

Criptografia

Relação com a matemática

Ana Carolina, Gustavo, João Augusto, Luca, Nicolas, Nicole e Tábata

Introdução

A palavra "criptografia" vem do grego: "kryptós" = escondido e "gráphein" = escrita.

Trata-se de uma técnica de escrita codificada, em que, apenas o emissor e o receptor da mensagem conseguem interpretá-la. Desde a antiguidade, diversas civilizações buscaram formas de proteger suas comunicações.

Os antigos romanos, por exemplo, utilizavam a criptografia para enviar planos de batalha sem que o inimigo pudesse compreendê-los. Mesmo que a mensagem fosse interceptada, a codificação utilizada era tal que apenas os romanos poderiam decifrá-la.

Conceitos matemáticos, como a teoria dos números e álgebra, são utilizados para desenvolver chaves criptográficas e funções de hash. Por exemplo, a criptografia RSA, baseada na fatoração de números primos, garante que mensagens cifradas permaneçam seguras e indecifráveis sem a chave correta.

Search



Mas como podemos
criptografar uma mensagem
utilizando o conhecimento
matemático?

Mas como podemos criptografar uma mensagem utilizando o conhecimento matemático?

A criptografia está profundamente relacionada à matemática, que utiliza de princípios matemáticos complexos para garantir a segurança da informação. Algoritmos de criptografia, como a cifra de César e o RSA, utilizam operações aritméticas e teóricas dos números, incluindo conceitos como congruência modular, números primos, funções totientes e logaritmos discretos.

- Essas operações matemáticas transformam dados legíveis em códigos cifrados, garantindo que apenas aqueles com a chave correta possam revertê-los ao seu estado original.
- A eficácia da criptografia moderna depende da dificuldade de resolver problemas matemáticos complexos, como a fatoração de grandes números primos, tornando a matemática essencial para a segurança digital.

Conclusão do grupo

Concluimos que a matemática foi fundamental para o desenvolvimento do conhecimento criptográfico ao longo dos tempos e principalmente nos tempos atuais, onde o uso da internet é constante e as grandes informações compartilhadas mundialmente em rede exigem segurança e privacidade. Sendo assim, se faz necessário estratégias que tornem essas codificações mais complexas para que os dados não sejam indevidamente usados, por exemplo, hackers. Contamos com os profissionais matemáticos pra isso.



Mensagem criptografada

```
1 def criptografar(frase, senha):
2     criptografada = ''
3     max_length = len(str(ord(max(frase, key=ord)) * senha))
4     for char in frase:
5         num = ord(char) * senha
6         criptografada += f'{num:0{max_length}}'
7     return criptografada
```



Google Colab

[google.com](https://colab.google.com)

Mensagem descriptografada

Search 🔍

```
9 def descriptografar(criptografada, senha):
10     frase = ''
11     max_length = len(str(ord('z') * senha))
12     for i in range(0, len(criptografada), max_length):
13         num = criptografada[i:i+max_length]
14         try:
15             char = chr(int(num) // senha)
16             frase += char
17         except ValueError:
18             continue
19     return frase
```



Google Colab

[google.com](https://colab.google.com)



Agradecemos pela
atenção!