# Segurança matemática: da teoria dos números ao hacking e pentesting - A

Data: 2025-09-22 07:58:35

Autor: Inteligência Against Invaders

Diego Bentivoglio**:22 Setembro 2025 07:03**

Quando falamos de cibersegurança, pensamos imediatamente em *firewalls, malware e exploits de dia zero.* Mas há um nível mais profundo, invisível e insuperável: as leis da matemática.

Porque, embora o software possa ser hackeado, os protocolos possam ser contornados, as configurações possam ser confusas, a matemática não possa ser corrompida.

E é justamente nesse pilar que se baseia a cibersegurança moderna.

## Porque segurança é (também) matemática

Toda tecnologia de defesa digital funciona não porque *"Alguém programou bem",* mas porque explora problemas matemáticos que não têm solução eficiente.

Aqui estão alguns exemplos concretos: RSA: Baseia-se na dificuldade de fatorar números de centenas de dígitos. Com os recursos atuais do universo, levaria mais tempo do que a idade do cosmos para resolver o problema. *ECC (criptografia de curva elíptica):* Ele explora a complexidade de logaritmos discretos em curvas elípticas, oferecendo segurança equivalente ao RSA, mas com chaves muito mais curtas.

A segurança não vem de um *"segredo escondido no código",* mas de um axioma matemático: certas operações são fáceis em uma direção, mas proibitivas em outra.

## Hashing: Irreversibilidade Matemática a Serviço da Defesa

Vamos pegar o exemplo do hash. Quando salvamos uma senha, ela nunca é armazenada em texto simples. Ele é passado para uma função de hash *(por exemplo, SHA-256, Argon2 ou Bcrypt-10).* Essas são características fundamentais (matemáticas, não "design").

- Unidirecionalidade: não há como voltar atrás.
- Efeito avalanche: basta mudar um bit e a saída fica completamente diferente.
- Resistência à colisão: Encontrar duas entradas diferentes que produzem o mesmo hash é matematicamente impraticável.

Essas propriedades não são convenções, são resultados decorrentes da matemática que impossibilitam a reversão da operação em um tempo útil.

## Matemática: o escudo que sustenta a Internet

Toda tecnologia de segurança que usamos diariamente é pura matemática disfarçada de software:

- *TLS/SSL (ao visitar um site HTTPS):* criptografia de chave pública e simétrica.
- Blockchain: assinaturas digitais e funções de hash vinculadas.
- Assinaturas digitais: garantindo autenticidade graças a funções matemáticas assimétricas. Sem matemática, tudo isso entraria em colapso.

A segurança cibernética não se trata apenas de ferramentas, explorações e testes de invasão. É sobre teoria dos números, álgebra, funções discretas, logaritmos e probabilidade.

Os hackers mais temidos não são aqueles que sabem como lançar uma ferramenta automatizada, mas aqueles que entendem os números por trás do código.

E é por isso que podemos dizer sem hesitação: **A matemática é uma das linguagens que garante a segurança no ciberespaço.** Se quisermos realmente entender a segurança, devemos primeiro entender a matemática.

**Diego Bentivoglio**
Apaixonado por hacking e segurança cibernética, especialista em testes de penetração, já trabalhei com empresas como Leonardo CAE AJT. Arquiteto de soluções da AWS e entre os 100 maiores hackers BMW 2024 no HackerOne, combino habilidades em infraestrutura e aplicativos da web com uma forte paixão por segurança.

Lista degli articoli