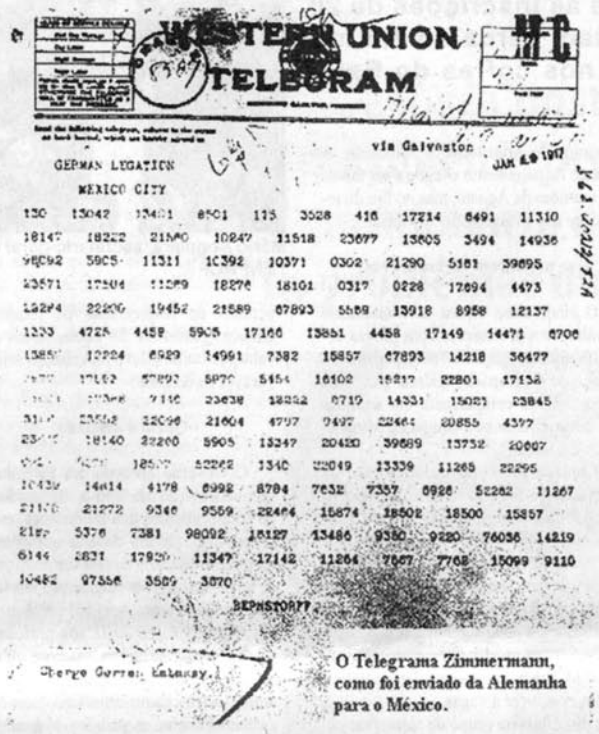
Matemática

A Criptografia

Por: João Cabral *

Neste último mês de Outubro de 2013, no Departamento de Matemática da Universidade dos Açores, concluiu-se três Mestrados que merecem o devido destaque no espaço científico no nosso pequeno universo da Região Autónoma dos Açores. Os novos mestres em Matemática para Professores são, usando uma ordem temporal de defesa, a Mestre Raquel Faria, professora na Escola Secundária da Ribeira Grande, que defendeu a Tese "Interpretação Geométrica dos Problemas Clássicos de Desargues, Fagnano e Malfatti"; o Mestre Paulo Fragata, professor na Escola Básica Integrada dos Ginetes, que defendeu a Tese "Tópicos da Teoria da Relatividade" e o Mestre José Sousa, atualmente professor na Escola Secundária Antero de Quental, que defendeu a Tese "Conjetura de Goldbach – Uma visão aritmética". Tendo sido júri na defesa da tese do Mestre Emanuel Sousa, fiquei pessoalmente impregnado com um pouco de nostalgia do passado, e por isso hoje vou falar sobre um tema que pretende homenagear duas pessoas, dois Açorianos, que tive o prazer de ouvir na qualidade de aluno, quando estudava assuntos relacionados com a Teoria dos Números. Não devemos só exaltar os feitos dos cientistas além fronteiras, temos que dar valor à prata da casa, pois estas duas pessoas muito contribuíram para que houvesse um leque de alunos, no qual eu estou incluído, que se interessassem pela Teoria dos Números e ficassem fascinados pela magia dos números primos. Falo da Professora Doutora Helena Melo, atualmente minha colega do Departamento, uma das primeiras professoras desta área na Universidade dos Açores, e o Dr. João Correia, atualmente um executivo do Colégio do Castanheiro, em Ponta Delgada, que deu continuidade ao trabalho da Professora Helena, contribuindo para o desenvolvimento do meu próprio interesse na área da Teoria dos Números, autor de um trabalho sobre Teoria dos Números e Criptografia (1994), que se pode consultar na biblioteca da Universidade dos Açores, e cuja introdução do mesmo serve de base para este artigo de jornal.

Em todas as épocas da evolução humana, mesmo nas mais distantes, encontra-se o sentido do número. Todo o ser humano aplica nas suas atividades do quotidiano, de forma consciente ou não, juízos aritméticos e propriedades geométricas. A Matemática, no geral, sempre foi e será um dos principais motores da evolução humana. Nesta evolução sempre houve a necessidade de comunicar, e mesmo que falemos dos povos primitivos das cavernas, é de conhecimento geral que estes tentavam comunicar mesmo com as gerações do seu tempo, até mesmo com as futuras, através de desenhos, tais como as pinturas rupestres. No momento em que o Homem atingiu a capacidade de abstração, transmitindo as suas ideias através de símbolos, para comunicar com o seu semelhante, passou a poder codificar a linguagem oral em escrita. Com a constante luta pela sobrevivência, mesmo entre a espécie humana, surgiu a necessidade de transmitir uma mensagem de forma secreta, nascendo assim os códigos.



O Telegrama Zimmermann, como foi enviado da Alemanha para o México.

Quando investigamos sistemas secretos de comunicação, trabalhamos no domínio da Criptologia, palavra que deriva da palavra grega "tratado". Esta ciência divide-se em dois ramos: (1) a Criptografia, palavra que resulta das palavras gregas "oculto" e "escrita", que é a ciência que estuda a estrutura e implementação do sistema de codificação; (2) a Criptanálise, que é a ciência que estuda a segurança dos sistemas, tendo como objetivo principal descodificar os criptogramas – documentos escritos com carateres secretos. Um dos mais antigos criptogramas data do século V a.C. : um mensageiro viajou da Pérsia para a casa de Aristágoras, na Grécia, com uma mensagem tatuada no seu escalpo e quando a sua cabeça foi rapada, e a mensagem descodificada, descobriram que se tratava de uma ordem do sogro de Aristágoras para que este iniciasse uma revolta contra o poder dominante.

Ao longo da história foram usados inúmeros métodos secretos de comunicação. Um dos mais famosos e simples, foi o adoptado por Júlio César, imperador romano, que para comunicar com os seus amigos substituía o valor de cada letra do alfabeto pelo valor da quarta letra seguinte, trocava assim o "a" pelo "d", o "b" pelo "e" e assim sucessivamente. Uma variante deste método ainda é usada hoje em dia pelo movimento escutista. Até nas sagradas escrituras podemos encontrar variantes deste método. Em Jeremias XXV, 26, o profeta escreve Sheshak em vez de Babel, em que a segunda e a décima segunda letra do alfabeto hebraico (B, B, L) do princípio é substituída pela segunda e pela décima segunda letra do fim (SH, SH, K). Carlos I, rei de Inglaterra também escrevia mensagens em linguagem criptográfica, onde as palavras apareciam com as letras trocadas ou com falsas divisões entre as sílabas.

Chegou-se a um ponto na história em que proliferava a transmissão codificada de mensagens, que variava desde uma simples mensagem de amor entre dois namorados secretos, até mensagens de ordem prática e útil de utilização militar. Assim surgiu a necessidade de tentar uniformizar a forma e o método de transmitir secretamente as mensagens, despoletada pelo interesse científico que os vários métodos iam causando na classe dos investigadores. John Trithenius, abade de Spanhein, foi o primeiro escritor em Criptografia, publicando um tratado em 1518 que forneceu todas as bases para os escritores subsequentes, sendo-lhe atribuídas as publicações dos vários volumes "Steganografie", publicados em Lion no ano 1551.

Desde a antiguidade que a história está ponteada de tragédias e de sucessos ligados à utilização de códigos secretos. Por exemplo, em 1894, a descodificação permitiu salvar um inocente. Foi o caso do capitão inglês Dreyfus, acusado de espião, ilibado quando uma mensagem telegráfica do Coronel Panizzardi, adido militar italiano, confirmou que Dreyfus não trabalhava para eles. Também a descodificação do telegrama Zimmermann ocupou o seu lugar na história pois tratava-se de um apelo alemão para que o México se aliasse à Alemanha numa guerra contra os EUA, e que ao ser interceptado contribuiu como fator para a entrada dos Americanos na I guerra mundial. Também durante a I guerra mundial, a Rússia sofria com a constante descodificação de mensagens secretas por parte do exército alemão, situação que se inverteu na II guerra mundial, que deu origem ao mais importante grupo de espiões soviéticos, os designados de "orquestra vermelha". Durante a II guerra mundial, o roubo do código americano "Black Code" permitiu a Rommel, general alemão ser bem sucedido no norte de África, enquanto os ingleses, ao tomarem posse da máquina codificadora alemã, conhecida por Enigma, levou os aliados a inverterem o rumo da guerra a seu favor.

Hoje em dia, os maiores utilizadores de técnicas de codificação e descodificação são entidades civis, embora o seu uso militar ainda seja de importância vital. Das aplicações mais relevantes surge na linha da frente a "assinatura digital" que permite uma identificação única para cada pessoa, substituindo a assinatura manual; os códigos usados na encriptação de dados comunicados pela internet; os códigos usados na segurança dos cartões de débito e crédito, do cartão de cidadão, que permitem a identificação de cada utilizador, evitando a fraude, etc. A complexidade do código depende da sua utilidade e necessidade de segurança. Antes do advento dos computadores, descodificar uma mensagem podia exigir o recurso a muita mão-de-obra humana, mas hoje em dia, já no século XXI, este é um trabalho que cabe aos computadores, que através de algoritmos de descodificação e codificação, criados principalmente por Matemáticos, permite poupar muito tempo, aumentando-se a eficiência e segurança da transmissão das mensagens.

No mundo global em que hoje vivemos, a segurança informática é um problema sempre crescente, requerendo cada vez mais soluções inovadoras. Desde a simples comunicação através de uma rede social, como por exemplo o "twitter", até à troca de informação que existe no mundo dos negócios, são precisos algoritmos cada vez mais complexos, recorrendo cada vez mais ao simples, simpático e mágico número primo, que mantêm a comunicação segura e fora do alcance de intrusos. Para haver uma eficiente segurança na encriptação de mensagens, por exemplo, são usados números primos que ultrapassam os milhares de dígitos. Para poder avaliar-se a magnitude da importância que tem de ser dada à segurança da transmissão de dados, basta pensarmos que atualmente existem mais de 100000 centros de computadores na Europa e nos Estados Unidos, que trabalham dentro do sistema bancário, a comunicarem entre si permanentemente, transmitindo dados críticos e transferindo fundos entre si. Um sistema muito apetecível para as organizações e indivíduos que tentam usurpar algo que não lhes pertence.

Professor do Departamento de Matemática
da Universidade dos Açores
Diretor do Centro de Matemática
Aplicada e Tecnologias de Informação
jcabral@uac.pt