Miniaturas matemáticas de La Gaceta de la RSME
Vol. 25 (2022), Núm. 1, Pág. 84

Rejewski: teoría de permutaciones para romper Enigma

Es bien conocida la participación de Alan Turing y su equipo para leer los mensajes que los alemanes cifraban con la máquina Enigma. Sin embargo, otros matemáticos tuvieron éxito antes que ellos. En 1932, el matemático Marian Rejewski y otros dos colegas fueron contratados por el gobierno polaco para romper Enigma. Hasta ese momento, toda la criptografía de los gobiernos estaba en manos de lingüistas. Dice Rejewski en sus memorias que fue inteligente pensar que el conocimiento de la lengua alemana era importante, pero lo era más tener conocimientos matemáticos.

El arma matemática de Rejewski fue la teoría de permutaciones [1, 2]. Recordemos que dos permutaciones son conjugadas si y solo si tienen la misma estructura como producto de ciclos disjuntos; este teorema fue fundamental para que pudiera encontrar los cableados de los rotores de la Enigma usada por el ejercito alemán.

Entre otras cosas, Rejewski tuvo que encontrar, a partir de tres permutaciones del mismo tipo β_i, $i = 1, 2, 3$, una permutación γ que por conjugación pasara de β_1 a β_2 y de β_2 a β_3. Por ejemplo, sean

$$\begin{array}{|c|}\hline \beta_1 = \texttt{(efwyxz)(codmtu)(aknqp)(blrsv)(gj)(hi)} \\ \beta_2 = \texttt{(ahydqc)(bfuzxv)(giowm)(eknst)(jl)(pr)} \\ \beta_3 = \texttt{(acekyx)(fgvojq)(bdupl)(hwmtz)(is)(nr)} \\ \hline \end{array}$$

El problema de la doble conjugación es equivalente al siguiente: fijándonos en el cuadro anterior, se trata de reordenar los ciclos de la misma longitud en las filas segunda y tercera y mover las letras de los ciclos, de modo que debajo de letras iguales haya letras iguales. Encontrar esta reordenación es un ejercicio divertido:

$$\begin{array}{|c|}\hline \beta_1 = \texttt{(efwyxz)(codmtu)(aknqp)(blrsv)(gj)(hi)} \\ \beta_2 = \texttt{(hydqca)(vbfuzx)(owmgi)(knste)(pr)(jl)} \\ \beta_3 = \texttt{(jqfgvo)(ekyxac)(bdupl)(wmtzh)(is)(rn)} \\ \hline \end{array}$$

La permutación que se busca se obtiene al escribir la sucesión de letras que aparecen cada una debajo de la anterior en el cuadro de la reordenación. Comenzando por la letra `a`,

$$\gamma = \texttt{(aobkwdfyqgpilnmuxcvehjrstz)}.$$

Referencias

[1] M. Rejewski, How Polish mathematicians deciphered the Enigma, *IEEE Ann. Hist. Comput.* **3** (1981), no. 3, 213–234.

[2] M. Vázquez y P. Jiménez-Seral, Recovering the military Enigma using permutations – filling in the details of Rejewski's solution, *Cryptologia* **42** (2018), no. 2, 106–134.

Paz Jiménez Seral, Dpto. de Matemáticas, Universidad de Zaragoza
Correo electrónico: paz@unizar.es