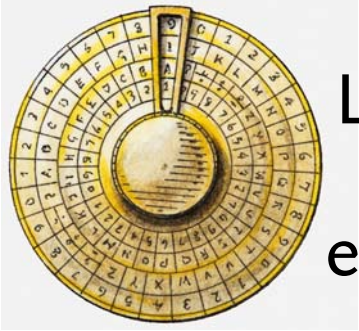


La criptología y la victoria aliada en la Segunda Guerra Mundial

Guillermo Morales-Luna

Durante la guerra las fuerzas armadas hitlerianas basaban sus comunicaciones secretas en la máquina cifradora Enigma. Este esquema fue quebrantado inicialmente por criptólogos polacos y, luego, en Inglaterra, el proyecto llamado Ultra quebrantó sus variaciones. Alan Turing fue el líder del grupo de criptólogos en Ultra y desarrolló procedimientos para romper los cifrados alemanes. Su contribución al triunfo aliado ciertamente fue invaluable.

Introducción

Alan Turing tuvo un papel muy importante durante la Segunda Guerra Mundial. Dirigió uno de los grupos de criptólogos encargados de romper los códigos secretos alemanes (Copeland, 2004; Leavitt, 2006). Los alemanes basaban sus comunicaciones secretas en la máquina Enigma, inventada a mediados de la década de 1920. Criptólogos polacos pudieron quebrantar las primeras versiones de Enigma, y sus trabajos sirvieron de base para los desarrollos criptológicos ingleses.

Enigma y la criptología polaca

Con el Tratado de Versalles se reconoce la restitución de Polonia. El gobierno de la República de Polonia establece un *Biuro Szyfrów* para interceptar las comunicaciones de la URSS y Alemania. Fue la primera vez que un centro criptológico incorporó a matemáticos: Stefan Mazurkiewicz, Wacław Sierpiński y Stanisław Leśniewski, entre otros.

En 1926 los polacos descubrieron que se estaba utilizando un procedimiento mecánico para cifrar las comunicaciones alemanas. Hugo A. Koch, holandés, y Arthur Scherbius, alemán, fueron los inventores de Enigma, alrededor de 1923, con el propósito de cifrar comunicaciones industriales y bancarias. La máquina no


02
01
26
15
14
13
12
11
24
23
22
21

atrajo la atención de los medios comerciales y la fábrica establecida por Scherbius fue liquidada. Pero los militares alemanes recuperaron ese invento, desde 1925, y fue utilizado hasta 1945.

Enigma se basaba en permutaciones de orden dos, llamadas "involuciones", sobre un alfabeto de 26 caracteres. Al ser las involuciones iguales a sus propias inversas, los procesos de cifrado y descifrado coincidían (Figura 1). Dos partes comunicantes debían ponerse de acuerdo en una misma configuración de sus máquinas: la configuración era, pues, la *clave de cifrado* (Gaj y Orlowski, 2003; Christensen, 2007; Miller, 1995; Copeland, 2004).

A fines de los años veinte del siglo pasado, la criptología en Polonia se desarrollaba bajo el mando del profesor Zdzisław Krygowski, anteriormente rector de la Politécnica de Lwów, junto con tres exalumnos suyos: Marian Rejewski, Henryk Zygalski y Jerzy Różycki, quienes en la década de 1930 descifraron el código de Enigma (Figura 2).

Rejewski hizo dos observaciones importantes: con el álgebra de permutaciones descubrió que toda involución producida por Enigma era el producto de 13 transposiciones (con símbolos ajenos a pares). Y luego encontró que la permutación del tambor inicial de la Enigma militar había sido cambiada respecto a las versiones originales, y pudo precisarla en 1932. En Polonia incluso se mecanizó el procedimiento de Rejewski. A unos *ciclómetros*, consistentes en rotores de Enigma, se aplicaban varios preámbulos de textos cifrados y así producían sus claves del día.

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. Se les llamó "bombas" debido al ruido que hacían; la primera se fabricó en noviembre de 1938 e incorporaba seis réplicas de Enigma. Zygalski inventó un sistema de "placas perforadas" para los ciclómetros. Hasta 1939, en Polonia eran capaces de descifrar las comunicaciones alemanas, pero se carecía de aptitudes para oponerse a la *blitzkrieg* ("guerra relámpago", táctica militar alemana). Para entonces, las Enigma alemanas habían sido dotadas de más rotores, lo que hacía inútiles las réplicas polacas, hecho que fue detectado por los polacos desde diciembre de 1938. La criptología polaca era formidable en el plano intelectual, pero estaba sujeta a limitaciones materiales (Rejewski, 1981).

En julio de 1939, en Syry, Polonia, el director del *Biuro Szyfrów* polaco, Gwido Karol Langer, y otros ofi-

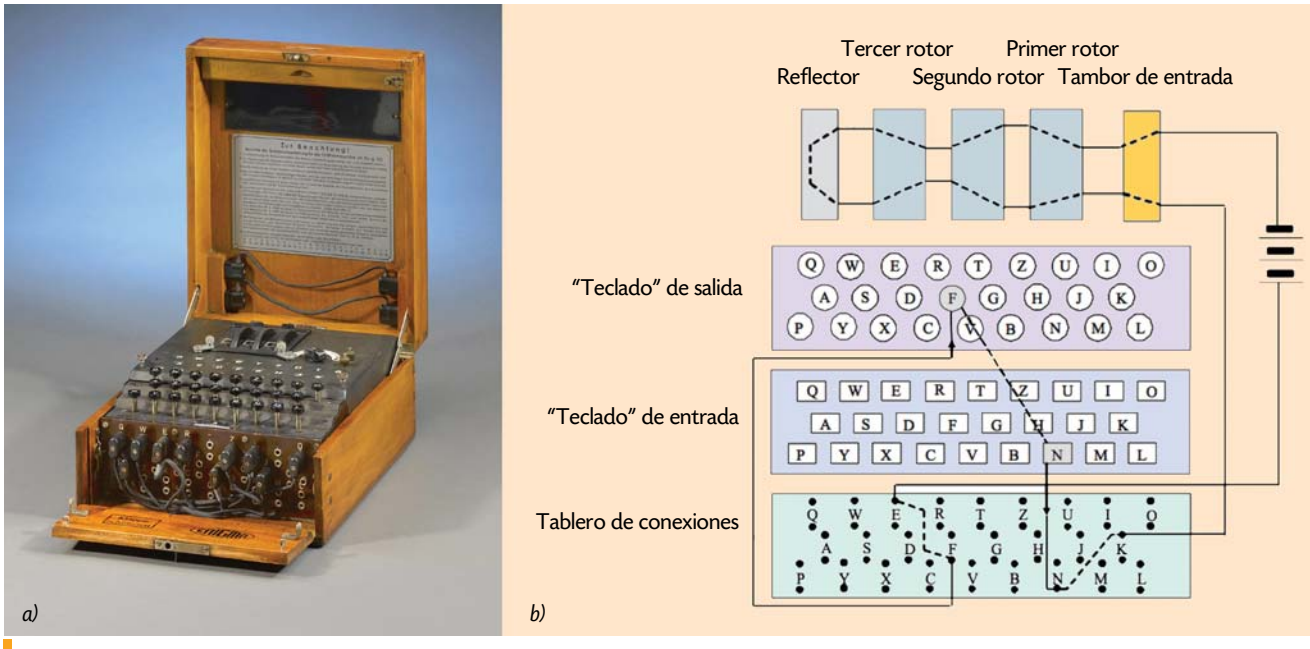


Figura 1. Máquina de cifrado Enigma de tres rotores. *a)* Fotografía de una máquina Enigma. *b)* Diagrama que muestra las partes principales. Se ilustra el proceso al oprimir N para obtener el cifrado F.

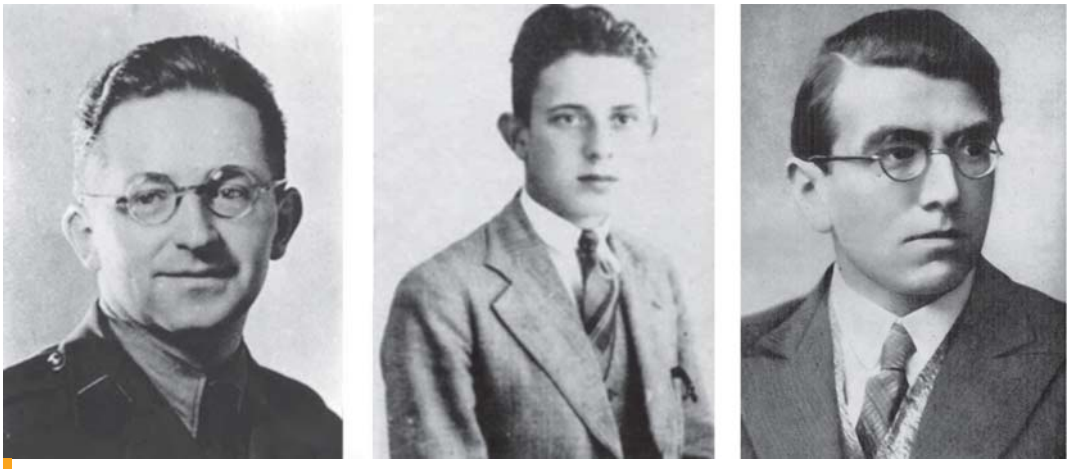


Figura 2. Marian Rejewski, Henryk Zygalski y Jerzy Różycki.

ciales, se reunieron con criptólogos franceses e ingleses. Dillwyn Knox participó por la parte inglesa y Gustave Bertrand por la francesa. Les entregaron réplicas polacas de la Enigma militar y los procedimientos para quebrantar su esquema. Ésta 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 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, al este de París, y continuaron sus actividades, cooperando con antiguos combatientes españoles republicanos.

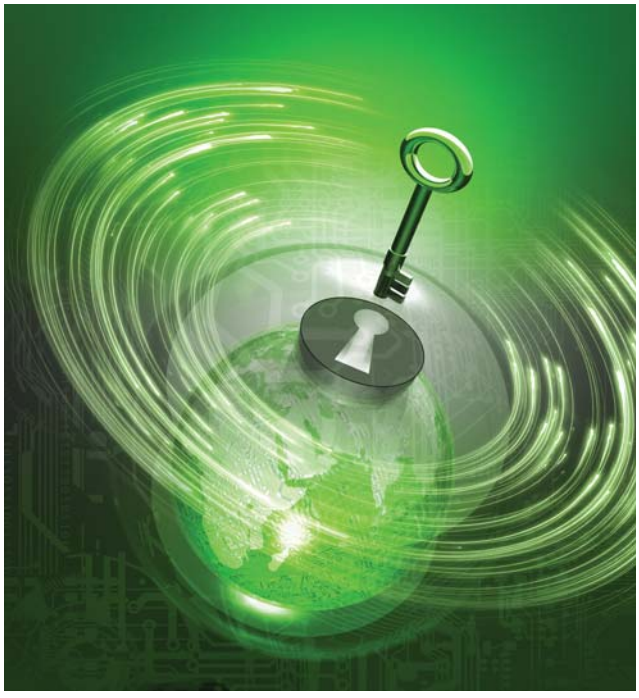
En enero de 1940 el gobierno inglés solicitó que los criptólogos polacos fueran llevados a Bletchley Park, pero el gobierno francés se opuso; sin embargo, se acordó que Alan Turing visitara Vignolles. El 17 de enero los polacos logran recuperar las primeras claves del día de la Enigma de cuatro rotores. En mayo de 1940, los alemanes cambiaron los procedimientos de transmisión de las claves, e invadieron Francia. El 21 de mayo Turing, en Bletchley Park, logró recuperar las nuevas claves y quebrantar las comunicaciones entre la *Luftwaffe* (fuerza aérea de la Alemania nazi) y el ejército de tierra.

En junio de 1940, con el territorio francés dividido, el gobierno de Vichy desmantela al ejército francés y el gobierno polaco, en el exilio, facilita que los criptólogos polacos sean transportados a Argelia. En octubre de 1940 fueron llevados de nuevo a Francia, al castillo de Fouzes. Ahí estuvieron en una situación ambigua: por un lado, para el gobierno de Vichy debían intervenir las comunicaciones alemanas con el fin de verificar que las condiciones del armisticio se cumplieran; por otro lado, transmitían al gobierno polaco en el exilio y a Bletchley Park las comunicaciones interceptadas, entre otras las de la Gestapo.

Parte del grupo de criptólogos polacos se mantuvo en Argel (la capital de Argelia), entre ellos Różycki, para interceptar las comunicaciones del ejército alemán en el norte de África. El 9 de enero de 1942 Różycki muere en un naufragio, cuando regresaba a Francia con otros oficiales polacos. En septiembre de 1942 los alemanes detectan al grupo de criptología en Fouzes. Prevenidos por Bletchley Park, se ordena evacuar al grupo polaco. En la evacuación se da prioridad a los oficiales franceses y se deja a los polacos a su suerte. Algunos lograron llegar a España, tras pagar a guías estafadores, y luego fueron llevados a Inglaterra por la Cruz Roja.

Rejewski y Zygalski llegaron a España, y fueron detenidos por la Guardia Civil en Lérida. Mediante la intervención de la embajada británica, fueron llevados a Inglaterra. Otros, como Antoni Palluth –constructor de las réplicas polacas de Enigma– y Gwido Karol Langer fueron aprehendidos por los alemanes en la frontera con España. Pero a pesar de las torturas de la Gestapo, no develaron la naturaleza de sus actividades.

Palluth murió en el bombardeo del 10 de abril de 1944 al campo de concentración en Sachsen Hausen-



Oranienburg, donde era prisionero. Otros oficiales polacos fueron liberados en mayo de 1945 por tropas yanquis. Sobre ellos pesó la sospecha de que el fracaso de su evacuación se había debido a una filtración de ellos mismos, lo que era absurdo, pues el secreto de Enigma se mantuvo.

En Inglaterra, Rejewski y Zygalski trabajaron para el gobierno polaco en el exilio. Zygalski se estableció ahí, dando clases en la Universidad de Surrey, en Londres. Murió en 1978. Rejewski regresó a Polonia en noviembre de 1946. En la República Popular no le fue posible emplearse como matemático en centros de educación superior (la gente ligada con el gobierno en el exilio era considerada poco confiable por el régimen), y no quiso involucrarse en la seguridad del Estado, así que trabajó como modestísimo administrador de una empresa estatal en Bydgoszcz, jubilándose en febrero de 1967. Murió en 1980.

Turing y Bletchley Park

Bletchley Park, al noroeste de Londres, se situaba en una conjunción de carreteras, vías férreas y telegráficas, por lo que en agosto de 1938 el gobierno británico estableció ahí la "Estación X". A finales de la década de 1930, el gobierno británico adquirió propiedades para sus organismos militares y de seguridad; la Estación X fue la décima. Tenía como misión quebrantar comunicaciones secretas enemigas. Desde agosto de 1939 llegaron criptólogos, conformando la que fue llamada, en clave, *Tropa de Cacería del Capitán Ridley*. La Estación X constaba de varias barracas: la 8, dirigida desde sus inicios por Turing, se encargaba del desciframiento de la Enigma naval; la 6, de la Enigma de aire y tierra; y la 4 realizaba las traducciones y el análisis de inteligencia de los mensajes recuperados por la 8 (Copeland y colaboradores, 2006).

En 1938 Turing visitó Princeton, lugar donde le ofrecieron una plaza. No la aceptó y regresó a Cambridge. En 1939 aparentaba hacer gestiones para recibir a un refugiado judío alemán, cuando en realidad trabajaba en la barraca 8 de la Estación X. El 3 de septiembre Inglaterra le declara la guerra a Alemania, y desde entonces Turing se dedica sólo a Bletchley Park.

Al recibir una de las Enigma polacas, en 1939, los ingleses descubren que pequeñas variaciones de sus propias máquinas *TypeX* habrían sido suficientes para quebrantar el código de Enigma. En mayo de 1940 una modificación a Enigma hace indescifrables las comunicaciones alemanas. El equipo de Turing logra quebrantar el nuevo esquema, aprovechando las debilidades debidas a formulismos lingüísticos alemanes. Este quebrantamiento fue especialmente importante, por lo tocante a la *Luftwaffe*.

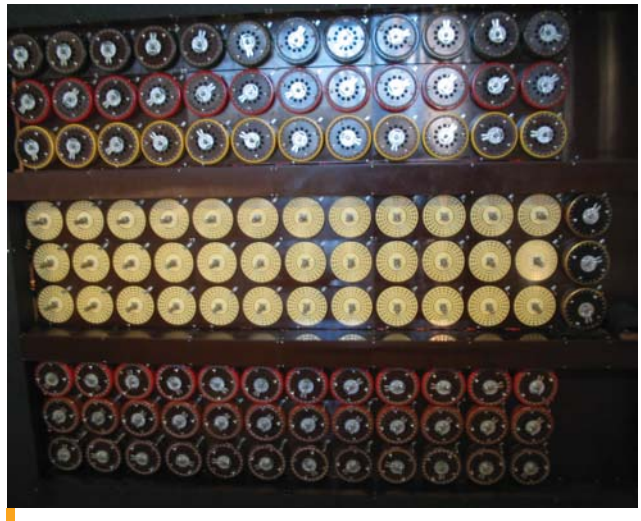


Figura 3. Reproducción de la "bomba" de Turing.

En octubre de 1940 entra en funcionamiento la primera bomba criptológica inglesa, llamada Ultra o "bomba de Turing" (Figura 3). Se valora el "proyecto Ultra" como el de mayor secreto en la Segunda Guerra, sólo detrás del proyecto Manhattan de la bomba atómica. En octubre de 1941 Turing, Hugh Alexander, Stuart Milner-Barry y Gordon Welchman habían escrito a Winston Churchill informándole que algunos recortes presupuestarios restringían la fabricación de bombas criptológicas. Tan pronto recibió la carta, Churchill ordenó otorgarles todas las facilidades requeridas, pues siempre consideró a Bletchley Park como "su arma secreta".

Ahí se criptoanalizaban esquemas, a los que se hacía referencia con nombres de peces. El principal, el "pez", era el esquema *Geheimschreiber*, y los demás eran derivaciones. "Tiburón" era una variación de la Enigma con cuatro rotores utilizada desde febrero de 1942. El Enigma de la Fuerza Naval era el "delfín", y se utilizaba para comunicaciones con los "botes-U", submarinos alemanes en el Atlántico Norte. En junio de 1941 Turing pudo quebrantar el delfín, al lograr descifrar reportes meteorológicos alemanes cifrados con él. Al conocer la ubicación de los botes-U, los barcos aliados podían desviarse y evitarlos, lo que era una maniobra de tipo defensivo. Pero desde 1943 esos métodos fueron utilizados de manera ofensiva por submarinos yanquis para combatir a los botes-U.

Cada vez que se desarrollaba un procedimiento criptológico se le ponía un nombre especial, casi cómico. Así, el inventado por Turing para quebrantar al delfín

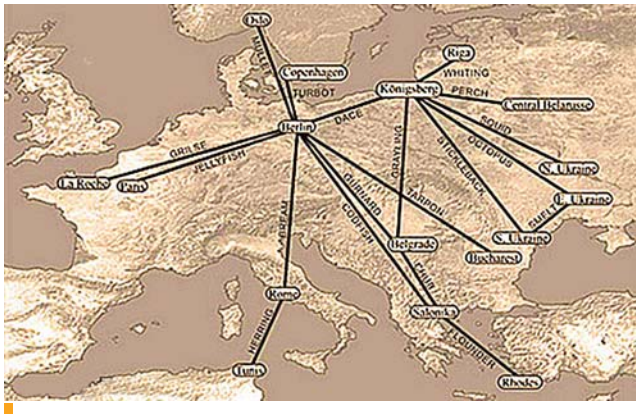


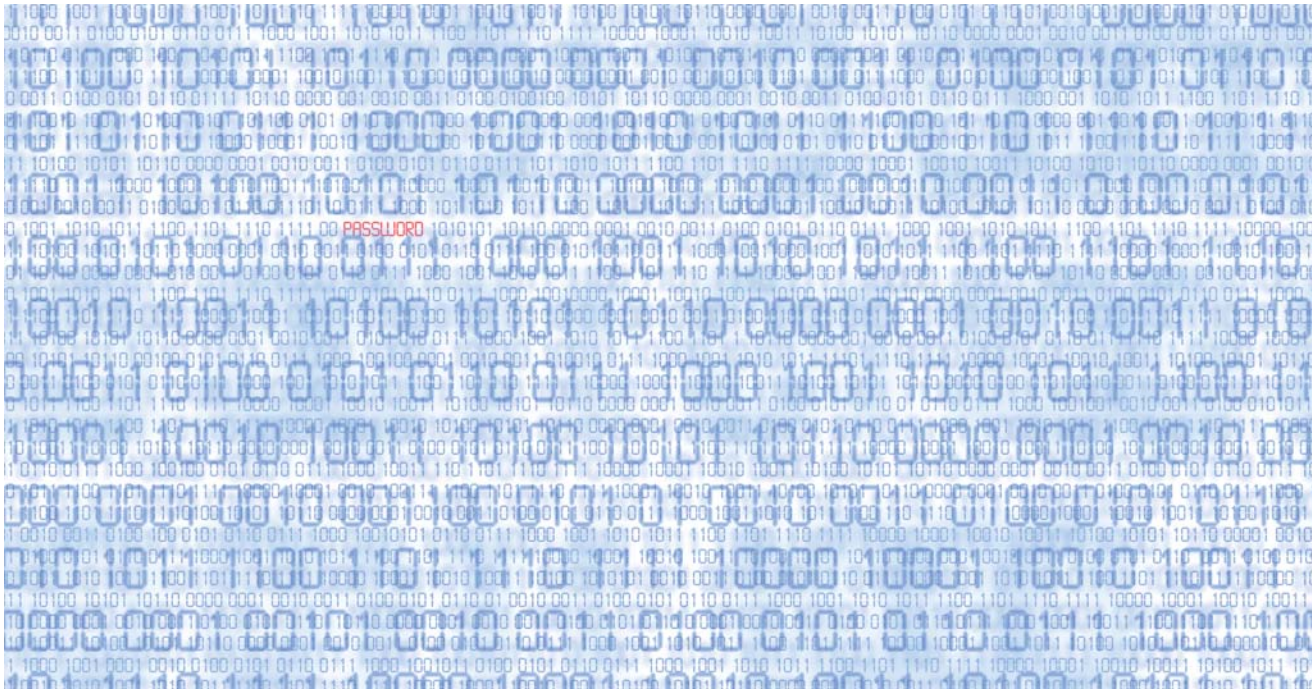
Figura 4. Líneas de comunicación cifrada alemana con los nombres puestos por criptólogos ingleses.

era llamado *Banburismus*, pues requería de tomar apuntes en tiras de papel producido en Banbury. Un método propuesto por Dillwin Knox se llamaba *Dillysimus*, y el *Yoxallismus* era debido a Leslie Yoxall, y fue utilizado para recuperar claves Enigma utilizadas por oficiales superiores de la Fuerza Naval (Figura 4).

En Bletchley Park se reclutó a muchos matemáticos muy talentosos. Joan Clarke, matemática, mujer criptoanalista a quien Turing le propuso matrimonio, aunque pronto se desdijo, recuerda que cuando fue reclutada se le advirtió que para "el trabajo a realizar no se requiere realmente de las matemáticas, pero los matemáticos son muy buenos en ello".

El "atún" era el esquema *Schlüsselzusatz SZ40*, quebrantado por Bill Tutte (especialista en teoría de gráficas) y por Peter Hilton (especialista en topología homológica). El quebrantamiento se basa en un método llamado *Turingismus* o *Turingery*, inventado por Turing en 1942 (Hilton, 2005; Crossley, 1975).

En febrero de 1942 los alemanes comenzaron a utilizar el "tiburón", y Bletchley Park quedó "sordo" durante casi diez meses. En octubre, un destructor británico recuperó de un submarino alemán las claves íntegras utilizadas en meses previos; así pudo quebrantarse el "tiburón", lo que permitió conocer la ubica-



ción de los botes-U hasta febrero de 1943. El 10 de marzo los alemanes cambiaron su sistema de cifrado, pero pudo quebrantarse en diez días. Las bombas criptológicas adaptadas al "tiburón" comenzaron a funcionar entre junio y agosto de 1943, lo que permitía romper claves en un día. En noviembre de 1943, al contar con bombas yanquis, esa labor se transfirió a Washington, D. C.

En 1944 se construyeron las primeras computadoras, las *Colossus*, en la "Newmanry", sección de Bletchley Park a cargo de Max Newmann (especialista en topología). Su constructor, Tommy Flowers, nunca pudo presentarse como quien produjo las primeras computadoras en el mundo. La "medusa" era utilizada por los altos mandos alemanes en transmisiones por teletipo, y fue quebrantada con computadoras Colossus. Sin embargo, mucho del trabajo mecánico en la "Newmanry" debía ser completado manualmente en la "Testery", sección a cargo del mayor Ralph Tester.

Son interesantes las relaciones de Bletchley Park con sus colegas estadounidenses. En noviembre de 1942, Turing visitó el Departamento de Defensa y el de la Armada en Washington. Hubo de sufrir varias complicaciones burocráticas al cruzar la frontera en la Isla Ellis de Nueva York, debido a que llevaba pasaporte oficial, mas no cartas que indicaran el propósito de su visita. En su reporte confidencial del 28 de noviembre, Turing menciona la insistencia estadounidense por conversar sobre el "atún" y la "medusa", y pide instrucciones al respecto, pues él prefería hablar sobre temas de probabilidad. Ahí plantea: "Estoy convencido de que no puede confiarse mucho en estas personas cuando se trata de decisiones sobre criptografía." Sin embargo, en su visita de 1942 Turing asesoró sobre bombas criptológicas. En abril de 1943 se inició la producción de bombas criptológicas en los Estados Unidos, y para finales de ese año 77 de ellas fueron instaladas en Washington.

Al término de la guerra, en 1945, se le concedió a Turing la Orden del Imperio Británico (que años después le sería conferida también a los *Beatles*, en 1965, y a Mick Jagger, en 2002). En el reconocimiento se dice que se le otorga por servicios "sin especificar". Todo el equipo de la Estación X fue desmantelado. Hubo matemáticos participantes que, luego de su trabajo, sólo obtuvieron becas universitarias. Max Newmann fue a la Universidad de Manchester a dirigir el Departamento de Matemáticas, e invitó a Turing para que continuara ahí sus trabajos.

Alan Turing era homosexual, pero esto no era evidente en Bletchley Park. Acaso la única en saberlo fue Joan Clarke, pues Turing le confesó que por eso no podía sostener su propuesta matrimonial. Uno de los principales personajes ahí, Jack Good (especialista en estadística) afirmó: "¡Qué bueno que las autoridades de Bletchley Park ignoraban que Turing era homosexual! Si lo hubieran sabido, habríamos perdido la guerra." Pero, ciertamente, aunque Turing era el más genial de las personalidades en ese sitio, Bletchley Park no era "la estepa de un lobo solitario", sino el fruto colectivo de muchos talentosos matemáticos.

Guillermo Morales-Luna es investigador en el Departamento de Computación del Centro de Investigación y Estudios Avanzados (Cinvestav) del Instituto Politécnico Nacional (IPN), licenciado en Física y Matemáticas por la Escuela Superior de Física y Matemáticas (ESFM) del IPN, maestro en Ciencias con especialidad en Matemáticas por el Cinvestav-IPN, y doctor en Ciencias Matemáticas por el Instituto de Matemáticas de la Academia Polaca de Ciencias, en Varsovia, Polonia. Sus áreas de interés son los fundamentos matemáticos de la computación, la lógica, la criptografía y la teoría de la complejidad. Ha sido profesor en el IPN y en la Benemérita Universidad Autónoma de Puebla (BUAP). Ha realizado dos estancias sabáticas en el Instituto Mexicano del Petróleo. Es mexicano por nacimiento y le fue concedida la ciudadanía polaca.
gmorales@cinvestav.mx

Lecturas recomendadas

Christensen, Chris (2007), "Polish mathematicians finding patterns in Enigma messages", *Mathematics magazine*, 80(4):247-273.

Copeland, B. Jack (2004), *The essential Turing: seminal writings in computing, logic, philosophy, artificial intelligence, and artificial life plus the secrets of enigma*, Oxford, Oxford University Press.

Copeland, B. Jack y colaboradores (2006), *Colossus: the secrets of Bletchley Park's code-breaking computers*, Oxford, Oxford University Press.

Crossley, J. N. (1975), "Reminiscences of logicians", *Algebra and logic: papers from the 1974 Summer Research Institute of the Australian Mathematical Society*, pp. 1-62, *Lecture notes in math*, vol. 450, Berlín, Springer.

Gaj, Kris y Arkadiusz Orlowski (2003), "Facts and myths of Enigma: breaking stereotypes", en EliBiham, editor, *Eurocrypt*, *Lecture notes in computer science*, vol. 2656, Berlín, Springer.

Hilton, Peter (2005), "Working with Alan Turing", *The mathematical intelligencer*, 13:22-25.

Leavitt, D. (2006), *The man who knew too much: Alan Turing and the invention of the computer*, Great Discoveries, W. W. Norton.

Miller, A. Ray (1995), "The cryptographic mathematics of Enigma", *Cryptologia*, 19(1):65-80.

Rejewski, Marian (1981), "How Polish mathematicians broke the Enigma cipher", *IEEE Ann. Hist. Comput.*, 3(3):213-234.