# Cifras de substuição e troca de chaves

Matemática

Nome: nº: data: 9º ano

**Exercício 1.** A letra mais frequente no português brasileiro é a letra **e**. O texto abaixo é encriptado com a cifra de César, e seu original está em português. Através da análise de frequência das letras que aparecem nele, descubra qual chave foi utilizada para encriptá-lo.[1]

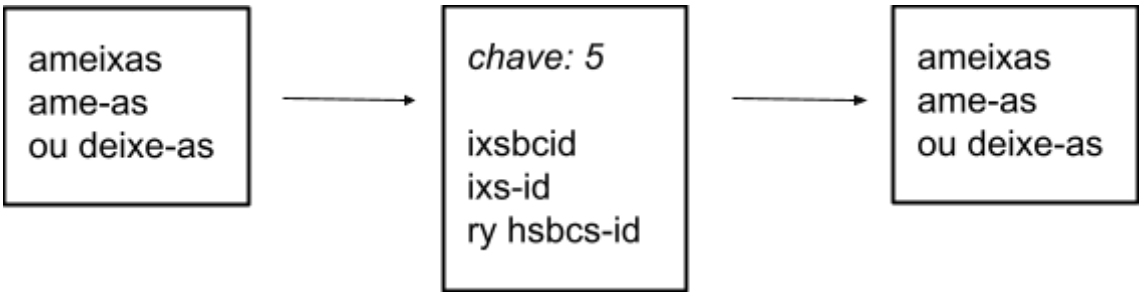
> "H tlyjhkvyph l, hualz kl abkv, bt viqlav lealypvy, bth jvpzh xbl, wlshz zbhz wyvwyplkhklz, zhapzmhg uljlzzpkhklz obthuhz kl xbhsxbly lzwljpl. Xbl lzzhz uljlzzpkhklz aluoht h zbh vypnlt uv lzavthnv vb uh mhuahzph, h zbh uhabylgh lt uhkh hsalyh h xblzahv. Uhv zl ayhah ahv wvbjv hxbp kl zhily jvtv zhv zhapzmlpahz lzzhz uljlzzpkhklz: ptlkphahtlual, zl v viqlav l bt tlpv kl zbizpzalujph, vb pukpylahtlual, zl l bt tlpv kl wyvkbjhv."

## Troca de chaves

Até agora, as técnicas de criptografia que analisamos contam com chaves criptográficas que são conhecidas por quem manda a mensagem e por quem a recebe: o remetente encripta a mensagem usando uma chave e o destinatário decripta a mensagem usando a **mesma chave.** Anteriormente, essas chaves eram compartilhadas presencialmente ou fisicamente. César contaria a um correspondente seu, usando sua voz, qual chave que deveria ser usada entre eles para se comunicarem. Durante a segunda guerra, os Alemães usavam tabelas de códigos a serem usados, um a cada dia, como chave criptográfica para sua comunicação.Na era da internet, isso passa a não fazer mais sentido. Imagine ter que consultar uma tabela de códigos para acessar a *Wikipedia*!

[1] Desafio: decripte esse trecho, revelando o texto original.

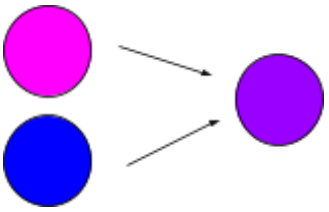
Também não é possível simplesmente enviar uma chave de um computador para o outro. Afinal, uma mensagem como a seguinte não é exatamente segura, certo?



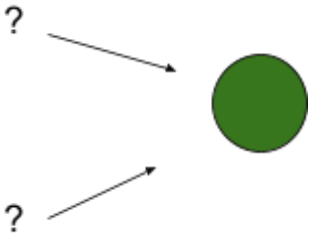

O objetivo da criptografia é que ninguém consiga ler a mensagem privada. Mas se a chave faz parte da mensagem, esse objetivo não é realizado! Fez-se necessário um método para que dois computadores **entrem em acordo** sobre qual chave usar sem que seja necessário enviar a chave junto da mensagem. Um algoritmo que realiza essa tarefa é chamado de **troca de chaves**.

A principal ferramenta para essa técnica são as chamadas **funções de mão única**. São funções fáceis de serem calculadas em uma direção, mas muito difíceis de inverter. Para entender melhor isso, vamos usar uma analogia com cores.

É fácil misturar duas tintas coloridas e formar uma nova cor.



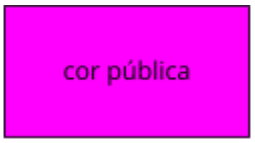
Mas é muito difícil, quiçá impossível, saber quais tintas formam uma cor qualquer.



Usando essa ideia, a troca de chaves acontece da seguinte maneira. Suponha que Alice e Bruno querem estabelecer uma comunicação segura. Primeiro, eles escolhem uma cor pública, que todos podem ver.


Alice Bruno

Em seguida, cada um escolhe uma cor secreta.





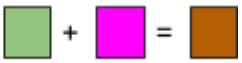
Alice


Bruno

O próximo passo é cada um misturar sua cor secreta com a cor pública.

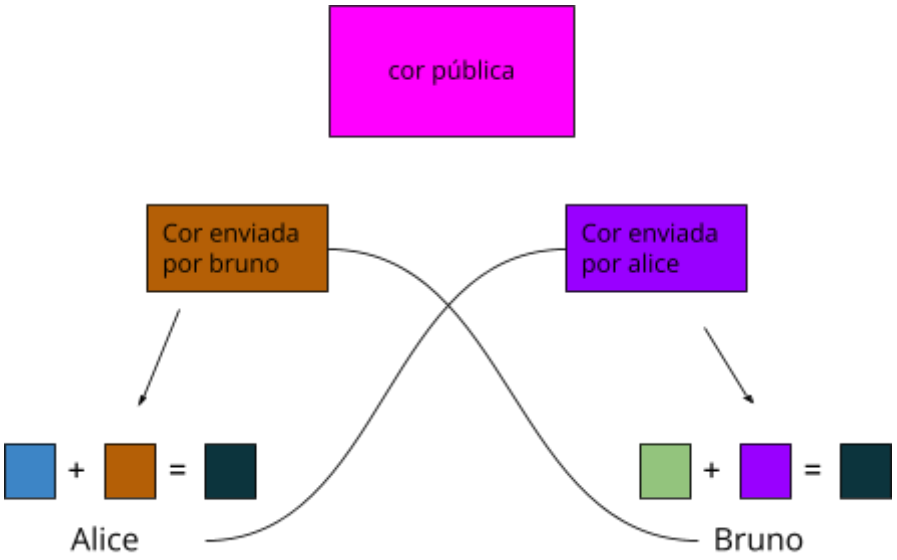


Alice




Bruno

Essa mistura é enviada de um para o outro. Cada um mistura, então, a sua cor secreta com a cor que recebeu do outro.




Pronto! Tanto Alice quanto Bruno chegaram na mesma cor sem nunca divulgar ela, nem a sua cor secreta, para o mundo. Agora podem usar essa cor como chave para sua comunicação criptográfica.

**Exercício 2.**

**a)** Explique porque as cores a que Alice e Bruno chegaram, ao final, são iguais.

**b)** Suponha que existe um algoritmo que funciona como a analogia, mas usa números ao invés de cores. Quando, na analogia, as personagens misturam cores, esse algoritmo **soma** os números. Esse algoritmo é seguro? Ou seja, ele consegue esconder os “números secretos” de cada personagem? Explique qual a relação disso com a ideia de função de mão única.