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.

A cada letra da mensagem cifrada deve-se substituir a letra que está 3 posições antes no alfabeto. O texto resultante é a mensagem decriptada.

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.

Eu “daria a volta” e começaria o alfabeto de novo. Assim o “x” vira “a”, o “y” vira “b” e assim por diante.

```
abcdefghijklmnopqrstuvwxyz
defghijklmnopqrstuvwxyzabc
```

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

ameixas
ame-as
ou deixe-as

Escolhemos a chave 5.

frjncfx
frj-fx
tz ijncj-fx

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

Até tu, brutus?

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

Sharkboy e lavagirl

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."

***

exercício 2.

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

Nesse caso existe um procedimento ou algoritmo para a criptografia: colocar uma palavra antes do alfabeto e excluir as letras que aparecem repetidas depois dessa palavra. Com isso, a chave de criptografia fica bem definida: é a palavra escolhida para ser colocada à frente do alfabeto.

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[1].

***

exercício 3.

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

[1] 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!

Alice e bruno misturaram as mesmas cores, porém em ordem diferente: a cor secreta do Bruno, a cor secreta da Alice e a cor pública. Logo, a cor resultante é a mesma.

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.

Não é seguro, pois qualquer um que intercepte as mensagens enviadas poderá ver o número público e os números enviados por Alice e Bruno. Mas o número enviado por Bruno é igual a seu número secreto mais o número público. Ora, ao atacante só é necessário subtrair o número público do número enviado por Bruno para obter o número secreto de Bruno. Analogamente para o número secreto de Alice. Logo, somando os números secretos e o público, o atacante teria acesso à chave criptográfica. Isso porque a soma não é uma função de mão única.