Aportaciones de la Criptología a la victoria aliada en la Segunda Guerra Mundial

Guillermo Morales Luna
gmorales@cs.cinvestav.mx CINVESTAV-IPN

Durante la Guerra Mundial del 39 al 45, el quebrantamiento hecho por Alan Turing a 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. Los métodos fueron utilizados también por submarinos norteamericanos al combatir a los buques-U alemanes. Fue tan importante el trabajo realizado en el centro criptológico de Bletchley Park que se ordenó el desmantelamiento total de ese centro 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.