.

Julio César es considerado por muchos el mayor genio militar de la historia, el método Cesar es uno de los más simples y extensamente aplicado por sus técnicas conocidas de encriptado. El mundo de la guerra siempre ha echado mano de la criptografía y grandes avances en este campo se deben a problemas de índole militar.

Los hebreos fueron los primeros en concebir un dios único y por constituir su religión el fondo del cristianismo, la Biblia tiene gran importancia literaria, histórica y moral; enseñanzas filosóficas, cánticos en honor del Eterno, todo escrito en un lenguaje de inspiración.

El nacimiento de Jesucristo, el mayor acontecimiento de la historia, predicó que el principal deber de los seres humanos es el amor a Dios y al prójimo; que todas la personas son hermanas e iguales; y que la misericordia, la humildad, la paciencia, la pobreza y el amor a la justicia tendrán un día su recompensa en el cielo.

En la Biblia, en Jeremías versículos 25,26 y 51,41 aparece el criptograma SHESHACH sustituyendo al texto plano Babel, nombre hebreo bíblico con el que se conoce a la ciudad mesopotámica de Babilonia. Esta sustitución resulta de utilizar la cifra tradicional hebrea atbash.[15]

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

Desde el siglo I de nuestra era, hasta el Renacimiento, este periodo será más oscuro en los métodos utilizados para asegurar y ocultar información. Lo más destacable son las recopilaciones y tratados escritos durante la expansión del imperio árabe.

---

[15]LA SANTA BIBLIA. *Antiguo Testamento, Jeremías 25,26 y 51,41,* p.792. y p.853.

Fig. 30 Disco cifrado, año 1467.

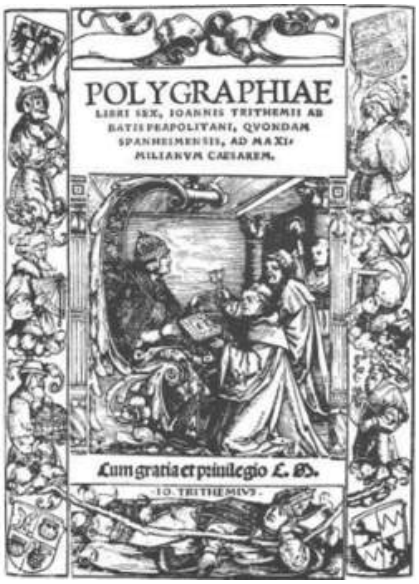


Fig. 31 Obra de Trithemius, Polygraphia, año 1518.

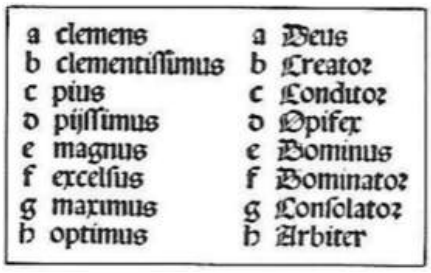


Fig. 32 Primera página del cifrado del Ave María, de Trithemius.

5.3. Edad Media.

5.3.1. Ingenio: periodo, Alta Edad Media.

El primer objetivo entonces era simplemente sobrevivir: un nivel de vida económica por debajo del cual es difícil, que las comunidades de seres humanos sobrevivan, con un mundo en ruinas, muchas comunidades europeas llegaron peligrosamente cerca de la pobreza más abyecta e incluso del hambre y la muerte
En el año 500 d.C. El astrónomo AryaBhatta de India, desarrollo el sistema de numeración decimal con el cual logró encontrar la facilidad de representar números largos con la adición de ceros decimales.
El Brāhmasphuṭasiddhānta de Brahmagupta es el primer texto conocido que trata al número cero con las propiedades que conocemos hoy en día, en lugar de un simple marcador de posición que representa otro número (como lo hicieron los babilonios), o como un símbolo que representa una cantidad nula.
Las letras fonéticas, lenguaje y forma mítica de la cultura occidental, tuvieron el poder de transformar o reducir todos nuestros sentidos en espacio visual, "pictórico" o "cerrado". El matemático tiene la conciencia del carácter arbitrario y ficticio de este espacio visual, continuo y homogéneo. Porque el número, lenguaje de la ciencia, es una ficción para volver a transformar el imaginario espacio auditivo y táctil.[16]
Los árabes, al dominar a lo pueblos más cultos de la antigüedad aprendieron de ellos, a los que supieron unificar creando una cultura árabe. El mérito mayor del mundo musulmán consiste en haber puesto en contacto la cultura oriental con la occidental y habernos transmitido gran parte de la herencia intelectual griega y de los pueblos orientales. Hicieron grandes progresos en las matemáticas, el álgebra; introdujeron en occidente la utilización de cifras nuevas, procedentes de la India y mucho más cómodas para el cálculo que las cifras romanas.
Abu Abdar-Raḥmān al -Khalīl 718-786 produjo el primer diccionario de la lengua árabe y el más antiguo que existe, fue el primer erudito en someter la prosodia de la poesía árabe clásica a un análisis fonológico detallado.
Los datos primarios que enumeró y clasificó con meticuloso detalle fueron extremadamente complejos de dominar y utilizar, y más tarde los teóricos han desarrollado formulaciones más simples con mayor coherencia y utilidad general.

---

[16]MARSHALL MCLUHAN, HERBERT. *La Galaxia Gutenberg,* p.257

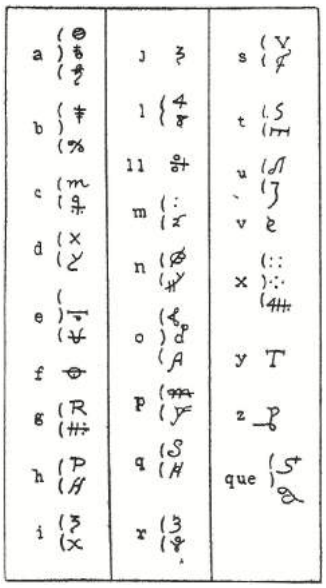


Fig. 33 La tabla de correspondencia usada por Cortés, año 1532.

Fig. 34 Alfabeto de Homófonos de Giovanni Battista Palatino, año 1540.

Fig. 35 Tabla reciproca, año 1553.

El "Libro de los mensajes criptográficos" de Al-Farahidi fue el primer libro sobre criptografía y criptoanálisis escrito por un lingüista. La obra perdida contiene muchas "primicias", entre ellas el uso de permutaciones y combinaciones para enumerar todas las posibles palabras árabes con y sin vocales.

El uso del cifrado ya existía en la Edad Antigua y los métodos criptográficos, se siguieron utilizando también durante la Alta Edad Media. Se trataba de métodos simples, ya que no será hasta el siglo XIII cuando la criptografía comienza a desarrollarse y a estructurarse, sobre en todo en las ciudades italianas y en el Papado.

En época altomedieval se utilizaban tres métodos principales de encriptación, transposición. sustitución o perturbación y ocultación. Carlomagno, quizás es el ejemplo más conocido de la época, ya que la cancillería carolingia utilizó tablas de sustitución muy simples.

Los caracteres ogámicos en Irlanda y los rúnicos en los países germánicos también fueron utilizados para hacer criptografía.

El imperio carolingio el primer gran esfuerzo de reintegración de Europa desde la caída del Roma. La renovatio es el aspecto cultural del empuje imperial. Construir y ordenar el imperio representaba, como punto de partida, establecer nexos, la necesidad de regulación lingüística . La corte de Carlos se decide por el latín, ya entonces una lengua muerta; nadie hablaba propiamente latín y el que se escribía en los distintos documentos había derivado junto a las diversas hablas. La tarea de crear un latín nuevo, único y destinado a todos los hombres de letras, aparece como principal en la renovatio. Había que enseñarlo a todos, cuanto menos a todos los clérigos, la caligrafía había evolucionado también, de la misma manera que las hablas, la necesidad de unificar la escritura.[17]

En la península Ibérica, durante la Alta Edad Media, la escritura utilizada en los documentos oficiales era la escritura visigótica, creada en el reino visigodo.

El primer método era simplemente, y de forma similar al código de Carlomagno, escribir las letras de forma distinta, utilizando una tabla.

Sustituir las vocales por su numeral romano en decenas, sustituir las vocales por grafías de puntos, sustitución de letras latinas por letras griegas.

También se utilizaron métodos de transposición como escribir al revés determinadas sílabas, palabras, oraciones o párrafos completos.

Los manuscritos están entre los artefactos más fascinantes de la Edad Media. Este post se centra en un manuscrito que fue secuestrado por los vikingos: El Códice Aureus de Estocolmo, producido alrededor del año 750 en el sur de Inglaterra.

---

[17]TOMÁS FERRÉ, FACUNDO. *Escrito, Pintado,* p.101

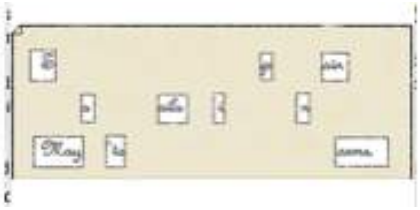


Fig. 36 Método Cardano, año 1554.

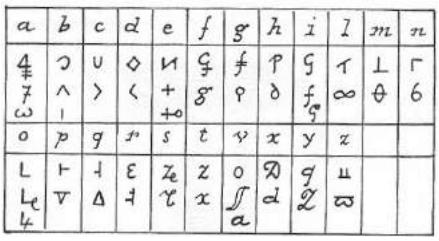


Fig. 37 Cifra General de Felipe II, año 1556.

Fig. 38 Cifra General de Felipe II, año 1556.

La escritura uncial, que en algunas páginas está organizada en un diseño conocido como carmina figurata (poemas en figuras), las miniaturas de los evangelistas y el uso de pergamino púrpura emulan el esplendor de los manuscritos imperiales de la última parte de la Antigüedad.

Otro método de cifrado, similar al de Hygeburg,(el nombre de la monja que escribió las vidas de Willibald y Wynnebald completado en el año 780) es la sustitución de las vocales por puntos, como el alfabeto benedictino.

En el periodo dorado en las artes y en la ciencia en que vivían, los criptógrafos árabes recurrieron explícitamente al análisis fonológico de al-Farahidi para calcular la frecuencia de las letras en sus propias obras. Su trabajo sobre criptografía influyó en Al-Kindi, que descubrió el método de criptoanálisis por análisis de frecuencia.Fig.25

Al-Kindi escribió el libro, Risalah fi Istikhraj al Mu'amma (Tratado de Descifrado de Mensajes Criptográficos), alrededor del año 850 d.C., el libro más antiguo que existe sobre criptografía. El sistema propuesto por Al-Kindi o análisis de frecuencia, permitía descifrar todos los sistemas anteriores de una manera simple. Bastaba con ver los símbolos que más se repetían y compararlo con las veces que las letras del alfabeto aparecían en el idioma del mensaje. Una vez que se vio que el análisis de frecuencias permitía criptoanalizar textos, los diseñadores de códigos inventaron algo nuevo: los nulos. Fueron árabes, los primeros en descubrir y escribir los métodos de criptoanálisis. Mi mayor referente es Abu Yusuf Ya'qūb ibn 'Ishāq as - Sabbāh **al-Kindi,** y su sistema consistía de la siguiente forma:

"Una manera de resolver un mensaje cifrado, si sabemos en qué lengua está escrito, es encontrar un texto llano diferente escrito en la misma lengua y que sea lo suficientemente largo para llenar alrededor de una hoja, y luego contar cuántas veces aparece cada letra. A la letra que aparece con más frecuencia la llamamos «primera», a la siguiente en frecuencia la llamamos «segunda», a la siguiente «tercera», y así sucesivamente, hasta que hayamos cubierto todas las letras que aparecen en la muestra de texto llano. Luego observamos el texto cifrado que queremos resolver y clasificamos sus símbolos de la misma manera. Encontramos el símbolo que aparece con más frecuencia y lo sustituimos con la forma de la letra «primera» de la muestra de texto llano, el siguiente símbolo más corriente lo sustituimos por la forma de la letra «segunda», y el siguiente en frecuencia lo cambiamos por la forma de la letra «tercera», y así sucesivamente, hasta que hayamos cubierto todos los símbolos del criptograma que queremos resolver".

En el 855 Abu Bakr escribió hace siglos un libro del frenético deseo del devoto de aprender el acertijo de los Escritos Antiguos , y expuso muchas reglas para componer y descifrar alfabetos misteriosos, útiles para las prácticas de magia pero también para la correspondencia entre ejércitos, o entre un rey y sus enviados.

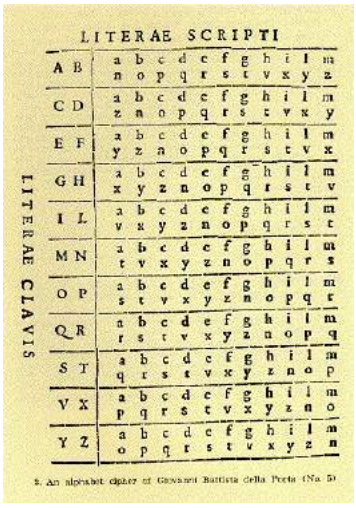


Fig. 39 Método Della Porta. año 1563.

Fig. 40 Nomenclator de Walsingham, año 1582.

Fig. 41 Nomenclator, de María Estuardo, año 1586.

5.3.2. Periodo, Plena Edad Media.

El papa Silvestre ll, (que gobernó entre 999 y 1003) ya era reconocido como un gran erudito, teólogo y filósofo. Lo que no era tan común fue su afición por las matemáticas. Sus ideas ayudaron a crear el reloj de péndulo, estudió las órbitas planetarias y escribió sobre geometría. Sustituyó los números romanos por los árabes (1,2,3,…hasta 9).
En criptografía utilizaba para sus notas un primitivo sistema taquigráfico inspirado en los romanos, concretamente en Marco Tulio Tirón, y por eso se denominan notas tironianas .[18]
Otro importante personaje de la Edad Media fue una mujer: Hildegarda de Bingen, abadesa nacida en 1098. Mente inquieta y polifacética que, entre sus muchos intereses, exploró los números y la criptografía. Utilizaba un alfabeto para cifrar, que le había sido revelado en un momento de inspiración.
La orden del Temple, desde su fundación durante la Primera Cruzada por Hugo de Payens y el rey de Jerusalén, Balduino II, en el día de Navidad de 1119 y en la Iglesia del Santo Sepulcro de Jerusalén, la Orden de los Caballeros Templarios (esto es, la Orden de los Pobres Caballeros de Cristo y del Templo de Salomón, que fue su denominación original) se auto impuso la misión de defender los Santos Lugares de la amenaza musulmana y a los peregrinos cristianos que a ellos se acercaran: concretamente, y en sus inicios, a aquellos que realizaban el trayecto, plagado de peligros, entre Jaffa y la propia Jerusalén. Desde entonces (y a pesar de la creación de otras Órdenes similares, como la de sus rivales los Hospitalarios), su poder fue aumentando década a década en Tierra Santa y Europa occidental, llegando a constituir un estado dentro del estado (cuyo ámbito de actuación era la Cristiandad), sólo obligado a rendir cuentas a través del Gran Maestre al Papa. Su ascenso y preeminencia se explican en gran parte por la dirección de San Bernardo, el reformador de la orden benedictina, sobre cuyo modelo articuló en el Concilio de Troyes de enero del año 1128 la regla primitiva que los caracteriza como “Militia Christi” (ejército de Cristo).
El alfabeto, se componía de: caracteres latinos, griegos y cuneiformes, principalmente del Alfabeto Ugarit. La escritura usaba una criptografía, que resultaba casi imposible descifrar.
El Temple uso diferentes modelos de cruces, que se utilizaban para desencriptar los documentos. Cada Maestre, tenia una Cruz, con sus particularidades. Siendo Maestre Robert de Craon, se efectuó transición hacia la Cruz de las Ocho Beatitudes, para permitir una mejora y un mayor número de combinaciones de las posiciones. La Criptografia Templaria era espacial y cada letra tenia un significado diferente según la posición que ocupaba. El método corresponde a un sistema de sustitución simple y se utilizó para cifrar las letras de crédito que ponían en circulación con el fin de evitar los envíos de dinero en metálico. Fig. 26

---

[18]PRIETO, MANUEL JESÚS. *Historia de la Criptografía,* p.59

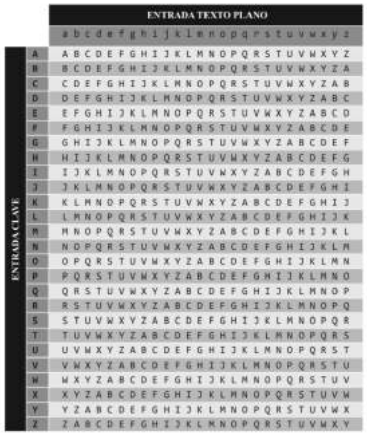


Fig. 42 Tablero de Vigenere, año 1587.

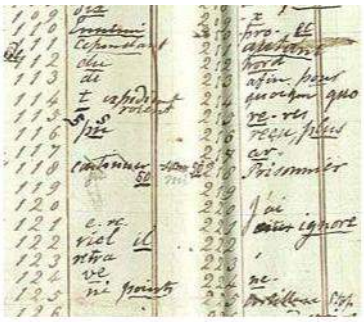


Fig. 43 El Gran Cifrado, año 1626.

Fig. 44 Método francmasón, año 1700.

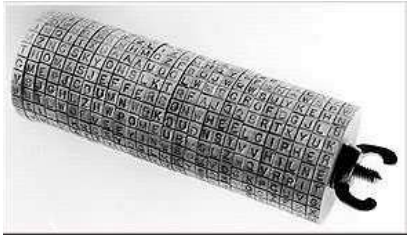


Fig. 45 Cilindro de Jefferson, año 1795.

También poseían un lenguaje dactiológico para comunicarse mediante gestos con las manos, que podría considerarse un lejano precedente del lenguaje de signos.

Ibrahim ibn Mohammad ibn Dunainir 1187–1229 introduce los cifrados algebraicos (sustituir las letras por números, transformarlos mediante operaciones aritméticas).

Subh al-aʿshā en 1193 escribe las instrucciones completas para el criptoanálisis, en sus dos obras principales: Al - mu'lam y Al - mu'allaf lil - malik al - Asraf.

Una de sus contribuciones más importantes fue el tamaño de la muestra para el uso del análisis de frecuencia. Creía que un criptograma "debería tener al menos 90 letras de longitud y que cada una de las 28 letras del árabe debería representarse al menos tres veces".

El poder mnemónico de la imagen, que es ciertamente importante para muchas formas de arte religioso y profano. Las vidrieras de Chartres muestran el poder del simbolismo que transforma una metáfora en una imagen memorable con la vivida presentación de la doctrina de que los apóstoles se apoyan en los hombros de los profetas del Antiguo Testamento. Todo el amplio género de las imágenes alegóricas atestigua esta posibilidad de transformar una idea abstracta en imagen. La capacidad de la imagen para ofrecer un máximo de información visual sólo podía explotarse en periodos en que los estilos del arte eran suficientemente flexibles y ricos para esa tarea.[19]

El primer libro que describe el uso de la criptografía fue escrito en 1250 por el monje franciscano Roger Bacon, con el título "La Epístola sobre las obras de arte secretas y la nulidad de la magia", en el que se describen siete métodos para mantener en secreto los mensajes.Fig.27 Consciente de la obra de Al-Kindi y de lo fácil que era descifrarlos usando las técnicas anteriores, usó varios trucos para luchar contra el análisis estadístico: los homófonos y las nulas.

Las especulaciones proféticas de Abraham ben Samuel Abufalia, le llevaron lejos de las ideas aceptadas en aquellos tiempos entre los cabalistas, sobre la naturaleza divina y la manifestación de ésta en los seres vivos. Él nos habla de una unión con Dios que se manifestará a través de los distintos nombres de éste utilizando la guemetria, ciencia que estudia la relación numérica de las letras del alfabeto hebreo; su estilo cabalístico fue denominado "cábala estática o profética".

Abulafia describe un tipo lingüístico de Cábala, produce una síntesis entre la comprensión como resultado de la transformación de la afluencia intelectual en un mensaje lingüístico y las técnicas para llegar a tales experiencias mediante combinaciones de letras y su pronunciación, ejercicios de respiración, contemplación de partes del cuerpo, movimientos de la cabeza y las manos y ejercicios de concentración. El reino supremo, especialmente el intelecto agente cósmico, en términos lingüísticos, como habla y letras.

---

[19]GOMBRICH, ERNST HANS. *La imagen y el ojo,* p.147

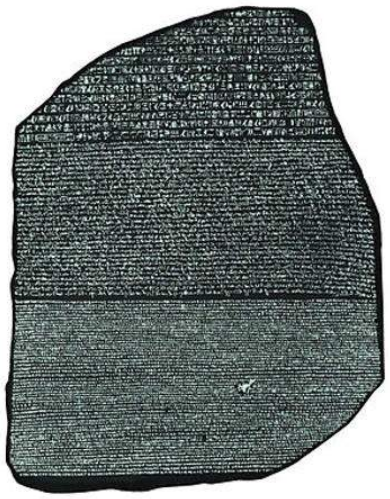


Fig. 46 La Piedra Rosetta, año 1799.

m	a	t	e	i
c	s	b	d	f
g	h	j	k	l
n	o	p	q	r
u	v	x	y	z

Fig. 47 Cifrado Playfair.

Fig. 48 Cifrado Playfair, año 1854.

Fig. 49 Cifrador por vallas, año 1861.

Abulafia desarrolló una sofisticada teoría del lenguaje, que asume que el hebreo representa no tanto el lenguaje como el escrito o hablado, sino los principios de todos los idiomas, a saber, los sonidos ideales y las combinaciones entre ellos. Por lo tanto, el hebreo como idioma ideal abarca todos los demás idiomas. En sus escritos, Abulafia utiliza palabras griegas, latinas, italianas, árabes, tártaras y vascas para la gematría.

5.3.3. Periodo, Baja Edad Media.

Ad - Duraihim (1312) escribe la clasificación de cifrados, análisis de frecuencias para muchos idiomas.
Palatino estaba fascinado por sistemas de cifrado y en general por la metamorfosis del alfabeto.
Gabriel di Lavinde de Parma escribió "Nomenclator"fig.28 en 1379 que es el primer manual europeo sobre cifrado.
Qalqashandi escribe "El amanecer de los ciegos", una enciclopedia de catorce volúmenes terminada en 1412. Constituye un manual administrativo sobre geografía, historia política, historia natural, zoología, mineralogía, cosmografía y medición del tiempo. Contiene un capítulo sobre criptología. El Subh al-aʿshā fue el primer debate publicado sobre la sustitución y la transposición de cifrados, y la primera descripción de un cifrado polialfabético, en el que a cada letra del texto plano se le asigna más de una sustitución.
Leon Battista Alberti fue uno de los ejemplos de "homo universalis" del Renacimiento. Leon Alberti inventó el disco cifrado fig.29,30 y la clave criptográfica. El disco de cifrado de Alberti era polialfabético, significando que un nuevo alfabeto podía ser creado cada vez que girara el disco. Este tipo de disco fue el único método de uso de este tipo de cifrado hasta el siglo XVI. Alberti pensó que este cifrado era irrompible, basando su afirmación en sus investigaciones sobre el análisis de frecuencia, que sería el método más efectivo de descifrado de criptogramas monoalfabéticos. En el mundo de la criptografía su aportación más importante es De Componendis Cyphris, escrito en 1466 (aunque fue publicado un siglo más tarde). Es el libro sobre criptografía más antiguo que se conoce en el mundo occidental, se ganó el título de padre de la Criptología Occidental.
Leonardo de Vinci, escribió el Tratado de la pintura, con la costumbre que tomó de escribir a lo oriental, esto es, de derecha a izquierda como los Hebreos y Arabes, es preciso que cause mucha dificultad para sacar la primera copia, y por consiguiente padecerían.[20]
Francesco Simonetta ha sido descrita en la literatura criptográfica como un criptoanalista importante en la consideración de sus reglas. Su trabajo es en realidad una colección de consejos para la resolución de sistemas de cifrado.

---

[20]DE VINCI, LEONARDO. *El Tratado de la Pintura,* p.42

Fig. 50 Disco de cifras, año 1861.

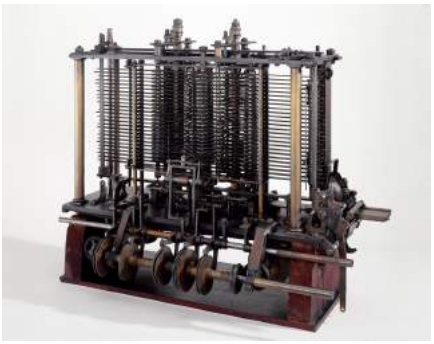


Fig. 51 La Máquina Analítica, construida por Charles Babbage hacia el final de su vida, año 1871.

Fig. 52 Cilindro de Bazeries, año 1901.

	A	D	F	G	V	X
A	8	p	3	d	l	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

Fig. 53 La cifra ADFGVX, año 1914.

5.4. Edad Moderna.

5.4.1. Capacidad creadora.

Giovanni Soro fue empleado en Venecia en 1506 por el Consejo de los Diez como jefe de descifrado. Dicho consejo podría considerarse como el primer servicio secreto especializado en descifrar códigos. Soro dirigió la operación de criptoanálisis en secreto como secretario de cifrado. Las tareas de Soro incluían descifrar los mensajes secretos capturados de los espías mensajeros de los rivales de Venecia y fue capaz de descifrar las claves de la mayoría de las otras Cortes. En 1510, había forzado a la mayoría de ellos a desarrollar sus claves con un grado mucho más alto de sofisticación.
Como resultado, la Curia Papal lo contrató para descifrar códigos que sus propios analistas de cifrado en Roma no podían. El Papa Clemente VII a menudo enviaba mensajes a Soro para el criptoanálisis para probar su impenetrabilidad. Fue el principal criptoanalista de Venecia durante casi 40 años; la reputación de Soro era grande entre los líderes de otras ciudades-estado italianas y de Europa. Hizo de Venecia un bastión renacentista de la criptología diplomática; escribió un tratado en italiano, francés, español y latín a principios del siglo XVI sobre criptografía y resolución de cifrados, fue el primer criptoanalista destacado del Renacimiento y el primer gran criptoanalista del mundo occidental.
Johannes Trithemius también está considerado como padre de la criptografía gracias a su publicación de 1518 de su obra Poligrafía, fig.31 considerado el primer libro impreso sobre Criptografía. En él, su autor utiliza un método mucho más complicado llamado codificación polialfabética. Esta codificación sería usada desde el siglo XV hasta el XX, fig.32 siendo el corazón de la máquina Enigma utilizada por Alemania durante la Segunda Guerra Mundial.
La carta cifrada del 25 de junio 1532 de Hernán Cortés a Núñez, está redactada en escritura humanística cursiva siendo, el sistema de cifrado empleado es el nomenclátor. Fig.33
Todos los signos cifrados están escritos de corrido, sin ningún espacio entre ellos que nos indique dónde empiezan y acaban las palabras, lo que hace más difícil su interpretación. Su desciframiento fue muy dificultoso ya que se usaron diferentes caracteres para una misma letra, mezclando los de tipo matemático con los alfabéticos. Sin embargo, no se utilizaron los nulos ya que Cortés empleó deliberadamente ciertos métodos para esconder el significado literal de los caracteres, usando un sistema criptográfico que mezcla cifras y códigos, un sistema basado en la sustitución homofónica.
Giovanni Battista Palatino, calígrafo italiano, fue autor del más notable tratado de escritura y muestras caligráficas del Renacimiento, titulado *Libro nuovo d'imparare a scrivere o Libro nuevo de aprender a escribir*, publicado en Roma en 1540 fig.34 reconocido sin duda como uno de los documento más interesantes de la cultura de la comunicación de la Edad Moderna.

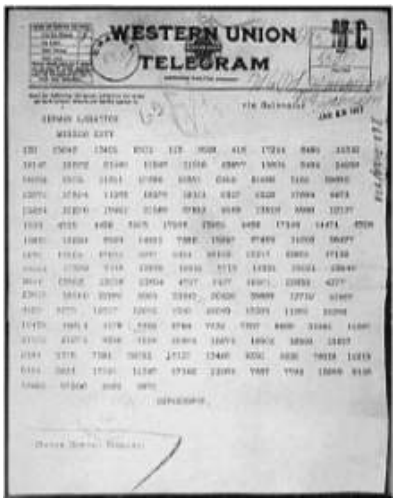


Fig. 54 Telegrama Zimmerman, año 1917.

Fig. 55 Libreta de un solo uso. año 1917.

Fig. 56 Precedente máquina Enigma, año 1918.

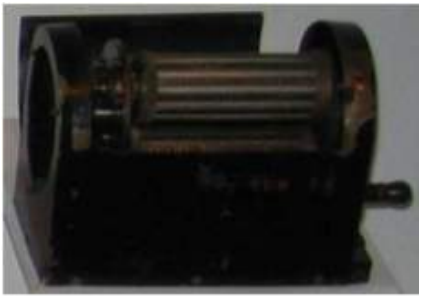


Fig. 57 Máquina de cifrado Damm, año 1919.

Giovan Battista Bellaso en 1553, publicó en Venecia un pequeño manuscrito de titulo La cifra del Signo, en el que proponía el uso de una tabla recíproca de once alfabetos de sustitución gestionados por una contraseña.Fig35 Bellaso fue quien primero sugirió identificar los alfabetos mediante una contraseña o palabra clave acordada fuera de línea. También enseñó varias formas de mezclar los alfabetos cifrados para liberar a los corresponsales de la necesidad de intercambiar discos o tablas preescritas: el cifrado se realiza mediante una frase acordada llamada contraseña, colocada sobre el texto claro. Con referencia a la tabla, se sustituye la letra del texto simple por la letra que está encima o debajo de ella en el alfabeto identificado por la letra mayúscula de la contraseña. Este cifrado es una polisustitución letra por letra usando una larga cadena de claves literales, el sistema sigue siendo periódico, aunque el uso de uno o más signos de interrogación largos lo hace suficientemente seguro.

Girolamo Cardano, su libro sobre juegos de azar,, constituye el primer tratado serio de probabilidad abordando métodos de cierta efectividad, también introdujo la rejilla de Cardano fig.36 una herramienta criptográfica. La Cifra General fig.37 en el siglo XVI era común que todos los gobernantes utilizaran algún método de cifrado, sobre todo si el mensaje debía atravesar algún territorio extranjero. La comunicación con los embajadores, y en general toda la diplomacia, utilizan de modo cotidiano la criptografía. En tiempos de Felipe II el método criptográfico más utilizado era el de sustitución, aunque con una serie de aditamentos. Trataremos aquí la conocida como La Cifra General que fue la primera que utilizó Felipe II, está fechada en 1556.Fig.38

En el ámbito de la criptografía, la obra más importante de Giovanni Battista Della Porta, en el ámbito de la criptografía su obra más importante data del 1563 y es De Furtivis Literarum Notis, compendio de cuatro volumenes donde además de estudiar los cifrados clásicos y su criptoanálisis, expone también un nuevo método de cifrado. La característica principal de este método es la utilización de distintos alfabetos y de una palabra clave.Fig.39 También inventó un método que le permitía escribir mensajes secretos en el interior de los huevos. Durante la Inquisición española, algunos de sus amigos fueron encarcelados y en la puerta de la prisión, todo era revisado excepto los huevos. Della Porta escribía mensajes en la cáscara del huevo usando una mezcla fabricada mediante pigmentos vegetales y alumbre. La tinta penetraba en la cáscara del huevo, que es semi-porosa, y cuando la pintura se secaba, hervía el huevo en agua caliente y la tinta del exterior del huevo desaparecía. Cuando el receptor en prisión eliminaba la cáscara, el mensaje se revelaba “impreso” en la clara del huevo cuajada.

María Estuardo desde su “prisión” contactó con don Juan de Austria, quién junto a otros nobles de la época deseaba ver destronada a la reina inglesa. Así que ambos entraron en contacto epistolar, mediante cartas que se encargaba cuidadosamente de cifrar y de las cuales tenía realizadas un amplio nomenclátor o libro de claves con sus equivalencias.Fig.41

Fig. 58 Agnes Meyer.

Fig. 59 Máquina Kryha, año 1920.

Fig. 60 Discos Cipher, año 1920.

Fig. 61 Primera máquina de cifrado con rotores, de Herbern, año 1917.

Un complejo y detallado manual de símbolos extraños, letras invertidas e indicaciones que se hacían en márgenes, encabezados o pie y que podían dotar de una significación diametralmente opuesta lo que se escribía y sólo descifrable por aquel que conocía el código.

María Estuardo era una gran criptógrafa, sus cartas así lo demuestran y se afanó en las técnicas de sustitución, creación y teoría de bloques. De todo ello confeccionaba un manual que formaba parte de su nomenclátor.

El problema para María Estuardo surgió cuando Francis Walsingham sospechó que en el correo entre la reina y el noble español podía contener algo más que alentadoras palabras y puso a trabajar a los criptógrafos de Isabel I en descifrar los códigos, se hablaba de los planes de María Estuardo para asesinar a Isabel I.

Francis Walsingham, secretario principal de la reina Isabel I de Inglaterra desde el 20 de diciembre de 1573 hasta su muerte, es recordado popularmente como su «maestro de espías» se denomina nomenclátor a una variante de las cifras de sustitución que se caracteriza por emplear signos o caracteres particulares para sustituir palabras específicas. Fig.40

Blaise de Vigenère, en sus trabajos como diplomático entró en contacto con el mundo de la criptografía y una vez retirado de su carrera, dedicó gran parte de su tiempo a este arte. En 1586 publica un libro sobre números o formas de encriptar y en él expone su nuevo método de cifrado, que está basado en la cifra de César y utiliza las ideas de Alberti. El método es tan bueno que lo pudo publicar sin guardarlo en secreto, porque aunque el comienzo del mensaje diga claramente "Este mensaje está codificado con la cifra de Vigenère", el desconocimiento de la clave hace prácticamente imposible su descifrado. Fig.42

La vida del acróstico. En el año 1600 los poetas provenzales son por algunos considerados como los primeros que se dedicaron a este género de composiciones y de ellos al parecer lo aprendieron los poetas castellanos.

En Gran Bretaña Francis Bacon en 1605 crea un sistema de combinaciones con los signos "A" y "B".

Francis Bacon ya propuso en su día que el texto cifrado no debería ser sospechoso, que debería tener una apariencia inocente. Este método, debido a Girolano Cardano, hace uso de este consejo y para cifrar un mensaje le introduce una serie de caracteres basura que son irrelevantes y que no hacen más que esconder el verdadero mensaje y despistar a un posible interceptor del mismo. Las letras que se introducen no son aleatorias, se trata de obtener un mensaje inocente y que parezca que no está cifrado.

El cifrado de Gronsfeld surgió como una mejora al cifrado Vigenère, ya que era susceptible a un análisis críptico con ciertas condiciones previstas.

Fue ideado por Jost Maximilian von Bronckhorst-Gronsfeld y se trata de un cifrado del tipo poli alfabético cuya característica es ser resistente tanto al des-encriptado por "fuerza bruta" como "al análisis de frecuencia" (número de veces que se repiten los caracteres).

5.5. Edad Contemporánea.

5.5.1. Talento constructivo.

Fig. 62 Máquina Hebern, año 1921.

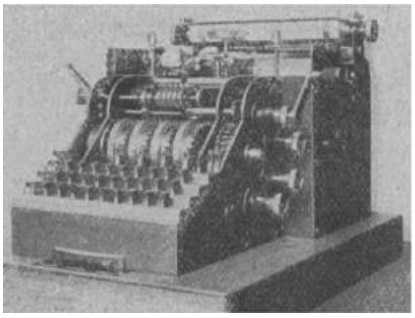


Fig. 63 Máquina Enigma, año 1923.

Fig. 64 Máquina Enigma, año 1924.

Antoine Rossignol y su hijo Bonaventure inventaron un código utilizando 587 números diferentes que era tan resistente que desconcertó a los criptoanalistas durante siglos hasta que el criptoanalista militar Étienne Bazeries, a petición de un historiador, lo descifró finalmente hacia 1893, después de tres años de trabajo, dándose cuenta de que cada número representaba una sílaba de la lengua francesa en lugar de una sola letra como los códigos tradicionales.
En 1691, el "Grand Chiffre" fue un directorio de sustitución de cifrado para mensajes de alto secreto desarrollado por los ruiseñores (juego de claves), varias generaciones de los cuales trabajaron para la corona francesa como criptólogos. También desarrollaron el "Petit Chiffre" para las comunicaciones de naturaleza puramente confidencial. Conocido como irrompible, cayó en desuso, habiendo desaparecido su secreto con la muerte de sus autores. Como resultado, los archivos que se utilizaban para cifrar (documentos diplomáticos en particular) permanecieron ilegibles durante mucho tiempo. El gran cifrado se empleó para encriptar los mensajes más secretos del Rey Luis XIV.Fig.43
Los Masones comienzan a utilizar el cifrado PigPen, que es una sustitución monoalfabética que toma un símbolo en función de un patrón preestablecido.Fig.44
Los cilindros de Bazeries fig. 52 y Jefferson son sistemas que funcionan mediante la rotación de una serie de anillos numerados fijados a un eje formando un cilindro. La diferencia entre ambos es el número de anillos que lo forman: 20 con 25 letras en cada anillo en el caso del de Bazeries, y 36 en el de Jefferson.Fig.45
Uno de los primeros estudiosos que cuestionó el prejuicio de que los jeroglíficos eran una escritura pictórica fue el prodigioso polifacético inglés Thomas Young. Cuando Young oyó hablar de la Piedra Rosetta, ésta se convirtió en un desafío irresistible.
En el verano de 1814 Young intentó descifrar los textos de la Piedra de Rosetta, fig.46 un fragmento de una antigua estela egipcia de granodiorita inscrita con un decreto publicado en Menfis en el año 196 a.C. Algunas de las conclusiones de Young aparecieron en el famoso artículo sobre Egipto escrito en 1818 para la Enciclopedia Británica. Aunque Young había logrado traducir correctamente algunos jeroglíficos de la piedra Rosetta, descifró en la piedra el nombre de Ptolomeo, la primera traducción completa la realizó el francés Jean-François Champollion.
En 1808, el estudioso francés François Champollion empieza a trabajar en la llamada Piedra de Rosetta, la triple inscripción en caracteres jeroglíficos, demóticos y griegos que en 1799 han descubierto las tropas napoleónicas en las proximidades de la ciudad de Rosetta, en el Delta. Champollion, estaba listo para

Fig. 65 Máquina Hagelin, año 1927.

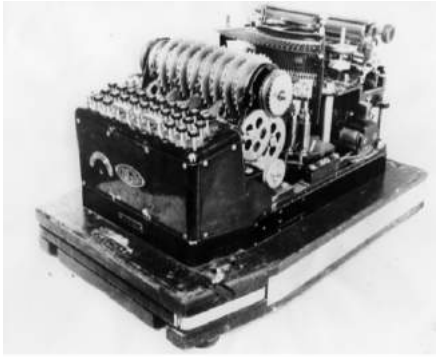


Fig. 66 Máquina Enigma, año 1929.

Fig. 67 Sistema de cifrado M - 138, año 1930.

llevar las ideas de Young a su conclusión natural. En 1822, 14 años después, presenta su método de traducción y la escritura jeroglífica desvela todos sus secretos.

El Cifrado Rail Fence o zig - zag fig.49 es una forma de cifrado por transposición que ha tomado su nombre la forma en que se codifican los textos al utilizarlo.

El sistema de cifrado Beaufort, creado por Sir Francis Beaufort , es una sustitución de cifrado similar al sistema de cifrado Vigenère, con un mecanismo de cifrado ligeramente modificado. Su aplicación más famosa fue en una máquina de cifrado basado en el rotor, el Hagelin M-209.Fig. 74

Charles Babbage logró resultados notables en criptografía, al darse cuenta de que cifrar texto plano con una palabra clave hacía que el texto cifrado se sometiera a la aritmética modular. Durante la Guerra de Crimea de la década de 1850, Babbage rompió el cifrado por autoclave de Vigenère, así como el cifrado mucho más débil que se llama hoy en día el cifrado de Vigenère.

Charles Babbage sentó los principios básicos de las computadoras modernas, como el concepto de programa o instrucciones básicas (que se introducen en la máquina de manera independiente de los datos), el uso de la memoria para retener resultados y la unidad aritmética. La máquina de Babbage, construida exclusivamente con piezas mecánicas y multitud de ruedas dentadas, utilizaba las tarjetas perforadas para la introducción de datos y programas, e imprimía en papel los resultados con técnicas muy similares a las que se emplearon hasta mediados de los años 70.Fig.51

Auguste Kerchoff es mejor conocido por una serie de dos ensayos que publicó en 1883 en el Periódico de Ciencia Militar. Estos artículos examinaban el estado del arte en la criptografía militar e incluía muchas piezas de recomendaciones y reglas generales, como la Ley de Kerckhoff. Esta ley establece que: “No hay secreto en el Algoritmo – Todo esta en la clave”.

También incluían muchos consejos prácticos y reglas generales, incluidos seis principios de diseño práctico del cifrado:

El sistema debe ser, si no teóricamente irrompible, sí en la práctica.

El diseño de un sistema no debe exigir el secreto, y el compromiso del sistema no debe incomodar a los corresponsales (principio de Kerckhoffs).

La clave debe ser memorable sin notas y debe ser fácilmente cambiable.

Los criptogramas deben ser transmisibles por telégrafo.

El aparato o los documentos deben ser portátiles y operables por una sola persona.

El sistema debe ser fácil, sin necesidad de conocer una larga lista de reglas ni de hacer esfuerzos mentales.

El más conocido es el segundo de sus seis principios, el de Kerckhoffs. Puede entenderse como la idea de que la seguridad de un criptosistema debe depender sólo de la llave, y no del secreto de cualquier otra parte del sistema.

Fig. 68 Máquina Hagelin, año 1930.

Fig. 69 La OMI Alpha, año 1930.

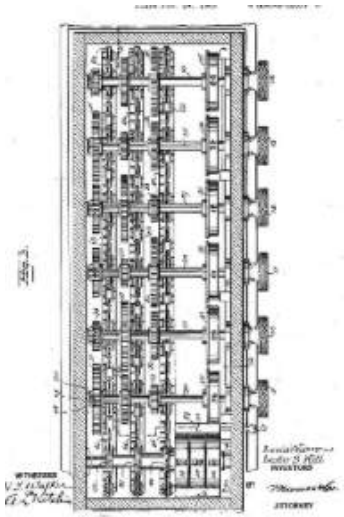


Fig. 70 Máquina del cifrado de Hill, año 1931.

Charles Wheatstone, aparte de crear uno de los métodos más originales de cifrado, el de playfair fig.47 alrededor de 1850, que fue utilizado por los militares de varias naciones al menos durante la Primera Guerra Mundial, y se sabe que fue utilizado también durante la Segunda Guerra Mundial por los servicios de inteligencia británicos, ideó una criptografía o máquina para convertir un mensaje en cifrado, lo que solo podía interpretarse colocando el cifrado en una máquina correspondientemente ajustada para descifrarlo.Fig.48

El código original de Baudot, desarrollado alrededor del año 1874, se conoce como *Alfabeto Internacional de Telegrafía Nº 1*, es un sistema mecánico capaz de traducir automáticamente el alfabeto latino al alfabeto Morse, y viceversa.

La cifra de Delastelle codifica cada grupo por separado, como un bloque, no obstante, bloques similares, dan como resultado bloques similares, que se diferencian, exclusivamente, en una o, a lo sumo, dos letras del anterior. Había descrito por primera vez el principio en la Revue du Génie civil en 1895, bajo el nombre de "nueva criptografía". Esta cifra combina fraccionamiento con la transposición y fue un sistema de cifrado que ponía en práctica los principios de la confusión y difusión, un "sistema de considerable importancia en la criptología". Cifra presenta dos variantes, la cifra bífida y la cifra trífida.

Disco de Alberti, un disco de cifras de la Confederación estadounidense utilizado en la guerra civil norteamericana. La clave del sistema viene definida por el orden de los símbolos en el anillo móvil y por la situación inicial relativa de los dos anillos.Fig50

En 1901, un granjero neozelandés llamado Donald Murray diseñó una nueva máquina de telegrafía, para la que modificó el código de Baudot. Este nuevo código, con caracteres de arranque y parada para funcionar con las nuevas máquinas asíncronas de la época, fue estandarizado en 1930 por el CCITT como "Alfabeto Telegráfico Internacional Nº 2", ITA2 o, como se conoce coloquialmente, "Código Baudot-Murray", y aún se usa hoy en día.

La cifra ADFGVX, fig.53 inventada por Fritz Nebel en 1917, al igual que la cifra ADFGX a la que sustituyó a partir de mayo de 1918, fue escogida por el Alto Mando alemán como la más segura para cifrar sus comunicaciones antes de las grandes ofensivas de 1918, durante la Primera Guerra Mundial. La cifra ADFGVX, al igual que la cifra ADFGX se dividía en dos fases: una primera fase de sustitución y una segunda de transposición. Durante el tiempo que la estuvieron empleando, y al igual que habían hecho con la cifra ADFGX, los ejércitos alemanes cambiaban las claves diariamente, tanto para la fase de sustitución como las palabras clave de la fase de transposición.

Fig. 71 Elizebeth Smith.

Fig. 72 William Friedman y Elizebet Smith.

Fig. 73 Máquina Enigma M 1, año 1934.

5.5.2. Máquina Enigma.

La primera máquina de cifrado de rotores fue inventada en los EE.UU por Edward Hugh Hebern. Entre 1912 y 1915 patentó varios dispositivos de cifrado como un teclado de cifrado y dos máquinas de escribir eléctricas conectadas con un cableado de 26 conexiones para el cifrado monoalfabético automático. Hebern construyó su primera máquina cifrado en 1917, fig.61 la cual tenía únicamente un rotor que podía ser extraído y cambiar su orientación con el fin de ser utilizado para cifrar y descifrar mensajes. Hugh Hebern mejoró su máquina y la implantó en 1921 con nuevos y mejorados rotores.Fig.62

El telegrama Zimmerman fig.54 daba instrucciones al embajador alemán en México para proponer a este país una alianza en caso de que estallara la guerra entre los Estados Unidos y Alemania, con la promesa de que México recuperaría Texas, Nuevo México y California - Zimmerman tuvo que cifrar su telegrama porque era consiente de que los aliados interceptaban todas sus comunicaciones trasatlánticas. En efecto, el telegrama fue interceptado por lo británicos quienes consiguieron descifrarlo completamente, prueba de la supremacía de los criptoanalistas aliados durante la Primera Guerra Mundial. El mensaje era el siguiente:

Nos proponemos comenzar la guerra submarina sin restricción el 1 de febrero. A pesar de ello, procuraremos mantener neutral a Estados Unidos. En caso de que esto no tenga éxito, hacemos a México una propuesta de alianza con la siguiente base: hacer la guerra juntos, hacer la paz juntos, ayuda económica generosa y el entendimiento por nuestra parte de que México reconquistará los territorios perdidos de Texas, Nuevo México y Arizona. El acuerdo detallado se lo dejamos a usted.

Usted informará al presidente [de México] sobre esto en el mayor de los secretos, en cuanto el estallido de la guerra con Estados Unidos sea seguro, y añadirá la sugerencia de que él podría, por iniciativa propia, invitar a Japón a adherirse inmediatamente y al mismo tiempo, de mediar entre Japón y nosotros.

Por favor, señale al presidente el hecho de que el uso sin restricción de nuestros submarinos ofrece ahora la perspectiva de obligar a Inglaterra a firmar la paz en pocos meses. Acuse recibo.

Zimmerman.

Fig. 74 Máquina Hagelin C - 35, año 1935.

Fig. 75 Máquina Enigma M 2, año 1938.

Fig. 76 Bletchley Park, Reino Unido, año 1939.

En 1917 durante la Primera Guerra Mundial EE.UU. utilizó 8 indios Chotaw como operadores de radio, en un plazo de 24 horas después de que la lengua Chotaw prestara servicios, el signo de la batalla se había vuelto y en menos de 72 horas, los alemanes se fueron en retirada.

Adolf Hitler sabía de la utilización con éxito de código que hablaron durante la Primera Guerra Mundial y se envió un equipo de unos treinta antropólogos para aprender las lenguas indígenas de América antes del estallido de la Segunda Guerra mundial.

El cifrado de Vernam es un cifrado de flujo en el que el texto en claro se combina, mediante la operación XOR, con un flujo de datos aleatorio o pseudoaleatorio del mismo tamaño, para generar un texto cifrado.

El uso de datos pseudoaleatorios proporcionados por un generador de números pseudoaleatorios criptográficamente seguro es una manera común y efectiva de construir un cifrado en flujo.

Josep Mauborgne se dio cuenta de que, si el flujo de datos que componían la clave era completamente aleatorio, el resultado sería una cifra con la que fallaría cualquier forma de criptoanalisis. La seguridad de esta cifra se debe enteramente a que la secuencia de las letras de la clave es totalmente aleatoria. La libreta de Vernam-Mauborgne poseía la propiedad: el secreto perfecto.Fig.55

En 1918 el cifrado ADFGVX fig.48 alemán fue el primer cifrado usado por la Armada Alemana durante la Primera Guerra Mundial. Este usaba un cifrado de transposición fraccionaria la cual combino una raíz Polybius modificada con una columna sencilla de transposición usada para codificar 36 letras de alfabeto (26 letras más 10 dígitos).

Al final de la Primera Guerra Mundial se produjo la aparición y proliferación de las máquinas de cifrado de rotores.Fig.56 Estas máquinas fueron desarrolladas de forma independiente por varios inventores de diferentes países en un lapso temporal de varios años. La inclusión de varios rotores se produjo con el fin de complicar el algoritmo de cifrado. Este tipo de máquinas daban la posibilidad además de simplificar al máximo su operatividad y funcionamiento.

Disco Cipher, prototipo de diseño de anillo concéntrico simplificado.Fig.60

El Biuro Szyfrów que en polaco significa "Oficina de Cifrado" se creó en mayo de 1919, durante la guerra polaco-soviética (1919-21) y era la unidad del Segundo Departamento del Estado Mayor polaco de entreguerras encargada de la SIGINT y de la criptografía y el criptoanálisis. Entre 1927 y 1928 Polonia se había hecho con una máquina de cifrado de códigos alemana al interceptar un envío de correos que oficialmente contenía equipos de radio sin mayor trascendencia; fig.64 en diciembre de 1932, la Oficina comenzó a descifrar los cifrados de (Enigma primera versión) de Alemania.

Fig. 77 Alan Turing.

Fig. 77 Alan Turing.

Fig. 78 Conel Hugh O'Donel.

Fig. 79 G. Welchman.

Durante los siete años siguientes, los criptólogos polacos superaron las crecientes complejidades estructurales y operativas del Enigma equipado con un tablero de conexiones. La Oficina también rompió la criptografía soviética.

La invención de la última máquina de cifrado de rotores se le atribuye al sueco Arvid Gerhard Damm, fig.57 que la patentó tan sólo tres días después que Koch, el 10 de octubre de 1919. Su invención utilizaba un rotor doble cuya cadencia era irregular. Dos de sus inversores eran Karl Wilhelm Hagelin fig.65 y Emanuel Nobel. Kryha fig.59 la máquina fue un dispositivo de cifrado y descifrado, que apareció a principios de la década de 1920 y se utilizó hasta la década de 1950.

Agnes Meyer Driscoll, también conocida como Madame X, fig.58 fue una criptoanalista estadounidense que descifró un gran número de sistemas navales japoneses y desarrolló sistemas para máquinas cifradoras. En 1921, Agnes Meyer consiguió descifrar un mensaje enviado por una máquina en teoría inexpugnable, creada por Edward Hebern. Meyer descifró los códigos manuales de la Marina Japonesa, el Código del Libro Rojo en los años veinte y el Código del Libro Azul en los años treinta.

Elizebeth Smith Friedman, fig71 terminó por convertirse en una de las pioneras de la criptología moderna entre 1926 y 1930, descifrando un promedio de "20.000 mensajes de contrabandistas por año en cientos de sistemas de código diferentes". Las fotografías del libro de códigos se les facilitó a los criptoanalistas de la Oficina de Investigación y el código de descifrado se guardó en carpetas de color rojo para indicar que su clasificación era Top Secret. Este código fue llamado "RED".

Lester Hill, se interesó en la aplicación de las matemáticas avanzadas a las comunicaciones y desarrolló muchos métodos para romper los errores en las comunicaciones telegráficas. Fue notablemente uno de los mayores contribuyentes de la criptología; el arte de hacer y romper códigos y cifrados. En 1929, inventó las cifras de Hill, que eran cifras de sustitución poligráfica basadas en el álgebra lineal.

Fig. 80 Milner-Barry.

Fig. 81 Margaret Rock.

Fig. 82 Joan Clarke.

Las matrices y la multiplicación de matrices se utilizaron para cifrar y descifrar el texto plano. Hill también creó una máquina de cifrado que se basaba en un sistema de ruedas y cadenas.Fig.70
En 1930, el gobierno japonés creó un código más complejo que fue el nombre en código AZUL, aunque el ROJO se seguía utilizando para comunicaciones de bajo nivel.Fig.67
La solución al fracaso en la seguridad de las comunicaciones alemanas durante la Primera Guerra Mundial fue la Enigma, fig.66 la máquina de cifrado de mensajes más avanzada hasta la llegada de la computadora y la cual supuso un punto de inflexión en la historia de la criptografía.
Los alemanes hicieron gran uso de diversas variantes de una máquina de rotores electromecánica llamada Enigma.Fig.63 El matemático Marian Rejewski, de la Oficina de Cifrado polaca, comenzó en diciembre de 1932 a descifrar los cifrados de (Enigma primera versión)fig.73 de Alemania. Durante los siete años siguientes, los criptólogos polacos superaron las crecientes complejidades estructurales y operativas del Enigma equipado con un tablero de conexiones, constituyendo **el mayor avance del criptoanálisis en más de mil años.** La Oficina también rompió la criptografía soviética.
El 15 de septiembre de 1938, los alemanes cambiaron completamente el procedimiento para cifrar las claves de los mensajes, y el método del catálogo se había vuelto completamente inútil. Esto impulsó a los polacos a encontrar nuevas soluciones, como las Hojas de Zygalski y la Bomba Kryptologiczna (bomba criptológica),fig.111 a menudo abreviada como Bomba. Zygalski diseñó las «hojas perforadas», también conocidas como las «hojas de Zygalski», un ingenio manual para detectar la configuración de Enigma. Este instrumento, al igual que el «catálogo de tarjetas» anterior, era independiente del número de conexiones utilizadas en el conmutador de Enigma.
La Bomba criptológica se basa en el principio de que la clave de mensaje de 3 letras aleatorias se envía dos veces al principio de cada mensaje y que de vez en cuando, una determinada letra de texto plano, da como resultado la misma letra de texto cifrado tres posiciones más adelante.
Entre 1934 y 1938 el ingeniero Antoni Palluth construyó en Varsovia 17 réplicas de la Enigma militar. Rejewski diseñó también las primeras bombas: ensambles de máquinas Enigma para buscar claves.Fig.84 Se les llamó “bombas” debido al ruido que hacían; la primera se fabricó en noviembre de 1938 e incorporaba seis réplicas de Enigma, (Enigma, primera generación).
La máquina Enigma fue inventada en 1938 por Arthur Scherbius, fig. 75 ingeniero alemán, básicamente. El ingenio fue mejorado rápidamente por diversos inventores basándose en la patente original de Hengel y Spengler. Scherbius era el encargado de lo que hoy denominamos I+D, fig.99 buscando continuamente nuevas oportunidades. Uno de sus proyectos preferidos era sustituir los inadecuados sistemas manuales de criptografía empleados en la

Fig. 83 Mavis Batey.

Fig. 84 Máquina Bomba criptológica de Rejewski, año 1939.

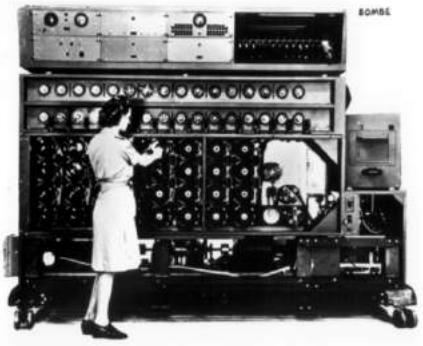


Fig. 85 Máquina La Bomba, año 1940.

Fig. 86 Château des Fouzes, año 1940.

Primera Guerra Mundial por una codificación mecánica y automática que mejorará las posibilidades de cifrado, aumentando la cifra de permutaciones posibles, y simplificando en gran medida la labor del emisor del mensaje cifrado. Desarrolló una pieza de maquinaria criptográfica que era esencialmente una versión eléctrica del disco de cifras de Alberti. Nadie podía sospechar que el invento de origen civil de Scherbius, **se convertiría en el más temible sistema militar de codificación de la historia.**

Cinco semanas antes del estallido de la Segunda Guerra Mundial, el 25 de julio de 1939, en Varsovia, la Oficina Polaca de Cifrado reveló sus técnicas y equipo de descifrado de Enigma a los representantes de la inteligencia militar francesa (Gustave Bertrand) y británica (Dillwyn Knox), que no habían podido hacer ningún progreso contra Enigma, explicando cómo habían roto Enigma. Se comprometieron a dar a cada país un Enigma reconstruido por Polonia y los procedimientos para quebrantar su esquema, con detalles de su equipo, incluyendo la bomba criptológica de Rejewski.Fig.84 Esta transferencia de inteligencia y tecnología polaca daría a los Aliados una ventaja sin precedentes, fue una decisión del Estado mayor polaco ante la inminencia de la guerra, decisión muy afortunada pues los alemanes siempre confiaron en la inviolabilidad de Enigma y nunca pudieron confirmar que sus comunicaciones hubieran sido interceptadas.

El 1 de septiembre de 1939 estalló la Segunda Guerra Mundial, el ataque de la Wehrmacht a Polonia no fue ninguna sorpresa para el Estado Mayor de ésta, adecuadamente advertido por el Biuro Szyfrów.

El 5 de septiembre de 1939, cuatro días después del inicio de la invasión alemana a Polonia, los criptólogos polacos debieron abandonar el país. Desde octubre de 1939 se establecieron en el castillo de Vignolles, fig.91 al este de París, y continuaron sus actividades, cooperando con antiguos combatientes españoles republicanos

Durante años, los aliados habían considerado que Enigma era indescifrable, pero los logros conseguidos por los polacos pusieron de manifiesto la importancia de emplear a matemáticos en las técnicas de criptoanálisis. Bletchley Park, fig.76 era la sede de la Escuela Gubernamental de Códigos y Cifras, una organización de descodificación recién fundada en Buckinghamshire, que tras el estallido de la guerra, se convirtió en la sede clandestina y secreta del ataque a Enigma.

Bletchley Park era un edificio de arquitectura gótico Tudor, situado a las afueras de la pequeña localidad rural de Milton Keynes, sin duda un lugar insólito para uno de los mayores triunfos tecnológicos de la guerra.

Alan Turing fig.77 desarrolló para facilitar la tarea Bombe, un ordenador producido en 1939, en Bletchley Park a partir del diseño que el criptologista polaco Marian Rejewski elaboró en 1938; y Colossus, una calculadora electrónica.Fig.100

Fig. 87 Trabajadores del centro polaco-hispano-francés de radioespionaje “Cadix” 1940-1942.

Fig. 88 Faustino Antonio Camazón Valentín, año 1940.

Fig. 89 Máquina Enigma M 3, año 1940.

Tras el comienzo de las hostilidades de la Alemania nazi en el otoño de 1939, el gobierno alemán comenzó a enviar asistencia técnica para mejorar sus comunicaciones y capacidades de criptografía de Japón. Una parte de la ayuda se basaba en facilitarle máquinas Enigma modificadas para asegurar las comunicaciones de alto nivel entre Japón y Alemania, el nuevo código, con nombre en código PURPLE.

Los criptógrafos estadounidenses y británicos habían desencriptado una parte de los mensajes PURPLE mucho antes del ataque a Pearl Harbor.

En 1939, Agnes Meyer Driscoll fig.58 fue la primera en encontrar los primeros patrones numéricos del código JN25, lo que dio las claves para lograr descifrarlo por completo. El JN25 fue el código más complejo de los empleados por la Armada Imperial Japonesa.

Criptografía-Alfa, o Alfa, fig.69 es una máquina de cifrado electromecánica basada en ruedas, desarrollada y producida en secreto por la OMI en Roma (Italia) alrededor de 1939, al comienzo de la Segunda Guerra Mundial. Estaba destinada a ser utilizada por el Ejército Italiano, es similar al Enigma Alemán fig.88 y tiene 5 ruedas cifradas, incluyendo un reflector móvil.

El grupo liderado por William Frederick Friedman fig.72 dentro de SIS/ASA se hizo famoso al romper PURPLE (el nombre que le daban a la máquina de cifrado del Japón), una proeza criptológica comparable a la de los polacos que rompieron la máquina Enigma de Alemania. El grupo también cooperó con la Marina para desarrollar lo que sería la máquina de cifrado más segura de esa Guerra, la SIGABA.Fig.101 También influyó en el desarrollo de la Agencia de Seguridad de las Fuerzas Armadas (AFSA) y la Agencia de Seguridad Nacional (NSA). El matemático Georg Hamel, evaluó la seguridad de la máquina Kryha y calculó el tamaño del espacio clave. También se contactó con el ejército de los EE.UU. para ver si les interesaba usar la máquina, y se les persuadió para que aceptaran un mensaje de desafío para evaluar la seguridad del dispositivo.

El mensaje de desafío, de 1135 caracteres de largo, fue resuelto por William Friedman, asistido por Solomon Kullback, Frank Rowlett y Abraham Sinkov, en 2 horas y 41 minutos. El criptoanalista estadounidense William Friedman, que conseguiría romper la japonesa máquina PURPLE, mejoró el diseño original de Hebern (en 1921),fig.62 con la invención de la SIGABA que tenía una rotación irregular, lo que hizo que fuera una de las pocas máquinas de cifrado cuyo código no fue roto durante la Segunda Guerra Mundial.

El mayor desarrollo de artilugios criptográficos se dio en el periodo de entreguerras por la necesidad de establecer comunicaciones militares y diplomáticas seguras. En 1940 se construyó la máquina Hagelin C-48 para cifrar y descifrar cartas, consistente en seis volantes unidos por el eje y con distinto número de dientes.

En octubre de 1940 entra en funcionamiento la primera bomba criptológica inglesa, llamada Ultra o “bomba de Turing”. Se valora el “proyecto Ultra” como el de mayor secreto en la Segunda Guerra

Fig. 90 Puesto de radio año 1940.

Fig. 91 Château de Vignolles, año 1941.

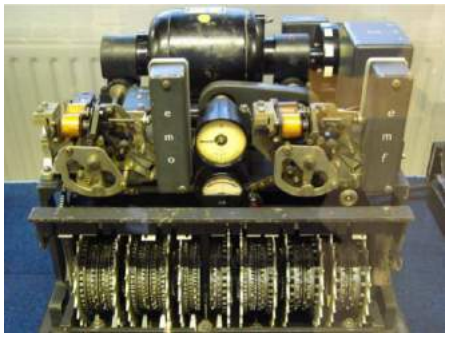


Fig. 92 Máquina de cifrado Lorenz, año 1941.

Mundial, sólo detrás del proyecto Manhattan de la bomba atómica.

Los polacos disponían de una máquina Enigma y los alemanes se dieron cuenta por lo que construyeron dos rodillos más: siendo cinco en total, de los cuales sólo introducían tres en la máquina.Fig.96 Por tanto las posiciones iniciales de los rodillos pasaron de ser 17576 a ser casi 12 millones, que, combinadas con las posiciones del tablero, dan cerca de 160 trillones de posibilidades, algo que complicaba demasiado las cosas.Fig.90

El encargado de recoger el testigo de los logros criptográficos conseguidos por los polacos fue el genio matemático del King's College de Cambridge, Alan Turing (1912-1954). Turing ya había trabajado anteriormente en el desarrollo del concepto de máquina computacional. Son célebres sus trabajos de 1938 en los que diseña, una máquina virtual o física en el que era posible definir el concepto de algoritmo que resulta fundamental en computación. En Bletchley, Turing se convertiría en una de las cuatro figuras al mando de la organización de los trabajos de desencriptado junto a Gordon Welchman, fig.79 Philip Stuart Milner-Barry fig.80 y Conel Hugh O'Donel Alexander.Fig.78 Estaba al cargo del barracón 8, responsable de descifrar los códigos de la Enigma de la marina alemana (una de las más complicadas dado que contaba con un rotor adicional y sus operadores eran extremadamente escrupulosos a la hora de su utilización, por lo que la hacía prácticamente impenetrable), con el fin de romper el bloqueo naval con el que los submarinos nazis tenían sometido al Reino Unido.

La máquina PURPLE fig.95 fue utilizada por primera vez en 1940 por el Ministerio de Relaciones Exteriores de Japón para las comunicaciones diplomáticas con sus embajadas. La marina de guerra japonesa utilizó un sistema de encriptación completamente diferente, conocido como JN-25.

Operación Primrose: los británicos se apoderan de una máquina Enigma fig.89 a bordo del submarino U-110 - 09/05/1941 y es entregada a los criptógrafos británicos y al genio matemático Alan Turing en Bletchey Park.

Joan Elisabeth Lowther Clarke fig.82 fue una criptoanalista y numismática británica que trabajó en Bletchley Park durante la Segunda Guerra Mundial, en el equipo del matemático Alan Turing en el proyecto Enigma, que desencriptó las comunicaciones secretas de la Alemania nazi. Su papel en este proceso le valió premios y citaciones, siendo distinguida como miembro de la Orden del Imperio Británico (MBE).

Mavis Lilian Batey, fig.83 fue una criptoanalista británica durante la Segunda Guerra Mundial y su trabajo en Bletchley Park fue una de las claves del éxito del día "d". Sin embargo, lejos de arrugarse, los criptólogos polacos y españoles, denominados "Equipo Z" y "Equipo D" respectivamente, fig.93 decidieron continuar con su peligrosa tarea. El mayor Gustave Bertrand regresó en septiembre a Francia y fue entonces cuando los integrantes de Bruno decidieron crear una nueva unidad encubierta denominada "Cadix", en el Château des Fouzes, fig.86 en Uzès, cerca de Nimes,

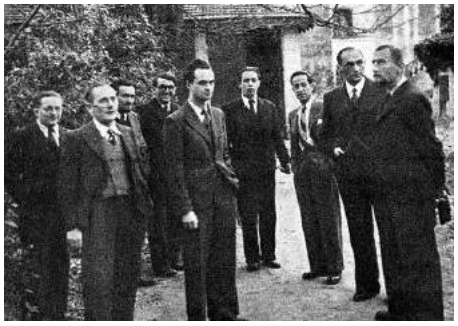


Fig. 93 Château des Fouzes, equipo Z y equipo D, año 1941.

Fig. 94 Modelo “Liliput”, año 1942.

Fig. 95 Máquina Púrpura, año 1942.

al sur de la Francia de Vichy, entre Montpellier y Avignon. Rejewski se empleó como profesor de matemáticas en Nantes, para evitar cualquier sospecha.

Los criptógrafos españoles que descifraron los códigos de Enigma, el "Equipo D”, eran siete españoles exiliados procedentes del servicio secreto de la República (5 oficiales y dos comisarios), dirigido por Faustino Antonio Camazón Valentín.fig.88 PC Bruno (Poste de Commandement Bruno), que colaboró en desentrañar el dispositivo que los alemanes usaron en la Segunda Guerra Mundial, para encriptar los mensajes que coordinaban sus operaciones, con la ayuda de quince criptógrafos polacos y nueve franceses, ya que el servicio secreto francés había sido informado de sus avances contra Enigma por los criptógrafos huidos de la invasión de Polonia Marian Rejewski, Jerzy Różycki y Henryk Zygalski, que pasaron a integrar el equipo de Bertrand junto a franceses y españoles. Se tardó tres años en romper el sistema criptográfico de Enigma. Aquellos criptógrafos españoles estuvieron al más alto nivel trabajando durante el conflicto. Camazón al finalizar la contienda se unió a las tropas norteamericanas de Eisenhower y fue testigo presencial de la liberación de algunos campos de concentración.

Margeret Rock, fue otra de las matemáticas que trabajó en Bletchley Park durante la Segunda Guerra Mundial, fue capaz de decodificar la máquina Enigma. Su trabajo durante la guerra fue clasificado por la Ley de Secretos Oficiales de 1939 del Reino Unido.Fig.81

El gran cerebro inglés que permitió el descifrado de Enigma fue Alan Turing precursor, como Babbage, de los ordenadores modernos, y como ya no podía basarse en la secuencia de tres letras que repetían los alemanes al principio de cada transmisión, observó que en las primeras palabras de cada mensaje hablaban siempre de las condiciones meteorológicas, por lo que palabras como tiempo, viento, frío... se repetían con bastante frecuencia. Se apoyó en este hecho y en el de que la máquina Enigma estaba construida de forma que nunca una letra codificaba a ella misma, para descubrir los códigos.

Cuando la guerra llegaba a su fin, Bletchley Park estaba dotada con 211 máquinas bomba, fig.85 que necesitaban más de 2.000 personas para su mantenimiento y utilización.Fig.97 El trabajo de Alan Turing y sus bombas ayudaron enormemente a que los aliados ganaran la guerra, el descubrimiento de los códigos de Enigma fue muy importante en la Segunda Guerra Mundial, ya que pudieron evitarse ataques del enemigo y pudieron provocarse ataques por sorpresa, lo que, sin duda, influyó en el rumbo de la guerra. Churchill siempre consideró a Bletchley Park como “su arma secreta”.

Magic, era el nombre en clave que los estadounidenses dieron a la información obtenida de los mensajes de radio japoneses interceptados y decodificados por los servicios de inteligencia del ejército norteamericano, especialmente los del código conocido como Purple, usado en comunicaciones diplomáticas. Venía a ser algo similar a "Ultra", el nombre que se dio a las decodificaciones de las comunicaciones cifradas alemanas.

Fig. 96 Máquina Enigma M 4, año 1942.

Fig. 97 Personal de Bletchley Park, año 1942.

Fig. 98 Mensajeros código Navajo, año 1942.

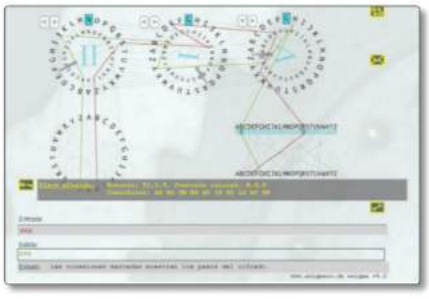


Fig. 99 Simulador de cifrado máquina Enigma.

Magic fue creado para combinar las capacidades en análisis criptográfico del gobierno de EE.UU. en una organización llamada Oficina de Investigación. Los oficiales de inteligencia del Ejército y la Armada estuvieron todos bajo un mismo techo, sus éxitos más importantes se lograron al descifrar tres códigos: RED, BLUE y PURPLE.

Después del ataque a Pearl Harbor, reclutaron a 3.600 Navajos, entre los cuales fueron escogidos 420 indígenas bilingües, conocedores de las costumbres de la población blanca y que fueron entrenados como “Habladores de Código” y asignados a las seis divisiones del Cuerpo de Marines que sirvieron en el teatro de Guerra del Pacífico. Fig.98

La Lorenz SZ 40 y la SZ 42 fig.92 eran máquinas alemanas de cifrado utilizadas durante la Segunda Guerra Mundial en circuitos de teletipo. Criptógrafos británicos, que se refirieron al tráfico alemán de datos de teletipo cifrados como "Fish", denominaron al aparato y su tráfico como “ Tunny ". Mientras la bien conocida Enigma fue usada generalmente por unidades de combate, la máquina de Lorenz fue usada para comunicaciones de alto nivel, los mecanismos implementaban un cifrado de flujo; esta máquina fue descifrada en Bletchley Park por los descifradores John Tiltman y Bill Tutte.

Las bombas no fueron suficientes para descodificar esta cifra, no eran lo suficientemente rápidas ni flexibles, siendo esta cifra descodificada con otra máquina llamada el Colossus, que fue diseñado por el matemático Max Newman siguiendo la idea de la máquina Universal de Turing y fue construido por Tommy Flowers, en diez meses el Colossus, fig.102 era considerablemente más rápido que las bombas y está considerado como el primer ordenador programable de la historia.

Las máquinas de cifrado aliadas utilizadas en la Segunda Guerra Mundial incluían la Typex británica fig.103 y la SIGABA estadounidense; fig.101 ambos eran diseños de rotores electromecánicos similares en espíritu a la Enigma, aunque con mejoras importantes, no se tiene constancia de que ninguna de ellas se rompiese durante la guerra. Los polacos utilizaron la máquina Lacida, pero se demostró que era poco segura y se canceló su uso. Las tropas de campo utilizaron las familias M-209 y M-94. Los agentes SOE utilizaron inicialmente «cifrados de poema» (las claves eran poemas memorizados), pero más avanzada la guerra empezaron a utilizar libretas de un solo uso. Fig.55

Como Jean-Frangois Champollion, Ventris se apasionó desde muy joven por las escrituras antiguas, a los siete años estudió un libro sobre los jeroglíficos egipcios, una hazaña impresionante para alguien tan joven, sobre todo porque el libro estaba escrito en alemán, este interés por los escritos de las civilizaciones antiguas le acompañó a lo largo de toda su infancia, en 1936, a los catorce años, se avivó todavía más cuando acudió a una conferencia dada por sir Arthur Evans, el descubridor del Lineal B.

El joven Ventris descubrió los detalles de la civilización minoica y del misterio del Lineal B y se prometió a sí mismo que descifraría esa escritura, ese día nació una obsesión que acompañaría a Ventris a lo largo de su corta pero brillante vida.

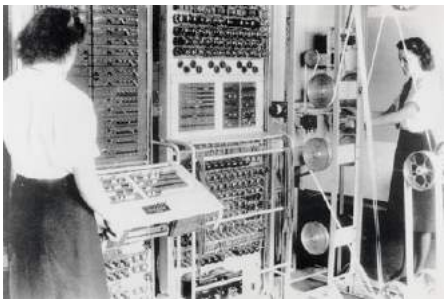


Fig. 100 Máquina Colossus, año 1943.

Fig. 101 Máquina SIGABA estadounidense, año 1944.

Fig. 102 La máquina Colossus, año 1944.

Fig. 103 Máquina Typex británica, año 1944.

John Chadwick, un investigador de Cambridge que había estado interesado en el desciframiento del Lineal B desde los años treinta, durante la guerra, había pasado tiempo como criptoanalista en Alejandría, descifrando cifras italianas, antes de trasladarse a Bletchley Park, donde atacó las cifras japonesas. Después de la guerra intentó de nuevo descifrar el Lineal B, esta vez empleando las técnicas que había aprendido mientras trabajaba con códigos militares, esto condujo a que el logro de Ventris y Chadwick se conoció como "el Everest de la arqueología griega". Al año siguiente, los dos hombres decidieron escribir un informe en tres volúmenes de su trabajo, que incluiría una descripción del desciframiento, un análisis detallado de trescientas tablillas, un diccionario de 630 palabras micénicas y una lista de los valores sonoros de casi todos los signos del lineal B.Fig.14

El Euskera también tuvo relevancia durante la Segunda Guerra Mundial, un grupo de 60 vasco-americanos comandado por un tal Frank D. Carranza contribuyó a la victoria americana contra los japoneses en la batalla de Guadalcanal (1942), tan importante para el desenlace final de la Segunda Guerra Mundial. Carranza y sus hombres se dedicaron a encriptar mensajes en euskera tales como "Sagarra Eragintza Saspi" (La Operación Manzana comenzará a las siete),o " Lurrepaira darrepairalndartsuak " (Tienen buenas trincheras y fortificaciones) causando el desconcierto en el ejército del Imperio del Sol Naciente al desconocer este peculiar idioma.

Sin embargo, el euskera no fue el único idioma empleado. Había que tomar muchas precauciones, Así que se escogieron otros idiomas y se estableció un calendario de uso de los mismos: lunes, euskera; martes, oswego, miércoles, iroqués; jueves shaishai; viernes, euskera; sábado, clave 2x2, domingo oswego. (El oswego, el iroqués y el shaishai son idiomas de tribus nativas americanas).

Durante la Segunda Guerra Mundial, Kryha trabajó como oficial de la Wehrmacht alemana, con varias versiones, la máquina estándar de Kryha, era totalmente mecánica y más tarde se introdujo una versión de bolsillo a escala, llamada el modelo " Liliput ".Fig.94 Ésta máquina fue utilizada durante un tiempo por el Cuerpo Diplomático Alemán, y fue adoptada por Marconi en Inglaterra.

En 1956 los rusos introdujeron la primera versión de una máquina de cifrado basada en rotores muy avanzada que se llamaba FIALKA.Fig.105 Por su parte, los estadounidenses empezaron a desarrollar su máquina basada en rotores, llamada KL-7fig.106 que se convirtió en el mecanismo principal de cifrado de la OTAN en la era de la posguerra.

A diferencia de Enigma, el KL-7 tenía ocho rotores, siete de los cuales se movían en un complejo patrón de pasos irregulares. Un ordenador moderno podría necesitar años para descifrar el código, no obstante, la suma de las capacidades de un ejército de ordenadores modernos permite disponer de una suerte de superordenador virtual, que acelera el trabajo y reduce considerablemente el tiempo: el software de Enigma @home, instalado en unos cien ordenadores entregados a la causa las 24 horas del día, sería capaz de dar con la solución en solo cuatro jornadas.

Fig. 104 Strip Cipher, año 1950.

Fig. 105 Máquina FIALKA, año 1956.

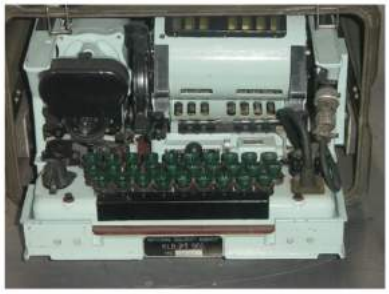


Fig. 106 Máquina KL-7, año 1956.

Fig. 107 Códigos M. Enigma.

5.6. Criptosecretismo.

El Cray X-MP fig.108 fue un supercomputador diseñado, construido y producido por Cray Research y fue la primera computadora de procesador vectorial, memoria compartida y proceso paralelo de la compañía. Fue el sucesor en 1982 del Cray-1 de 1976, y fue el computador más rápido del mundo entre 1983 y 1985. Un código que no es secreto en absoluto, es el código ASCII fig.109 (- American Standard Code of Information Interchange - Código estándar americano para intercambio de informaciones) que se utiliza para comunicar con los ordenadores modernos: los mensajes se transcriben empleando un «alfabeto binario» formado tan sólo por las dos cifras (o bit = binary digit = cifra binaria) 0 y 1. El cracker DES fig.110 de la EFF (apodado Deep Crack) es una máquina construida por la Fundación de Fronteras Electrónicas (EFF) en 1998, para realizar una búsqueda por fuerza bruta del espacio de claves de la norma de cifrado de datos (DES), es decir, para descifrar un mensaje cifrado probando todas las claves posibles. El objetivo de hacer esto era probar que el tamaño de la clave del DES no era suficiente para ser seguro.
Para analizar la complejidad de la máquina Enigma, y saber de lo que era capaz, el sistema contaba con seis cables de conexión que también permitían introducir modificaciones dado que podrían conectarse a 26 lugares (representando a las 16 letras del alfabeto de enigma) lo que producía 100.391.791.500 maneras distintas de conectar los cables que unidos a los 105.456 alfabetos arrojaba distintas posibilidades de codificación, la cifra es inmensa:
3.283.883.513.796.974.198.700.882.069.882.752.878.379.955.261.095.623.685.444.055.315.226.006.433.616.627.409.666.933.182.371.154.802.769.920.000.000.000 de codificaciones.Fig.107

5.6.1. La era digital.

La teoría de la comunicación y la cibernética han revolucionado tanto la idea de máquina como la de organización, al relacionarlas. Los conceptos de control, de retroalimentación, de tratamiento cuantitativo de la información, aplicado a las máquinas (ordenadores) hicieron nacer de la nada unos seres hasta ese momento inexistentes: las máquinas organizadas, las máquinas lógicas, de pura organización.[21]
Diffie y Hellman en 1976 introdujeron, el concepto de firma digital a través de protocolos criptográficos que son básicamente es un conjunto de datos asociados a un mensaje que permiten asegurar la identidad del firmante y la integridad del mensaje.

---

[21]SERRANO FARRERA, SEBASTIÀ. *La Semiótica,* p.17

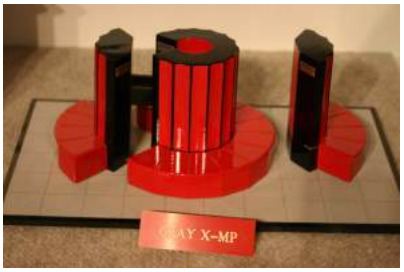
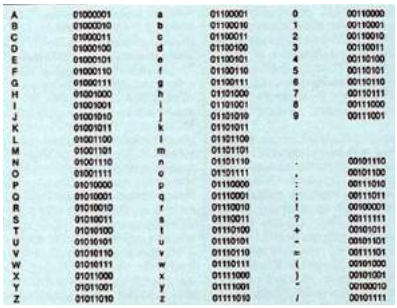


Fig. 108 Cray X - MP, año 1976.



A	01000001	a	01100001	0	00110000
B	01000010	b	01100010	1	00110001
C	01000011	c	01100011	2	00110010
D	01000100	d	01100100	3	00110011
E	01000101	e	01100101	4	00110100
F	01000110	f	01100110	5	00110101
G	01000111	g	01100111	6	00110110
H	01001000	h	01101000	7	00110111
I	01001001	i	01101001	8	00111000
J	01001010	j	01101010	9	00111001
K	01001011	k	01101011		
L	01001100	l	01101100		
M	01001101	m	01101101		
N	01001110	n	01101110	.	00101110
O	01001111	o	01101111	,	00101100
P	01010000	p	01110000	:	00111010
Q	01010001	q	01110001	;	00111011
R	01010010	r	01110010	!	00100001
S	01010011	s	01110011	?	00111111
T	01010100	t	01110100	+	00101011
U	01010101	u	01110101	-	00101101
V	01010110	v	01110110	=	00111101
W	01010111	w	01110111	(	00101000
X	01011000	x	01111000	)	00101001
Y	01011001	y	01111001	'	00100010
Z	01011010	z	01111010	/	00101111

Fig. 109 Código ASCII, año 1981.

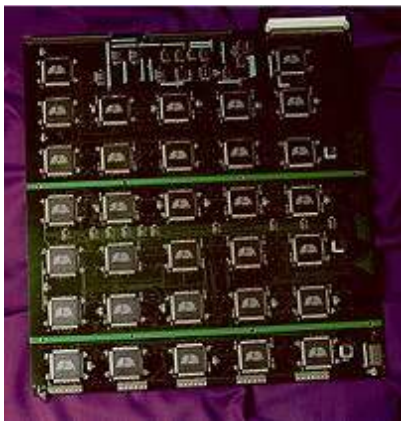


Fig. 110 Placa del DES, año 1998.

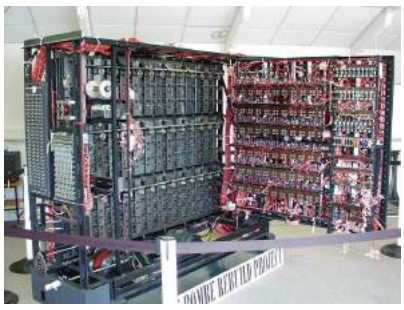


Fig. 111 Museo Bletchley Park, La Bomba.

El nacimiento de la firma electrónica se debe sin duda a la necesidad de una respuesta técnica segura para poder realizar la conformidad o el acuerdo de voluntades en una transacción electrónica. En 1997, el Instituto Nacional de Normas y Tecnología (NIST) decidió realizar un concurso para escoger un nuevo algoritmo de cifrado capaz de proteger información sensible durante el siglo XXI. Este algoritmo creado en Bélgica se denominó Advanced Encryption Standard (AES), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos, creado en Bélgica. El AES fue anunciado por el Instituto Nacional de Estándares y Tecnología (NIST) como FIPS PUB 197 de los Estados Unidos (FIPS 197) el 26 de noviembre de 2001 después de un proceso de estandarización que duró 5 años. Se transformó en un estándar efectivo el 26 de mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica. RSA es uno de los sistemas de cifrado asimétricos más exitosos de la actualidad. Originalmente descubierto en 1973 por la agencia de inteligencia británica GCHQ, recibió la clasificación "top secret". Debemos agradecer a los criptólogos Rivest, Shamir y Adleman por su redescubrimiento civil en 1977. El futuro del criptoanálisis, a pesar de la enorme potencia de RSA y otras cifras modernas, los criptoanalistas aún pueden desempeñar un valioso papel a la hora de recoger inteligencia, hecho demostrado sabiendo que los criptoanalistas están más solicitados que nunca antes en la historia.

La criptografía cuántica marcaría el fin de la batalla entre los creadores de cifras y los descifradores siendo los primeros los claros vencedores.

El problema generado de almacenamiento de claves, se ha resuelto mediante el denominado efecto EPR (Einstein - Podolsky - Rosen), que se produce cuando un átomo emite dos fotones en direcciones opuestas, por lo que el valor de sus polarizaciones debe ser también opuesto, por tanto, queda determinado en cuanto uno de ellos haya sido objeto de medida; el otro puede ser almacenado mientras las intervenciones en el proceso conocen si están o no siendo espaciados y trabajando con aquellos que no han sido intervenidos, pueden elaborar la clave de manera confidencial. Este proceso teórico no puede llevarse a la práctica, puesto que no existe posibilidad de almacenar fotones más allá de una fracción de segundo.[22]

---

[22]TARANILLA de la VARGA, CARLOS JAVIER. *Criptografía. Los Lenguajes secretos a lo largo de la Historia,* p.256

6. MENSAJES OCULTOS DE LA CAPILLA SIXTINA Y LA ÚLTIMA CENA.

Para abordar este capítulo nos vamos a centrar en dos obras del Renacimiento, movimiento artístico que trató de rescatar la cultura olvidada durante la Edad Media con la difusión de las ideas del humanismo. Principales referentes de este movimiento: Leonardo Da Vinci y Miguel Angel Buonarroti introdujeron mensajes ocultos en sus obras, desafiando a los poderes fácticos de su época para poder expresar su conocimiento y opiniones contrarias al orden establecido. La libertad de expresión en aquella época solo podía existir a través del ingenio y la astucia de los mensajes ocultos en el arte.

Previo a la Edad Moderna, la humanidad pensaba que todo lo que necesitaba saber para su existencia se encontraba en las Sagradas Escrituras, “La Biblia”. La Santa iglesia consideraba este divino tesoro, como la fuente más preciosa de la fe y la moral.

El Nuevo Testamento que narra la historia de la vida de Jesús de Nazaret, tiene cuatro versiones, al ser contada por cuatro discípulos. Por un lado, existen diferencias entre el evangelio de San Lucas y el evangelio de San Juan, sumiendo a la realidad ocurrida en un misterio. Por otro lado, los "hechos" sobre Jesús expuestos en las Biblias modernas se basan en siglos de copias y traducciones, por lo que puede que no sepamos lo que los textos originales decían en realidad, por ello conocer el verdadero mensaje y el origen del origen del mismo se dificulta.

En 1947, unos jóvenes pastores de cabras beduinas se asomaron a una caverna cercana,”las cuevas de Qumran” en la Cisjordania ocupada por Israel e hicieron uno de los mayores descubrimientos arqueológicos del siglo XX: siete pergaminos enrollados cubiertos en la antigua escritura hebrea, el primero de los famosos Rollos del Mar Muerto.Fig.112 Miembros de la secta separatista Qumran probablemente escondieron los pergaminos en la cueva alrededor del 70 d.C., cuando las tropas romanas se acercaron para aplastar la Primera Revuelta Judía. Posteriormente, cientos de pergaminos más datados en el siglo III a.C. salieron a la luz, siendo los textos bíblicos más antiguos que se han encontrado.Fig.113

Los judíos y los cristianos comparten muchos escritos sagrados, aunque los judíos no consideran el Nuevo Testamento como la Escritura. Para aquellos que creen que Dios habla a través de palabras escritas por profetas y apóstoles en épocas pasadas, los textos antiguos son fundamentales para su fe.

Konstantin von Tischendorf, teólogo y filósofo alemán que en 1844 hizo un largo y peligroso viaje a través del desierto de Sinaí hasta el monasterio cristiano de Santa Catalina, el más antiguo del mundo habitado continuamente.

Allí encontró "el más preciado tesoro bíblico que existe", un texto antiguo en forma de libro en lugar de un pergamino, que databa de mediados del siglo IV. Conocido hoy como el Códice Sinaítico, es una de las dos Biblias Cristianas más antiguas que sobreviven de la antigüedad y la copia completa más antigua del Nuevo Testamento.

La otra es el Codex Vaticanus, ligeramente anterior al Codex Sinaiticus, y probablemente copiado, como aquél, durante el siglo IV. Está escrito en griego, en pergamino, con letras unciales en formato "Escritura continua", y se conserva en la Biblioteca Apostólica Vaticana.

El arte no es solo belleza, sino también significado, a veces, oculto más allá de lo que simplemente se muestra. Varias de las obras de arte más importantes de la historia no solo transmiten sentimientos, sino que también guardan mensajes secretos que poco a poco se ha logrado descifrar.

La perspectiva de estos dos artistas con las creencias religiosas y en el conocimiento que ocultaba la iglesia, es similar y ello se puede comprobar con el análisis de los mensajes ocultos en dos de sus grandes obras: La Capilla Sixtina de Miguel Angel y La Última Cena de Leonardo.

Fig. 112 Fragmento del Evangelio de Juan, siglo II, más antiguo del Nuevo Testamento.

Fig. 113 Fragmento del Evangelio de Marcos, siglo II, III. Papiros de Oxirrinco.

6.1. La Capilla Sixtina.

Fig. 114 La Capilla Sixtina.

Fig. 115 Circunvolución cingulada del cerebro.

Fig. 116 Circunvolución cingulada del cerebro.

Miguel Ángel, qué mensaje secreto quería dejar en su obra.

Hay lo menos veinte de ellos en el techo; si uno fue ejecutado con maestría, el siguiente habría que superarlo; y apenas cabe dudar de que muchas de las ideas que nacerían a la vida en los mármoles de Carrara se agolparon en la mente de Miguel Ángel mientras pintó el techo de la Capilla Sixtina. Puede verse la extraordinaria maestría que poseyó y cómo su contrariedad y su cólera al verse obligado a no seguir trabajando en su materia preferida le espoleó aún más a demostrar a sus enemigos, verdaderos o imaginarios, que si ellos le comprometían a pintar, ¡ya verían![23]

Esta pintura, que adorna el techo de la Capilla Sixtina, fig.114 es mucho más que una de las obras de arte más famosas de la historia, sin embargo, aunque parece un trabajo más del renacimiento de la época, algunos expertos creen que en realidad fue creada para revelarse contra la figura del papa**.** Creando detalles ocultos que señalan al hombre como un símbolo mucho más poderoso que cualquier ente divino.

Miguel Ángel comentó "Estoy doblado tensamente como un arco sirio". Plasmó su rostro en la piel desollada de San Bartolomé, dejando su firma en una obra, fig.126 algo que estaba prohibido. Más de 300 figuras tapizan la bóveda de la capilla Sixtina. De ellas, 95% son judías y el 5% restante paganas, no hay ninguna cristiana.

El artista ocultó en esos frescos secretos que solo pueden leerse con el Talmud, y la Cábala. En la adolescencia se sintió atraído por el misticismo judío (y también por los hombres) y en su obra habría intentado transmitir un mensaje de tolerancia y amor universal, y de paso "vengarse" de Julio II, tiránico y ególatra, así como denunciar la corrupción de la Iglesia católica.

Entre las pruebas que aportan están los gestos vulgares de algunas figuras o la inclusión de héroes judíos y símbolos paganos. También se apoya en la ausencia de figuras cristianas, pues ni siquiera están presentes Jesucristo y la Virgen María.

En la comparación de las dos imágenes de la circunvolución, fig.115 esa área denominada "circunvolución cingulada"fig.116 es la que funcionalmente interviene en la manera en que el ser humano se adapta al medio para asegurar su supervivencia.

La "V" era el símbolo pagano para representar a la mujer, a la vagina y la energía femenina.Fig.127

Y los cuernos de los carneros podrían representar el sistema reproductivo femenino; el símbolo pagano para representar a los hombres, es un triángulo.Fig.117

---

[23]GOMBRICH, ERNST HANS. *Historia del Arte*, p.255

Fig.117 Cuernos carnero.

Fig. 118 Profeta Zacarias.

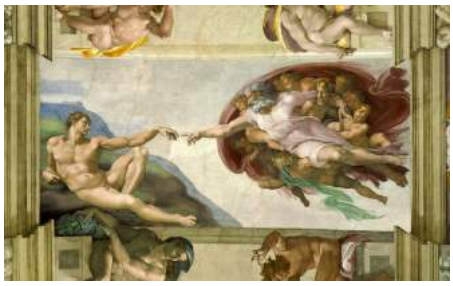


Fig. 119 Creación de Adan.

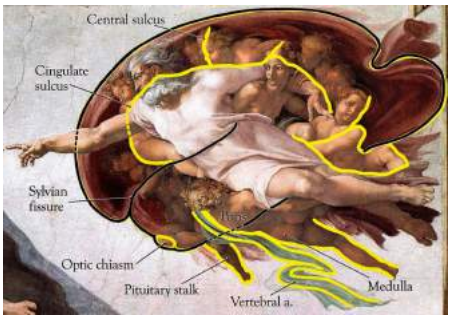


Fig. 120 Corteza cerebral.

Uno de sus mensajes se puede apreciar, justo donde Julio II quería que estuviese la imagen de Jesucristo, aparece la del profeta Zacarías, que animó a los judíos a reconstruir Jerusalén.fig.118 Tomó la licencia de colocar junto al profeta a dos putti, uno de estos angelitos tiene la mano cerrada en un puño y el pulgar asomado entre los dedos índice y corazón: es el equivalente de la época a levantar hoy el dedo corazón con el puño cerrado.
En las cuatro esquinas están: Ester y Amán en el lado derecho, y Judith, David y Goliat en el izquierdo, todos ellos protagonizan salvaciones del pueblo judío, se relaciona con la visión cabalística que hace hincapié en la dualidad de la identidad sexual de Dios. "En la base de todo hay un mensaje universal de paz para todos los pueblos, de no abandonar nunca por muy negro que se presente el futuro".
Profetas, mensajeros celestiales y sibilas fig.125 ocupan el resto de la bóveda. Hay siete de cada, y no es un número casual. El siete parece omnipresente en el judaísmo.
Las imágenes de los profetas que esconderían más secretos serían las de Jeremías quién advirtió a los sacerdotes que el Templo de Jerusalén sería destruido si no abandonaban la corrupción y Jonás fue el único profeta enviado a predicar a los gentiles.
Los protagonistas de la franja central de la Capilla son los cinco libros del Génesis. En la creación de Adán, fig.119 el dedo índice de Dios se encuentra con el de Adán rozando la perfección.
En la fruta prohibida , el árbol es una higuera en lugar de un manzano y en el sacrificio de Noé reprodujo el arca como una gran caja, como se describe en la Torá. Y hay dos hombres a cuatro patas con los colores rojo y amarillo, característicos de la ciudad de Roma, con ello humillaba discretamente a la ciudad que le mantenía, contra su voluntad, lejos de Florencia y sus queridas esculturas.
Una hipótesis ampliamente conocida es que los contornos de la tela alrededor de Dios repiten los del cerebro humano, fig.120 y los bordes de las figuras de las personas que se encuentran a su lado, sus secciones.Fig.121 Sin embargo, existe otra versión, según la cual, la tela representa el contorno del útero, y el velo verde, un cordón umbilical recién cortado.Fig.122 Miguel Ángel quiso mostrar el proceso idealizado del nacimiento de una persona, lo que explica la presencia del ombligo en el cuerpo de Adán.

Juicio final

Los bienaventurados no estaban separados de los condenados. En la parte superior, situó a los ángeles con los instrumentos del martirio.
Aunque los judíos no podían aspirar a disfrutar de la recompensa celestial, ocupan el centro del fresco. A la izquierda se ve a las mujeres justas, que situó muy cerca de Jesucristo pese a que los teólogos aún discutían si las féminas tenían o no alma.

Fig. 121 Corteza cerebral.

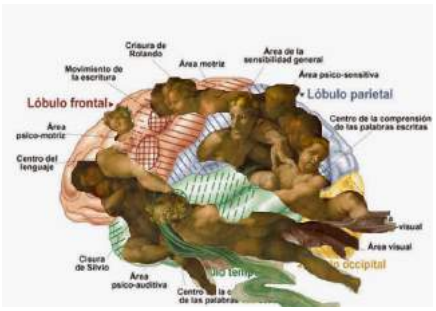


Fig. 122 Corteza cerebral con ángeles.

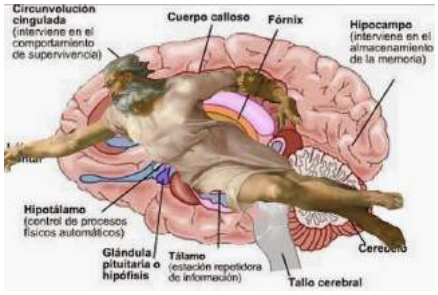


Fig. 123 Sistema límbico.

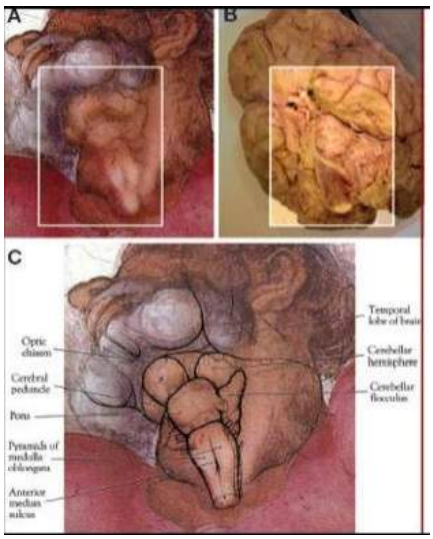


Fig. 124 La glándula pineal.

Junto a ellas aparecen los hombres justos, cuerpos desnudos abrazándose o besándose. Dada la probable homosexualidad del autor, sería otra señal de una declaración de intenciones.
Un atípico Jesucristo, musculado y sin barba, se sitúa en el centro. A su izquierda, San Pedro y San Pablo, y a su derecha, la Virgen María, que aparta la vista , como si no quisiera ver los castigos. Incluyó rostros de enemigos de la iglesia, entre ellos el de la monja Vittoria Colonna, líder de los iluminados. La Virgen la mira, mientras Jesucristo mira a un personaje al que Miguel Ángel puso el rostro de su gran amor: Tommaso Cavalieri.
El Juicio Final, que refleja el gran tormento espiritual del autor, se consideró escandaloso y llegó a hablarse de Herejía. Miguel Ángel incluyó en la Capilla Sixtina gran cantidad de ideas atrevidas, las suyas: amar a quien se quiera, respetar a los judíos y a las distintas creencias, indignarse ante la corrupción y la inmoralidad de la Iglesia.[24]
En la traducción en imágenes de esta verdad, Miguel Ángel desconcertó a muchos de sus contemporáneos, fig.122 representando ángeles sin alas, santos sin aureolas y demonios de una deformidad inimaginable. Pero la originalidad del artista se manifiesta sobre todo en el haber creado la impresión de un vacío inmenso, en el cual una vorágine misteriosa imprime un movimiento irresistible a los cuerpos, siendo el poderoso Cristo centro y origen del mismo.
La resurrección constituye un símbolo de la trascendencia, que se relaciona en parte con la creencia, ya presente en pueblos de la antigüedad, en la posibilidad de una «vida después de la muerte». «Si Cristo no resucitó, vacía es nuestra predicación, vacía es también nuestra fe»
Corintios 15,14-19
14 Y si Cristo no resucitó, vana es entonces nuestra predicación, vana es también vuestra fe.
15 Y aún somos hallados falsos testigos de Dios; porque hemos testificado de Dios que él haya levantado a Cristo; al cual no levantó, si en verdad los muertos no resucitan.
16 Porque si los muertos no resucitan, tampoco Cristo resucitó.
17 Y si Cristo no resucitó, vuestra fe es vana; aun estáis en vuestros pecados.
18 Entonces también los que durmieron en Cristo son perdidos.
19 Si en esta vida solamente esperamos en Cristo, los más miserables somos de todos los hombres[25]

---

[24]MUY HISTORIA. *Los Misterios del Vaticano,* p.59
[25]LA SANTA BIBLIA. *Primera Epístola a los Corintios. 15-14 al 19,* p.163

Fig. 125 Sibila Délfica.

Fig. 126 San Bartolomé.

Fig. 127 Eva implora.

Me enteré de este secreto en beneficio de la humanidad, para que vuelva a la fe verdadera, alcance el conocimiento total y abjure de toda doctrina falsa. Ese Jesús al que nosotros consideramos un profeta mortal, y en contra de lo que creen aquellos que lo tienen por el hijo de Dios, no resucitó al tercer día de entre los muertos, sino que su cadáver fue robado por gentes adictas a nuestra doctrina, que se lo llevaron a Safed, en las tierras altas de Galilea, donde Simón Ben Jeruquim le dio la sepultura en su propia tumba. Hicieron aquello con el fin de prevenir la difusión del culto que empezaba a formarse alrededor de la muerte del nazareno. Por supuesto que nadie podía adivinar que aquella acción fuese a desembocar precisamente en todo lo contrario y que los seguidores del profeta utilizarían aquel hecho como pretexto para aseverar que Jesús había subido al cielo en carne y hueso.[26]

Una semana después Jesús apareció de nuevo en el aposento alto en Jerusalén a los Apóstoles pero esta vez ya estaba Tomás, quien no había creído en la resurrección de Jesús. Tomás, el Dídimo, significa "gemelo". Parece que Tomás era pesimista por naturaleza. No le cabía la menor duda de que amaba a Jesús y se sentía muy apesadumbrado por su pasión y muerte.

Jesús no murió en la cruz, sino que salvó la vida gracias a una trama muy bien organizada, en la que Lázaro y José de Arimatea tuvieron gran protagonismo.

Tras su detención, Jesús fue torturado y, el 4 de abril del año 30, crucificado. Pero, como resultado de un plan muy bien organizado, no murió en la cruz. La operación tuvo tres fases esenciales. La primera consistió en darle a tomar un brebaje el teórico vinagre mencionado por san Juan (19, 29) o la pretendida mezcla de vino e hiel referido por san Mateo (27, 34) capaz de provocarle una inconsciencia tan profunda que, a los ojos de todos, pareciera muerto. La segunda y aún más complicada fue convencer a Pilatos de que Jesús había fallecido, que, por ende, podía ser ya bajado de la cruz sin esperar el tiempo comúnmente estipulado y sin quebrarle las piernas, como era norma usual y que autorizara su enterramiento circunstancia nada frecuente en caso de crucificados. Y la tercera y última, propiciar a Jesús lo antes posible los medicamentos y atenciones requeridos por alguien que había sufrido todo lo que él soportó.

La incredulidad de Santo Tomás, cuando éste asegura: “Si no veo la marca de los clavos en sus manos, si no pongo el dedo en el lugar de los clavos y la mano en su costado no lo creeré”. Ocho días más tarde aparece Jesucristo y le pide a Tomás que vea sus heridas y deje de ser incrédulo. (Juan 20:24-29).

---

[26]VANDENBERG, PHILIPP. *La Conjura Sixtina,* p.273

6.2. La Última Cena.

Fig. 128 Última Cena.

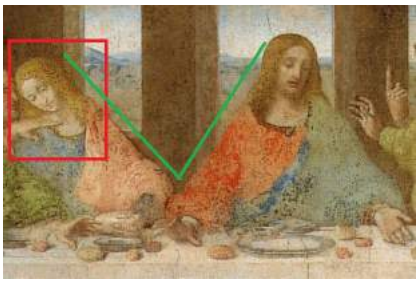


Fig. 129 María Magdalena, "v".

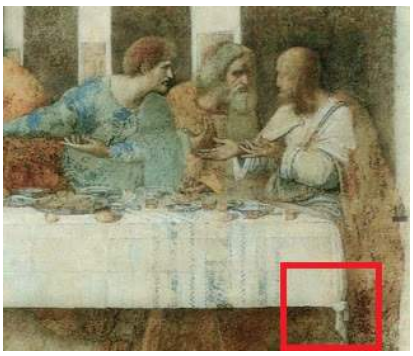


Fig. 130 Presencia de una mujer.

Fig. 131 Apóstol Tadeo como Leonardo.

Pues más allá de aspectos técnicos, como la composición y el dibujo, tenemos que admirar la profunda penetración de Leonardo en lo que respecta a la conducta y reacciones humanas y la poderosa imaginación que le permitió colocar la escena ante nuestros ojos. Un testigo ocular nos refiere que vio a menudo a Leonardo trabajando en "La última Cena", y que se pasaba todo un día sobre el andamio en continua meditación y sin dar una sola pincelada, es el fruto de este pensar lo que él nos ha legado.[27]

Una pintura que muestra a Jesús en la Última Cena con sus apóstoles y que se cree esconde claves sobre el fin del mundo. Mediante un puzle matemático oculto, es posible descifrar que, según Da Vinci, el fin del mundo se dará en el año 4406, como se pone de manifiesto en el Apocalipsis, Da Vinci había visto que la historia de la humanidad conduce a "la suma de todas las cosas, el juicio final", y que en ello veía el comienzo de una nueva era.

Doce apóstoles, el primer ciclo del sol ocurrió hace 25.800 años el ciclo de precesión, cada 2.150 años, avanzamos un Ciclo, una nueva Era. Para llegar a la cifra de 25.800 años, hay que pasar por 12 Eras (las doce constelaciones), los doce apóstoles. Ahora estamos en la Era de Piscis (por eso, el símbolo de Jesucristo son los peces).

El enigmático fresco de Santa María delle Grazie, en Milán, desvela la existencia de un gemelo de Jesús, segunda figura por la izquierda, y, con ello, el secreto de la resurrección.

La disposición de los apóstoles se corresponde con el zodiaco, agrupando los signos en cuatro grupos de tres, y oculta un código alfanumérico relativo a la estructura organizativa del Priorato de Sión. Y tomando como base la narración de la cena del Evangelio de San Juan, se ofrece una colosal alegoría sobre el Santo Grial: Leonardo coloca copas delante de todos los comensales, desmitificando la idea del único cáliz que se pasan entre ellos; sienta a María Magdalena a la derecha de Cristo; dibuja ambas figuras con ropajes de idénticos colores, aunque invertidos; las dos forman una "V" abierta, fig.129 con forma de recipiente, haciendo todo un guiño sobre el auténtico origen del cristianismo y el mito de la "sangre real". Hay varios detalles que muestran una composición musical que se nota en la posición de las manos y la distribución de los pedazos de pan de todos los comensales se puede apreciar una partitura que podría corresponder a un réquiem, quizás un himno a Dios. Da Vinci, dibujó en su obra una "M", para revelar que en la mesa estaba sentada y presente María Magdalena (de forma terrenal).Fig.133 El evangelio apócrifo de María Magdalena muestran que ella fue compañera de Jesús y tuvo un papel en la cristiandad de un nivel mayor que el de los apóstoles. Los más de cien evangelios apócrifos presentan a María Magdalena como la consorte e incluso como la apóstol más cercana a Jesús.

---

[27]GOMBRICH, ERNST HANS. *Historia del Arte,* p.247

Fig. 132 Apóstol Simón como Platón.

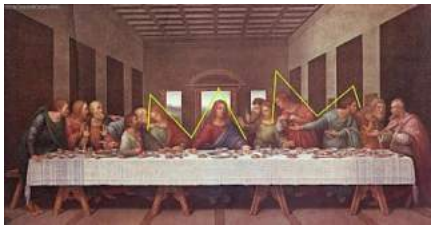


Fig. 133 María Magdalena.

Fig. 134 Mismo color de ropa.

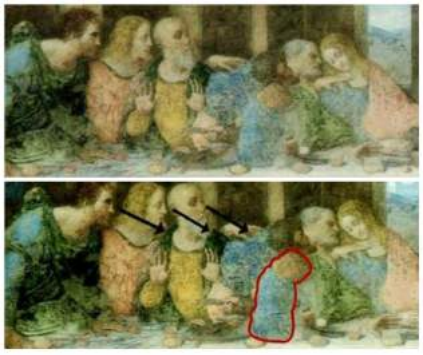


Fig. 135 Estereograma.

A nadie puede extrañar que Jesús, como todo judío devoto, se casase. Las pautas sociales de la época prácticamente prohibían que un hombre judío fuese soltero y en la tradición hebrea el celibato era censurable, siendo obligación del padre buscarle una esposa adecuada a sus hijos. Y sobre el enlace matrimonial entre Jesús y María Magdalena hay numerosas referencias en muy diversos textos. Así, por ejemplo, en escritos apócrifos como el Evangelio de Felipe, que en su Sentencia 55 señala que "la compañera del Salvador es María Magdalena; Cristo la amaba más que a todos sus discípulos y solía besarla en la boca". Lo cierto es que las bodas de Caná, en Galilea, por el año 27, fueron las de María Magdalena y Jesús, siendo coincidente, por tanto, su identidad con la del esposo en calidad de tal lo trata el maestre sala en el episodio evangélico (san Juan 2, 9-10).

María Magdalena fue la esposa de Jesús, tuvo con él descendencia, al menos tres hijos (una hembra y dos varones), y desempeñó una función crucial en el apoyo permanente a la labor de su marido y como depositaria de la semilla de su estirpe real. Y si fue "pecadora" se debió a que profesaba de manera abierta su devoción por dioses y, sobre todo, diosas ajenos a las creencias judías y que enlazaban directamente con la tradición egipcia. Asimismo, tuvo profundos conocimientos esotéricos, lo que sumado a su saber acerca de la misión política y espiritual de Jesús provocó que en algunos textos se la señale como "la que lo sabía todo". La sola idea que Jesús hubiese tenido una vida sexual, hace temblar a los cristianos y la iglesia, y más si esa mujer es Magdalena, una mujer que según la iglesia era una prostituta. La Iglesia, a través de la manipulación de textos y de mentiras, inculcó en la sociedad que Magdalena era impura, una prostituta arrepentida. Esta interpretación sirve a la iglesia para transmitir dos mensajes importantes: 1.- que María Magdalena y las mujeres en general, eran impuras y espiritualmente inferiores a los hombres, 2.- sólo la Iglesia ofrece la redención.

En la Última Cena, el propio Leonardo Da Vinci se pintó a sí mismo en el rol del apóstol Judas Tadeo (un gran predicador que evangelizó a muchos pueblos y que fue el portador de la Sábana Santa después de la muerte de Cristo).Fig.131 Y al apóstol Simón, como Platón.Fig.132 Da Vinci dejó una pista para establecer que sí hubo presencia de mujeres en dicha cena: un nudo que aparece en un extremo del mantel (La palabra "nudo" en italiano hace referencia a un vínculo " vincoli ", por lo que Da Vinci con este detalle estaría dando un indicio que en la mesa existe un vínculo muy especial).Fig.130 Los ropajes de Jesús son azul y rojo, y el de María Magdalena son casi los mismos, únicamente cambia la posición, ya que están de forma inversa, fig.136 intentó decirnos que uno completaba al otro, que estaban unidos mucho más allá de un simple trato afectuoso maestro-discípulo.Fig.134

Tiene un equilibrio perfecto, fig.138 y es peculiar que no haya ningún cáliz sobre la mesa.

Fig. 136 Escritura invertida.

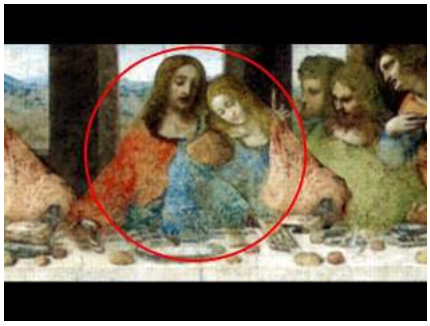


Fig. 137 Presentación.

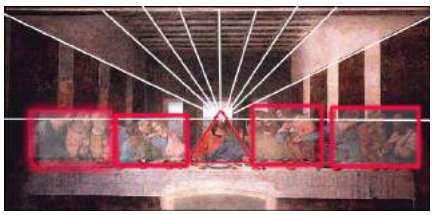


Fig. 138 Equilibrio.

Fig. 139 Última Cena.

Tomás, fig.142 quien alza su dedo índice a los cielos, indica con su gesto que él, como hermano de Jesús, debería ser el verdadero príncipe, el heredero legal al puesto que va a dejar vacante Jesús, y sabe que con un heredero real, de la sangre de Jesús, ese puesto no lo ocupará.

Da Vinci también dejó otro mensaje oculto. Si trazamos una línea entre las manos de Jesús, María Magdalena y Pedro, obtenemos una exacta imagen de espejo de la Constelación de Casiopea fig.144 (de forma celestial). En la mesa, se encuentra el heredero terrenal así como celestial, la "M" y la "M" invertida "W".

Entre sus hermanos, hubo uno que fue su gemelo. Se trató de Tomás, al que san Juan (11,16 y 20,24) llama Dídimo, esto es, gemelo en griego, y del que el Evangelio de Bartolomé, uno de los abundantes escritos no reconocidos por la Iglesia romana, dice ¡Salud a ti, gemelo mío, segundo Cristo!. Su condición de hermano gemelo de Jesús, explica, también, el curioso episodio que narra el Evangelio de Tomás (en su logión 13), texto apócrifo sobre el que se incidirá más adelante, cuando, al preguntar Jesús a sus discípulos a quién se parece, Tomás afirma: mi boca no aceptará en modo alguno que yo diga a quien te pareces.

Por tener Jesús un gemelo, adquirió gran relevancia su presentación en el Templo de Jerusalén para, como primogénito, ser consagrado ante Dios (san Lucas, 2, 25-35). Con ello, sus padres quisieron despejar cualquier tipo de duda sobre la linea sucesora y contar con el veredicto notarial del rabí Simeón.

En la Última Cena no sólo aparecería María Magdalena al lado de Jesucristo, sino que también el Santo Grial en sentido figurado, es decir, el hijo de ambos.Fig.137 El supuesto bebé aparece en una posición sentada, y Da Vinci lo habría ocultado utilizando una ingeniosa técnica, en que la cabeza del bebé se confunde con el cuello de Judas, y su espalda y piernas, con el brazo del mismo discípulo.Fig.135

Haciendo un ejercicio visual, María Magdalena se ajusta perfectamente entre Jesús y los demás apóstoles de la derecha, también mirando supuestamente hacia su hijo.Fig.141

El trinomio más alejado a la izquierda de Jesús, éste es el único donde los discípulos tienen sus manos alzadas hacia arriba. Simón, enfrascado con un diálogo con Judas Tadeo (que sería el mismo Leonardo Da Vinci) no parece estar tan sorprendido por la noticia que acaba de darles Jesús, más bien su gestualidad expresa afirmación, como aseverando las palabras del Nazareno.Fig.143

Si Jesús tenía mujer e hijo, o bien no habrían hablado de ellos o habrían hablado en clave. Jesús, su familia y sus seguidores eran plenamente conscientes de que estaban viviendo en una sociedad romana y que los romanos mataban a todos los herederos de cualquier aspirante a un reino en territorios que controlaban.[28]

---

[28]JACOBOVICI, SIMCHA y PELLEGRINO, CHARLES. *La Tumba de Jesús y su familia,* p.147

Fig. 140 Técnica espejo.

Qué pasa si Jesús fue oficiante de unas nupcias sagradas y, por tanto, participante voluntario en un rito pagano. Qué pasa si María Magdalena era la suma sacerdotisa de un culto a la diosa y por lo menos espiritualmente, igual a Jesús. Y qué pasa si en realidad Pedro y los demás discípulos varones no formaban parte del círculo interior de aquel movimiento. Pero aún nos queda otra pregunta que formulamos: una vez considerada esta situación tan radicalmente inédita, aunque sólo sea como hipótesis, ¿qué clase de hombre pudo ser el que ocupaba el lugar central de ese panorama? ¿Quién era el auténtico Jesús?[29]

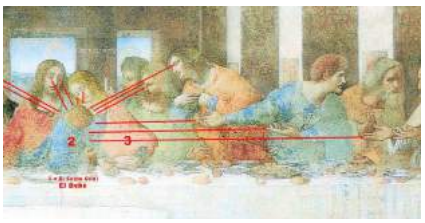


Fig. 141 Visión de Leonardo.

Fig. 144 Mensaje oculto entre Jesús, María Magdalena y Pedro. Imágen de espejo de la Constelación Casiopea.

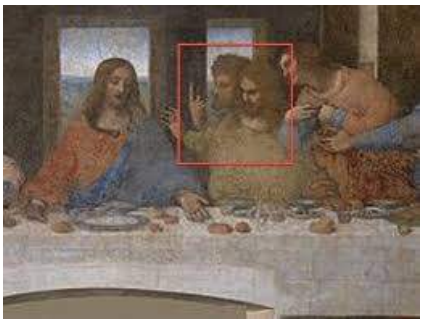


Fig. 142 Apóstol Tomás.

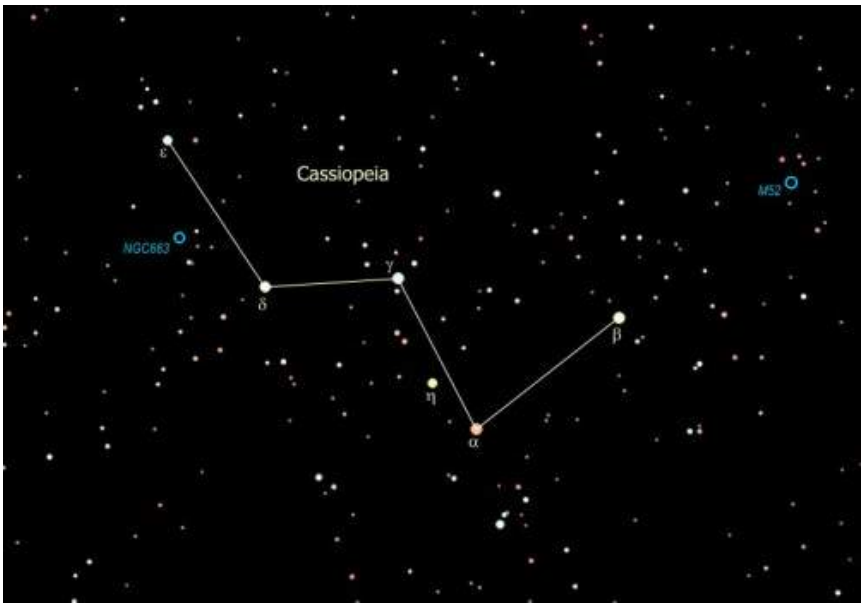


Fig. 145 Constelación Casiopea.

Fig. 143 Apóstoles Mateo, Tadeo y Simón.

---

[29]PICKNETT, LYNN y PRINCE, CLIVE. *La Revelación de los Templarios*, p.291

Fig. 146 Göbekli Tepe, grulla, zorro y vaca.

Fig. 147 Göbekli Tepe, grulla, zorro y vaca. Constelación de Escorpio.

7. CONCLUSIONES.

Para concluir, haré una reflexión sobre el Trabajo Final de Grado, cuya limitada extensión me obliga a tratar el tema como una mera pincelada de lo que podría ser. Desde el comienzo me ha fascinado las inscripciones de Göbekli Tepe fig.146, sobretodo porque representan el avance de la humanidad en su imaginación, ingenio y talento después de muchas generaciones. El mundo árabe me fascinó, por el gran salto en el conocimiento científico a lo largo de los siglos VI al XII con referentes asombrosos y avances importantísimos en criptografía.

El trabajo consigue su objetivo principal, pues describe cronológicamente la evolución de la criptografía a lo largo de la historia del ser humano, desde la prehistoria hasta los comienzos de la era digital. Un paseo por la historia de los conocimientos y la pericia necesaria para crear métodos criptográficos. A destacar la relevancia que la criptografía tuvo dentro de las organizaciones gubernamentales dedicadas al espionaje y el contraespionaje. La gran importancia que le doy al apartado 5.5.2. Máquina Enigma, es sin duda por ser el más temible sistema militar de codificación de la historia.

Los motivos que han llevado al ser humano a ocultar o codificar mensajes se han ido ampliando y sofisticando a la par que el desarrollo social. En los comienzos de la humanidad su necesidad iba más vinculada al poder y la guerra. En la actualidad, la encriptación se encuentra en muchos ámbitos de nuestra vida diaria, ya sea por motivos económicos, como por protección de datos de carácter personal. Hoy en día, estamos rodeados de información encriptada, tanto en un simple mensaje de wassap, como en un pago con tarjeta de crédito. La encriptación está más presente de lo que somos conscientes y en la actualidad, su elaboración es muy sofisticada siendo un producto de la inteligencia artificial, que ha llegado a desbancar a la inteligencia humana.

El apartado 6 referente a los mensajes ocultos, en la Capilla Sixtina y la Última Cena en la representación de pasajes bíblicos muestra como el talento, el ingenio y la creatividad podían ocultar lo que estaba a la vista. Es la criptografía en estado puro evidenciando la victoria de la inteligencia frente a los necios. Es la muestra más sublime que tiene el ser humano para, a través de su capacidad artística, revelarse frente al poder y expresar su frustración y rabia. A pesar de los numerosos estudios e investigaciones que hay sobre esas dos obras, todavía tienen muchos secretos por descubrir.

Comencé el trabajo con un misterio sin resolver, la inscripción de Shugborough y finalizo con uno todavía mayor y más fascinante, con múltiples enigmas y preguntas sin contestar.

Ha sido un tema muy interesante, una búsqueda intensiva de información, la cual me gustaría poder ampliar y tratar con mayor profundidad, para poder seguir aprendiendo.

Como sentenciaba en criptografía Francis Bacon, canciller de Inglaterra, ***"una cifra perfecta no debe ser trabajosa de escribir ni de leer, debe ser imposible de descifrar"***.

8. GLOSARIO Y SISTEMAS CRIPTOGRÁFICOS.

Acróstico, composición poética leída en vertical o en ese.
Algoritmo criptográfico, algoritmo que modifica los datos de un texto.
Cifra, el algoritmo que se utiliza para cifrar.
Cifrado, escrito con letras, símbolos o números.
Cifrar, utilización de un algoritmo para transformar un mensaje.
Claro, texto original antes de ser cifrado.
Clave, identificación personal.
Código, sistemas criptográfico a base de símbolos.
Criptoanálisis, estudia los sistemas criptográficos.
Criptografía, es el arte de ocultar en un mensaje la información que deseas confidencial.
Criptografía asimétrica, criptografía de dos claves.
Criptografía simétrica, criptografía de una clave.
Criptograma, fragmento de un mensaje cifrado.
Criptología, disciplina que se dedica al estudio de la escritura secreta.
Decodificar, aplicar las reglas adecuadas a un mensaje.
Descifrar, convertir le texto cifrado en sexta en claro.
Desencriptar, transformar información encriptada para hacerla legible.
Encriptación, simétrica y asimétrica.
Esteganografía, técnicas que permiten esconder un mensaje.
Estenografía, signos y abreviaturas para poder transcribir.
Estereograma, imágenes que permiten obtener una ilusión óptica.
Gematría, estudia el empleo simbólico de las letras como números.
Los nulos, tiene la función de confundir al criptoanalista.
Método, conjunto de procedimientos.
Nomenclator, signos o caracteres para sustituir palabras especificas.
Pasigrafía, escritura de conceptos.
Perlustrar, examinar con la vista.
Petroglifos, diseños simbólicos grabados o tallados en roca.
Petrogramas, diseños simbólicos dibujados o pintados en roca.
Semasiografía, fase en que las pinturas pueden expresar, sentido, escritura.
Signos, caracteres empleados.
Sistema, conjunto de métodos.
Sistema criptográfico, elementos y composición del sistema.
Sistema de sustitución, sustitución del texto plano por texto cifrado.
Sistema de transposición, Sistema de cifrado de letras o signos permutándolos de acuerdo a un determinado método.
Texto plano, no requiere ser interpretado para leerse.

Método de alternación, M. ADFGX, M. ADFGVX, M. del escítalo, M. del telégrafo, M. de rejilla, M. de tablas, M. de Baudot, M. de Baudot-Murray, M. de Kerckhoffs, M. de Julio Cesar, M. por signos convencionales, M. masónico, M. disco de cifrado, M. de Della Porta, M. de Polibio, M. Hygeburg, M. por análisis de frecuencia, M. de Vigenère, M. de Gronsfeld, M. de Beaufort, M. el Gran Cifrado, M. pigpen, M. de Bazeries, M. de Jefferson, M. Playfair, M. Hill, Cifra rail fence, C. de Delastelle, C. bífida, C. trífida, C. de Vernam.

9. BIBLIOGRAFÍA.

AUGÉ, MARC. *Los no lugares. Espacios del anonimato*. Ediciones Gedisa, S.A. Barcelona, 1998.
CALABRESE, OMAR. *El Lenguaje del Arte*. Ediciones Paidós Ibérica, S.A. Barcelona, 1987.
DE VINCI, LEONARDO. *El Tratado de la Pintura*. Ediciones, A. G. Novocraf, S.A. Murcia, 1985.
ENCICLOPEDIA UNIVERSAL, EL PAIS. *Historia Universal, Los Orígenes*. Salvat Ediciones, Madrid, 2004.
GIEDION, SIGFRIED. *El presente eterno: Los comienzos del arte*. Alianza Editorial, S.A. Madrid, 1981.
GIEDION, SIGFRIED. *El presente eterno: Los comienzos de la arquitectura*. Alianza Editorial, S.A. Madrid, 1986.
GOMBRICH, ERNST HANS. *Historia del Arte*. Alianza Editorial, S.A. Barcelona, 1984.
GOMBRICH, ERNST HANS. *La imagen y el ojo*. Alianza Editorial, S.A. Madrid, 1987.
JACOBOVICI, SIMCHA y PELLEGRINO, CHARLES. *La Tumba de Jesús y su familia*. Ediciones El Andén, S.L. Barcelona, 2007.
JAY GELD, IGNACE. *Historia de la escritura*. Alianza Editorial, S.A. Madrid, 1976.
LA SANTA BIBLIA. *Antiguo Testamento*. Editorial Planeta, S.A. Barcelona, 1966.
LA SANTA BIBLIA. *Nuevo Testamento*. Editorial Planeta, S.A. Barcelona, 1966.
LEVI-SRAUSS, CLAUDE. *El Pensamiento Salvaje*. Librairie Plon, París, 1994.
MARSHALL MCLUHAN, HERBERT. *La Galaxia Gutenberg*. Ediciones Aguilar S.A. Barcelona, 1993.
MOURE ROMANILLO, JOSÉ ALFONSO. *El Origen del Hombre*. Biblioteca Historia 16, Madrid, 1989.
PICKNETT, LYNN y PRINCE, CLIVE. *La Revelación de los Templarios*. Ediciones Martínez Roca, S.A. Barcelona, 1998.
PRIETO, MANUEL JESÚS. *Historia de la Criptografía*. Ediciones, La Esfera de los Libros, Madrid, 2020.
REZNIKOV OSIPOVICH, LAZAR´. *Semiótica y teoría del conocimiento*. Editor Alberto Corazón, Madrid, 1970.
SERRANO FARRERA, SEBASTIÀ. *La Semiótica*. Montesinos Editor, S.A. Barcelona, 1981.
TARANILLA de la VARGA, CARLOS JAVIER. *Criptografía. Los Lenguajes secretos a lo largo de la Historia*. TALENBOOK, S.L. Cordoba, 2018.
TOMÁS FERRÉ, FACUNDO. *Escrito, Pintado*. Visor Dis. S.A. Madrid, 1998.
VANDENBERG, PHILIPP. *La Conjura Sixtina*. Editorial Planeta, S.A. Barcelona, 2005.
ZÖLLENR, FRANK. *Leonardo da Vinci*. TASCHEN, LocTeam, S. L. Barcelona 2003.

CATÁLOGOS.

NATIONAL GEOGRAPHIC. *Cueva de Chauvet*. España. Editor, Susan Goldberg. National Geographic Society, Communications, 2001.
NATIONAL GEOGRAPHIC. *La secta de los números*. Edición, RBA Revistas, S.L. Barcelona, 2012.
MUY HISTORIA. *Los Misterios del Vaticano*. Madrid. Directora, Carmen Sabalete. Zinet Media Global, 2011.

WEBS.

https://monoskop.org/images/2/2c/McLuhanMarshallPowellsBRLaaldeaglobal.pdf [consulta: 2020-03-15].
https://jorgepalazon.wordpress.com/2012/07/01/gobekli-tepe-el-jardin-del-eden-biblico-episodio-ii/ [consulta: 2020-03-15].
https://jorgepalazon.wordpress.com/2012/02/01/la-verdadera-historia-del-mundo-parte-i/. [consulta: 2020-03-16].
https://jorgepalazon.wordpress.com/2012/07/08/fe-religiosa-vs-fe-agnostica-episodio-i-2/. [consulta: 2020-03-17].
https://radiomitre.cienradios.com/los-10-secretos-de-la-capilla-sixtina/. [consulta: 2020-03-19].
https://genial.guru/admiracion-curiosidades/16-secretos-de-los-frescos-de-la-capilla-sixtina-que-desconocen-incluso-los-guias-turisticos-1092810/. [consulta: 2020-03-16].
http://www.innsitu.es/ocultismo-la-creacion-adan-miguel-angel-racionalismo-la-capilla-sixtina-los-secretos-explicados/. [consulta: 2020-03-20].
https://books.google.cl/books?id=Y36Zuqd8yh8C&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false. [consulta: 2020-03-22].
http://www.librosmaravillosos.com/loscodigossecretos/index.html. [consulta: 2020-03-22].
https://www.delacuadra.net/escorial/arquitec.htm. [consulta: 2020-03-24].
http://online-keyboard.org/Alfabeto-ogamico-Tastiera/ANCIENT-Ogham/german/es-ES. [consulta: 2020-03-25].
http://reader.digitalbooks.pro/book/preview/22390/html59993. [consulta: 2020-03-24].
https://es.wikipedia.org/wiki/Codex_Sinaiticus. [consulta: 2020-03-27].
https://es.wikipedia.org/wiki/Palimpsesto_Sina%C3%ADtico [consulta: 2020-03-26].
https://www.um.es/tonosdigital/znum25/secciones/peri-2-en_busca_de_la_escritura_perdida.htm. [consulta: 2020-03-27].
https://es.scribd.com/document/351651852/Hegemonia-y-Lucha-Politica-en-Gramsci-Seleccion-de-Textos [consulta: 2020-03-28].
http://www.oyp.com.ar/nueva/revistas/236/1.php?con=6. [consulta: 2020-03-29].
https://www.cryptomuseum.com/crypto/bombe/. [consulta: 2020-03-28].
https://www.elconfidencial.com/tecnologia/2016-05-07/hagelin-purple-enigma-turing-cifrado_1195860/.[consulta: 2020-03-30].
https://www.eldiario.es/turing/criptografia/Breve-historia-criptografia_0_261773822.html. [consulta: 2020-03-30].
https://irreductible.naukas.com/2008/07/27/la-aventura-de-la-historia-mensajes-secretos-y-criptografia/[consulta: 2020-03-30].
https://www.bbc.com/mundo/noticias-44943402. [consulta: 2020-03-31].
http://juan-el-justo.blogspot.com/2007/12/jess-o-juan-de-gamala.html. [consulta: 2020-03-31].
https://www.condadodecastilla.es/blog/criptografia-en-la-alta-edad-media/. [consulta: 2020-03-31].
https://es.wikipedia.org/wiki/Edad_Media. [consulta: 2020-04-1].
https://ontranslation.es/origen-del-lenguaje/. [consulta: 2020-04-1].
https://aemetblog.es/2016/06/06/el-dia-d-la-prediccion-meteorologica-mas-importante-de-la-historia/. [consulta: 2020-04-3].
http://www.ordendeltemple.com/Logistica/LogisticaOrdenTemple.htm. [consulta: 2020-04-3].
https://www.periodistadigital.com/cultura/libros/20161115/antiguo-manuscrito-asegura-jesucristo-caso-tuvo-hijos-noticia-689401504077/. [consulta: 2020-04-7].
https://es.wikipedia.org/wiki/Brahmagupta. [consulta: 2020-04-10].
https://hipertextual.com/2011/07/la-maquina-enigma-el-sistema-de-cifrado-que-puso-en-jaque-a-europa. [consulta: 2020-04-11].
https://es.wikipedia.org/wiki/Exégesis_del_Alma. [consulta: 2020-04-11].
https://es.wikipedia.org/wiki/Libro_de_Tomás_el_Contendiente. [consulta: 2020-04-11].

10. ÍNDICE DE IMÁGENES.

Periodos de la Historia, cronología y evolución de la criptografía.