El héroe Alan Turing: Aportaciones de la Criptología a la victoria aliada en la Segunda Guerra Mundial

Guillermo Morales-Luna
Departamento de Computación
Centro de Investigación y de Estudios Avanzados del IPN, Cinvestav-IPN
gmorales@cs.cinvestav.mx

7 de mayo de 2013

Resumen

En la segunda mitad de la década de los 30, funcionaba en Inglaterra una modesta oficina gubernamental: la *Government Code and Cypher School (GC & CS)* que en 1937 descifraba, entre otros documentos, la correspondencia de unidades militares italianas participantes en la Guerra Civil Española. En 1939 la GC & CS se estableció en Bletchley Park y el 4 de septiembre, Alan Turing se incorporó a ella para dirigir la Barraca 8. Turing desarrolló un importantísimo trabajo en la primera mitad de la década de los 40 descifrando las comunicaciones secretas alemanas. Winston Churchill consideraba a Bletchley Park como su *arma secreta* y en alguna parte en sus memorias escribió que "nunca antes se había peleado una guerra en la que una parte estaba al tanto de los movimientos a realizar por sus contrincantes". Sin duda, el quebrantamiento de Turing de las comunicaciones cifradas alemanas aminoró los efectos que los ataques alemanes habrían podido ocasionar en el Reino Unido, y propició el triunfo inglés en la Batalla del Atlántico. Fue tan importante el trabajo realizado en Bletchley Park que se ordenó el desmantelamiento total de ese centro criptológico al final de la guerra.

Los cifrados alemanes se realizaban con la máquina Enigma, cuyas primeras versiones fueron quebrantadas por geniales criptólogos polacos, inventores de las primeras *bombas criptológicas*, quienes transmitieron luego su experiencia a los ingleses. La *Bomba de Turing* fue esencial para descifrar modificaciones más sofisticadas de Enigma.

Presentamos una breve reseña histórica del desarrollo criptológico polaco en los años 20 y 30 y posteriormente del desarrollo, dirigido por Turing al frente de un distinguido grupo de matemáticos, en Bletchley Park hasta 1945. Hacemos una breve descripción del mecanismo de cifrado de Enigma y de los métodos empleados para quebrantarlo.

1 Introducción

Alan Mathison Turing nació en 1912, por lo que recientemente se ha conmemorado en todo el Mundo el Centenario de su Nacimiento. Turing fue el inventor del concepto moderno de "computadora" y sus trabajos en Matemáticas y en Lógica lo colocan como uno de los grandes pensadores del S. XX. Biografías extensas de Turing aparecen en los libros [2] y [7].

Pero también Turing jugó un papel my importante durante la Segunda Guerra Mundial. Dirigió uno de los grupos de criptólogos encargados de romper los códigos secretos alemanes. Turing colaboró efectivamente en la victoria de los Países Aliados sobre las Potencias del Eje. Los alemanes basaban sus comunicaciones secretas en la máquina Enigma, inventada a mediados de los años 20. Los criptólogos polacos pudieron quebrantar las primeras versiones de Enigma y sus trabajos sirvieron de base para desarrollos criptológicos ingleses, entre ellos las llamadas *bombas de Turing*, que constituyeron una fuerte defensa de la Gran Bretaña contra ataques alemanes y que incluso sirvieron a las fuerzas aliadas en ataques contra la Marina Alemana.

Presentamos una historia suscinta del desarrollo de la Criptología Polaca y sus ataques a Enigma. Luego, presentamos una historia muy resumida de Bletchley Park, centro de Criptología donde sirvió y destacó Alan Turing.

2 Enigma

Con el Tratado de Versalles de 1919 se reconoce en Europa la restitución de Polonia. Por su posición geográfica entre la U.R.S.S. y Alemania, el Gobierno de la República de Polonia establece una oficina de cifrado, *Biuro Szyfrów*, con el fin de interceptar las comunicaciones, de radio principalmente (los mensajes cifrados eran comunicados en el código Morse), de los gobiernos de esos países. Sin grandes dificultades, los criptólogos polacos de esa época pudieron descifrar los esquemas criptográficos utilizados. Uno de los principales criptólogos de los años 20 en esa oficina fue el lugarteniente Jan Kowalewski, matemático y lingüista, quien en 1921 fue condecorado luego de la guerra con la URSS y posteriormente fue asesor del Imperio Japonés para criptografía. Entre los matemáticos que entonces participaron en el *Biuro Szyfrów* estaban Stefan Mazurkiewicz, Wacław Sierpiński y Stanisław Leśniewski [11].

En 1926, los polacos notaron un cambio en los métodos usados y llegaron a la conclusión de que se estaba utilizando un procedimiento mecánico para cifrar las comunicaciones alemanas. Era imperativo para la seguridad polaca quebrantar ese método de cifrado.

Hugo Alexander Koch, holandés, y Arthur Scherbius, alemán, fueron los inventores de la máquina *Enigma*, alrededor de 1923, con el propósito inicial de cifrar, con propósito comercial, las comunicaciones industriales y bancarias. La máquina cifradora llamó poco la atención de esos medios y la fábrica establecida por Scherbius fue liquidada. Sin embargo, los militares alemanes recuperaron ese invento, desde 1925, y fue utilizado hasta 1945 por el ejército de tierra, la marina y la aviación. En los 20 y los 30 hubo en el Mundo varias máquinas cifradoras. En los Estados Unidos de Norteamérica se utilizaba la máquina *SIGABA*, inventada por William Friedman, y en la Gran Bretaña, *TypeX*. De hecho, hasta la década de los 70 se seguía utilizando máquinas cifradoras, de rotores.

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. Así que cuando un texto en claro se aplicaba a una máquina, ésta producía un correspondiente texto cifrado, y cuando el texto cifrado se aplicaba a la misma máquina, ésta producía el correspondiente texto en claro. Por lo cual, dos partes comunicantes debían ponerse de acuerdo en una misma configuración de sus propias máquinas Enigma para poder comunicarse. La configuración era pues la *clave de cifrado*.

Descripciones completas del funcionamiento de Enigma aparecen en [5], en [1], en [8] y en los capítulos 5–6 de [2]. En la figura 1 presentamos una fotografía de una máquina Enigma y un diagrama de sus principales componentes. En lo que sigue, haremos solamente un ejercicio de conteo para ilustrar que el espacio de posibles claves es muy, pero muy, grande.

El alfabeto que utilizaban las máquinas Enigma consistía de las 26 letras del alfabeto latino, no incluían ni los dígitos ni los signos de puntuación. Las primeras máquinas Enigma utilizaban un tambor de entrada, tres rotores, un "reflector" y un "tablero de conexiones". El "teclado" de salida era una colección de bulbos que se iban iluminando consecutivamente para mostrar el texto cifrado correspondiente al texto en claro introducido mediante el teclado de entrada.

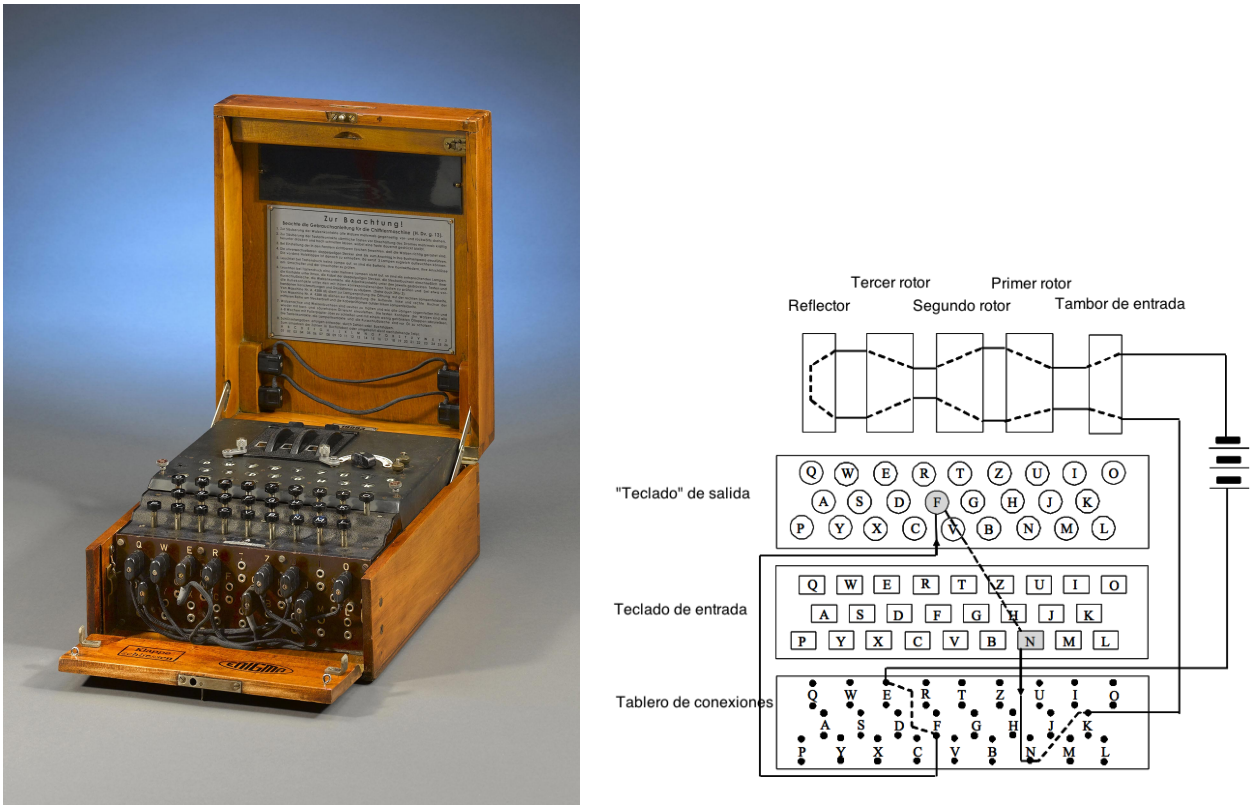
El tablero de conexiones consistía de 26 empalmes, correspondientes a las letras, los cuales se conectaban a pares por un cierto número de cables, que podía ser entre 0 y 13 inclusive. El número de posibilidades para el tablero de conexiones era pues

$$n_1 = \sum_{i=0}^{13} \binom{26}{2i} \prod_{j=1}^{i-1} (2j+1) = \sum_{i=0}^{13} \frac{26!}{(26-2i)!i!2^i} = 532\,985\,208\,200\,576.$$

El reflector trabajaba como el tablero de conexiones con exactamente 13 pares de conexiones, por lo que el número de posibilidades era $n_2 = \frac{26!}{13!2^{13}} = 7\,905\,853\,580\,625$.

Los rotores podían ser colocados, cada uno, en una de 26 posibles maneras iniciales, por lo que el conjunto de los tres rotores daba $n_3 = 26^3 = 17\,576$ posiciones iniciales. En cada rotor se colocaba un disco de 26 dientes, por lo que se tenía hasta $n_4 = 26!$ posibles discos, mas como los discos debían ser distintos, para evitar ataques "de frecuencias" a los textos cifrados, se tenía hasta $n_4(n_4-1)(n_4-2)$ posibilidades para configurar los tres rotores.

Finalmente, si se usara una permutación fija, entonces el sistema de cifrado sería susceptible de ser atacado mediante frecuencias: los caracteres que más aparecieran en el texto cifrado corresponderían a los que aparezcan más en el idioma del texto en claro. Para evitar esto, los rotores iban girando, a manera de



(a) (b)

Figura 1: Máquina de cifrado Enigma de tres rotores. (a) Fotografía de una máquina Enigma. (b) Diagrama mostrando las partes principales. Se ilustra oprimiendo N para obtener el cifrado F.

un tacómetro, al cifrar letra a letra. El giro de los rotores se hacía mediante anillos que descubrían tan solo uno de los caracteres en los rotores. La ingeniería de Enigma hacía que al fijar la disposición de los primeros dos anillos, la del tercero quedaba determinada. Así pues, se tenía $n_5 = 26^2 = 676$ posibilidades iniciales.

En consecuencia, el número de posibles claves para las máquinas Enigma de tres rotores era

$$n_1\, n_2\, n_3\, n_4 (n_4 - 1)(n_4 - 2)\, n_5$$

que es un número gigantesco, del orden de 10^{114} (se estima, por ejemplo, que el número de átomos en el Universo es "apenas" del orden de 10^{80}).

El Ejército Alemán utilizaba exactamente 6 pares en el tablero de conexiones, con un reflector fijo, y tres discos determinados para los rotores, por lo que el número de claves efectivas era

$$\frac{26!}{(14)!6!2^6}\, n_3\, n_5$$

que es del orden de 7×10^{18} (siete millones de billones).

Ahora bien, en el alfabeto de 26 caracteres latinos hay

$$\sum_{i=0}^{13} \binom{26}{2i} \binom{2i}{i}\, i!$$

involuciones, entre las que estaban las generadas por máquinas Enigma, y este número es del orden de 1×10^{18} (un millón de billones). Así pues, varias claves darían una misma involución de cifrado y descifrado. Para quebrantar el esquema de Enigma, más que calcular la clave utilizada, era importante caracterizar la involución utilizada.

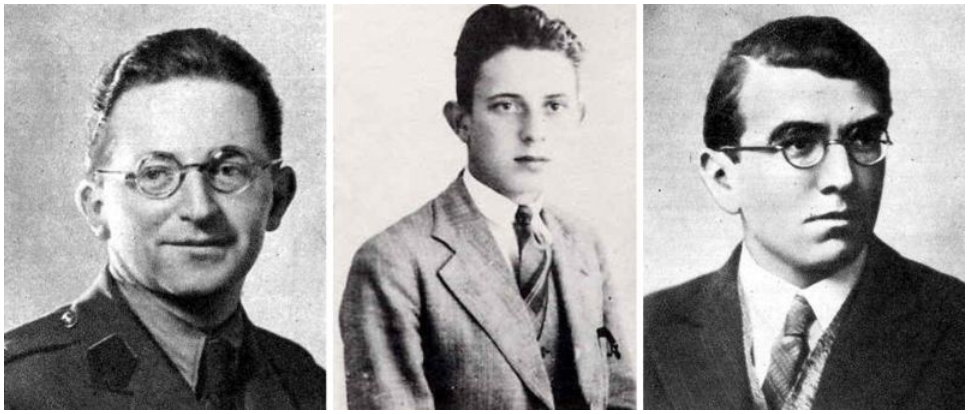


Figura 2: Marian Rejewski, Henryk Zygalski y Jerzy Różycki.

La Criptología en Polonia se desarrollaba en los años 20 y principios de los 30 bajo la conducción del prof. Zdzisław Krygowski, procedente de Poznań y anteriormente rector de la Politécnica de Lwów, junto con tres ex-alumnos suyos: Marian Rejewski, Henryk Zygalski y Jerzy Różycki, quienes en los 30 lograron descifrar comunicaciones cifradas con Enigma al poder reconocer las involuciones utilizadas.

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, en consecuencia, ninguna letra se cifraba con ella misma, por lo que, por ejemplo, un trigrama `jep` no podía corresponder a `der`. Utilizando primeros modelos de Enigma de tipo comercial, Rejewski hizo un estudio algebraico completo de las involuciones de Enigma y tras de ver que los cifrados no correspondían a su análisis hizo un descubrimiento esencial: la permutación del tambor inicial de la Enigma militar había sido cambiada respecto a la versión original comercial. Mediante la conversión de un mero formulismo idiomático, como un "buenos días", pudo descubrir la permutación en el tambor de entrada, desde 1932. Años más tarde, en 1939, cuando Rejewski explicó a criptólogos ingleses cuál era la permutación de entrada, Dillwin Knox, fundador de Blenchley Park se enfureció por la simpleza del método, escribió: "Era una cosa tan obvia de hacerse, incluso algo tonto, que ni Alan Turing ni yo pensábamos que era algo que valiera la pena intentarse".

En la práctica, en las comunicaciones militares, el elemento principal que variaban las partes comunicantes alemanas era la configuración inicial de los rotores: Tres letras indicaban cuál debía ser la posición inicial. Cuando se enviaba un criptograma, al inicio de él se incluía la configuración inicial. Debido al ruido de las comunicaciones por radio, ese trigrama se repetía y la cadena de 6 caracteres se cifraba a su vez con Enigma. Así, si por ejemplo `csg` era la configuración inicial, al inicio debía colocarse repetida, `csgcsg`, y luego debía ser cifrada, digamos `jhnqbs`. Rejewski sabía que la primera y la cuarta permutaciones cifraban un mismo símbolo, la segunda y la quinta también, al igual que la tercera y la sexta. Así que recolectando varios mensajes, podía descubrir las composiciones de la "clave del día", y mediante operaciones algebraicas guiar una búsqueda para descubrirla por completo. De hecho, Rejewski resultó beneficiado de que en septiembre de 1932, Hans-Thilo Schmidt, agente que trabajaba en una oficina de cifrado del Ejército Alemán, contactó al Cap. Gustave Bertrand, del Servico de Inteligencia Francés ofreciéndole materiales que incluían las claves del día utilizadas en dos meses. Bertrand hizo llegar esta información a los polacos, con lo que Rejewski pudo verificar que sus técnicas de quebrantamiento eran correctas. Los criptólogos polacos pudieron incluso mecanizar el procedimiento de Rejewski. Inventaron unos *ciclómetros*, consistentes de rotores de Enigma, en los que se aplicaba varios preámbulos de seis caracteres y producían la clave del día con el que habían sido producidos los criptogramas correspondientes.

Entre 1934 y 1938 se construyeron en Varsovia, en la fábrica *Wytwórnia Radiotechniczna, AVA*, 17 máquinas que cifraban según la Enigma militar cuyo diseño partía de un primer modelo de la Enigma comercial de los 20. El constructor de estas réplicas fue el Ing. Antoni Palluth, colaborador cercano de Rejewski, Zygalski y Różycki. Marian Rejewski diseñó también las primeras *bombas*: ensambles de máquinas Enigma para probar automáticamente del orden de las 26^3 posibilidades. Se les nombró "bombas", modestamente, debido al ruido que hacían. La primera se fabricó en AVA en noviembre de 1938 e incorporaba

6 réplicas de Enigma. Al mismo tiempo, Zygalski inventó un sistema de "placas perforadas" que fueron empleadas en los ciclómetros.

Hasta 1939, el Gobierno Polaco era capaz de descifrar las comunicaciones alemanas de las S.S. y del Ejército de Tierra, pero carecía de capacidad para oponerse al ataque de la *blitzkrieg*, la guerra motorizada alemana. Además, para entonces las máquinas Enigma alemanas habían sido dotadas de más rotores, lo que hacía inútiles a las réplicas hechas en Polonia, hecho que fue detectado por los polacos desde diciembre de 1938. La construcción de los correspondientes ciclómetros excedía las capacidades industriales y financieras del gobierno de Polonia. La criptología polaca era fromidable en el plano intelectual, pero estaba sujeta a limitaciones materiales. Un recuento personal de estos trabajos lo escribió el propio Rejewski [9].

Del 24 al 27 de julio de 1939, en Syry, entre Varsovia y Lublin, el director del Biuro Szyfrów polaco, Gwido Karol Langer, y otros oficiales, se reunieron con criptólogos franceses e ingleses, Dillwyn Knox participó por la parte inglesa y Gustave Bertrand por la francesa, y les entregaron réplicas polacas de la máquina Enigma militar así como los procedimientos para quebrantar el esquema. Esta fue una decisión del Estado Mayor Polaco ante la inminencia de la guerra, decisión que fue muy afortunada pues los alemanes tenían una gran confianza en la inviolabilidad de Enigma y no pudieron confirmar en su momento que sus comunicaciones eran interceptadas.

El 5 de septiembre de 1939, cuatro días después del inicio de la invasión alemana a Polonia, los criptólogos polacos recibieron la orden de abandonar el país. Fueron llevados a Francia a través de Rumanía e Italia, y a partir de octubre de 1939 se establecieron en el castillo de Vignolles, cerca de Gretz-Armaivilliers, en Seine-et-Marne, a unos cuarenta kilómetros al este de París, y continuaron con su labor de quebrantamiento de comunicaciones alemanas, ahí, cooperando con antiguos combatientes españoles republicanos. En enero de 1940, el Gobierno Inglés solicita que los criptólogos polacos sean llevados a Bletchley Park, pero el Gobierno Francés se opone, sin embargo acepta que Alan Turing visite 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 cambian los procedimientos de transmisión de las claves del día y se invade Francia. El 21 de mayo, Turing en Bletchley Park logra recuperar las nuevas claves del día y quebrantar las comunicaciones entre la Luftwaffe 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, pues las actividades de la Inteligencia Francesa, de acuerdo con el Armisticio pactado por Pétain, quedaron suspendidas. Sin embargo, en octubre de 1940 fueron llevados de nuevo a Francia, a Uzés, al castillo de Fouzes. Ahí estuvieron en una situación ambigua: por un lado para el Gobierno de Vichy habían de supervisar las comunicaciones alemanas para verificar que las condiciones del Armisticio se cumplieran, pero por otro lado transmitían al Gobierno Polaco en el Exilio y a Bletchley Park las comunicaciones alemanas interceptadas, entre las que estaban las comunicaciones de la Gestapo en el Territorio Libre de Francia. Al ver que mandos alemanes utilizaban todavía los esquemas previos de cifrado con Enigma, comprobaron que ellos desconocían que los esquemas habían sido quebrantados. Parte del grupo de criptólogos polacos se mantuvo en Argel, entre ellos Różycki, para interceptar las comunicaciones del Ejército Alemán en el Norte de Africa. El 9 de enero de 1942, mueren en un naufragio Ciezki, Gralinski y Smolinski, oficiales del *Biuro Szyfrów*, y el criptólogo Różycki, cuando se transportaban hacia Francia. En septiembre de 1942, los alemanes detectan al grupo de criptología en Fouzes, y el Gobierno de Vichy, de manera paradójica, facilita que los alemanes acudan en noviembre a desmantelar el centro que Vichy mismo había establecido. Prevenidos por Bletchley Park, se ordena evacuar de manera urgente al grupo polaco. Sin embargo, se da prioridad en la evacuación a los oficiales franceses y se deja a los polacos a su suerte. Algunos lograron llegar a España, tras pagar a guías estafadores, y fueron luego llevados a Inglaterra por la Cruz Roja. Rejewski y Zygalski llegaron a España pero fueron detenidos por la Guardia Civil franquista en Lérida. Mediante la intervención de la Embajada Británica en Madrid, fueron liberados y transportados también a Inglaterra. Otros, como Antoni Palluth, constructor de la réplicas polacas de Enigma, y Gwido Karol Langer, director del *Biuro Szyfrów*, fueron aprehendidos por los alemanes en la frontera con España. A pesar de torturas infringidas por la Gestapo, no develaron la naturaleza de sus actividades, por lo que el secreto del quebrantamiento de Enigma se mantuvo. 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 de ese campo 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 por ellos mismos, lo que era absurdo pues el secreto de Enigma se mantuvo. Luego de la Liberación, oficiales como el propio Langer, exigieron a las

Figura 3: Timbre postal polaco: "Polacos en el mundo".

autoridades francesas una aclaración sobre este punto, pero nunca la obtuvieron. Gente que había hecho una gran contribución al triunfo aliado veía así manchado su honor. En Inglaterra, Rejewski y Zygalski trabajaron para el Gobierno Polaco en el Exilio. Zygalski se estableció ahí, enseñando 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 le era poco confiable al régimen) y no quiso involucrarse en la seguridad del estado, así que trabajó como un modestísimo administrador de empresas estatales en Bydgoszcz, jubilándose en febrero de 1967. Murió en 1980.

En los 40, los criptólogos ingleses en Bletchley Park, entre ellos Alan Turing de manera relevante, se abocaron a descifrar, con éxito, las comunicaciones de la Marina Alemana, partiendo de la metodología polaca. En 1974 David Kahn escribió un artículo para *The New York Times* mostrando la contribución de los polacos en la criptología de los Aliados en la Segunda Guerra Mundial. En 1999, cuando Polonia se incorporó a la OTAN, se reconoció formalmente este trabajo y en 2004 se colocó una placa en el museo de Bletchley Park acreditando a Rejewski, Zygalski y Różycki los primeros quebrantamientos de Enigma.

3 Turing y Bletchley Park

Bletchley Park, 80 kilómetros 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 decidió establecer ahí la *Estación X*, conocida oficialmente como *Escuela Gubernamental de Códigos y Cifrados* (*Government Code and Cypher School* (GC & CS)), que luego sería el *Cuartel General de Comunicaciones Gubernamentales* (*Government Communications Headquarters* (GCHQ)). Bletchley Park era una residencia de campo construida en la segunda mitad del S. XIX por un banquero londinense, Herbert Samuel Leon. A finales de los 30, el Gobierno Británico adquirió propiedades similares para asentar fuera de Londres sus organismos militares y de seguridad y la Estación X era, precisamente, la décima tal propiedad. Tenía como misión el quebrantamiento

de comunicaciones secretas enemigas y su primer director fue Alastair Denniston. Desde agosto de 1939 comenzaron a llegar criptólogos, conformando la llamada, en clave, *Tropa de Cacería del Capitán Ridley*. La Estación X constaba de varias *barracas*, abocadas a tareas específicas. La 8, dirigida desde sus inicios por Alan Turing, se encargaba del desciframiento de la Enigma naval, la 6 de la Enigma de aire y tierra y estuvo dirigida primero por John Jeffreys y luego por Gordon Welchman, la 4 realizaba las traducciones y el análisis de inteligencia de los mensajes recuperados por la 8. Una antología de artículos sobre el centro de Bletchley Park, algunos escritos por participantes en él, es [3]. Remitimos ahí a todos los lectores interesados en profundizar en esta importante etapa de la Criptología Militar.

En 1938 Turing había visitado Princeton y por medio de Von Neumann se le había ofrecido una plaza ahí. No la aceptó, regresó a Cambridge y en 1939 aparentaba gestionar el 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 exclusivamente a Bletchley Park.

Al recibir una de las máquinas Enigma polacas en 1939, los ingleses descubren que pequeñas variaciones de sus propias máquinas *TypeX* habrían sido suficientes para quebrantar Enigma, por lo que se incrementó la producción de éstas y se fabricó también las placas perforadas de Zygalski para recuperar claves del día utilizadas por Enigma.

En mayo de 1940 una modificación a Enigma hace indescifrables las comunicaciones alemanas. Es entonces que el equipo dirigido por Turing en Bletchley Park logra quebrantar el nuevo esquema aprovechando las debilidades debidas a los formulismos lingüísticos alemanes. El quebrantamiento de comunicaciones es especialmente importante por lo tocante a la fuerza aérea alemana, la *Luftwaffe*.

En octubre de 1940 entra en funcionamiento la primera bomba criptológica inglesa en Bletchley Park, ésta invención de Turing, llamada *Ultra* o *bomba de Turing*, con una variante *bomba de Turing-Welchman*. A diferencia de las bombas polacas que buscaban reconstruir claves, las bombas de Turing buscaban patrones que correspondieran a texto en claro conocido, tales como destinatarios, direcciones, o formulismos idiomáticos muy usuales por las fuerzas armadas alemanas. Hay autores que valoran el *proyecto Ultra* como el de mayor secreto en la Segunda Guerra, sólo detrás del proyecto Manhattan de la Bomba Atómica. A lo largo de 1941, Ultra fue esencial para conocer con antelación las maniobras navales alemanas, y a partir de 1942 también en operaciones terrestres.

En octubre de 1941, Alan Turing y otros tres decodificadores de Bletchley Park, Hugh Alexander, Stuart Milner-Barry y Gordon Welchman habían escrito a Winston Churchill informándole de algunos recortes presupuestarios que 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". En respuesta, escribe a su Jefe de Estado, el General Ismay: "Asegúrese de que se les dé lo que piden, en prioridad extrema, e infórmeme cuando esto se haya hecho".

En Bletchley Park se criptoanalizaba diversos esquemas, y ahí se les refería con nombres de peces. El principal, el "pez" (*fish*), era el esquema *Geheimschreiber* y los demás eran derivaciones. "Tiburón" era una variación de la Enigma con cuatro rotores comenzada a utilizar en febrero de 1942. El Enigma de la Fuerza Naval era llamado "delfín" y se utilizaba para comunicaciones con los botes-U, submarinos alemanes en el Atlántico Norte, que por ese entonces impedían el abastecimiento hacia Inglaterra proveniente de los Estados Unidos. En junio de 1941, Turing pudo quebrantar el sistema delfín, al lograr descifrar reportes meteorológicos alemanes cifrados con ese sistema. Al conocer la ubicación de los botes-U, los barcos aliados podían desviarse y evitar a los botes-U, lo que era, evidentemente, una maniobra de tipo defensivo. Pero además, entre 1943 y 1944, fueron utilizados esos métodos de manera ofensiva por submarinos norteamericanos para combatir botes-U.

Actualmente se ensalza con justicia el trabajo criptológico del lado inglés para descifrar las comunicaciones alemanas, pero esctrictamente es necesario reconocer también la excelencia que en su momento mostraron los criptógrafos alemanes, los militares bajo el mando de la *Comandancia Suprema de las Fuerzas Armadas* (*Oberkommando der Wehrmacht* (OKW)) y los técnicos civiles provenientes de la industria proveedora de las máquinas cifradoras, principalmente de Siemens & Halske y de la sueca Ericsson. En [10] se puede ver transcripciones faccimilares de mensajes cifrados alemanes, provenientes de diversas fuerzas armadas. En 1942 un joven oficial se desempeñaba como criptógrafo de la *Wehrmacht*, Thomas Sylvester Barthel, y luego, desde la ocupada Noruega, fue criptoanalista a su vez de los mensajes ingleses provenientes de Escocia y yanquis provenientes de Sicilia. De formación etnógrafo, en 1952 se doctoró en la Universidad de Hamburgo presentando una tesis sobre los jeroglíficos mayas del Códice de Dresden, y logró descifrar en 1958 la escritura

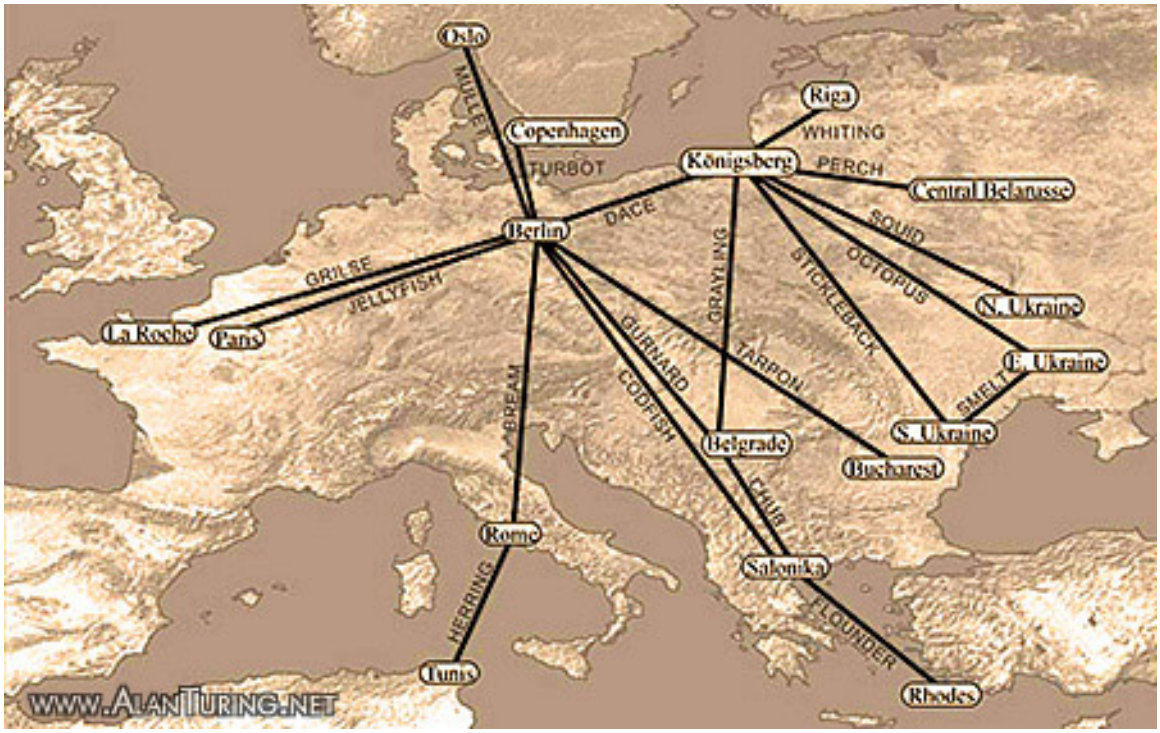


Figura 4: Esquemas de comunicación secreta alemanes, con nombres puestos en Bletchley Park.

rongorongo de la Isla de Pascua. De 1964 a 1966 hizo investigaciones de campo en Yucatán. Murió en 1997.

Desde agosto de 1942, los alemanes acostumbraban cambiar los rotores de sus Enigma cada dos días. Así las bombas criptológicas debían correr en días alternos a los del cambio de rotores con datos capturados, éstos desde la Barraca 10, de reportes meteorológicos de la marina mercante alemana.

Toda vez que se desarrollaba un procedimiento criptológico, en Bletchley Park se le ponía un nombre especial, casi cómico. Así, el inventado por Turing para quebrantar al delfín era llamado *Banburismus* pues requería de tomar apuntes, esencialmente bigramas, en tiras de papel producido en Banbury. Un método propuesto por Dillwin Knox se llamaba *Dillysimus*, y *Yoxallismus* era debido a Leslie Yoxall, el cual fue utilizado para recuperar claves Enigma del tipo *Offizier*, utilizadas por oficiales superiores de la Naval.

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

El "atún" (*tunny*), era el esquema *Schlüsselzusatz SZ40*, quebrantado por Bill Tutte (especialista en Teoría de Gráficas que posteriormente se incorporó a la Universidad de Waterloo en Canadá) y por Peter Hilton (especialista en Topología Homológica que posteriormente trabajó en diversas universidades norteamericanas de la Costa Este), el cual consistía de un doble cifrado de manera que ni siquiera los operadores de Enigma pudieran conocer el mensaje en claro. El quebrantamiento se basa en un método llamado *Turingismus* o *Turingery* inventado por Turing en 1942, que involucraba una fuerte componente de análisis probabilista. Hilton narra su experiencia personal en Bletchley Park en su artículo [6] y en [4] participa en una deliciosa conversación con lógicos de suma relevancia en el S. XX, repleta de anécdotas sobre Turing.

En febrero de 1942, los alemanes comenzaron a utilizar el sistema tiburón, y Bletchley Park quedó "sordo", respecto a sus usuarios, durante diez meses aproximadamente. En octubre un destructor británico recuperó de un submarino alemán, antes de ser hundido, las claves íntegras utilizadas en los meses previos y con esta información se pudo quebrantar el tiburón, lo que redundó en conocer la ubicación de los botes-U hasta febrero de 1943. El 10 de marzo, los alemanes cambiaron su sistema de cifrado, pero en 10 días pudo ser quebrantada esa nueva modificación.

Las bombas criptológicas adaptadas al tiburón, de cuatro rotores, comenzaron a funcionar entre junio y agosto de 1943, lo que permitía localizar claves en 24 horas. Para noviembre de 1943, cuando las bombas yanquis entraron en funcionamiento, esta labor se transfería a la Avenida Nebraska, en Washington, D. C.

En 1944 y 1945 se construyeron las primeras computadoras, las llamadas *Colossus*, en la "Newmanry", sección de Bletchley Park a cargo de Max Newmann (especialista en Topología, adscrito luego a las universidades de Manchester y Warwick). Su constructor, Tommy Flowers, nunca pudo presentarse como quien produjo las primeras computadoras en el Mundo debido a la confidencialidad de su trabajo. La "medusa" (*jellyfish*), conocido también como el *esquema de Lorenz*, era utilizado por los altos mandos alemanes en transmisiones por teletipo. Su rompimiento significó igualmente una proeza conjunta de matemáticas y de ingeniería. Diseñado el procedimiento de descifrado, éste se realizaba con máquinas Colossus. Sin embargo, mucho del trabajo mecánico realizado en la "Newmanry" debía ser completado manualmente, con ingenio humano, en la "Testery", sección de Bletchley Park a cargo del Mayor Ralph Tester.

Entre otros matemáticos que participaron en la Estación X estaban Donald Michie, especialista en Inteligencia Artificial, adscrito a la Universidad de Edimburgo y fundador de la Criptografía de Clave Pública en los años 70, Hugh Alexander, campeón británico de ajedrez y quien sucedió a Turing al frente de la Barraca 8, Henry Whitehead, especialista en Topología Combinatoria, profesor de la Universidad de Oxford, y Shaun Wylie, especialista en Teoría de Homología, profesor en Cambridge.

Como una muestra palpable del impacto que tuvieron en la guerra los trabajos de la Barraca 8, basta ver la estadística[1] de embarcaciones inglesas hundidas por los alemanes mes a mes. Los valores máximos (entre 25 y 45) corresponden a los meses de febrero y octubre de 1940, septiembre de 1941, febrero y noviembre de 1942, meses en los que los alemanes ponían en operación nuevas modalidades de cifrado, en tanto que los mínimos (entre 5 y 8) corresponden a marzo de 1940, julio de 1941, marzo de 1942, y febrero de 1943, meses inmediatos a los quebrantamientos de los respectivos cifrados alemanes. El trabajo criptológico efectivamente significó salvar muchas vidas y toneladas de abastecimiento por vía marítima.

Sin embargo, surgió también una "leyenda negra" sobre el trabajo criptológico de la Estación X. En mayo de 1940 se autorizó a la Real Fuerza Aérea a emprender bombardeos contra instalaciones industriales alemanas al este del río Rhin, con el propósito de desviar a la aviación alemana del frente francés. La *Luftwaffe*, a pesar de una prohibición expresa previa del propio Hitler, fue autorizada entonces a bombardear poblaciones inglesas, aunque esto lo hizo sólo seis semanas después de la campaña en Francia. Tuvo lugar la llamada Batalla de Inglaterra. Coventry, pues, fue objeto de varios bombardeos y el que causó mayores daños fue el realizado al anochecer del 14 de noviembre de 1940, noche de Luna llena, bombardeo codificado por los alemanes como *Sonata Claro de Luna* (*Mondscheinsonate*). El capitán británico F. W. Winterbotham publicó su libro *The Ultra Secret* en 1974, afirmando que los mensajes preparativos del ataque alemán habían sido interceptados y descifrados en Bletchley Park, y que al informar de esto a Winston Churchill, él decidió no tomar ningunas medidas defensivas, para evitar que los alemanes descubrieran que sus comunicaciones secretas estaban siendo quebrantadas. Winterbotham se desempeñaba entonces como supervisor de los "Oficiales de Enlace Especial" en Bletchley Park que precisamente comunicaban a Churchill los mensajes interceptados por la Estación X. Su opinión pues puede considerarse calificada. Sin embargo, algunos otros participantes del proyecto Ultra aseveran que, aunque Churchill estaba enterado del ataque aéreo en preparación, no se podía determinar el blanco. Peter Calvocoressi, quien trabajaba en la Barraca 6 rechaza la afirmación de Winterbotham, y, en cambio, asevera que el blanco esperado era precisamente Londres, y que Churchill ordenó que se resguardara la ciudad y por eso permaneció ahí. En abril de 1941 e incluso en agosto de 1942, Coventry volvió a sufrir bombardeos. Hay una polémica, considerada por algunos como irresuelta, sobre si prevaleció el interés por mantener el resguardo de las comunicaciones secretas sobre el interés de la defensa de la población. Parece cierto que, en efecto, mediante Ultra se supo que se ejecutaría la Sonata Claro de Luna, pero se ignoraba cuáles serían sus blancos, y se llegó incluso a suponer que eran varios, pues una sonata consta de tres partes.

Son interesantes también las relaciones del grupo de Bletchley Park con colegas norteamericanos. En 1942 estaba vigente un acuerdo de compartición de la información entre Inglaterra y los Estados Unidos de América. El gobierno yanqui estaba interesado en conocer los métodos criptológicos ingleses y el inglés en los avances estadunidenses en la construcción de máquinas computadoras.

En noviembre de 1942, Turing visitó el Departamento de Defensa y el de la Armada en Washington.

[1] Agradezco al Prof. Ricardo Mansilla del CEIICH de la UNAM esta información.

Hubo de sufrir varias complicaciones burocráticas al cruzar la frontera en la famosa Isla Ellis de Nueva York, debido a que llevaba pasaporte oficial mas no cartas que indicaran el propósito de su visita (ni más ni menos que intercambiar información de tareas secretas en tiempos de guerra con militares norteamericanos). En su reporte confidencial del 28 de noviembre, menciona la insistencia norteamericana en conversar sobre el atún y la medusa y Turing pide instrucciones al respecto pues él preferiría hablar sobre temas de probabilidad, inocuos para develar el análisis realizado en Bletchley Park respecto a modificaciones de Enigma y a otros sistemas como el de Lorenz. Posteriormente plantea que el trabajo criptológico norteamericano es puramente mecánico y matemático, por lo que ellos ven el bosque sin mirar los árboles, y no admiten que el uso de conocimiento y experiencias previas, junto con un trabajo manual, pueden producir resultados más rápidos. Concluye *"I am persuaded that one cannot very well trust these people where a matter of judgement in cryptography is concerned"*. Sin embargo, en su visita de 1942, Turing dió asesoramiento sobre bombas criptológicas, aunque llegó a calificar de *crazy scheme* algunos rasgos del diseño original de esas bombas. En abril de 1943 se inició la producción de bombas criptológicas en los Estados Unidos y, para fin de ese año, 77 fueron instaladas en Washington, D. C.

En 1945 se le concedió a Turing la Orden del Imperio Británico en grado de *Officer* (en orden de relevancia los grados son *Grand Cross*, *Knight*, *Commander*, *Officer* y *Member*. Como mera referencia recordamos que el MBE se les concedió a *The Beatles* en 1965 y a Mick Jagger en 2002). Turing tan solo conservó esta distinción en su empaque original. En el reconocimiento se dice que se le otorga por servicios "sin especificar", los cuales eran secretos, evidentemente.

Al final de la guerra, en 1945, todo el equipo de Bletchley Park fue desmantelado. Hubo matemáticos participantes que sólo obtuvieron una beca universitaria temporal luego de su trabajo en la Estación X. Max Newmann fue a la Universidad de Manchester, a dirigir el Departamento de Matemáticas, e invitó a Turing para que continuara ahí sus trabajos respecto a la construcción de computadoras.

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 de matrimonio. De hecho, uno de los principales personajes ahí, Jack Good (especialista en Estadística, adscrito luego al Instituto Politécnico de Virginia) decía "¡qué bueno que las autoridades de Bletchley Park ignoraban que Turing era homosexual!, si lo hubieran sabido habríamos perdido la guerra". Pero ciertamente, aunque Alan Turing era el más genial de la personalidades ahí, Bletchley Park no era "la estepa de un lobo solitario" sino el fruto colectivo de matemáticos muy talentosos.

Referencias

[1] Chris Christensen. Polish mathematicians finding patterns in Enigma messages. *Mathematics Magazine*, 80(4):247–273, 2007.

[2] B. Jack. Copeland. *The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life plus The Secrets of Enigma*. Oxford University Press, 2004.

[3] B. Jack Copeland et al. *Colossus: The secrets of Bletchley Park's code-breaking computers*. OUP Oxford, 2006.

[4] J. N. Crossley. Reminiscences of logicians. In *Algebra and Logic: Papers from the 1974 Summer Research Institute of the Australian Mathematical Society*, pages 1–62. Lecture Notes in Math., Vol. 450, Berlin, 1975. Springer.

[5] Kris Gaj and Arkadiusz Orlowski. Facts and myths of Enigma: Breaking stereotypes. In Eli Biham, editor, *EUROCRYPT*, volume 2656 of *Lecture Notes in Computer Science*, pages 106–122. Springer, 2003.

[6] Peter Hilton. Working with Alan Turing. *The Mathematical Intelligencer*, 13:22–25, 2005.

[7] D. Leavitt. *The Man Who Knew Too Much: Alan Turing and the Invention of the Computer*. Great Discoveries. W. W. Norton, 2006.

[8] A. Ray Miller. The cryptographic mathematics of Enigma. *Cryptologia*, 19(1):65–80, January 1995.

[9] Marian Rejewski. How Polish mathematicians broke the Enigma cipher. *IEEE Ann. Hist. Comput.*, 3(3):213–234, July 1981.

[10] Forde Weierud. Forde Weierud's CryptoCellar. http://cryptocellar.org/.

[11] S. Wikipedia, B. Group, and LLC Books. *Biuro Szyfrów: Waclaw Sierpinski, Marian Rejewski, Jan Kowalewski, Bomba, Zygalski Sheets, Stanislaw Lesniewski, Cadix, Cyclometer*. General Books LLC, 2010.