En torno a la figura de Alan Turing: desarrollos tecnológicos e implicaciones sociales de los logros científicos

MÓDULO 4
Lógica matemática: Colossus contra la máquina Enigma

En 1936 Alan Turing se desplaza a la Universidad de Princeton como estudiante ya graduado (1936-38). Allí completó la tesis doctoral con A. Church. Trabajó además con von Neumann y conoció a otros importantes científicos emigrados de Alemania. Allí trabajo en su proyecto "Ordinal Logics" probablemente su trabajo más difícil y profundo matemático; que le acercó al mundo de lo abstracto e incalculable y también utilizó para sus trabajos sobre la naturaleza de la mente. Ante lo inevitable de la guerra, redobló su interés por la Criptografía y desarrolló una máquina de cifrado. Rechazó una oferta de von Neumann y regresó a Cambridge, donde le habían renovado su beca.

La GCCS (Government Code and Cipher School), agencia del Servicio Secreto, estableció a 60 Km de Londres su centro de desciframiento de mensajes. En Bletchley Park llegaron a trabajar hasta 10.000 personas. En Agosto de 1939, Turing fue reclutado entre otros profesores, como experto en criptografía. El problema central era el descifrado de los mensajes transmitidos por la máquina Enigma, usada por Alemania desde los años 20 y de la que existían versiones comerciales. Los matemáticos polacos llevaban 7 años de ventaja a los británicos y habían construido unas máquinas electromecánicas, las Bombas, para ayudar a descifrar los mensajes de Enigma.

La primera contribución de Turing fue generalizar las Bombas para que no dependieran de los indicadores ni del panel. La idea era suministrarle hipótesis en base al texto del mensaje y que ella descartara las combinaciones que entraban en conflicto con ellas.

Las nuevas Bombas empezaron a construirse en 1940. Turing diseñó la mayoría de los circuitos. En 1940 pasó a dirigir “Hut-8", equipo responsable de la Enigma naval, que tenía un juego de 8 rotores, a elegir 3 (336 variaciones). Diseñó otras Bombas más generales que funcionaban por probabilidad. Desarrolló además una teoría matemática específica.

Con la nueva era electrónica, Max Newman (Cambridge) y Tommy Flowers (Postal Office) son encargados para diseñar una máquina electrónica, denominada Colossus, para descifrar el nuevo código secreto empleado para los mensajes del alto mando alemán (Fish). Turing contribuye con métodos estadísticos. Completada en 1943, se llegaron a construir 11 Colossus.

A finales de 1942, Turing es enviado a EE.UU. por unos meses a entrenar a los analistas americanos en Enigma, a estudiar electrónica y a diseñar un método irrompible para cifrar voz. Se estima que las contribuciones de Alan Turing al desciframiento de mensajes, acortaron la Guerra en dos o tres años.

Los objetivos principales de este módulo son:

- Conocer que son la Criptografía y el Criptoanálisis.
- Describir la importancia de ambos campos a lo largo de la historia.
- Transmitir la importancia de las investigaciones llevadas a cabo por científicos como Alan Turing durante la II Guerra Mundial.
- Aprender la relación existente entre dichas investigaciones y el desarrollo de los primeros computadores.