De Turing y la criptografía

José de Jesús Ángel Ángel

Máquina Enigma. Fotografía: I. Walter, 1943

La computación es un invento del siglo xx, sin embargo, han existido diferentes hechos desde los inicios de la humanidad que marcan el desarrollo de las computadoras: desde el ábaco hasta las primeras máquinas electromecánicas para realizar operaciones entre números. Finalmente llegan a su máxima expresión en las modernas computadoras que todos conocemos en nuestros días. Esto es en lo que se refiere al hardware y al aspecto conocido como software, que tiene como inicio la creación del término algoritmo, la programación estructurada, la basada en orientación a objetos, los algoritmos genéticos y hasta los complejos modelos de la inteligencia artificial.

Muchas áreas tecnológicas han sido beneficiadas por las computadoras y sus programas: en la tecnología del transporte, de viajes espaciales, en las comunicaciones telefónicas, en comunicaciones satelitales, en el mundo de la medicina con complejos aparatos automatizados, en la construcción de infraestructura, en fin, la sociedad como la conocemos no sería lo mismo sin las computadoras. El impacto de éstas en el mundo

Soldados alemanes utilizan la máquina Enigma.
Fotografía: Erich Borchert, 1940

aún no ha sido comprendido y es posible que en los próximos años sean aún más imponentes sus aportes.

Alan Turing nació en junio de 1912 y es considerado uno de los padres de la computación moderna. El trabajo de Turing formalizó el modelo de una computadora. Participó activamente en la Segunda Guerra Mundial involucrado en el grupo inglés que pudo romper la máquina de cifrado alemana conocida como Enigma y su trabajo es base incluso en la moderna computadora cuántica.[1]

[1] Modelo virtual de la máquina Enigma *http://bit.ly/enigmaflash*

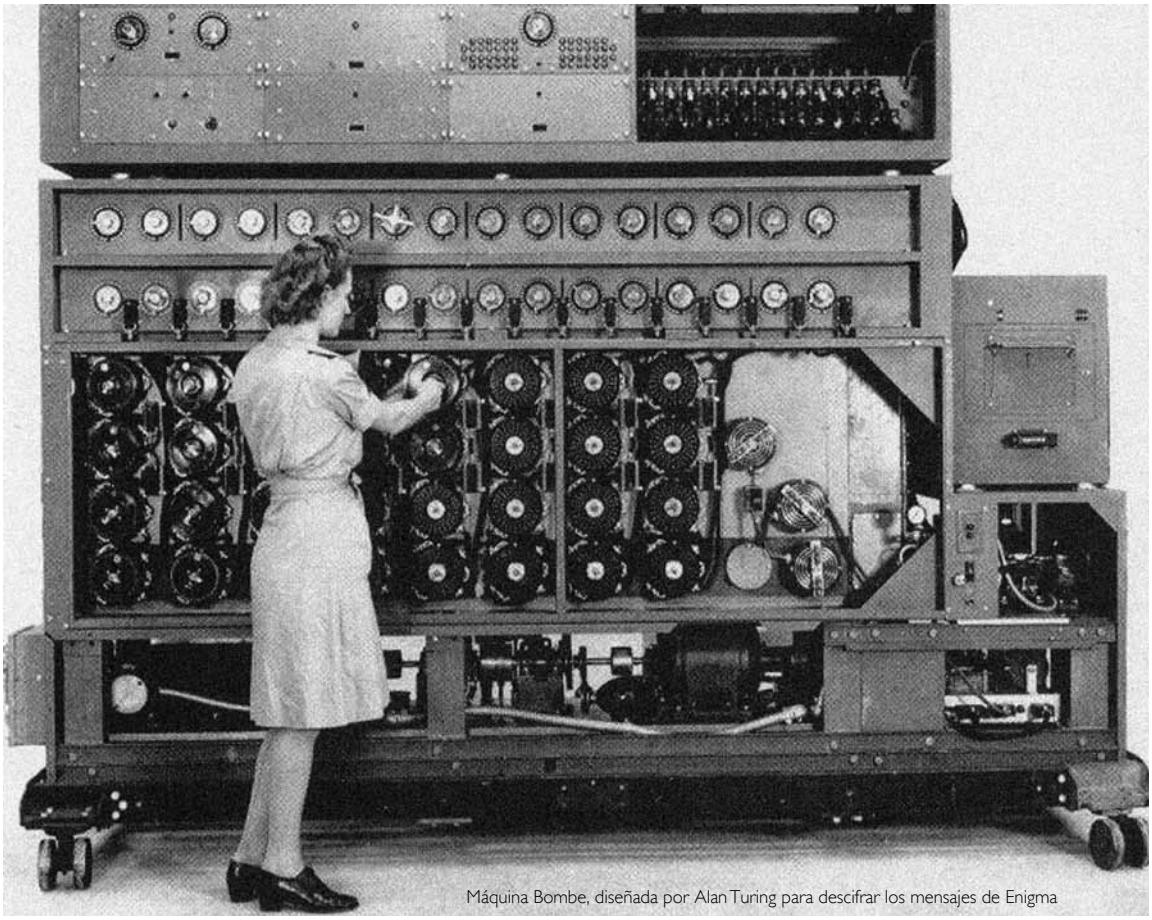
La criptografía en la Segunda Guerra Mundial

Aunque la historia de la criptografía tiene antecedentes cientos de años antes de la Segunda Guerra Mundial, es en esta etapa cuando el uso de la criptografía se hace más común. Los conflictos anteriores a la segunda gran guerra —como la Primera Guerra Mundial de 1914 y las guerras de Independencia de los Estados Unidos— tenían incorporada a la criptografía como parte esencial de la estrategia militar. En 1918 es patentada por Arthur Scherbius la máquina de cifrado Enigma, y se dispone su venta de manera comercial en 1922. La Enigma es muy parecida a una máquina de escribir. Tenía diferentes formas de configuración inicial, contaba con tres discos y diferentes posiciones de sus otros componentes, así llegaba a un número total de 2, 741, 856 diferentes claves. La máquina Enigma que usó la armada y fuerza aérea alemana fue modificada para alcanzar el orden de 10^{17} posibilidades. Sin embargo, se encontraron debilidades.

En 1938, Edward Travis, Hugh Foss, John Tiltman y Dilly Knox, miembros de la The Govermment Code and Cypher School (GC&CS) en Londres, tenían ya conocimiento de la Enigma comercial usada en la Guerra Civil Española, y la conocían también como la QWERTZUIO, debido a la posición inicial de sus teclas. Al parecer, Turing en esos tiempos ya estaba en contacto con este grupo de criptoanalistas.

Por otra parte, en Polonia un grupo de matemáticos encabezados por Marian Rejewski había también estudiado la Enigma comercial y conocían algunas de sus debilidades, lograron romper a la versión de Enigma que los alemanes usaban antes de la invasión a Polonia.

Para julio de 1939, se concreta la primera reunión entre criptoanalistas polacos, ingleses y franceses cerca



Máquina Bombe, diseñada por Alan Turing para descifrar los mensajes de Enigma

de Varsovia. En septiembre, Turing se incorpora a Bletchley Park con el objeto de romper la Enigma que ya habían modificado los alemanes.

Turing usó diferentes caminos para criptoanalizar a Enigma, desde ingeniería en reversa hasta el desarrollo de un complejo análisis estadístico. Con la ayuda de todo el conocimiento del equipo polaco y los mensajes que eran interceptados, poco a poco lograron afinar ciertas técnicas que finalmente lograron descifrar menajes. Se ayudaban con una máquina llamada "bomba" que el grupo polaco ya había probado. La bomba de Turing usaba una técnica llamada "cribs", pequeños fragmentos de texto plano y texto cifrado que se podían conocer de las intercepciones hechas a los alemanes. La técnica más conocida diseñada por Turing fue llamada "Banburismus", ésta se apoyaba en un análisis bayesiano para diseñar cartas llamadas "banburies" que finalmente apoyaban a la "bomba" para descifrar mensajes. El nombre al parecer se deriva de la ciudad Banbury, cerca de Bletchley. Para el año de 1945, era posible romper los mensajes alemanes en uno o dos días. Aparentemente, los alemanes siempre confiaron en la seguridad de sus mensajes y no se dieron cuenta que eran conocidos sus mensajes secretos.[2]

Aunque mucho del trabajo de Turing ha quedado en secreto, el pasado abril de 2012 fueron liberados por *The National Archives* (Reino Unido) dos documentos escritos por el propio Alan. Uno es "The applications of probability to cryptography", donde se describen las bases del criptoanálisis para el método de Vigenere, la teoría de Repeats, y sistemas de transposiciones. El otro documento es "On statistics of repetitions". Estos documentos son una pequeña muestra del inmenso trabajo que Turing realizo en esa época.

Turing también rompió la máquina llamada "The Geheimschreiber", usada por Hitler y su alto mando. Después de esto desarrollo la máquina de criptoanálisis *Colossus,* considerada como una de las primeras computadoras en 1944.

[2] En la actualidad se conoce a un *ban* como la unidad de información $log_{10}p$ que tiene como origen el "Banburismus".

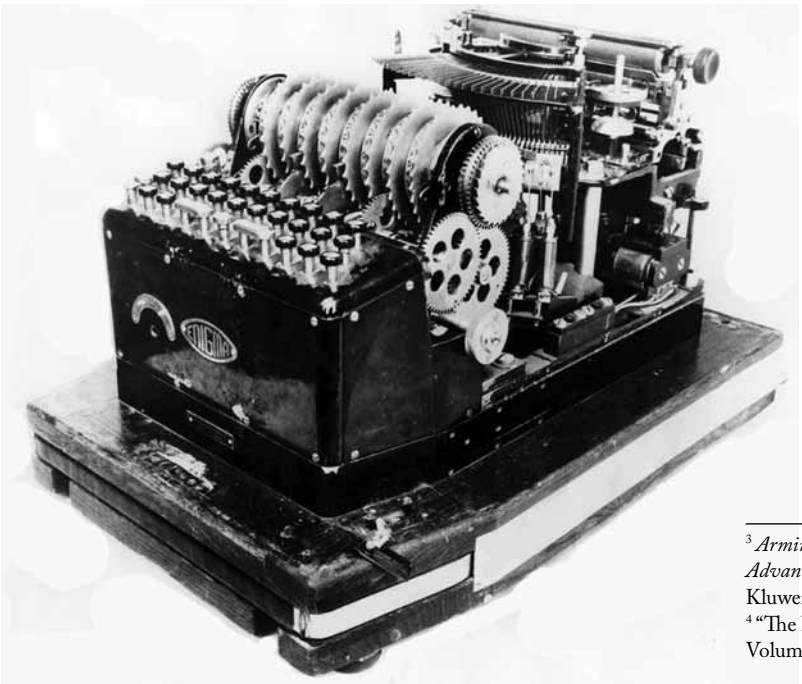
Turing y la inteligencia artificial

En 1950, Turing publica el artículo "Computing Machinery and Intelligence" en el cual describe cómo las computadoras pueden o no pensar o comportarse como un cerebro humano. Los primeros intentos para que trabaje una computadora son sin duda el poder ejecutar combinaciones lógicas binarias básicas como AND, NOT y OR; posteriormente, el que puedan ejecutar simples instrucciones secuenciales como los lenguajes estructurados lo hacen ahora, y en seguida se desarrolla la teoría de cómo es posible crear modelos básicos como lo hacen los lenguajes orientados a objetos.

Finalmente, lo que se ha podido desarrollar en los años noventa con los agentes inteligentes es que son programas que pueden "aprender" y a partir de esto decidir. Sin duda, la computación junto con la programación que hoy existe tiene bases fundamentales en el trabajo de Turing. En la actualidad, la inteligencia artificial tiene diferentes y diversas aplicaciones, desde la construcción de robots, hasta tecnología que es usada en las diferentes guerras.

Una de las aplicaciones importantes que tiene la inteligencia artificial es la que se ha desarrollado en los últimos diez años, y que ha permitido involucrar a programadores y matemáticos en la lucha en contra del crimen organizado y el lavado de dinero. En el laboratorio de inteligencia artificial de la universidad de Arizona se desarrolló un producto llamado COPLINK, que incorpora diferentes herramientas de software inteligente. Por ejemplo, con COPLINK es posible ubicar el lugar y el tiempo de un próximo probable robo a banco. El fundamento básico de COPLINK parte de la administración de conocimiento que se tienen en las bases de datos policiales.[3]

Otro importante caso de estudio es el referente al problema de transacciones fraudulentas y lavado de dinero. En el *Financial Crimes Enforcement Network*, del Departamento del Tesoro de los Estados Unidos, se usan diferentes técnicas de minería de datos como el análisis de enlaces para la detección de actividades principalmente de fraude y lavado de dinero en el sector financiero. Este sistema incorpora algoritmos de minería de datos e inteligencia artificial y se denomina *FinCEN Artificial Intelligence System* (FAIS).[4]



No es posible conocer toda la influencia que ha tenido el trabajo de Turing en los últimos 70 años, incluso en la nueva generación tecnológica, con la que David Deutsch en 1985 partió hacia la teoría de la computadora cuántica, sin embargo, esa es una historia que deberá ser contada en otra ocasión.

[3] *Arming Law Enforcement with New Knowledge Management Technologies, Advances in Digital Government Technology, Human Factors, and Policy*, Kluwer Academic Publishers, 2002. *http://bit.ly/digitalgov*

[4] "The Financial Crimes Enforcement Network AI System", *AI Magazine*, Volumen 16, Number 4, 1995. *http://bit.ly/FinCEN*