Matemática e as mensagens secretas

Alice e Bob vivem isolados e apenas podem comunicar através do correio. Mas sabem que o carteiro lhes lê todas as cartas. Alice tem uma mensagem para Bob e não quer que ela seja lida. Que é que pode fazer? Já pensou em fazer-lhe chegar um cofre com a mensagem, fechado a cadeado. Mas como lhe fará chegar a chave? Não pode enviar-lha dentro do cofre, pois assim Bob não o poderá abrir.

Depois de muito pensar, tem uma ideia. Envia-lhe o cofre fechado com um cadeado. Sabe que Bob é esperto e acabará por perceber a sua ideia. Com mais umas voltas do correio e sem nunca terem trocado chaves, a mensagem chega ao destinatário, que abre o cofre e a lê. *Como é que o leitor acha que resolveram o problema?* Se gosta de desafios lógicos, pare aqui e pense um bocado.

É simples... depois de ser descoberto.

Bob recebe o cofre e fecha-o com um outro cadeado, de que tem a chave. Devolve o cofre a Alice por correio, desta vez fechado com os dois cadeados. Esta remove o seu cadeado, utilizando a chave em seu poder, e faz seguir de novo o cofre por correio. Bob, quando o recebe, apenas tem que utilizar a chave do seu cadeado para abrir o cofre e ler a mensagem. O carteiro fica a ver navios. Esta história relata um velho quebra-cabeças e uma das suas soluções. E inspirou três jovens norte-americanos, Whitefield Diffie, Martin Hellman e Ralph Merkle, a construir em 1976 um sistema de criptografia em que o segredo da comunicação é assegurado por duas chaves, que os intervenientes não trocam entre si. Foi esta invenção que inspirou o sistema RSA, discutido na «Revista» de 8 de Setembro.