

Vida científica

LAS MUJERES Y LA CIENCIA

MUJERES EN LA CRIPTOGRAFÍA

El 9 de noviembre se celebra en los países de habla alemana el *día del inventor*. La fecha elegida por un empresario e inventor berlinés para conmemorar el cumpleaños de la actriz Hedy Lamarr, nacida en Viena (Austria) el 9 de noviembre de 1914. No fue un acto arbitrario de banalidad de un hombre seducido por la excepcional belleza de la actriz, sino que su intención era instaurar ese día como homenaje para animar a las personas a que materializasen sus ideas y recordar a inventores olvidados. Precisamente la actriz Hedy Lamarr había patentado en 1940 un sofisticado método para cifrar las comunicaciones y, sin embargo, su papel más original e inteligente, el de criptógrafa, pasó desapercibido porque su diseño se anticipó a las técnicas en uso y no se empleó hasta la entrada en funcionamiento de los sistemas digitales de comunicación.



Figura 1. Hedwig Eva Marie Kiesler, de nombre artístico Hedy Lamarr.

Hoy en día el ciudadano vive en un mundo de mensajes cifrados; cada vez que entra en Internet, consulta su saldo en el banco, hace una compra, utiliza su

tarjeta o accede a páginas privadas, está enviando datos que son sometidos a alguna técnica criptográfica: enviados, descifrados, utilizados y devueltos. Es un proceso complejo en el que la persona muchas veces sólo sabe la clave que le piden y en el que está en juego el que la información transmitida sea interceptada y utilizada incorrectamente por terceras partes, pero desconoce la complejidad de los procedimientos de criptografía aparejados para preservar la confidencialidad de los mensajes y mantener a raya a los “hackers” o espías de la red.

La criptología, que comprende tanto las técnicas de encriptado o codificado de la información como las desarrolladas para romper los códigos, es hoy en día un campo de investigación para las matemáticas, pero en el pasado fue un arte donde los individuos hacían gala de ingenio e imaginación para disimular sus palabras y comunicar sus secretos. Por supuesto, los avances y cambios han estado siempre asociados a alguna contienda internacional, cuando la información es absolutamente vital y se escoge a los mejores profesionales para que apliquen su inteligencia para hacerse con las comunicaciones secretas del enemigo y diseñar equipos y técnicas que les procuren ventajas significativas sobre el otro bando, como ocurrió en Europa en pleno siglo XX.

La actriz Hedy Lamarr vivió de cerca la Segunda Guerra Mundial y contribuyó a sentar las bases para una tecnología que revolucionaría los sistemas de las comunicaciones. Su nombre de nacimiento era Hedwig Eva Marie Kiesler. Su padre era un banquero y su madre una pianista, ambos de origen judío. Estudió ballet, piano y era considerada una niña prodigio. Inició estudios de ingeniería a los 16 años pero los abandonó para incorporarse a la compañía del director artístico Max Reinhardt, quien la describió como la mujer más bella de Europa.

En 1933 protagonizó la película *Éxtasis*, donde aparecía desnuda caminando por un bosque y provocando el consiguiente escándalo por ser la primera vez que se veían ese tipo de escenas en una película comercial.

Un fabricante e industrial de armas alemán, Friedrich Mandl se encaprichó y se casó con ella, compran-

do y destruyendo las copias de la película que la habían dado notoriedad. La prohibió seguir con su carrera y la privó de la libertad, obligándola a permanecer en casa. Hedy aprovechó para continuar con sus estudios de ingeniería y asistir a las reuniones de negocios de su marido con altos mandos del ejército nazi, aprendiendo técnicas militares y procurándose documentos valiosos que más tarde cedería al Gobierno americano.

En su libro autobiográfico, *Éxtasis y yo*, cuenta cómo consiguió librarse del régimen de cautividad a la que le tenía sometida su marido, disfrazándose de una de sus criadas y huyendo a París y después a Londres. En esta ciudad conoció al productor Louis B. Mayer, quien la recomendó escoger el nombre artístico de Hedy Lamarr y trasladarse a EE.UU. Su carrera cinematográfica no fue espectacular, su mayor éxito lo consiguió como protagonista de la película *Sansón y Dalila*, pero se equivocó al rechazar los papeles principales de las películas *Luz de Gas* y *Casablanca*. Se casó 6 veces y se retiró a Florida donde murió el 19 de enero del año 2000.

Nunca perdió su afición heredada por la música y fue ésta la que le unió a un compositor vecino suyo, George Antheil, también de origen alemán, para experimentar con los sistemas de control automático de instrumentos que él había empleado como compositor de la película abstracta, *Ballet Mecanique*. Hedy Lamarr era consciente de las dificultades que entrañaban las comunicaciones secretas, la fragilidad de las emisiones por radio y, en particular, los inconvenientes para desarrollar misiles teledirigidos, ya que si las señales emitidas eran detectadas por las potencias enemigas, éstas podían localizar el emisor e interceptar el misil. Discutió con su amigo Antheil sus ideas y le animó a buscar un método alternativo, inspirado en los tambores de una pianola, que permitiera enviar señales cambiando continuamente de canal para que el enemigo no pudiera rastrear la señal. Juntos, Antheil y Lamarr, ésta bajo su nombre de casada H.K. Markley, solicitaron en 1940 la concesión de una patente para un "sistema de comunicaciones secretas" que les concedieron en 1942. El desarrollo de la patente no era simple y durante años no fue utilizada hasta que una empresa de ingeniería, *Sylvania Electronic Systems Division*, se fijó en ella para diseñar un sistema que aseguraba la integridad de las comunicaciones militares. Se instaló en los barcos que intervinieron en el bloqueo a Cuba en 1962 y, a pesar de que los derechos de la patente habían caducado, los ingenieros reconocieron que se habían basado en la patente de Lamarr-Antheil.

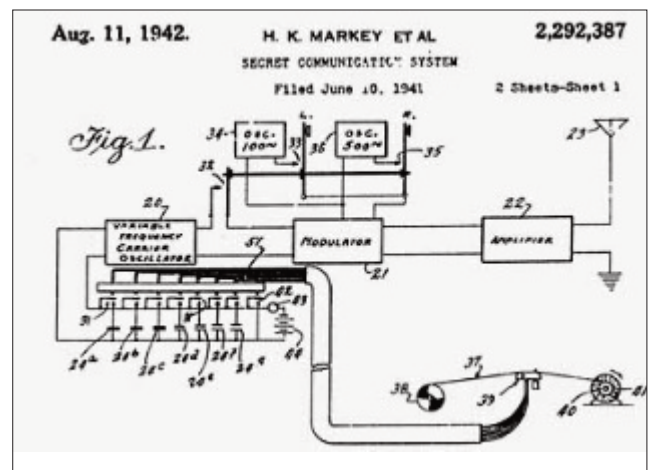


Figura 2. Patente Lamar-Antheil.

Pero la inventora Hedy Lamarr no ha sido la única mujer que ha destacado en este campo. El mundo de la creación de los mensajes secretos data de antiguo y el Kamasutra, del siglo IV a.C. ya recomienda, entre las 64 artes que deben aprender las mujeres, el de la escritura secreta para encubrir sus amoríos.

Una fe ciega en la fortaleza de los mensajes cifrados le costó la cabeza a la reina de Escocia María Estuardo, pretendiente al trono de Inglaterra. Recluida en un castillo por su hermana la reina Isabel I, que le costaba aceptar su traición, se carteó con sus aliados franceses convencida de que los servicios de espionaje de su hermana no detectarían su sistema de códigos y claves. Pero el maquiavélico y astuto primer secretario de la reina, Francis Walsingham, averiguó la forma en que se intercambiaban las misivas, camufladas en unos barriles, y una vez en su poder las envió a sus adiestrados espías para que las descifrarán y aportar pruebas sobre el complot de los aliados de María Estuardo para derrocar a su hermana.

El verdadero auge de la criptología y su transformación en una ciencia ocurre durante la Segunda Guerra Mundial, al producirse un cambio cuantitativo y cualitativo en la transmisión de señales cifradas. La cantidad de información secreta intercambiada entre los mandos militares y sus ejércitos exigió la introducción de sistemas mecánicos de cifrado y descifrado, obligando al empleo y adaptación de máquinas, como *Purple* o *Enigma*, que estando en el mercado no habían encontrado una adecuada utilidad. Y por otro lado, los esfuerzos de los aliados por criptoanalizar la ingente cantidad de mensajes interceptados por radio les empujó a diseñar los primeros sistemas informáticos, las llamadas "bom-

bas”, y posteriormente el *Colossus*, verdaderos antecedentes de los modernos ordenadores, concebidos para realizar miles de tentativas hasta dar con una secuencia de letras que permitiese leer los mensajes.

El cuartel general de los servicios de criptoanálisis ingleses se instaló en Bletchley Park, al norte de Londres, donde actualmente existe un museo dedicado a la criptografía y a los principios de la informática. El personal se reclutó especialmente entre matemáticos y científicos, pero también recurrieron a desafiar a los lectores de un diario con un crucigrama complejo. Aquellos que lo resolvieron en poco tiempo tenían que acudir a una dirección para reclamar un premio y entre ellos escogieron a hombres y mujeres para trabajar en los servicios secretos, exigiéndoles una absoluta discreción sobre el lugar y las tareas desempeñadas. Al acabar la guerra, se pidió a todos los que trabajaron en Bletchley Park que mantuviesen la confidencialidad de sus misiones y no lo contaran a nadie, para salvaguardar las ventajas adquiridas sobre las potencias enemigas y no comprometer secretos estratégicos. Durante años se supo muy poco de las actividades allí realizadas, hasta que en 1975 se desclasificaron los documentos e historiadores, investigadores y periodistas tuvieron acceso a la documentación militar de aquellos años y se publicaron datos, artículos y libros sobre aquella etapa. Cuando Simon Singh, en el año 2000, presentó su libro *Códigos Secretos* en Hay-on-Wye, donde recoge una buena parte de esa historia, en el turno de preguntas se levantó una señora mayor entre el público y dijo que ella era una de las que habían trabajado allí y había acatado las órdenes recibidas al acabar y jamás comentó las características de su trabajo durante la guerra.



Figura 3. Cuartel general del servicio de criptoanálisis inglés en Bletchley Park, Londres.

Ella era una de las tantas mujeres que, como Mavis Lever, contribuyeron a ganar la guerra y, sin embargo, se vieron obligadas a guardar un absoluto silencio sobre sus actividades sin poder reclamar ningún reconocimiento público. Mavis Lever fue contratada por el Ministerio de Guerra por sus conocimientos de alemán y enviada a Bletchley Park en mayo de 1940 a las órdenes de uno de los más destacados criptoanalistas, Dyllwyn Knox. Allí se interceptaban las comunicaciones por radio de los alemanes y se intentaba dar con las claves empleadas. Su intuición y talento resultaron muy valiosos para reconstruir el funcionamiento de los rotores de la máquina Enigma y comprender su operativa. En una ocasión llegó un mensaje donde no aparecía la letra “L”. Sabiendo que la máquina Enigma nunca transformaba una letra en sí misma supuso, acertadamente, que el mensaje era uno para despistar, un *dummy*, y que en realidad el operador, por desidia, en lugar de generar uno falso se había limitado a teclear la letra “L” repetidamente. Ese detalle les facilitó duplicar las máquinas Enigmas de los militares italianos.



Figura 4. Mavis Lever.

En Bletchley se casó con un colega matemático, formado en Cambridge, Keith Batey, y aunque nunca contaron a sus hijos lo que habían hecho durante la guerra, por lo menos pudieron hablarlo entre ellos y mantener vivos sus recuerdos. No así Ruth Borne, quien cuenta en una entrevista para la BCS (*British Computer Society*) que cuando salieron a la luz los libros hablando de sus proezas le dijo a su marido que ella había sido una de ellas, a lo que el marido indiferente respondió: “¡Qué interesante!... ¿Cuándo tomamos el té?”.

En estos últimos años Mavis Lever ha colaborado en la biografía del antiguo director Dyllwin Knox, quien

murió antes de acabar la guerra y cuya figura quedó un tanto oscurecida por el prestigio y atención dedicada a Alan Turing. Recientemente asesoró a la actriz Kate Winslet para interpretar a la protagonista de la película *Enigma* sobre aquellos críticos años.

También en el museo de la *National Security Agency* (NSA) americano, situado próximo a Washington, existe una placa donde se recogen los nombres de muchas mujeres que trabajaron calladamente en el campo de la criptología al otro lado del Atlántico.

Agnes Meyer Driscoll, una de ellas, había nacido en Illinois en 1889 y estudió matemáticas, física, lenguas extranjeras y música. En 1918, un año después de que EE.UU. entrara en la Primera Guerra Mundial, se alistó en la Marina y le asignaron a la sección de *Códigos y Señales* en la Dirección de Comunicaciones Navales. Hasta 1949, año de su jubilación, trabajó como criptógrafa de la Armada donde era conocida como *Madame X*. Agnes Driscoll se especializó en diseñar sistemas de cifrado y en introducir progresivamente las tecnologías emergentes. A lo largo de sus 30 años de carrera uno de sus éxitos consistió en descifrar los complejos códigos japoneses.



Figura 5. Agnes Meyer Driscoll.

La pionera de la criptología americana más famosa es **Elizbeth S. Friedman**, quien junto a su marido **William Friedmann** cosechó una cierta celebridad. Aunque algunos la ponen en un papel secundario respecto a su pareja, fue ella la que le introdujo en ese campo. **Elizbeth** había estudiado lenguas y era una entusiasta de Shakespeare. Un industrial la contrató para que ayudara a unos familiares suyos a demostrar que en realidad el verdadero autor de las piezas de teatro y los sonetos de Shakespeare había sido **Francis Bacon** y que había es-

condido en los escritos una información cifrada para acreditarlo.



Figura 6. Elizbeth S. Friedman.

En 1923, la Armada americana la empleó como criptoanalista. Entre sus objetivos era luchar contra el tráfico internacional de alcohol y drogas. Los traficantes recurrían a la radio para enviar información cifrada sobre sus envíos y operaciones convencidos de que aunque las misivas fueran detectadas nunca podrían descifrarlas. El panorama cambió en el momento en que **Elizbeth Friedmann** se dedicó a atacar sus claves y códigos y lograr repetidos éxitos. Se convirtió en un personaje esencial en los juicios contra los traficantes al aportar el testimonio sobre el contenido de las comunicaciones cifradas.

Recientemente ha habido un caso muy interesante de una mujer, en este caso casi una niña, que diseñó un sistema de encriptado para el comercio. **Sarah Flannery**, una estudiante irlandesa de 16 años escogió como tema de un proyecto escolar los sistemas de cifrado, desde los más antiguos empleados por Julio Cesar hasta el sistema actual, el RSA (inventado por **Ronald Rivest**, **Adi Shamir** y **Leonard Adelman**) básico para las transacciones comerciales por Internet y para la autenticación de los e-mails. Para profundizar en el proyecto tuvo que aprender lenguajes de programación para ordenadores y profundizar en las matemáticas. Su esfuerzo se vio recompensado porque ganó varios premios.

Animada por los resultados se apuntó a un trabajo de becaria en una empresa de seguridad de datos en Dublín, donde trabajó en nuevos procedimientos para encriptar datos basados en las sugerencias del fundador de la empresa. Tras varios meses diseñó un algoritmo que permitía cifrar los mensajes con el mismo nivel de seguridad pero requiriendo menor tiempo de uso de ordenador que los normalmente empleados. Su método fue sometido a un escrupuloso examen por los jueces que decidieron conceder-



Figura 7. *In Code*, libro escrito por Sarah Flannery y su padre, David Flannery.

que su algoritmo presentaba fallos, no ha impedido que siguiera una exitosa carrera de matemática en Cambridge y hoy en día trabaja en ese campo.

Hedy Lamarr, Mavis Lever, Agnes Driscoll, Elizebeth Friedmann y Sarah Flannery son algunos ejemplos de mujeres que destacaron y contribuyeron al desarrollo de la criptología, una ciencia en expansión y esencial ante el auge de las comunicaciones y la transmisión de información, y en la que actualmente trabajan numerosas profesionales.

le el premio del “Mejor joven científico del año 1999 de Irlanda”.

Su experiencia, las matemáticas necesarias, su entusiasmo por la ciencia son el tema de “*In code*”, libro escrito en colaboración con su padre que resulta muy estimulante y didáctico y constituye un pequeño manual de criptografía básica.

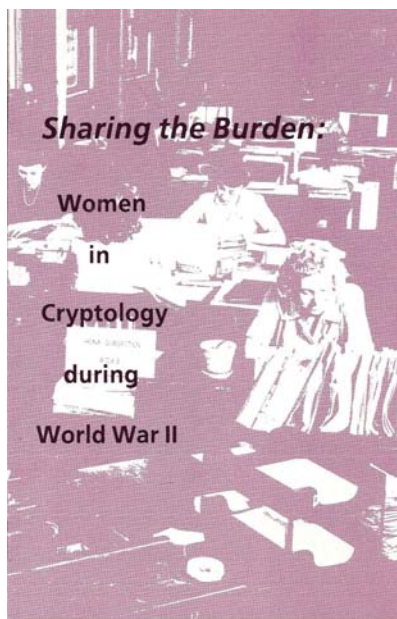
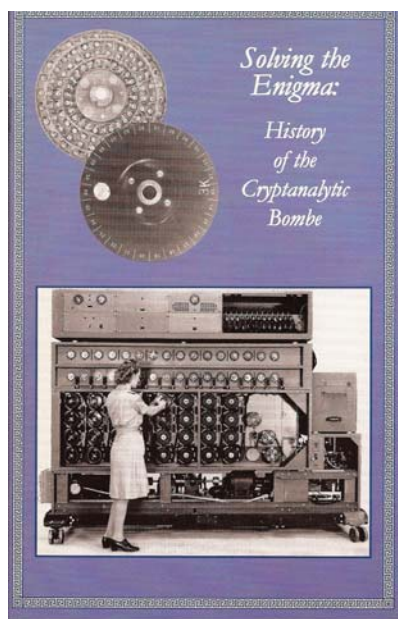
Aunque más tarde se comprobó

BIBLIOGRAFÍA

- [1] Hedy Lamarr: www.hedylamarr.com. Wikipedia: www.exordio.com/1939-1945/civilis/cine/lamarr.html
- [2] *Sharing the Burden. Women in cryptology during the World War II*, por Jennifer Wilcox. Documento del Center for Cryptologic History. National Security Agency (USA). March, 1998.
- [3] *Mavis Lever y su experiencia en Bletchley Park*. Boletín Enigma 52 (2 de mayo 2007). Taller de criptografía de Arturo Quirante. www.cripto.es.
- [4] *In Code. A mathematical journey*. Sarah Flannery with David Flannery. Profile books Ltd. (2001). ISBN: 1-86197-271-7.
- [5] *Codebreakers. The inside story of Bletchley Park*. Edited by F.H. Hinsley and Alan Stripp. Oxford University Press. ISBN 0-19-285304-X.
- [6] *Criptografía*. Conferencia del Curso “Matemática Recreativa” del Prof. Luis F. Rodríguez Marín, del Dpto. de Matemática Aplicada I de la ETSI Industriales de la UNED.
- [7] *The women in Bletchley Park*: www.squidoo.com/women-bletchley-park.
- [8] *National Cryptologic Museum*: www.nsa.gov/about/cryptologic_heritage/museum/.

Susana Mataix¹

Figura 8. Libros sobre mujeres y criptografía.



¹ Autora de *Lee a Julio Verne. El amor en tiempos de criptografía*. Editorial Rubes. ISBN: 84-497-0015-9.