Celebrando el centenario del nacimiento de Alan Turing, este artículo narra el viaje que realizó a Estados Unidos para ayudar a los norteamericanos en la construcción de máquinas *Bombe*. Allí aprendió electrónica y conoció el sistema de encriptación vocal SIGSALY. Cuando regresó a Gran Bretaña, Turing inventó su propio aparato encriptador llamado "Dalila", aunque no lo terminó.

Voces secretas. Alan Turing en Estados Unidos, de "SIGSALY" a "Dalila"

Luis Fernando Real Martín,
Ingeniero Técnico de Telecomunicación
lrealmar@gmail.com

Dalila le dijo:
— ¿Cómo puedes decir que me amas si no tienes confianza en mí?. Por tres veces te has burlado de mí y no me has revelado el secreto de tu extraordinaria fuerza.

Jueces 16,15

Entonces Sansón dijo al lazarillo:
— Llévame hasta las columnas sobre las que descansa el edificio para que pueda apoyarme en ellas.

Jueces 16,26

FRÍO OCÉANO

La silueta de un hombre se recorta en la baranda del barco en esta noche serena y despejada. No hay luces, navega oscuro y silencioso para no ser descubierto. Chapotea lejana el agua, no hay orquesta, ni fiesta. –Un iceberg se vería perfectamente con esta luna llena–, piensa para si, recordando aquel transatlántico. Hace frío, mucho frío. Se cierra el cuello del abrigo con una mano y entra buscando en su camarote algo de calor.

A TRAVÉS DEL ATLÁNTICO

A finales de 1942 el Atlántico fue un lugar un poco más seguro gracias al trabajo de este hombre. Y nada más arriesgado para verificar los resultados que

Figura 1. Retrato de Alan Turing. (Acuarela del autor).

Figura 2. Lugares visitados por Turing en Estados Unidos.

embarcarse en un viaje desde Gran Bretaña hacia los Estados Unidos. Alan Turing cruzaba el océano hacia Nueva York.

El personal de Blentchley Park (Figura 3) y las máquinas *Bombe* habían descifrado el sistema de codificación de la máquina Enigma de tres rotores, la M3, utilizada para las comunicaciones de la marina alemanas. Al contrario que con el ejército o la aviación, descifrar los mensajes de la marina había costado más tiempo y trabajo debido al riguroso cumplimiento de las normativas de seguridad de sus comunicaciones. Pero ahora era posible conocer las posiciones de los terribles submarinos U-boat. Los convoyes transportaban más seguros los suministros materiales y los alimentos básicos hacia las islas británicas.

Las *Bombe* eran unas máquinas que iban buscando rápidamente combinaciones entre el mensaje cifrado interceptado y una clave cambiante hasta obtener como respuesta, la relación de ésta última con el mensaje original. La búsqueda no era a ciegas, el contenido y la estructura de la información era hasta cierto punto previsible[1] y conocida. Los aliados habían capturado los cuadernos de los códigos de señales para la transmisión de los partes meteorológicos y de la posición de los navíos que los buques alemanes intercambiaban entre si. El inconveniente era que estos mensajes eran muy cortos para evitar que las posiciones de las emisoras de radio de los barcos fuesen detectadas y localizadas por métodos de triangulación.

A partir de febrero de 1942 los británicos captaron un nuevo tráfico de mensajes codificado que denominaron "shark" y que eran incapaces de descifrar (el tráfico de la M3 era llamado "dolphin"). La marina alemana había añadido un nuevo rotor a las Enigma, el modelo M4. Las aguas del Atlántico volvían a ser inseguras.

Figura 3. Bletchley Park. Cortesía Matt Crypto (Wikipedia Commons)

LA UNIÓN, A VECES, NO HACE LA FUERZA

Los americanos se habían introducido tarde en el desciframiento de Enigma. Apenas se habían preocupado y carecían de adiestramiento. Cuando Alemania declaró la guerra a los Estados Unidos en diciembre de 1941, los submarinos bordeaban su costa y hundían los barcos cerca de los puertos. Entonces reaccionaron.

Los británicos y los americanos necesitaban unir sus fuerzas y compartir sus conocimientos en el desciframiento de los complejos mensajes "shark". Los éxitos de Blentchley Park demostraban la ventaja de los británicos, pero carecían de los medios económicos para construir más *Bombe*. En cambio, los americanos tenían su industria a pleno rendimiento.

En abril de 1942, dos oficiales americanos visitaron Bletchley Park, conocieron las *Bombe* y se llevaron los planos para su construcción. Los americanos, ante el fracaso de los británicos, querían aportar nuevos cambios al diseño. También deseaban

1. Eran las denominadas "cribs". Por ejemplo, después de un ataque se captaban mensajes referentes a él. Las "crib" eran posibles palabras como el lugar, la hora, el nombre del oficial responsable, etc. A partir de aquí se especulaban soluciones al texto original.

Figura 4. Isla de Ellis. Cortesía de Library of Congress

los conocimientos que pudiesen tener de "Lorenz" (denominada "Tunny" por los británicos). Esta máquina estaba destinada a la transmisión de la información de alto nivel alemán, entre el propio Hitler y sus generales de campo. Los británicos estaban muy adelantados en su desciframiento, descubierto de una forma casual, porque aún no habían logrado capturar ninguna de estas máquinas. Los británicos solo iban a aportar lo que considerasen que los americanos debían saber sobre "Lorenz". No tenían plena confianza en que la información suministrada se mantuviese en un entorno seguro y que fuese aprovechada para los fines previstos. El ejército de tierra y la marina americana eran tan independientes, que a veces actuaban de forma descoordinada e incluso contradictoria, en cambio, los británicos necesitaban conocer los avances en criptografía americana y los cambios introducidos en las *Bombe*. La información indirecta no satisfacía a nadie, el recelo y la desconfianza era mutua. Se acrecentó cuando el alto mando de Washington no recibió la noticia de los británicos sobre la captura de una Enigma M4 de un submarino[2].

Dispuestos a normalizar las relaciones y facilitar la cooperación acordaron que sería una persona cualificada la que viajase a Estados Unidos para compartir conocimientos. Alan Turing fue la persona elegida para encontrarse con los técnicos y colegas matemáticos americanos. Visitaría la empresa National Cash Register Company, NCR, (en Dayton, Ohio) que albergaba U.S. Naval Computing Machine Laboratory donde se construían las Bombe para la marina americana. Quería comprobar las modificaciones funcionales y formas de uso. (una "NCR Bombe" se encuentra en el National Cryptologic Museum de la NSA). El acuerdo consistía en permitir que Turing pudiese aprender y comprender el método de encriptación vocal que se estaba empleando con éxito en las comunicaciones telefónicas entre Roosevelt y Churchill, y debía conocer el sistema SIGSALY (para conocer más sobre SIGSALY en la revista ANTENA n.º 184).

Figura 5. Main Navy Building. Washington D. C. 1953. Cortesía Naval History and Heritage Command.

2. Posiblemente fuese el submarino U-559 en el Mediterráneo

TURING EN "MAIN NAVY BUILDING"

La estancia de Turing en Estados Unidos fue bastante ajetreada debido a la descoordinación de los responsables de ambos países. Carecía de unas órdenes precisas de lo que debía o no contar a los americanos sobre el desciframiento de "Lorenz".

El 12 de noviembre de 1942 desembarcó en la isla de Ellis en Nueva York (Figura 4). El Mayor Geoffrey Stevens, Oficial de Enlace Técnico de los Servicios de Información de Señales, su guía, tuvo que intervenir con las autoridades de inmigración para permitir la entrada al país. Cinco días más tarde cruzaban las puertas del edificio del Departamento de Marina de Washington, posiblemente el "Main Navy" (Figura 5 y 6) donde se encontraban el Servicio Secreto de Información[3] o la Naval Security Station[4] donde se analizaban los mensajes japoneses.

En el informe que Turing redactó del 28 de noviembre sobre su visita acusa decepción sobre el trabajo que realizan los norteamericanos. Turing escribió en las últimas notas: "En general, su actitud es tan puramente mecánica y matemática que los árboles no dejan ver el bosque y no les gusta admitir que la experiencia y el conocimiento de los acontecimientos inmediatamente anteriores, combinado con un poco de trabajo manual, a menudo se puede producir la respuesta más rápidamente que las máquinas".

Los americanos tenían interés en que les explicase el método de desciframiento de la máquina "Lorenz". El día 25 fue requerido para responder sobre el tráfico "tunny" emitido con la "Lorenz" pero Turing no aportó nada reseñable.

TURING EN LOS LABORATORIOS DE BELL TELEPHONE

El 26 de noviembre, regresando a Nueva York, Turing y el Mayor Stevens

3. Derribado en 1970. Ocupó el solar del Constitution Gardens Park y el Vietnam Memorial
4. Actualmente "Naval Security Station", NAVSECSTA en Nebraska Ave. Washington D. C.

Figura 6. Main Navy Building, people and buses. Government employees pouring out of the Navy Department at 4:30 pm. Washington, DC, US. 1942. Myron Davis. Cortesía LIFE.

hicieron parada en Murray Hill, la nueva sede de los laboratorios Bell, inaugurada el año anterior (Figura 7). Turing debía reunirse con un tal Potter, (tal vez se refiera Ralph K. Potter ingeniero del proyecto SIGSALY), pero no fue posible debido a las restricciones de las visitas y la consecuencia inmediata fue la desautorización. No le permitieron acceder al proyecto SIGSALY completo pero si a determinadas maquetas (según se desprende del informe del 28 de noviembre de 1942).

TURING EN LOS LABORATORIOS DE LA NATIONAL CASH REGISTER

El día 27 de noviembre llegaba a la ciudad de Dayton para visitar la fábrica NCR (Figura 8) acompañado por el Mayor Stevens y varios militares. En el informe comenta las diferencias de funcionamiento introducidas por los americanos a sus modelos de *Bombe*. El informe del 21 de diciembre contiene discusiones de carácter técnico. Es completamente negativo, demostrando una falta de confianza en las mejoras de las *Bombe* americanas, como mayor velocidad o manejo de fragmentos "crib" más cortas. En el informe criticaba cada una de las partes y aconsejaba modificaciones. El informe se lo entregó a los militares pero no a los ingenieros de NCR que nunca lo conocieron; de este modo, los ingenieros continuaron la construcción de sus variantes.

TURING ENCUENTRA SIGSALY

Esta etapa supuso para Turing disfrutar del ambiente liberal de Nueva York. Recuperó el placer de asistir a reuniones sociales. Hacía años que estos eventos habían desaparecido de la vida en Gran Bretaña.

A primeros de año debió visitar durante un tiempo los laboratorios Bell. Le enseñaron el sistema SIGSALY. Aprendió los conceptos básicos de electrónica y cómo la voz, a través del muestreo y la cuantificación, se puede manipular numéricamente y cómo recuperar finalmente su forma original. En 1940, Claude W. Shannon se había incorporado a Bell para resolver problemas de conmutación de circuitos telefónicos y en 1941 pasó a trabajar en los departamentos de criptografía, ambos coincidieron allí. El tema de conversación que más ha trascendido fue sobre las ideas de computación de Turing y la posibilidad de construir un cerebro electrónico pensante.

REGRESO A HANSLOPE PARK

Turing se embarcó de regreso a Gran Bretaña en marzo de 1943. Entre sus lecturas para el viaje destacaron varios libros de electrónica y catálogos de válvulas. Turing había descubierto como los triodos son los elementos ideales para construir su "máquina universal", aquella vieja idea que concibió antes de la guerra.

El ambiente distendido de las metrópolis americanas y las recién tecnologías aprendidas nos traen a la castigada Europa un Turing rejuvenecido.

Cuando llega a Bletchley Park, la nueva máquina Colossus diseñada para enfrentarse al desciframiento de "Lorenz" está concluida y el equipo humano para su manejo adiestrado. La base funcional es la misma que en *Bombe*. Las válvulas electrónicas de Colossus son capaces de realizar las mismas funciones, pero más rápidamente que los conmutadores rotativos de *Bombe*. Turing no quiere incorporarse al grupo, está libre para dedicarse a otras actividades que no sean el desciframiento. Se traslada junto con el joven ingeniero electrónico Donald Bayley y el joven matemático Robin Gandy a trabajar a Hanslope Park, la sede de *Secret Intelligence Service*, popularmente conocido como MI6 [5].

LA SEDUCCIÓN DE DALILAH

Turing, por fin, puede construir "su máquina" que oculte mensajes, después de estar años desentrañando los escritos por una ajena. A comienzos de mayo de 1943 inicia los trabajos sobre el encriptador vocal denominado "Dalilah". El objetivo de Turing, al contrario que los americanos, consiste en reducir el tamaño del aparato, así lo reconoce en el informe del 6 de junio de 1944. Rechaza la utilización de varios equipos para diversas funciones y busca un sistema pequeño y compacto.

El prototipo construido por Bayley consiste en la unidad encriptadora (mezcla la voz con la clave), que a su vez, mediante

5. Actualmente "Her Majesty's Government Communications Centre", HMGCC

Figura 7. Vistas de los Laboratorios Bell en Murray Hill en 1942. Cortesía de Library of Congress

un interruptor, se transforma en la unidad desencriptadora. Parece que "Dalilah" era básicamente el circuito muestreador y el cuantificador. Según el informe anterior el programa para los próximos meses será investigar la unidad generadora de la clave, el acoplamiento para la transmisión por radio y la construcción de otro modelo similar para las pruebas reales.

Turing pensó algunas ideas sobre el tipo de clave. Una era la utilización de una "clave pública" que se transmitiese al receptor aleatorizada. Solución rechazada por ser técnicamente compleja. Otra consistía en el cambio dinámico de la clave durante la conversación.

Estas ocurrencias son fruto de su estancia en los laboratorios Bell porque allí, los ingenieros ya habían probado circuitos similares como hemos visto en "Voces secretas. Encriptación telefónica en los años 20" (Revista ANTENA n.º 179 y otros posteriores).

Figura 8. NCR Building. 1960 Cortesía Ohio Historical Society.

COMIENZA OTRA HISTORIA

Los americanos, ignorando los consejos de Turing, probaron los modelos de *Bombe* "Adán" y "Eva" en mayo de 1943. Se inició su fabricación en junio. Las salas de la Naval Security Station en Washington se llenaron de ellas. La eficacia fue tan alta, que en 1944 los británicos delegaron en los americanos la resolución de los mensajes de Enigma. Cuando los aliados desembarcaron en Normandía, los servicios secretos ya desencriptaban todos los mensajes alemanes.

Turing abandonó el proyecto "Dalilah" y retomó su idea de la máquina universal. Su biógrafo Andrew Hodges destaca tres experiencias importantes que le animaron a tomar esta decisión:

— El propio concepto de máquina universal creado en 1936.
— La velocidad y la fiabilidad de la tecnología electrónica.
— La posibilidad del diseño de una única máquina capaz de realizar las diversas funciones lógicas.

Había encontrado la manera práctica de llevar a cabo su idea de computadora universal y comentaba a sus compañeros en Hanslope la construcción de un "cerebro electrónico".

En 1945 los americanos anuncian la construcción del EDVAC *(Electronic Discrete Variable Automatic Computer)* en la Universidad de Pensilvania y los británicos reclutan a técnicos e ingenieros para el National Physical Laboratory,

NPL, con el objetivo de construir el ACE *(Automatic Computer Machine)*, entre ellos se encuentra Turing. A partir de este momento comienza otra historia.

CONCLUSIÓN

Todavía falta mucho por descubrir de lo acontecido durante la visita de Turing a Estados Unidos en 1942 y 1943, relacionar hechos, situaciones y personajes. Poco a poco de los archivos surgen a la luz documentos e informes porque dejan de ser "confidenciales". Las fuentes de esta recopilación apenas se han conocido hace diez años, y la historia, una vez más, se vuelve a reescribir.

REFERENCIAS

CASCIANI, Dominic "Wartime code-breakers failed to click". BBC News, 20 October 2004. http://news.bbc.co.uk/2/hi/uk_news/3758276.stm (consulta 31 enero 2011)

DAVIS, Martin. *La computadora universal: de Leibniz a Turing*. Ed. Debate. 2002 Barcelona.

Weierud, Frode. CryptoCellar. Cryotology and its history. Breaking German Wehrmacht Ciphers.

ERSKINE, Ralph. "Breaking Naval Enigma (Dolphin and Shark)
http://cryptocellar.web.cern.ch/cryptocellar/bgac/HMTR-2066-2.pdf (consulta febrero 2011)

HODGES, Andrew: "The Alan Turing Internet Scrapbook" 1998
http://www.turing.org.uk/turing/scrapbook/ukusa.html (consulta 1 febrero 2011)

HODGES, Andrew "Alan Turing: a short biography. Part 5, - Emergence of the Computer",1995, http://www.turing.org.uk/bio/part5.html (consulta 1 febrero 2011)

LEAVITT, David. *Alan Turing: un hombre que sabía demasiado*. Antoni Bosch Editor, S. A. 2008. Barcelona.

PROC, Jerry, Crypto Machines, BOMBE (NCR). (2008)
http://www.jproc.ca/crypto/bombe_us.html (consulta enero 2011)

REAL Martín, Luis Fernando. "Voces secretas. Encriptación telefónica en los años 20". *Antena* nº 179. Abril 2010. Edita COITT.

"Voces secretas. "SIGSALY, sistema encriptador de la Segunda Guerra Mundial". *Antena* nº 184. Diciembre 2011. Edita COITT.

TURING, A. "Report on cryotographic machinery available at Navy Department Washington", 28 noviembre 1942. (transcript)
Alan Turing Home Page del biógrafo Andrew Hodges:
http://www.turing.org.uk/sources/washington.html (consulta enero 2011)

TURING, A. "Visit to Nacional Cash Register Corporation of Dayton, Ohio" 21 diciembre 1942.
Se puede encontrar el mismo documento en varias localizaciones y formatos:
Hodges, Andrew. Alan Turing Home Page :
http://www.turing.org.uk/sources/dayton123.html (consulta enero 2011)

Weierud, Frode. CryptoCellar. Cryotology and its history. Con el título "Turing's report on his visit to NCR" está editado, trascrito y comentado por Ralph Erskine, Philip Marks y Frode Weierud. Septiembre 2000.
http://cryptocellar.web.cern.ch/cryptocellar/USBombe/turncr.pdf (trasnscript and coment) (consulta enero 2011)

Documento digitalizados del Turing Digital Archive de King's College Cambridge: http://www.turingarchive.org/browse.php/C/31 (consulta enero 2011)

Copeland, Jack & Proudfoot, Diane. Documentos digitalizados en Alan Turing.net. The Turing Archive of the History of Computing. Catalogue of Documents on World War Two Codebreaking.
http://www.alanturing.net/turing_archive/archive/b/B013/B13-001.html (consulta enero 2011)

TURING, A: "speech system "Delilah", Report on progress" June 1944 (transcript)
Alan Turing Home Page del biógrafo Andrew Hodges:
http://www.turing.org.uk/sources/delilah.html (consulta 1 febrero 2011)

HELGASON, Gudmundur, http://uboat.net

Erskine, Ralph, "Allied breaking of naval Enigma"
http://uboat.net/technical/enigma_breaking.htm (consulta enero 2011)

DeBROSSE, Jim. "Dayton's Code Breakers"
Reportajes en el periódico Dayton Daily News, del 25 febrero hasta el 3 mayo 2001
http://www.daytondailynews.com/project/content/project/enigma/enigma_index.html
http://www.jproc.ca/crypto/dayton_cb.html
También con la entrada.
"Dayton's WWII Enigma Codebreakers"
http://www.daytondailynews.com/n/content/oh/index/news/special-reports/enigma/index.html

"Solving the Enigma: History of the Cryptanalytic Bombe". Center for Cryptologic History, National Security Agency.
Versión on-line en:
http://ed-thelen.org/comp-hist/NSA-Enigma.html

THELEN, Edward: http://ed-thelen.org ; Computer-History