Nome: Kelly Ishiara da Silva Nº USP: 10264056

Como a Matemática se tornou tão importante na segurança de dados

Conceito antigo, porém poderoso: a criptografia hoje é questão de preservação ou exposição, sucesso ou fracasso, vida ou morte

O ser humano é um ser social, e nos comunicamos desde que entendemos a capacidade que temos para fazê-lo. Em pleno século XXI, precisamos enviar e receber mensagens a todo instante.

"Criptografia" é uma palavra que vem do grego: "κρυπτός" ("kryptós") significa "escondido" e "γράφειν" ("graphein") significa "escrita", ou seja, é como se fosse uma técnica de transformar uma mensagem escrita claramente (plaintext) para um código secreto, seguro, que possa viajar por servidores de rede e chegar ao destinatário, o único que realmente precisa ler a mensagem. Uma comparação comum é com chaves: a pessoa escreve um texto, tranca-o com essa chave em um algoritmo (que é como se fosse a fechadura) e envia, e só quem vai receber o texto vai poder destrancar seu conteúdo. Parece algo bem simples, mas proteger uma informação é, na maioria das vezes, bem mais difícil que roubá-la.

Figura 1 - Criptografia com importância em escala mundial (Foto: Publicação/Disponível em: https://www.oficinadanet.com.br/artigo/443/o_que_e_criptografia)

A criptografia, além de estar na vida real, já foi filme: "O Jogo da Imitação", de Morten Tyldum, mostra Benedict Cumberbatch como Alan Turing, e o árduo trabalho para conseguir interceptar mensagens dos nazistas durante a Segunda Guerra Mundial. Ou seja, a dificuldade está em encontrar o "código certo" e decifrar o "enigma". Aí entra a matemática: técnicas de Combinatória e Teoria dos Números são muito usadas para criptografar esses textos. De milhares e milhares de possibilidades, qual é o código correto?

A Matemática está em tudo

A menor parcela de informação que um computador pode processar é um "bit" (dígito binário): um valor 0 ou 1. É assim que ele executa suas tarefas e os processos de criptologia.

Voltando a falar de chaves, há dois tipos básicos: simétricas e assimétricas, sendo as assimétricas mais comuns, porque são geradas mais de uma vez (ou seja, mais de uma chave abre a fechadura, mas só o dispositivo certo sabe quais cálculos fazer para ler a mensagem). Às vezes, se fala em "chave de 64 bits" ou "chave de 128 bits", e a "segurança" de um algoritmo costuma ficar em torno de 50% a 100% do número de bits da chave.

Veja este exemplo:

Suponha que você precisa enviar uma mensagem, e escolhe um software com criptografia de ponta-a-ponta (só você e o destinatário saberão o que diz a mensagem). Para codificar, seu computador vai transformar tudo em uma mensagem binária (ela pode ser alterada depois), e a cada dígito, tem duas escolhas possíveis (0 ou 1). Se esse programa ou aplicativo usa uma chave de 64 bits, em um algoritmo que que tem segurança igual à da chave:

Nº de chaves possíveis = 2 x 2 x ... x 2 = 2^{64} = 18.446.744.073.709.551.616

Ou seja, há 18 quintilhões de chaves possíveis! Se o computador de um hacker demorasse 1 segundo para testar cada uma, demoraria apenas 602 milhões de anos.