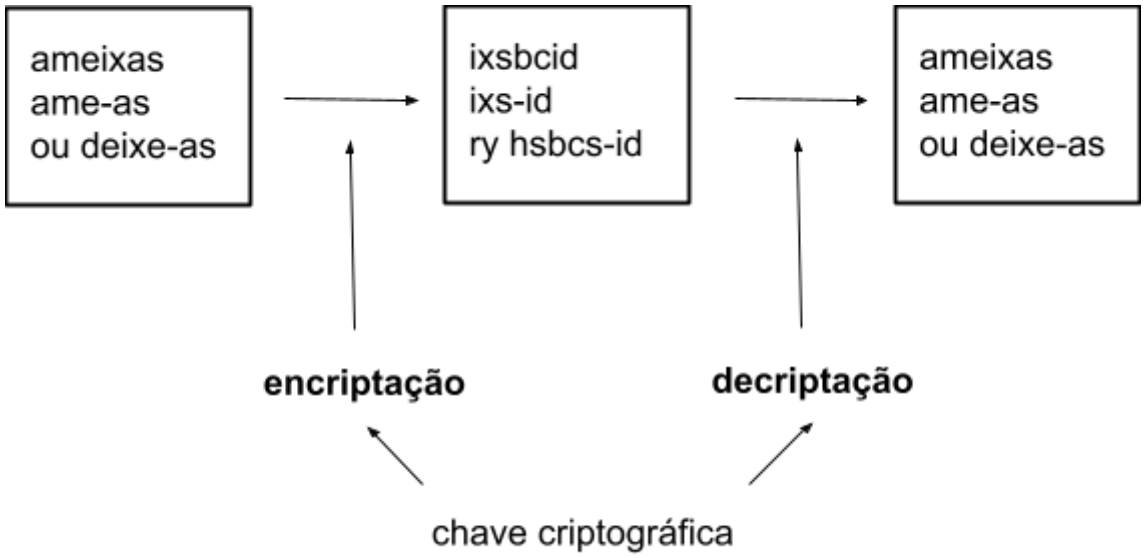
A palavra **criptografia** provém etimologicamente das palavras *kryptós*, "escondido", e *gráphein*, "escrita"[1], o que sugere a ideia de uma “escrita escondida”. A criptografia possibilita que uma mensagem seja enviada sem que qualquer pessoa, a não ser o remetente e o destinatário, consiga lê-la.

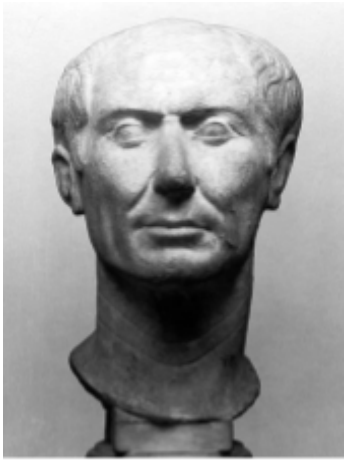
Para tornar uma mensagem secreta, usa-se uma **cifra**: um algoritmo ou procedimento que converte um texto em um texto cifrado. Chamamos essa conversão de **encriptação**. A não ser que se tenha a chave criptográfica que permita reverter a cifra, o texto cifrado é incompreensível. Chamamos essa reversão de **decriptação**.



Há muitas décadas, a teoria e técnicas da criptografia estão intimamente ligadas ao computador e à computação. No entanto, cifras são usadas desde muito antes disso sequer existir: os primeiros usos de criptografia datam do século XX a.C. Muito tempo depois, no primeiro século antes de Cristo, em Roma, um tipo importante de cifra ganharia seu nome.

[1] Pense nas palavras *cripta* e *cartografia*, por exemplo.

Cifra de César



"alea jacta est"

Acredita-se que Júlio César, o político e líder militar romano, usava esse tipo de criptografia em suas correspondências pessoais. Para encriptar suas mensagens, César deslocava cada letra três (por exemplo) posições no alfabeto à frente. Nesse caso, a letra "a", por exemplo, vira "d". A letra "e" vira "h".

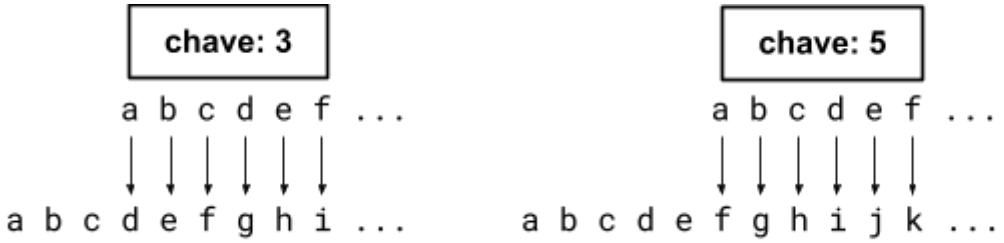
a → d

e → h

o → r

Assim, a aplicação da cifra na mensagem *"brutus"* resulta na palavra *"euxwxv"*. Aqui o número 3 funciona como **chave criptográfica**: o remetente da mensagem deve usar esse número para encriptar a mensagem e qualquer um que queira ler a mensagem deve conhecer esse número para decriptá-la. Se se escolhesse outra chave, por exemplo, o número 5, o texto cifrado seria diferente: "*brutus*" tornaria-se "*gwzyzx*".

Pense que a criptografia é como um **cadeado**. A encriptação é **trancar** o cadeado, e a decriptação é **abri-lo**. Para fazer as duas coisas, precisamos de uma chave. Quem conhece ou tem uma cópia dessa chave consegue abrir o cadeado.



exercício 1.

a) Explique com suas palavras qual deve ser o procedimento de decriptação de uma mensagem encriptada com a cifra de césar usando como chave o número 3.

b) Para usar a cifra de César na chave 3 devemos substituir cada letra por outra, que esteja três posições no alfabeto à frente dela. Mas as letras finais do alfabeto (“x”, “y”, “z”, etc) não têm uma letra “três à frente” delas. O que você faria com elas? Escreva com suas palavras e use um diagrama como o da página anterior para explicar sua solução.

c) Escolha uma chave criptográfica e encripte a seguinte mensagem usando a cifra de César:

> ameixas
> ame-as
> ou deixe-as

d) Sabendo que a chave criptográfica utilizada foi o número 5, decripte a seguinte mensagem: “*fyj yz, gwzyzx?*”

e) Descubra você mesmo a chave e decripte a seguinte mensagem: “*ncxciktn g ujctmdqa*”

f) Descubra a chave e decripte seguinte mensagem (desafio):

> “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.”

***

A cifra de César faz parte de uma classe maior de técnicas chamadas de **cifras de substituição**. Em sua forma mais simples, são cifras que atrelam ao alfabeto convencional um outro alfabeto, chamado alfabeto de substituição, e trocam as letras de um pelo outro. É o que acontece na cifra de César, em que o alfabeto de substituição é o alfabeto comum deslocado para a direita. Outro modo de criar um alfabeto de substituição é escrever alfabeto convencional de trás para frente. Outro exemplo ainda é colocar uma palavra à frente do

alfabeto convencional e excluir do restante dele as letras repetidas. Veja alguns exemplos:

1. abcdefghijklmnopqrstuvwxyz
   defghijklmnopqrstuvwxyz
   cifra de César

2. abcdefghijklmnopqrstuvwxyz
   zyxwvutsrqponmlkjihgfedcba
   cifra de Atbash

3. abcdefghijklmnopqrstuvwxyz
   criptoabdefghjklmnqsuvwxyz

exercício 2.

a) Considere o terceiro exemplo acima. O que pode, nesse caso, ser considerado como chave criptográfica?

b) Crie a sua própria cifra de substituição (sugestão: misture as técnicas já apresentadas). Em seguida, escolha uma palavra ou frase curta para aplicar sua cifra[2].

***

Uma grande desvantagem dessas formas simples de substituição é que a **frequência** com que cada letra aparece é preservada. Em português, a letra “a” é usada com mais frequência que qualquer outra. Se sua cifra traduz “a” para “d”, como nosso primeiro exemplo, então a tendência é que a letra “d” seja a que mais aparece no texto cifrado! Esse fato pode ser usado para descobrir a chave criptográfica e decriptar a mensagem.

Esse raciocínio foi usado no século XVI para desvendar mensagens conspiratórias de Maria da Escócia contra a Rainha Elizabeth, levando à sua execução em 1587.

[2] Quer ver se sua cifra é boa mesmo? Entre nesse site: www.guballa.de/substitution-solver, escolha a língua portuguesa e veja se ele consegue decriptar a sua mensagem!

O advento dos computadores

Os desenvolvimentos na área da computação do século XX fizeram avançar imensamente as técnicas de criptografia — mas também as de **criptoanálise**, ou seja, as técnicas que permitem decriptar uma mensagem mesmo não conhecendo a chave criptográfica.

Uma das primeiras cifras usadas por computadores utilizada em larga escala foi a **DES** (*Data encryption standard*, do inglês "padrão de criptografia de dados"), desenvolvida em 1977 pela **IBM**, uma empresa americana de tecnologia, e pela **NSA**, a agência de inteligência americana. Essa cifra usava uma chave criptográfica binária, ou seja, composta de zeros e uns — ideais para o uso por computadores. De início, essa chave era composta de 56 dígitos binários (*bits)*, ou seja, 56 zeros ou uns. Um exemplo de uma chave usada por essa cifra seria, portanto:

```
10001011100011111110111111110011000110111011010100101100
```

Isso significa que existem 2^{56}chaves diferentes que podem ser usadas pela cifra. Hoje em dia existem computadores que conseguem **testar** todas as chaves possíveis de serem usadas (todas as 2^{56} chaves) em apenas alguns dias. Esse tipo de ataque é chamado de **ataque de força bruta**. Qualquer um com acesso a um computador desse consegue, portanto, quebrar a criptografia da DES. Portanto, ela foi considerada **insegura**.

Em 2001, esse protocolo foi atualizado e renomado para **AES** (*Advanced encryption standard*, do inglês "padrão de criptografia avançado"). O novo protocolo usa chaves de até 256 *bits*. Um exemplo de uma chave dessa é a seguinte:

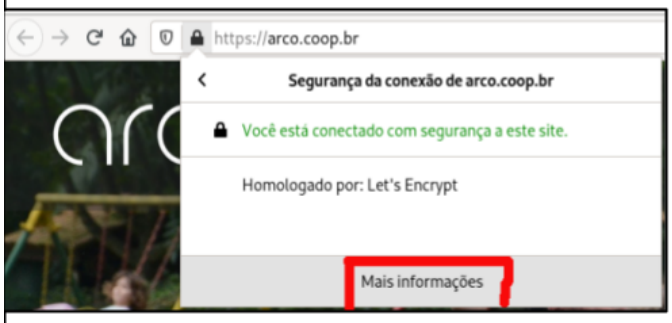
```
1100010101101110111011001110100011011111000011011010001011011000001101111011110111011111111011101001000111001100100111110011111000010001001001101011111010000011100101001101011110001010011101000101001111011010000100100001110100000010010011111001010111000001
```

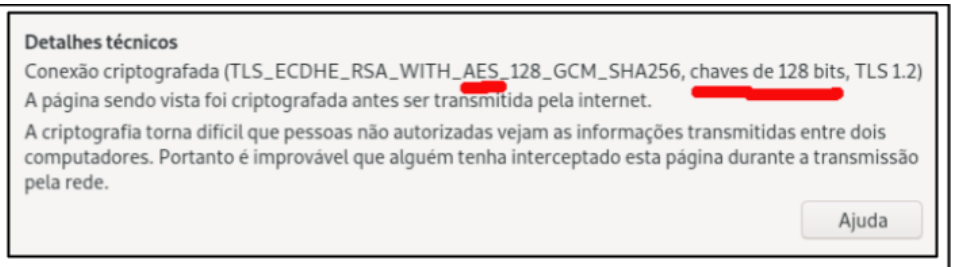
Isso significa que existem 2^{216}chaves diferentes que podem ser usadas pela cifra.

Essa nova versão é considerada segura, tanto é que é usada diariamente no mundo inteiro. Agora mesmo, muito provavelmente, há alguns dados armazenados no seu celular ou computador criptografados com AES; sua conexão wifi é criptografada usando AES; e o seu acesso à internet é quase sempre criptografado com AES.

Quer ver se sua conexão na internet está criptografada mesmo? Nos navegadores de internet modernos (*firefox* e *google chrome*, por exemplo) é possível verificar algumas informações sobre a criptografia. Vamos usar o *firefox* como exemplo. Clique no pequeno cadeado ao lado do endereço do site para mais informações:

Parece que o site da Arco usa conexões criptografadas! Vamos ver mais informações...





Nessa caixa de informações, podemos ver que de fato estou usando o padrão AES, com uma chave de 128 bits, para criptografar todo o tráfego do meu computador com o site da Arco! Se não houver criptografia, o navegador avisa com um cadeado riscado ou aberto:

Evite compartilhar informações pessoais e senhas em sites que não usam criptografia. Algum agente malicioso espionando o seu tráfego poderá ficar sabendo essas informações.

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: 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

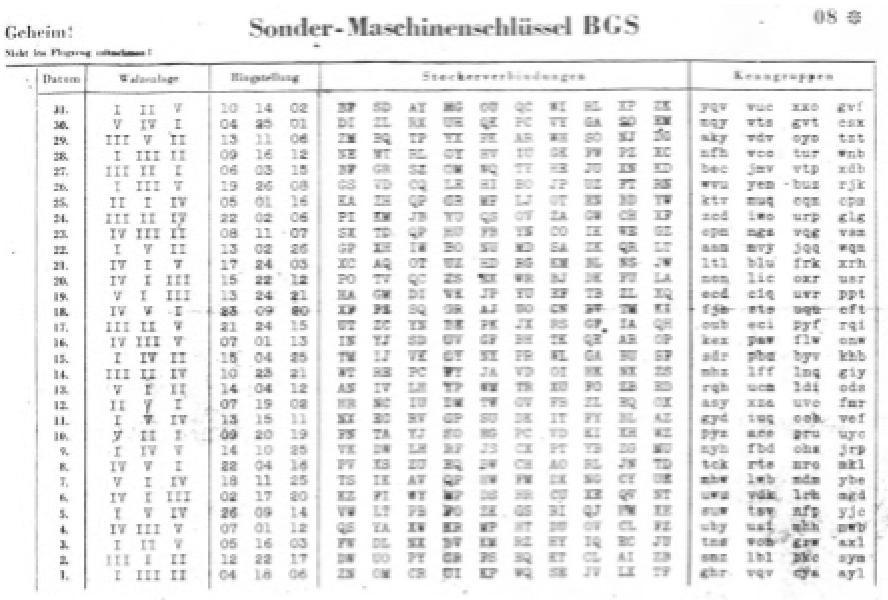
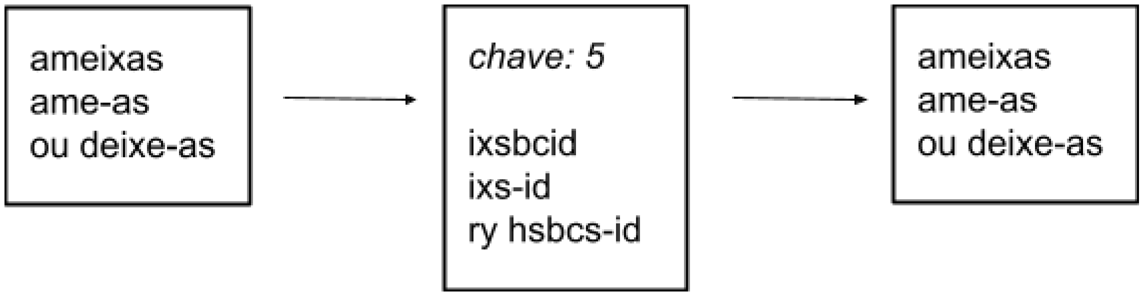


Tabela de chaves usada pelos alemães na segunda guerra mundial

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*!

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?

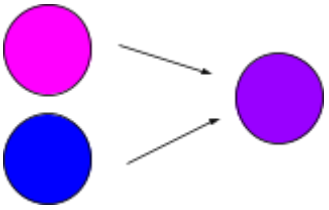


O objetivo da criptografia é que ninguém consiga ler a mensagem privada. Mas se a chave faz parte da mensagem, esse objetivo não é

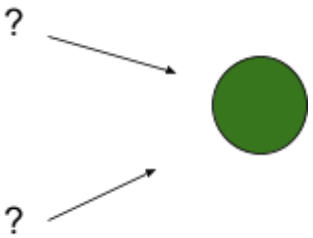
realizado! Fez-se necessário um método para que dois computadores **entrem em acordo** sobre qual chave usar sem que seja necessário enviar a chave junto da mensagem. Um algoritmo que realiza essa tarefa é chamado de **troca de chaves**.

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.

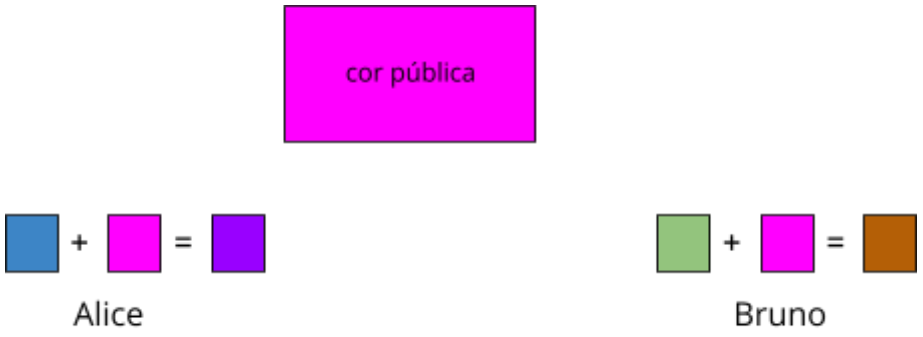


Usando essa ideia, a troca de chaves acontece da seguinte maneira. Suponha que Alice e Bruno querem estabelecer uma comunicação segura. Primeiro, eles escolhem uma cor pública, que todos podem ver.

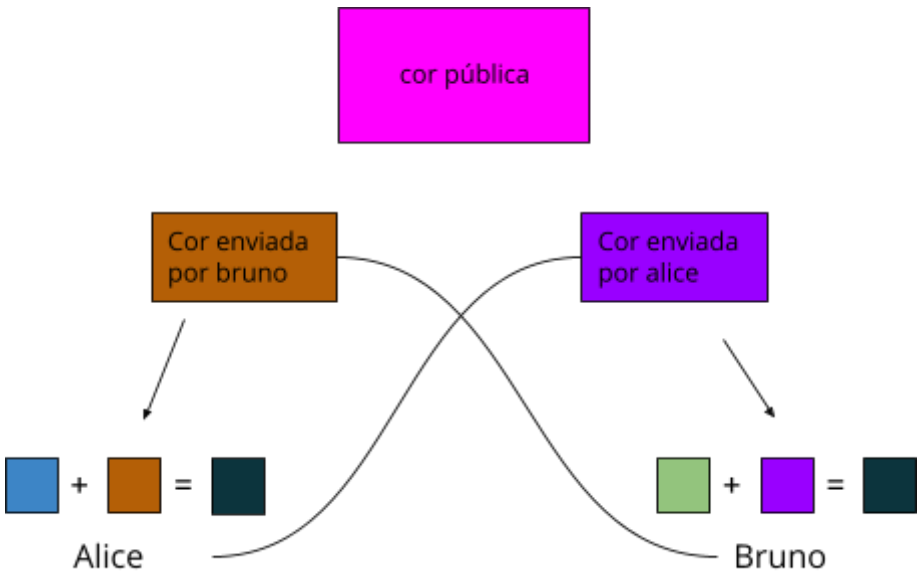
Alice Bruno

Em seguida, cada um escolhe uma cor secreta.

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



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 3.

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.

***

Conclusão

Os conceitos apresentados aqui são uma introdução ao assunto da criptografia. Para uma introdução mais completa, faltou mencionar os conceitos de chave simétrica e chave assimétrica, com o qual poderemos entender a criptografia de aplicativos como o *Whatsapp* e *Signal* e o protocolo PGP. A quem interessar, deixo alguns links.

- Essa atividade foi inspirada nesse vídeo:
  youtube.com/watch?v=jhXCTbFnK8o
  que não tem legenda, infelizmente, e nesse material:
  wiki.imesec.ime.usp.br/books/criptografia
- Materiais sobre chave simétrica e assimétrica:
  youtube.com/watch?v=AQDCe585Lnc (legendado)
  youtube.com/watch?v=GSIDS_lvRv4 (sem legenda)
  pt.wikipedia.org/wiki/Criptografia_de_chave_p%C3%BAblica