



Simon Singh

o livro dos códigos

A ciência do sigilo — do antigo Egito à criptografia quântica

Autor de *O último teorema de Fermat*



Resumo de O Livro Dos Códigos

Confrontados com o prospecto da derrota, os criptógrafos Aliados trabalharam dia e noite para decifrar códigos alemães. Parecia que o medo era a força motriz e a adversidade um dos alicerces do sucesso para a decodificação.

O segredo é a alma do negócio e um vício para a humanidade. Desde que passou a se comunicar, o homem tratou de arrumar formas de esconder o verdadeiro significado das mensagens atrás de códigos e palavras dúbias.

Em O Livro Dos Códigos, Simon Singh - autor do bestseller O último teorema de Fermat - descreve a história da arte de escrever segredos desde o Antigo Egito. Singh narra, ainda, a luta entre criadores e decifradores de códigos, começando quinhentos anos antes de Cristo e chegando até hoje, quando a criptografia é usada na Internet e em operações bancárias.

O Livro Dos Códigos analisa a importância e o papel dos códigos nas operações militares, na política e nas intrigas palacianas. O tema central do livro é a batalha entre o bem e o mal -codificadores e decodificadores - analisada, principalmente, nos capítulos sobre a Segunda Grande Guerra.

A criptografia se desenvolveu durante o conflito, quando o sigilo de comunicação se tornou crítico para a corrida pela vitória tanto para os Aliados quanto para o Eixo. Na era da informação, o medo que alimenta o desenvolvimento criptográfico é tanto capitalista quanto pessoal - as grandes corporações necessitam de códigos para assegurar que seus segredos não caiam nas mãos de competidores e pessoas comuns precisam do segredo para executar suas transações e manter suas comunicações de forma privada.

O sigilo é um dos direitos constitucionais garantidos por lei em praticamente toda sociedade livre, a única garantia de segurança enquanto conversas privadas e números de cartões de crédito passeiam pelo mundo através de e-mails e Internet.

O Livro Dos Códigos é uma excelente introdução para os que desejam entender a necessidade humana por privacidade e o desenvolvimento da criptografia e das tecnologias de comunicação. Singh apresenta complexos algoritmos e detalhes matemáticos com um estilo acessível e explicações simplificadas.

O autor faz uma analogia usando a evolução de bactérias como exemplo: assim como os antibióticos precisam ser cada vez mais fortes para vencer a resistência dos novos vírus, as mensagens necessitam de uma codificação cada vez mais a prova de hackers.

Simon Singh mostra, em O Livro Dos Códigos, que a codificação de mensagens torna possível e seguras transações eletrônicas. Apesar de uma ou outra fraude ou quebra de sigilo, o autor prova que o desenvolvimento do segredo nas mensagens e na criptografia faz do uso do cartão de crédito na Web mais seguro que deixar uma carteira dentro de um ônibus.

"Em uma era em que a criptografia está assumindo significado crescente, seu livro traz um perene e envolvente resumo do assunto." - The Economist "O autor de O último teorema de Fermat obteve sucesso em fazer códigos secretos e criptogramas inteligíveis ao leigo.

Os heróis deste absorvente relato são decifradores de códigos, alquimistas lingüísticos cuja obsessiva ocupação com a criptografia através dos tempos mudou o curso da História." - The Observer

[Acesse aqui a versão completa deste livro](#)