Píldora nº 8: ¿Qué relación existe entre Alan Turing y la criptografía?

Escena 1: El padre de la informática

Alan Turing fue un destacado matemático de la Universidad de Cambridge. Nace en Londres el 23 de junio de 1912 y muere trágicamente un 7 de junio de 1954, víctima de la ingratitud y la represión social.

Considerado el padre de la informática, gracias a él entre otros temas hoy hablamos de máquinas de Turing y autómatas para referirnos a un ordenador, así como del test de Turing para detectar la existencia de inteligencia en una máquina, idea suya que hoy usamos para evitar la suplantación de personas por máquinas o programas, conocido como captcha, acrónimo de Completely Automated Public Turing test to tell Computers and Humans Apart.

Escena 2: Alan Turing, la Segunda Guerra Mundial y la criptografía

La gran movilidad del ejército nazi le obligaba a utilizar comunicaciones a través de la radio que cifraba con la máquina Enigma. Era un cifrado tan fuerte, que no podía ser roto con las técnicas lingüísticas tradicionales. El Servicio de Inteligencia británico conocía el trabajo de los polacos que utilizando a un grupo de matemáticos, entre los que destacaba Marian Rejewski, habían creado varios ataques contra Enigma. En 1938, cuando la guerra era inminente, este Servicio asigna a Turing la misión de recrear y mejorar las técnicas polacas.

En la mansión de Bletchley Park, situada lejos de Londres para evitar los bombardeos, con la ayuda de algunos criptoanalistas tradicionales y de varios matemáticos, Turing crea varias técnicas de ataque que rompen una y otra vez las variantes mejoradas de Enigma que desarrollan los alemanes.

Escena 3: Bombas de Turing y Colossus

Al igual que los polacos, Turing y sus colegas basan los ataques en una combinación de ingenio manual y fuerza bruta mecanizada. La fuerza bruta se aplica mediante el uso masivo de unos aparatos llamados Bombas, que reproducen el funcionamiento de muchas máquinas Enigma simultáneas. El criptoanalista determina manualmente unos patrones del criptotexto llamados "menús", que mediante conectores son convertidos en circuitos eléctricos dentro de la Bomba. Al lanzar la prueba, el aparato va probando todas las claves posibles y se detiene cuando se cierra el circuito representado por el "menú".

Posteriormente Turing desarrolla un sistema completo de probabilidad bayesiana que se utiliza para romper el cifrado para teletipo basado en XOR que usan las máquinas Lorenz SZ 40 y 42. Esta comunicación por teletipo es aún más valiosa que Enigma puesto que transporta mensajes de muy alto nivel. En 1944 se romperá utilizando Colossus y las técnicas de Turing y sus colegas. Colossus fue el primer equipo electrónico programable, el antecedente de todos los ordenadores actuales.

Además del avance intelectual que produjeron, se considera que la aportación de Bletchley Park a la guerra permitió acortarla en por lo menos dos años.

Escena 4: Un genio reconocido tardíamente

Aunque hoy se le considera uno de los hombres más influyentes del siglo XX, Turing pagó muy caro su contacto con el mundo de los servicios secretos. Después de la guerra, trabajó en el desarrollo de los primeros ordenadores electrónicos pero sin dejar de ser un miembro de ese mundo clandestino. El éxito del descifrado computarizado contra Enigma, hizo que el gobierno inglés controlara la nueva tecnología informática.

Turing era homosexual, lo cual estaba prohibido para los servidores del Estado. Cuando por casualidad esto se hizo público, fue tratado de forma indigna y desposeído de todas sus credenciales de seguridad, impidiéndole seguir con su trabajo en computación digital. Desesperado, aceptó inyectarse hormonas que en esa época se consideraba una cura para la supuesta enfermedad. La humillación y el desprecio social, unidos al horror del tratamiento, provocaron en Turing una espiral depresiva que culminó con su trágico suicidio.

Madrid, septiembre de 2014

Más información: La máquina Enigma (Román Ceano, web Kriptópolis)

http://www.kriptopolis.com/enigma

Autores del guion: *Román Ceano, Jorge Ramió*

Dirección Proyecto Thoth: *Jorge Ramió Aguirre, Alfonso Muñoz Muñoz*