Como partilhar um segredo

António Pereira Rosa
Escola Secundária Maria Amália Vaz de Carvalho
antoniopereirarosa@gmail.com

Os métodos de partilha de segredos têm vindo a adquirir grande importância em organizações como as Forças Armadas e os bancos. Em 1979, o criptógrafo israelita Adi Shamir descobriu um processo de partilha de segredo que recorre apenas a propriedades elementares dos polinómios e dos sistemas de equações lineares, podendo assim ser explicado a alunos do 11º ano.

1. UM SEGREDO A PARTILHAR

Uma base de mísseis nucleares é comandada por um general G, pessoa de absoluta confiança do Governo e que é a única pessoa que conhece o código de lançamento dos mísseis (uma sequência de números *inteiros*, como, por exemplo, $8, -1, 3, 6$). Para impedir que a base seja colocada fora de serviço se o general ficar incapacitado, os seus quatro adjuntos A, B, C e D também têm de conhecer o segredo. No entanto, o grau de confiança que o Governo deposita nestes adjuntos é menor e, para evitar problemas, pretende-se que tenham um conhecimento parcial do segredo, nos seguintes termos:

- nenhum dos adjuntos sabe o código;
- dois quaisquer deles, trabalhando em conjunto, são incapazes de reconstituir o código;
- três quaisquer deles, trabalhando em conjunto, são capazes de reconstituir facilmente o código.

Será possível conceber um tal sistema de partilha do segredo?

Três pessoas podem guardar um segredo se duas delas estiverem mortas.

Benjamin Franklin

2. UMA SOLUÇÃO ELEMENTAR

Vamos apresentar por meio de um exemplo uma solução simples para este problema, baseada em propriedades elementares dos polinómios[1] e que é devida ao criptógrafo israelita Adi Shamir, um dos inventores do famoso sistema RSA (o "S" é de Shamir), que a descreveu em[1], no ano de 1979.

Suponhamos que o código é (4, 5, 7). O general G considera o polinómio $p(x) = 4x^2 + 5x + 7$ e dá a cada um dos adjuntos a informação que consta da seguinte tabela:

Adjunto	Informação [2]
A	$p(0) = 7$
B	$p(1) = 16$
C	$p(2) = 33$
D	$p(3) = 58$

Supomos, é claro, que os adjuntos sabem como funciona o processo, isto é, que o código é (a, b, c), sendo a, b e c os coeficientes do polinómio $p(x) = ax^2 + bx + c$ e que nenhum deles pode descobrir sozinho a informação dada aos outros.

É fácil ver que o sistema apresentado cumpre as condições impostas.

Com efeito, suponhamos que o adjunto B tentava descobrir o código sozinho; de $p(1) = 16$ vem a equação com três incógnitas $a \times 1^2 + b \times 1 + c = 16 \Leftrightarrow a + b + c = 16$ e, como há uma infinidade de valores possíveis para a, b e c, a tentativa falha.

Se dois adjuntos (digamos C e D) trabalharem em conjunto, vem

$$\begin{cases} p(2) = 33 \\ p(3) = 58 \end{cases} \Leftrightarrow \begin{cases} 4a + 2b + c = 33 \\ 9a + 3b + c = 58 \end{cases},$$

sistema este que é indeterminado e a tentativa de descobrir o código falha novamente.

[1] O que está em jogo é o seguinte resultado: "O conhecimento das coordenadas de $n+1$ pontos do gráfico de um polinómio de grau n determina completamente esse polinómio." Assim, uma recta é definida por dois quaisquer dos seus pontos, uma função quadrática por três pontos, uma função cúbica por quatro e assim sucessivamente.

[2] É claro que pode ser dada ao adjunto A apenas a indicação (0, 7), ao adjunto B a indicação (1, 16), etc. Repare-se ainda que nada obriga a que as abcissas dos pontos sejam igualmente espaçadas.

Finalmente, se se juntarem três adjuntos (digamos *B*, *C* e *D*), eles conseguem descobrir facilmente o segredo. Com efeito, obtêm um sistema de três equações com três incógnitas possível e determinado:

$$\begin{cases} p(1) = 16 \\ p(2) = 33 \\ p(3) = 58 \end{cases} \Leftrightarrow \begin{cases} a + b + c = 16 \\ 4a + 2b + c = 33 \\ 9a + 3b + c = 58 \end{cases} \Leftrightarrow \begin{cases} a = 4 \\ b = 5 \\ c = 7 \end{cases}$$

e o código é (4, 5, 7). É fácil de ver que se obtém o mesmo resultado se se escolher outra qualquer das quatro hipóteses possíveis para o conjunto de três adjuntos em colaboração.

O processo descrito por meio deste exemplo é perfeitamente geral, podendo ser aplicado a códigos de qualquer comprimento.

É interessante dar uma interpretação geométrica[3] a este processo: se considerarmos os sistemas apresentados, podemos pensar que a informação dada a cada adjunto é uma equação de um plano no espaço tridimensional usual, correspondendo o segredo às coordenadas do ponto de intersecção. Assim, por exemplo, a tentativa falhada dos adjuntos *B* e *C* anteriormente descrita reflecte apenas que dois planos distintos não podem ter apenas um ponto em comum, têm de ter uma recta.

A interpretação geométrica sugere um refinamento do sistema: em vez de o segredo corresponder às três coordenadas, pode convencionar-se que será apenas uma delas, digamos a cota.

Este refinamento corresponde a "esconder" o código (que será agora um número inteiro) no termo constante de um polinómio conveniente. Vejamos como proceder, recorrendo de novo ao exemplo do general *G* e seus adjuntos com o código (4, 5, 7), que será agora o número "457".

Para tanto, basta seleccionar aleatoriamente dois números para os coeficientes dos termos quadrático e linear do polinómio do segundo grau $p(x) = ax^2 + bx + c$ e atribuir a c o valor 457. Depois, damos a cada um dos três adjuntos o conhecimento do valor de $p(x)$ num ponto conveniente (em zero não, é claro!) e o resto do esquema é igual ao já descrito.

3. VARIANTES DESTE SISTEMA DE PARTILHA DO SEGREDO

Uma primeira observação é a de que o sistema é independente do número de adjuntos: se o general *G* passasse a ter mais dois adjuntos, *E* e *F*, bastaria indicar ao primeiro o valor $p(4) = 91$ e ao segundo o valor $p(5) = 132$ e o sistema funcionaria exactamente da mesma forma.

Uma modificação óbvia diz respeito ao grau do polinómio: se trabalhássemos com um polinómio do terceiro grau, seria fácil construir da mesma forma um sistema em que seria necessário a colaboração de quaisquer quatro adjuntos para reconstituir o segredo. A generalização a graus superiores é imediata.

Descrevemos a seguir uma modificação mais interessante.

No exemplo que demos, todos os adjuntos eram iguais no que diz respeito ao conhecimento do segredo. É fácil modificar o sistema de modo a passar a haver um "adjunto de 1ª classe" (*A*, um brigadeiro) e três "adjuntos de 2ª classe" (*B*, *C* e *D*, coronéis), no seguinte sentido:

- o brigadeiro *A* pode, em colaboração com qualquer dos coronéis, descobrir facilmente o segredo;
- se o brigadeiro não participar, os três coronéis terão de agir em conjunto para obter o código.

É fácil ver que para isto basta distribuir a informação de acordo com a seguinte tabela:

Adjunto e posto	Informação
A, brigadeiro	$p(0) = 7$ $p(1) = 16$
B, coronel	$p(2) = 33$
C, coronel	$p(3) = 58$
D, coronel	$p(4) = 91$

Para simplificar, usámos sempre polinómios de coeficientes naturais ou nulos, sucedendo o mesmo com as abcissas dos pontos. Pode então perguntar-se: por que motivo não nos limitamos a considerar segredos consistindo apenas em sequências de números *naturais*? A resposta é que essa alteração enfraqueceria consideravelmente o sistema, permitindo a um dos adjuntos descobrir sozinho (com algum trabalho…) o código, pelo que deve ser rejeitada.

Para vermos qual é o problema, pensemos no adjunto *B*: ele está na posse da equação $a + b + c = 16$. Se souber que apenas devem considerar-se as soluções *naturais* desta equação, haverá um número finito de códigos possíveis (repare-se que, nesta hipótese, *a*, *b* e *c* serão números naturais inferiores a 16; pode mesmo mostrar-se, por um argumento combinatório[4], que esta equação tem $(16 - 1) \times (16 - 2)/2 = 105$ soluções naturais), e o segredo poderá ser desvendado por tentativas sistemáticas![5] Uma solução alternativa é admitir o uso de

números inteiros negativos nas abcissas dos pontos; assim, os segredos podem ser sequências de números naturais.

4. OBSERVAÇÕES FINAIS

Os esquemas descritos até aqui são elementares e perfeitamente compreensíveis por um aluno do Ensino Secundário; o autor utilizou o esquema de Shamir no tema I de Matemática A do 11º ano para dar um exemplo de aplicação do estudo dos sistemas de três equações com três incógnitas[6]. Há, no entanto, sistemas matematicamente mais sofisticados, como os baseados no Teorema Chinês dos Restos. Muito resumidamente, seja S o segredo, n o número total de adjuntos e k o número mínimo de adjuntos que podem desvendar o segredo trabalhando em conjunto. Seleccionam-se números primos[7] $m_1 < m_2 < \ldots < m_n$ tais que

$$\prod_{i=n-k+2}^{n} m_i < S < \prod_{i=1}^{k} m_i$$

e dá-se ao i-ésimo adjunto o valor s_i que é o resto de S quando dividido por m_i. Resulta do Teorema Chinês dos Restos que o conjunto de condições (sistema de congruências) que se obtém juntando quaisquer k dos adjuntos tem uma solução única, menor do que o produto dos inteiros correspondentes e que é precisamente o segredo pretendido. Para os detalhes e variantes deste esquema, o leitor pode consultar [5], [6] ou [7].

5. REFERÊNCIAS

[1] Shamir, A. (1979), "How to Share a Secret", **Communications of the ACM 22** (11): 612 - 613 (disponível em *http://www.cs.tau.ac.il/~bchor/Shamir.html*).

[2] "Secret Sharing" (artigo na Wikipedia).

[3] Simões Pereira, J. M. S. (2006), "Tópicos de Combinatória", Editora Luz da Vida, Lda., Coimbra.

[4] Silva, J. N. (2009), "Polinómios", *Gazeta de Matemática*, 157, 5-6.

[5] "Secret Sharing with the Chinese Remainder Theorem" (artigo na Wikipedia).

[6] Koblitz, N. (1994), "A Course in Number Theory and Criptography" (2nd edition), Springer-Verlag, New York.

[7] K. Kaya, A. A. Selcuk, Z. Tezcan (2006), "Threshold Cryptography Based on Asmuth-Bloom Secret Sharing", The 21st International Symposium on Computer and Information Sciences (ISCIS 2006). Lecture Notes in Computer Science v. 4263, Springer-Verlag. Istanbul, Turkey (disponível em *http://www.cs.bilkent.edu.tr/~selcuk/publications/ab_ISCIS06.pdf*)

[3] Também em 1979, e independentemente de Shamir, o criptógrafo americano George Blakley descobriu um sistema de partilha de segredo que corresponde essencialmente à versão geométrica que a seguir se apresenta. Para uma descrição deste sistema e suas relações com o sistema de Shamir, veja-se [2].

[4] Veja-se [3], páginas 142 e 144.

[5] Para um exemplo ainda mais pertinente do perigo deste tipo de restrições, veja-se [4].

[6] Uma alternativa à resolução por meio de sistema é a utilização da regressão quadrática para a determinação directa do polinómio; este processo pode ser feito facilmente numa sala de aula recorrendo às calculadoras gráficas existentes no mercado ou a *software* imediatamente disponível, como o *Geogebra*.

[7] Rigorosamente falando, basta que sejam primos entre si dois a dois.

SOBRE O AUTOR

António Pereira Rosa é licenciado em Matemática (1986) e mestre em Matemática para o Ensino (2008) pela Faculdade de Ciências da Universidade de Lisboa. É professor do quadro da Escola Secundária Maria Amália Vaz de Carvalho desde 1994.