

Atividade 0 - Criptografia

Matemática



Nome:

nº:

data:

9º ano

Exercício 1.

a) Escolha uma frase curta e encripte-a usando a cifra de César com chave 10.

b) A seguinte frase foi encriptada usando a cifra de César usando chave 8. Decripte-a, revelando o texto original.

“ITMI RIKBI MAB”

c) O texto abaixo foi criptografado com a cifra de César. Descubra qual foi a chave utilizada, sabendo que ele está em português (não precisa decriptar o texto todo).

“hzn abvgr qrfgnf, ivaqb qn pvqnqr cnen b ratraub abib, rapbagerv ab gerz qn prageny hz encnm ndhv qb onveeb, dhr rh pbaurpb qr ivfgn r qr puncrb. pbzcevzragbh-zr, fragbh-fr nb cr qr zvz, snybh qn yhn r qbf zvavfgeb, r npnobh erpvgnaqb-zr irefbf. n ivntrz ren phegn, r bf irefbf cbqr fre dhr anb sbffrz vagrvnzragr znhf. fhpprqrh, cberz, dhr pbzb rh rfgnin pnapnqb, srpurv bf byubf gerf bh dhngéb irmrf; gnagb onfgbh cnen dhr ryyr vagreebzcrffr n yrvghen r zrggrffr bf irefbf ab obyfb”

Exercício 2.

Durante as aulas, vimos alguns exemplos de cifra de substituição.

1. abcdefghijklmnopqrstuvwxyz
defghijklmnopqrstuvwxyzabc

cifra de
César

2. abcdefghijklmnopqrstuvwxyz
zyxwvutsrqponmlkjihgfedcba

cifra de
Atbash

3. abcdefghijklmnopqrstuvwxyz
criptoabdefghjklmnqsuvwxyz

cifra de
palavra-
chave

Cláudio tentou inventar sua própria cifra de substituição. Observe o resultado a que ele chegou:

abcdefghijklmnopqrstuvwxyz
torrefghijklmnpqsuvwxyzabc

- a) Explique com suas palavras qual é o procedimento inventado por Cláudio para formar o alfabeto na linha de baixo. Identifique qual é a chave utilizada.
- b) A chave utilizada por Cláudio, nesse caso, tem um problema. Que problema é esse?
- c) Faça como Cláudio e invente a sua própria cifra. Pode ser uma cifra de substituição ou não. Seja criativo! Em seguida, descreva como sua cifra funciona e dê um exemplo, criptografando a seguinte frase:

“A ponte não é sustentada por esta ou aquela pedra, mas pela curva do arco que estas formam”

Exercício 3. Releia a seção “troca de chaves” da ficha da aula do dia 22/02. Em seguida, responda: qual é a importância da ideia de “função de mão única” para que o procedimento de troca de chaves descrito funcione com segurança? O que um agente malicioso teria que fazer para descobrir os segredos da conversa se fosse possível **reverter** a mistura de cores?