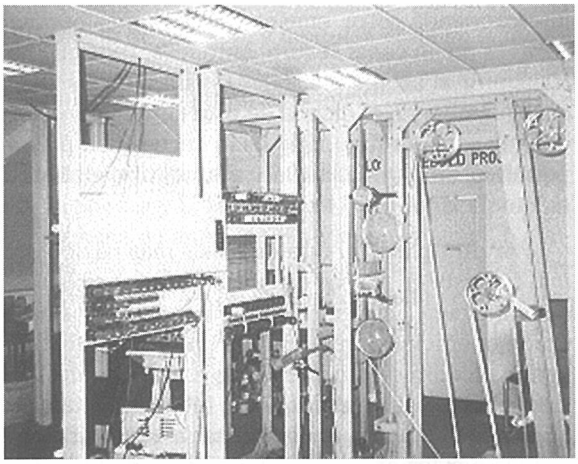
ALGUNOS HITOS DE LA CRIPTOGRAFÍA DEL SIGLO XX

Pino Caballero Gil

Historia

La criptografía, o ciencia que estudia las comunicaciones cifradas, ha ido siempre de la mano de las matemáticas. Desde el punto de vista de la matemática moderna, nos encontramos con nombres de criptógrafos en los campos de la estadística (W. F. Friedman, 1920), el álgebra combinatoria (L. S. Hill, 1929) y la teoría de la información (C. E. Shannon, 1941). Pero además de estas disciplinas matemáticas, juegan un papel fundamental en el estado actual de la criptografía, la teoría de números, la teoría de grupos, la lógica combinatoria, la teoría de la complejidad y la teoría ergódica. De hecho, esta ciencia puede verse como una subdivisión de las matemáticas aplicadas y de las ciencias de la computación.

Antes del siglo XX la criptografía se consideraba un arte que resultaba útil sólo para unos pocos políticos y militares. Durante el presente siglo se produjo un cambio radical en su concepción. En la primera mitad, aunque se realizaron las primeras aproximaciones científicas importantes, todavía su uso se restringía a ámbitos político-militares. Durante las dos guerras mundiales, se produjeron sendos hitos criptográficos que modificaron el curso de la historia. En la primera, la ruptura del cifrado del famoso telegrama *Zimmermann* hizo entrar en guerra a los EEUU al descubrir los planes alemanes. Por otra parte, desde el principio de la Segunda Guerra Mundial, los aliados eran capaces de leer los mensajes secretos alemanes ya que habían roto su máquina de cifrar, la Enigma. Para ello diseñaron una máquina de cálculo gigantesca, el Colossus, precursora de los ordenadores modernos. Uno de sus artífices fue el matemático inglés A.M. Turing (1912-1954), fundador de las ciencias de la computación y de la inteligencia artificial.



El Colossus, *precursor de los ordenadores modernos.*

La criptografía empezó a ser considerada una ciencia