O que vem à rede...

António Machiavelo
Departamento de Matemática Pura da Faculdade de Ciências da Universidade do Porto

ENIGMA: uma história que devia ser melhor conhecida

Iniciamos esta nova rubrica da Gazeta, onde se pretende sugerir viagens a páginas da internet de algum modo relacionadas com matemática, e que pensamos serem interessantes e úteis, com um tópico que é um bom exemplo para utilizar como uma de entre muitas possíveis respostas à pergunta tantas vezes disparada contra quem ensina a Rainha das Ciências: para que serve a Matemática?

A mansão de Bletchley Park

É infelizmente ainda relativamente pouco conhecido que a arma mais secreta, e provavelmente a mais eficaz, utilizada pelos ingleses durante a Segunda Guerra Mundial consistia num grupo de cripto-analistas, que incluia vários matemáticos, reunidos numa mansão com o nome de Bletchley Park, a uns 90Km a noroeste de Londres. Foi aí que foi eventualmente decifrado o código secreto, ou cifra, utilizada pelas tropas nazis para enviar mensagens confidenciais, contendo informações militares cruciais, via rádio, cifra essa conhecida pelo nome de Enigma. Estima-se que o trabalho desenvolvido em Bletchley Park, e no qual desempenhou um papel fundamental a Matemática, evitou, pelo menos, mais dois anos de guerra, salvando assim centenas de milhares de vidas! Uma das armas matemáticas usadas para quebrar a cifra Enigma é um resultado básico sobre grupos de permutações, que duas permutações conjugadas têm decomposições semelhantes em ciclos disjuntos, resultado este que foi descrito pelo criptólogo C. A. Deavours como "*o teorema que ganhou a Segunda Guerra Mundial*"!

A história do trabalho desenvolvido em Bletchley Park está contada em vários documentos acessíveis através da página *Decoding Nazi Secrets (NOVA Online)* da cadeia de televisão pública[1] norte-americana, cuja visita vivamente recomendamos:

http://www.pbs.org/wgbh/nova/decoding/

Aconselhamos começar pela transcrição do correspondente programa televisivo (disponível via um ponteiro colocado no fim da página), embora certamente tal não seja tão interessante como ver o próprio documentário, e depois consultar as páginas intituladas *How the Enigma Works* e *Mind of a Codebreaker*. Há ainda uma série de páginas contendo várias ideias, sugestões de actividades e alguns materiais para professores que queiram incluir algo sobre o assunto nas suas aulas, acessíveis através do "link": *Teacher's Guide*.

Bletchley Park, que durante a guerra era conhecida por "Station X", é agora um museu, com várias páginas sobre a sua história em:

http://www.bletchleypark.org.uk/

A descrição detalhada da cifra Enigma, e das máquinas com o mesmo nome que eram usadas para codificar e descodificar as mensagens com essa cifra, pode ser lida numa série de páginas escritas por aquele que foi o primeiro curador do museu de Bletchley Park, em:

http://www.codesandciphers.org.uk/enigma/index.htm

Nestas páginas pode-se ainda ler sobre o papel crucial desempenhado em Bletchley por Alan Turing (1912—1954), um dos grandes nomes da Matemática do século XX e um dos pioneiros da Ciência dos Computadores, assim como da Inteligência Artificial.

Alan Turing

A história da cripto-análise da cifra Enigma tem de facto início ainda antes da guerra, em 1932, quando os serviços secretos polacos enlistam os esforços de uma equipa de jovens matemáticos. Com o aumento do poderio militar alemão na década de 1920-30, os polacos tinham boas razões para se sentir ameaçados e começaram a escutar atentamente as comunicações militares do país vizinho de tendências bélicas. Eventualmente perceberam que estas eram codificadas com máquinas Enigma, mas que as tropas alemãs usavam uma versão modificada da versão comercial, em uso desde 1923, da máquina Enigma inventada em 1918 por Arthur Scherbius. A equipa de matemáticos, que incluia Marian Rejewski (1905-80), estava encarregue de quebrar a cifra que os alemães estavam a utilizar.

Rejewski rapidamente se apercebeu que podia usar resultados de Teoria dos Grupos para cripto-analisar a cifra Enigma. Os leitores que conhecerem os resultados básicos sobre grupos de permutações podem ler como Rejewski os usou para quebrar a cifra Enigma utilizada antes da guerra (os alemães introduziram posteriormente várias complicações que tornaram a cripto-análise substancialmente mais difícil) no seu artigo intitulado *An Application of the Theory of Permutations in Breaking the Enigma Cipher*, que está disponível no endereço:

http://frode.home.cern.ch/frode/crypto

que contém muitas outras coisas interessantíssimas.

O papel desempenhado no esforço de guerra por Bletchley Park foi mantido secreto durante cerca de 30 anos, e as pessoas que lá trabalharam nunca receberam qualquer reconhecimento oficial pelo seu papel, que foi decisivo na vitória dos aliados. Conhecer e divulgar esta história é assim honrar a memória desses heróis anónimos, além de ser uma história verdadeiramente fascinante! Fica pois o leitor convidado a um passeio pelas páginas atrás indicadas, e possivelmente outras que encontrará pelo caminho. É necessário no entanto não esquecer que muitas páginas na internet são escritas por pessoas com conhecimentos muito superficiais dos assuntos sobre os quais se decidem a dissertar ou simplesmente sumariar, e o resultado é por vezes de uma fraca, ou mesmo verdadeiramente má qualidade. Também na internet, nem tudo o que

vem à rede é peixe...

Uma máquina Enigma

[1] no sentido de ser financiada directamente pelo público, e não pelo governo, e por ser não-comercial.