suma+ 72
Secciones
Marzo 2013
pp. 105-114

Alan Turing y la manzana envenenada (1.ª parte)

Joaquín Collantes Hernáez
y Antonio Pérez Sanz

En puertas del tercer milenio

Siglo XX cambalache, problemático y febril… Así comenzaba el famoso tango (1934) de Enrique Santos Discépolo, en el que se recoge uno de los más ácidos diagnósticos de la condición humana en el cierre del segundo milenio de nuestra era.

Y si es verdad que el siglo XX fue febril en los aspectos sociales, políticos, económicos, tecnológicos, científicos y culturales, no es menos cierto que fue un siglo de lo más agitado y apasionante desde el punto de vista matemático. Y aún no ha terminado. Sí, los siglos matemáticos no terminan siempre cuando caen los dos ceros. Algunos duran 110 años; otros, sólo 90.

Si el siglo XX matemático empezó en el Congreso de París del año 1900 con la formulación de los 23 problemas de Hilbert, para nosotros, al menos, no terminó hasta el año 2006, coincidiendo con el *International Congress of Mathematics* (ICM) de Madrid y la demostración de la Conjetura de Poincaré por parte de Perelman.

En esta sección intentaremos hacer un recorrido rápido y discontinuo por las mentes matemáticas más notables de los últimos cien años. Por ella desfilarán hombres y mujeres que han iluminado con su genio alguno de los campos más actuales y potentes de la

Artículo solicitado por *Suma* en noviembre de 2012 y aceptado en enero de 2013

matemática actual. Turing, Wiles, Gödel, Kolmogorov, Santaló, Mandelbrot, Perelman, Noether, Kline y Thom, entre otros, visitarán estas páginas.

Pero no queremos mostrar sólo al personaje (sus obras y aportaciones), sino sobre todo a la persona, al ser humano que hay detrás de cada teorema y de cada demostración. Personaje + persona. Esa es nuestra intención: presentar a los lectores el rostro más humano de las matemáticas a las puertas del tercer milenio.

No estaré solo en esta mi tercera colaboración estable, en forma de sección fija, con la revista Suma. Esta aventura por la historia de la matemática reciente la intentaré llevar a buen puerto con mis jóvenes amigos y colegas José Luis Muñoz y Francisco Maíz. Y con los sabios consejos literarios de Joaquín Collantes.

Y para empezar, nada mejor que nuestro modesto homenaje, con unos meses de retraso por su centenario, a Alan Turing, el hombre que sabía demasiado. Es de justicia.

Buckinghamshire, Inglaterra: 1938

El hombre que tenía la carpeta sobre la mesa se revolvió incómodo en su asiento y miró con un punto de desconfianza a su interlocutor, un joven excesivamente atildado, para su gusto, que le había entregado el dossier encargado… y que en ese momento, ante la desconfianza de su superior, insistía:

> —¿Usted cree que es de fiar?
> —Sí, señor.
> —¿Esta seguro?
> —Por encima de todo es un gran matemático.
> —¿Por encima de todo?
> —He querido decir… bueno, quiero decir… que es el mejor de todos nosotros. Y, por supuesto, el que con mayor eficacia puede ayudar a Inglaterra en las actuales circunstancias —contestó el joven, desviando su mirada hacia el suelo—.
> —Está bien, está bien, está bien… Pero sepa usted que estará especialmente vigilado. En estos tiempos todos somos susceptibles de cometer errores que pueden ser fatales para la patria. Los homosexuales y las mujeres, y espero que esté de acuerdo conmigo, son personas especialmente sensibles, especialmente vulnerables a los ataques de agentes extranjeros. Además, la homosexualidad es una actividad (¿actividad? —se preguntó sorprendido el que escuchaba—) prohibida en Inglaterra y por lo tanto penada por la Ley. Por otra parte, tengo entendido que el señor…
> —Turing. Alan Mathison Turing, señor —añadió el que estaba de pie, al ver dudar a su superior—.
> —Pues bien, tengo entendido que el señor Alan Mathison Turing es, además, un hombre hermético y de personalidad un tanto complicada, por utilizar un término… En fin, no me fío de quienes no saben separar su vida privada de su vida profesional…
> —Pero, de momento, señor, no sabemos…

Claramente molesto por la interrupción, el hombre sentado fulminó con la mirada a su interlocutor, para continuar diciendo:

> —Además, el trabajo que va a llevar a cabo va a ser de estricto secreto. Pero ya veo que las referencias son inmejorables –dijo, ojeando el primer folio del dossier, y añadió- pero a mí, como militar, siempre me queda un poso de desconfianza… –iba a decir hacia los civiles, y probablemente hacia las mujeres y los homosexuales, pero frenó el comentario por respeto al civil que tenía delante y que, al igual que el matemático que le proponían, tenía un brillante expediente académico, más que suficiente para formar parte del Government *Code and Cypher School* (Escuela Gubernamental de Código y Cifrado)—.

En cuanto se quedó solo en el despacho, situado en la planta baja de la mansión conocida por el nombre de *Bletchley Park*, el militar vestido de civil que se sentaba ante la barroca mesa de caoba, se arrellanó en su asiento, abrió la carpeta en la que una letra ordenada y picuda había escrito «Informe secreto sobre Alan M. Turing», y comenzó a leer… (págs. 108 y 109).

Terminada la lectura del informe el hombre abrió un cajón de su mesa, sacó un tampón y una almohadilla y estampó en tinta roja en la carpeta, sobre el nombre que la identificaba, la palabra «APROBADO». Después, levantó el auricular de uno de los tres teléfonos que había sobre la mesa y dijo:

> —¡Que se incorpore a su trabajo mañana mismo!

Bletchley Park: 1938-1945

Bletchley Park estaba situado en la región de Buckinghamshire, en plena campiña inglesa, a 50 millas al noroeste de Londres. En este lugar se instaló la sede del *Government Code and Cypher School* (GC&CS) una nueva organización creada para descifrar códigos militares secretos que reemplazaba a otro departamento gubernamental llamado *Room 40*, organización creada para interceptar y controlar las comunicaciones del ejército alemán durante la I Guerra Mundial.

Los extensos terrenos que rodeaban la mansión de estilo neogótico Tudor, y que en su día tuvieron unos jardines en consonancia con la edificación, alojaron una serie de edificaciones auxiliares y barracones, o *huts*, donde se llevaba a cabo el trabajo real que efectuaban las doscientas personas que inicialmente se instalaron allí en el año 1938, cuando se tuvo la certeza de que la guerra con Alemania sería inevitable.

Una vez iniciada la II Guerra Mundial y con los ejércitos alemanes avanzando imparables por Europa, los esfuerzos para contrarrestar ese avance por parte de los aliados hicieron que aumentara la llegada de los llamados técnicos a *Bletchley Park*. Así, del grupo inicial de doscientos expertos se alcanzaría la cifra de diez mil en 1945, a modo de ejército en la sombra que luchaba a su manera, pero eficaz e inteligentemente, contra el enemigo. Eran hombres y mujeres de total y absoluta confianza reclutados principalmente mediante la llamada red de *old-boys* y *old-girls*, es decir, por veteranos del citado *Room 40*, cuya eficacia ya había sido sobradamente demostrada.

Así, aquellos veteranos técnicos se encargaron de ponerse en contacto con sus antiguos compañeros y profesores de Oxford, Cambridge, del *Newnham College* y del *Girton College* de Cambridge, indagando y confiando en su consejo acerca de quiénes podrían ser susceptibles de ser reclutados para una misión tan secreta que ni siquiera podían explicar de qué misión se trataba. Secreto absoluto: el enemigo lo ve todo, lo escucha todo. Un comentario imprudente puede significar el fracaso de una operación militar o una derrota en el frente (sigue en pág. 110).

Bletchley Park, en Buckinghamshire, al noreste de Londres

Informe secreto sobre Alan M. Turing

a) Alan Mathison Turing nació el 23 de Junio de 1912, en una clínica de la zona de Paddington, en Londres. Su padre, Julius Mathison Turing, era un alto funcionario del gobierno británico destinado en India que se casó con Ethel Sara Stoney, de origen irlandés e hija del ingeniero jefe de los ferrocarriles de Madrás. La madre del matemático se trasladó a Londres para que su hijo naciera en la metrópoli. En 1913 regresó junto a su marido dejando a su hijo, de tan solo un año, en Londres al cuidado de unos parientes. En 1926 volvieron definitivamente a Inglaterra.

b) Desde una edad muy temprana el niño dio muestras de una gran inteligencia. Y también desde muy pequeño mostró su interés por los rompecabezas y los juegos matemáticos. En el año 1918, a la edad de seis años, ingresó en el colegio St. Michael. Sus profesores observaron enseguida su interés por el cálculo y la facilidad con que resolvía problemas inaccesibles para un niño de su edad. Más tarde ingresó en la Hazlehurst Preparatory School donde fue un alumno normal, sin destacar especialmente en ninguna materia pero donde se interesó por primera vez en la práctica de deportes y por el ajedrez, intereses que mantendría durante toda su vida.

c) En 1926, a la edad de catorce años, ingresó en la Sherborne School, en el condado de Dorset, (se cuenta como anécdota que su primer día de clase coincidió con una huelga de transportes. El joven Turing, sin arredrarse ante tal contingencia y demostrando su magnífica condición física, recorrió en bicicleta las más de 60 millas que separaban su casa de la escuela, hazaña que fue recogida en la prensa local y que le haría muy popular entre sus compañeros de estudios). En la *Sherborne School* chocó con un sistema educativo poco estimulante para él. Su inclinación hacia las ciencias, la física, la química y las matemáticas lo enfrentaron a una línea educativa cuyas directrices estaban más encaminadas hacia el estudio de los clásicos y de las lenguas muertas. A pesar de todo, consiguió seguir adelante con sus preferencias científicas que lo llevarían a ganar premios escolares de matemáticas.

d) En 1928, recién cumplidos los dieciséis años, descubrió los trabajos de Albert Einstein sobre la Teoría de la Relatividad y sobre mecánica cuántica[1] a través del libro «La naturaleza del mundo físico», de A. S. Eddington. Y no

sólo pudo comprenderlos, sino que además los discutió con sus profesores, sorprendiéndoles con sus propias notas al respecto. Este año también conoció a Christopher Morcom, estudiante de un curso superior, cuya intensa amistad tuvo un gran efecto intelectual sobre el joven Turing, ya que trabajaron juntos en ideas científicas. La repentina muerte de Morcon en el mes de febrero de 1930 le produjo una profunda crisis nerviosa.

Por culpa de la crisis y de centrar su atención solamente en las disciplinas de ciencias, descuidando las materias de letras, no superó los exámenes para ingresar en el *Trynity College* de la universidad de Cambridge, que era su primera opción, teniendo que contentarse con la segunda: el *King´s College* de la misma universidad, donde estudió con el reputado matemático Godfrey Harold Hardy.

e) En 1932 centra su interés en la física a partir del descubrimiento de tres obras: el «Estudio de los fundamentos lógicos de mecánica cuántica», de John von Neumann, la obra de Bertrand Russell[2] titulada «Introducción a la filosofía matemática», y el libro «Principia Matemática», obra conjunta de A. N. Whitehead y B. Russel, considerada la obra maestra de la lógica matemática.

f) Entre 1932 y 1933 forma parte de movimientos y asociaciones estudiantiles, al tiempo que asume plenamente su identidad homosexual. Se sabe que tuvo un «más que amigo» llamado James Atkins, también estudiante de matemáticas. Ambos, homosexuales discretos, evitaron los ambientes homosexuales de todos conocidos en los círculos universitarios e intelectuales[3]. Además, y dada su complexión atlética, dedicó en esta época gran parte de su tiempo a actividades deportivas al aire libre, preferentemente a correr o remar, obteniendo muy buenos registros.

g) En 1933 es iniciado en los principios lógicos matemáticos por el ya citado Bertrand Russel, filósofo y matemático de enorme prestigio. Con la llegada al poder de los nacionalsocialistas de Adolf Hitler, se adhirió a los movimientos antibélicos que estallaron en Inglaterra y en el resto de Europa. Con todo, la postura de Turing fue netamente patriótica, ya que no se decantó, como algunos de sus compañeros de universidad, hacia movimientos revolucionarios de ideología marxista.Este mismo año concluye su estudio «Los números computables, con una aplicación al *Entscheidungsproblem*», que publicaría al año siguiente. En dicho estudio reformuló los resultados obtenidos por Kurt Gödel en 1931 sobre los límites de la demostrabilidad y la computación, sustituyendo al lenguaje formal universal descrito por Gödel[4].

i) En 1936 obtiene el Smith Prize por su trabajo sobre Teoría de Probabilidades titulado «Sobre la función de error de Gauss». Curiosamente, en este trabajo, y casi sin proponérselo, presenta una demostración del teorema central del límite, sin saber que Lindeberg lo había demostrado diez años antes. Este hecho le proporcionará a pesar de su corta edad un gran prestigio nacional e internacional.

j) En el mes de septiembre de este mismo año viajó a los Estados Unidos de América para trabajar durante los dos años siguientes en la Universidad de Princeton. En dicha universidad trabajó en el equipo del investigador especialista en lógica Alonzo Church, con quien haría sus estudios de doctorado en lógica matemática, analizando la noción de intuición en la matemática. También avanzó en su proyecto «Ordinal Logics», probablemente su más profundo trabajo matemático y que lo aproximaría al mundo de lo abstracto. Durante el verano de este mismo año publica su obra más significativa «On Computable Numbers with an Application to the Entscheidungsproblem» donde pone la simiente de la Teoría de la Computabilidad y presenta la idea de la llamada «Maquina de Turing»[5].

j) En 1938 obtuvo el Doctorado en Princeton con la tesis que llevaba por título «Systems of Logic Based on Ordinals», trabajando posteriormente como becario de John von Neumann en el Institut for Advanced Studies, donde le ofrecieron un puesto académico, puesto que Turing rechazó para volver a Inglaterra durante el verano del presente año.

1 El hombre que leía el informe empezó a subrayar en rojo algunos párrafos.

2 Doble subrayado en rojo con el añadido al margen y en letras mayúsculas: «ATENCIÓN: PACIFISTA»

3 Doble subrayado en rojo de los tres renglones.

4 Nota: Ya desde sus primeras publicaciones aparece un proyecto de máquina autómata, no física sino abstracta. Y en uno de de sus trabajos sienta con gran brillantez las bases teóricas del problema formulado por David Hilbert a principios de siglo, el citado Entscheidungsproblem, o problema de decisión, sobre la existencia de un algoritmo de respuesta universal.

5 Nota: la información sobre las características de la citada máquina, por extensas, se presentan en informe aparte.

Otro tipo de reclutamiento fue, cuando menos, original: a través de un crucigrama publicado en el periódico *The Daily Telegraph* y presentado como un concurso. Los concursantes que lograban hacer los crucigramas en menos de 12 minutos eran seleccionados y se les proponía realizar un trabajo especial para contribuir al esfuerzo bélico de Gran Bretaña. De esta manera se crearon equipos de cripto-analistas cuya única e importante misión consistiría en descifrar el mayor volumen de mensajes secretos del ejército alemán interceptados y, sobre todo, en el menor tiempo posible.

Los equipos estaban compuestos por un heterogéneo grupo de matemáticos, ingenieros, traductores de alemán, físicos, químicos, expertos en geografía e historia, lingüistas, especialistas en cultura clásica, maestros del juego de ajedrez, arqueólogos expertos en jeroglíficos, expertos en crucigramas, psicólogos y hasta filósofos. En fin, por una variopinta amalgama de mentes preparadas para abordar todo tipo de problemas y, sobre todo, con capacidad y entusiasmo para resolverlos. A este grupo se uniría Alan Turing como responsable de descifrar los códigos secretos de los mensajes interceptados procedentes de la marina alemana.

El sistema de trabajo consistía en que un problema a primera vista irresoluble pasaría de experto en experto hasta que cayera en las manos de quien tuviera las herramientas mentales apropiadas para resolverlo…, o para seguir resolviéndolo, ya que a veces cada experto resolvía el problema parcialmente. Así que lo volvía a pasar a otra persona para que lo siguiera construyendo sobre el trabajo de descifrамiento ya efectuado por él; y a veces éste lo pasaba a otro experto, y ése a otro…, hasta que tenían la completa seguridad de que el problema estaba resuelto.

El trabajo de los expertos se organizó como en una fábrica. Cada grupo de criptoanalistas, también llamados rompecódigos, trabajaba en distintos pabellones separados entre sí a modo de secciones de una misma cadena de trabajo. A estos pabellones se los denominaba cabañas o *hut* y estaban numerados para distinguir la especialidad de quienes trabajaban en ellos. De esta manera mientras técnicos y criptoanalistas de un *hut* se dedicaban a interceptar mensajes del espionaje alemán o de sus ejércitos, los de otro tenían por misión el descifrado de estas comunicaciones encriptadas, pasando los mensajes descifrados a un tercer *hut* donde se traducían al inglés; y de allí, a un cuarto departamento dedicado a analizar los resultados obtenidos y a recomponer una imagen de las operaciones desentrañadas. Trabajando ininterrumpidamente las 24 horas del día aquellos equipos fueron piezas fundamentales para la victoria de los ejércitos aliados. Además, la tecnología que inventaron y desarrollaron marcaría el comienzo de la era de la informática que dominaría el resto del siglo XX.

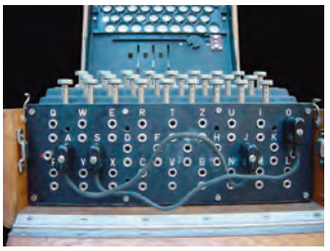
Enigma: 1917-1945

En 1917 el norteamericano Edward H. Hebern ideó un sistema mecánico de rotores mediante los cuales transformaba caracteres utilizando alfabetos independientes, como método de sustitución polialfabética. Pero sería un año después, a finales de la I Guerra Mundial, cuando un ingeniero llamado Arthur Scherbius patentó una máquina para encriptar textos en clave a la que bautizó con el nombre de *Enigma*, sin poder imaginar en ese momento que su máquina sería decisiva para las operaciones militares en la segunda gran guerra europea que nadie esperaba, pero que apenas tardaría veinte años en llegar.

Scherbius se asoció con E. R. Ritter fundando la empresa *Scherbius & Ritter* con la idea de que la máquina se vendiera a las grandes empresas con vistas a transacciones comerciales más o menos secretas que lo serían del todo encriptándolas. Convencidos de sus posibilidades militares para la elaboración de mensajes en clave, se la ofrecieron a la marina alemana, que no mostró

un especial interés ella. Decepcionados, los dos socios vendieron su empresa a la alemana *Chiffriermaschinen*, que durante los años siguientes comercializaría máquinas de distintas características para uso exclusivamente civil, distinguiendo cada uno de los modelos de venta en el mercado con las primeras letras del alfabeto.

A medida que se asentaba el prestigio de la máquina entre las empresas alemanas y también europeas, la marina alemana recapacitó y desarrolló sus propios modelos de *Enigma*.



La máquina *Enigma*

Con la llegada de los nacionalsocialistas al poder en el año 1933, las prioridades del ejército alemán pasaron a un primer plano y la marina, como precursora del proyecto, contó con todas las facilidades gubernamentales para desarrollar y mejorar una máquina que, ahora que otros vientos distintos a los de la década anterior corrían por Europa, parecía más que imprescindible para el engreído III Reich.

Las investigaciones y los modelos de *Enigma* habían ido avanzando hasta que en 1934 apareció el modelo más sofisticado, considerado secreto de estado, y conocido con el nombre de *Wehrmacht*, que sería utilizado por el ejército alemán para cifrar sus mensajes antes de ser emitidos a sus tropas a través de radio por el sistema Morse. A pesar de todo, y al ser la marina alemana el cuerpo de ejército de élite mimado por Berlín, desarrollaron su propio modelo de Enigma que bautizaron como *Funkschlüssel 4*, o simplemente, *M-4*.

Los fallos de *Enigma*

1. La codificación era una función letra a letra.

2. La imagen de cada letra no podía ser la propia letra.

3. La clave inicial diaria de tres letras que informaba de la codificación utilizada se repetía dos veces para garantizar una recepción correcta, lo que hacía más fácil descifrarla.

La máquina combinaba componentes eléctricos y mecánicos ingeniosos, pero no excesivamente complicados de manejar. La dificultad estribaba en la capacidad de cambio de posibilidades de escritura y número de combinaciones que la máquina, convenientemente manejada, producía. Los componentes mecánicos eran el cerebro de la máquina y estaban formados por un teclado a semejanza de los de las máquinas de escribir y un grupo de rotores, normalmente cinco, pero que la marina alemana, para aumentar la complejidad de sus máquinas, llegaría a aumentar hasta ocho. De la elección inicial de tres de esos ocho rotores y de sus posiciones iniciales dependía la encriptación obtenida. Así, los mensajes se escribían tal como eran redactados, pero cada vez que se pulsaba una tecla se producía un giro en uno de los rotores que a su vez giraba el resto.

Al principio del mensaje iba la clave local, habitualmente tres letras, con la que se había codificado el mensaje. Esta clave se cambiaba diariamente. De esta manera se lograba que una letra no estuviera siempre codificada por el mismo carácter inicial pues a cada pulsación de una tecla, y como consecuencia del giro secuenciado de los rotores, variaban las letras que escribían dicho mensaje. Cada rotor contenía todas las letras del alfabeto, en una de sus caras había un disco dentado de baquelita y en otra una serie de contactos eléctricos también colocados en círculo, lo que hacía que las combinaciones para transformar una letra en otra distinta creciera hasta un número considerablemente grande y dificultando así la lectura de cualquier mensaje interceptado. De hecho, los alemanes para simplificar su uso, redujeron las más de 10.114 configuraciones posibles a ¡sólo! 1.023. El trabajo de Turing consistió en diseñar algoritmos basados en la periodicidad forzosa de los engranajes para facilitar la búsqueda de las claves diarias.

Aunque el ejército alemán fue el que comenzó a utilizarla, los demás ejércitos europeos también adquirieron sus propias máquinas *Enigma* y a partir de 1938, cuando ya estaban claras las intenciones expansionistas de la Alemania nazi, estalló una guerra de espionaje industrial —un año antes de que estallara la guerra real— en la que todos querían saber cómo eran las máquinas *Enigma* de los demás y si su modelo de *Enigma* era superior al de los ejércitos de los otros países, sobre todo al de Alemania. Se estima que desde 1933 a 1945 se fabricaron más de cien mil unidades de estas máquinas.

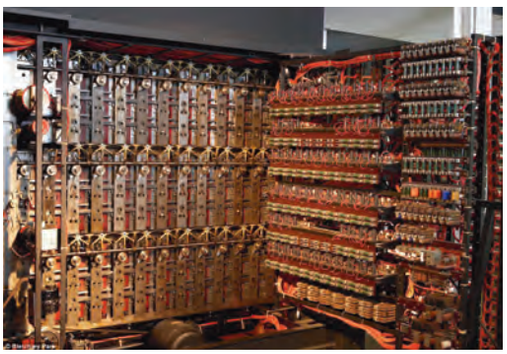
Bombe: 1938

Cuando Alan Turing llegó a *Bletchley Park* se encontró un mundo rígido y cerrado en el que los llamados técnicos llevaban a cabo un trabajo considerado esencial que era mantenido en secreto, no sólo para sus familiares y amigos, sino hasta para los mismos compañeros de trabajo. Los técnicos de un barracón desconocían el trabajo que hacían los del barracón de al lado.

La misión de Turing, así como la de todos los que trabajaban en el *hut 8*, era perfeccionar las máquinas que se utilizaban para descifrar los mensajes en clave que se interceptaban a los alemanes. Así, el trabajo de los técnicos del *hut 8* sería esencial para intentar romper el bloqueo naval que llevarían a cabo los submarinos alemanes, los temidos *U-boot*, contra Inglaterra a partir de agosto de 1940.

Años antes de que estallara la guerra los alemanes enviaron una máquina *Enigma* a Varsovia y, por azar, cayó en manos de los polacos que la estudiaron durante una semana, enviándola de nuevo a su destino tal y como había llegado a sus manos. Un grupo de matemáticos polacos, dirigidos por Marian Rejewski consiguió descubrir los códigos de la máquina en ese tiempo record. Aunque fuera solamente un primer paso, la labor de los matemáticos polacos fue la clave para el éxito posterior obtenido en *Bletchley Park*.

Los alemanes sospecharon que sus claves iniciales habían sido descubiertas y en 1938, un año antes de la invasión de Polonia, decidieron cambiar su estrategia. Pero a cada paso hacia delante que daban los técnicos alemanes, otro tanto hacían los matemáticos polacos logrando localizar los nuevos códigos a partir del análisis de las frecuencias que denominaron «hembras», lo que les permitió configurar sus máquinas *Enigma* para descifrar los mensajes interceptados. La amenaza de la guerra llevó a los polacos a plantearse la posibilidad de sustituir el método manual utilizado hasta entonces para analizar las frecuencias por una máquina electromecánica, una batalla de máquina contra máquina. Así surgió la máquina denominada *Bombe*. La falta de recursos de los polacos llevó a que, a principios de 1939, sus servicios de inteligencia pasaran la información obtenida y los trabajos realizados a ingleses y franceses para que continuaran la importante labor por ellos comenzada.



Recreación de una máquina *Bombe*

La invasión de Polonia el día 1 de septiembre de 1939 precipitó los trabajos de investigación en *Bletchley Park*. Afortunadamente, los matemáticos que allí trabajaban ya eran expertos en las complejidades que presentaba la *Enigma*. Las aportaciones hechas por los matemáticos polacos unos años antes allanaron el camino para que los ingleses trabajaran ahora sobre los mensajes codificados alemanes elaborados con la máquina polaca *Bombe* y por las versiones perfeccionadas de *Enigma*, convertida a esas alturas en

una máquina casi perfecta por indescifrable…, o al menos eso creían los alemanes. Una vez descubiertos los métodos utilizados por los alemanes para encriptar sus mensajes ahora deberían averiguar los cambios en las claves que a diario hacían en sus máquinas. La captura de algunas máquinas *Enigma* alemanas facilitó el trabajo de los criptoanalistas ingleses, al descubrir que los operarios alemanes que manejaban las máquinas cambiaban cada noche las claves a usar al día siguiente.

De esta manera, aunque los ingleses descubrieran una clave utilizada para descifrar los mensajes, al día siguiente se encontrarían con otra distinta. Así, los ingleses tenían que averiguar cada día la nueva clave impuesta. Era un trabajo de nunca acabar que les llevaba a trabajar las veinticuatro horas de día, ya que en cuanto descubrían la clave cambiada tenían que descifrar y traducir los mensajes interceptados…, para ponerse a trabajar a continuación en el descubrimiento de la siguiente clave. Los alemanes nunca utilizaban un rotor en la misma posición durante más de dos días, lo que llevó a los aliados a intentar nuevas técnicas al ser conscientes de que la suya era una lucha agotadora contra una máquina cuya forma de ser manejada variaba constantemente.

Esta situación los empujó a recuperar las investigaciones de sus colegas polacos, dándose cuenta de que la clave podría estar en rediseñar la máquina *Bombe* polaca y partir de nuevo de ella para conseguir formas más rápidas de desciframiento.

Alan Turing, desde su llegada a *Bletchley Park*, se incorporó, como hombre clave, a trabajar en el diseño mejorado de la máquina *Bombe* polaca. Trabajó en la nueva *Bombe,* una máquina que nació de su ingenio personal y a la que ya todos llamaban la *Bombe* de Turing, ya que suya fue la idea original perfeccionada con mejoras sugeridas por el también matemático Gordon Welchman y cuyo diseño y construcción recayó en Harold Keen, miembro de la empresa *British Tabulating Machina*. La nueva máquina *Bombe* se convirtió en la herramienta más importante para leer con mayor precisión y rapidez las transmisiones de las maquinas Enigma alemanas.

El primer diseño de Turing fue bautizado con el nombre de *Victory* instalándose en *Bletchley Park* en marzo de 1940. En agosto de 1940 se fabricó e instaló una máquina de prestaciones más avanzadas con el nombre de *Spider* y en la primavera del año siguiente, se instaló un tercer modelo, aún con más prestaciones, llamado *Jumbo*. Gracias a la popularidad de su trabajo, ya en 1942 Alan Turing era considerado un auténtico genio entre sus compañeros de *Bletchley Park*.

A principios del año 1943 nuevas versiones de la máquina *Bombe* mejoradas se empezaron a fabricar en Estados Unidos hasta llegar a 120 unidades, aunque en la actualidad solamente se conserva una en el Museo Nacional de Criptografía. Por su parte, a finales de la II Guerra Mundial llegó a haber instaladas en *Bletchley Park* 210 *Bombes* que requerían del trabajo de 2.000 especialistas para su mantenimiento y funcionamiento. Una vez terminada la guerra, el primer ministro inglés, Winston Churchill mandó destruir todas las máquinas, al considerarlas secreto de Estado.

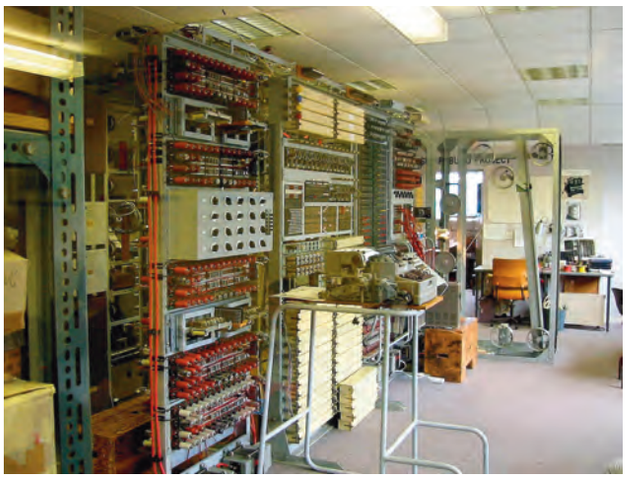
Concluida la guerra, Alan Turing sería condecorado con la Orden del Imperio Británico en reconocimiento a su contribución a la victoria de los Aliados.

Colossus

En paralelo al desarrollo de las *Bombes*, en *Bletchley Park* tuvo lugar otro acontecimiento ideado y desarrollado por el matemático inglés y que en aquel momento se mantendría en un modesto segundo plano: el nacimiento de la máquina *Colossus*.

Este primer computador fue diseñado también con el único objeto de ayudar a su compañera *Bombe* a descifrar los códigos alemanes. *Colossus* surgiría de la

imperiosa necesidad de aumentar la eficacia en el descifrado de los códigos y, sobre todo, la rapidez de su ejecución. La idea surgió al trabajar sobre la interceptación de teletipos codificados por los alemanes en sus transmisiones. Los ingleses llamaron *Fish* a las claves alemanas que circulaban a través de teletipo para distinguirlas de las recibidas a través de las máquinas *Bombe*, ya que los alemanes utilizaban conjuntamente las máquinas *Enigma* junto a dichos teletipos codificados para dificultar el descifrado de sus claves. La nueva máquina se utilizaría inicialmente para descifrar los llamados códigos *Fish*.



Colossus.
Reconstrucción del Museo de la Computación Británico

A comienzos de la guerra los servicios ingleses interceptaron señales de teletipo en las que no se utilizaba el código *Morse* y que eran distintas a las codificadas normalmente con las *Enigma*. Se trataba de señales codificadas por el ejército alemán mediante una máquina diferente, conocida con el nombre de *Lorenz*, consistente en un accesorio que conectado a un teletipo cumplía los mismos propósitos que *Enigma*, pero con distintas claves. Serían precisamente sus observaciones del sistema *Fish* las que llevarían a Turing a idear la primera máquina programable, electrónica y digital. Turing fue el creador de la idea inicial y de la base lógica en los computadores. El primer prototipo de esta máquina fue diseñado por Tommy Flowers, un técnico de la *British Post Office Research Station* que planteó la utilización de válvulas, convirtiendo así su propuesta en el primer ordenador de la historia. Aunque, de hecho, no era un computador de propósito general. La máquina como tal sería diseñada y construida por Maxwell Newman en 1943.

Así, una primera versión de *Colossus* llamada *Markus 1* se construyó a comienzos de 1944 seguida de una nueva versión mejorada en junio de ese mismo año denominada *Markus 2*. A finales de la II Guerra Mundial estaban en servicio diez máquinas *Markus 2* en *Bletchley Park*. Gracias a las *Colossus*, 63 millones de caracteres contenidos en mensajes alemanes cifrados interceptados por los aliados fueron descifrados con éxito. Todas esas máquinas y las *Bombe* fueron destruidas al final de la guerra por orden del primer ministro británico, así como los planos y estudios del proyecto con objeto de preservar lo considerado como alto secreto militar.

Treinta años después de terminada la guerra, en 1976, una vez concluido el plazo que imponía la ley de secretos militares, el proyecto *Colossus* volvió a salir a la luz sacando al escenario de la Historia a los protagonistas del proyecto, con Alan Turing a la cabeza, quienes desde entonces serían considerados los creadores del primer ordenador, por delante de los creadores del norteamericano *ENAC*.

Pero no será *Colossus* la máquina más famosa de Turing. El padre de la computación se hará famoso por una máquina que nunca existió: la famosa «Máquina de Turing». Pero esa es otra historia que..., continuará.

Antonio Pérez Sanz
IES Salvador Dalí, Madrid
SMPM
Joaquín Collantes Hernáez
<tercermilenio@revistasuma.es>