Lista de exercícios: Criptografia Clássica

Prof. Gabriel Rodrigues Caldas de Aquino

Compilado em:
April 3, 2026

1 Cifra de César

Instruções: Decifre a mensagem abaixo, que foi cifrada usando uma Cifra de César com k=5.

Ufwfgjsx athj ijxhtgwnz f kwfxj

Observação: Considere o alfabeto inglês de 26 letras (A-Z).

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

Responda

- O tamanho do conjunto de chaves possíveis para a Cifra de César é um problema? Explique.
- Apesar de trocar as letras da frase, a cifra de césar ainda mantém a frequência das letras. Qual é o problema disso? Explique.

2 Cifra Monoalfabética

Background: A cifra monoalfabética usa uma permutação completa do alfabeto como chave. Cada letra do texto claro é substituída por uma letra correspondente no alfabeto cifrado.

Exemplo de chave:

Texto claro	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Chave	Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

Tarefa: Considerando a chave acima, encripte a frase: *Chegamos na Sexta Feira*

Responda

- Qual o avanço da Cifra Monoalfabética para a cifra de césar? Explique.
- Apesar do avanço, qual problema ainda persiste nessa cifra em relação à Cifra de César? Explique.

3 Cifra de Substituição Simples com Frase-Chave

Motivação: Um modo de solucionar o problema de distribuição de chave é usar uma linha de um livro que o emissor e o receptor possuem. Normalmente, pelo menos em romances de espionagem, a primeira sentença de um livro serve como chave. O esquema em particular discutido neste problema é de um dos melhores romances de suspense envolvendo códigos secretos, *Talking to Strange Men*, de Ruth Rendell.

Descrição: Na Cifra de Substituição Simples, cada letra do texto plano é substituída por outra letra, usando um **alfabeto substituto** gerado a partir de uma frase chave.

Passos:

1. Escolher uma chave (frase).
2. Remover letras repetidas, mantendo apenas a primeira ocorrência.
3. Completar o alfabeto com as letras que não apareceram na chave.

Exemplo:

- Chave: `segurança da informação`
- Alfabeto cifrado: `s, e, g, u, r, a, n, c, d, i, f, o, m, b, h, j, k, l, p, q, t, v, w, x, y, z`

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
s	e	g	u	r	a	n	c	d	i	f	o	m	b	h	j	k	l	p	q	t	v	w	x	y	z

Tarefa: Descubra a frase: `SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA`

Chave: *"the snow lay thick on the steps and the snowflakes driven by the wind looked black in the headlights of the cars"*

Curiosidade: Essa chave é a primeira sentença de *The Other Side of Silence.*

Passo a passo da resolução:

1. *Remover letras repetidas da frase da chave, mantendo a primeira ocorrência.*
2. *Completar com as letras faltantes do alfabeto (q, z, m, j) em ordem alfabética*

4 Cifra de Playfair

A Cifra Playfair foi o sistema de campo padrão do Exército britânico na Primeira Guerra Mundial. Além disso, ainda foi usada pelo Exército dos EUA e forças aliadas na Segunda Guerra Mundial.

Considerando a cifra de playflair, use a chave **PROBLEMS** para criar a tabela abaixo e Use a tabela para encriptar a frase: **SHE WENT TO THE STORE**

P	R	O	B	L
E	M	S		

Para isso, faça o seguinte:

1. Divida a frase em grupos de duas letras
2. Verifique se há letras duplicatas no mesmo grupo - se tiver use uma outra letra que não tenha duplicata para separar (ex. sempre que uma letra repetida acontecer insira Q entre elas)
3. Se a última letra ficar sozinha, também adicione uma letra sem duplicata (Se você usou o Q, use nesse caso também)

Lembre-se das regras pra encriptação:

1. **Letras na mesma linha da matriz:** Substituir cada letra pela à direita, de forma rotativa.
2. **Letras na mesma coluna da matriz:** Substituir cada letra pela abaixo, de forma rotativa.
3. **Caso geral (retângulo):** Cada letra do par é substituída pela letra na sua linha e na coluna da outra letra do par.

Responda

- Qual a motivação para a cifra Playfair? Explique.
- Apesar do avanço, a cifra Playfair ainda deixa rastros da estrutura da linguagem do texto claro? Explique.

5 Cifra de Vigenère

A Cifra de Vigenère é uma cifra **polialfabética**, onde diferentes substituições ocorrem ao longo da mensagem usando um conjunto de regras de substituição monoalfabéticas. Nesse caso, uma **chave** define qual regra é aplicada a cada posição da mensagem. Na cifra Vigenère, caractere do texto claro é cifrado com uma cifra de César diferente, determinada pela letra da **chave**.

Considere a chave: **VULNERABILIDADE**

Encripte a mensagem: **"Fomos descobertos fujam agora"**

Responda

- Na cifra de Vigenère, cada letra do texto claro pode gerar múltiplas letras cifradas dependendo da letra correspondente da chave. Diga como isso pode acontecer e qual a vantagem disso.
- Apesar das vantagens do uso da Cifra de Vigenère, ainda existem problemas. Quais são eles?

6 Criptoanálise

A **criptoanálise** é o uso de técnicas para decifrar uma mensagem sem conhecimento prévio da chave ou do método usado. Pode ser visto como o famoso "quebrar o código". O texto cifrado a seguir é em inglês e foi gerado usando um algoritmo de substituição simples:

```
53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;;]8*;:‡*8†83
(88)5*†;46(;88*96*?;8)*‡(;485);5*†2:*‡(;4956*2(5*-4)8¶8*
;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡1;48†85;4)485†528806*81
(‡9;48;(88;4(‡?34;48)4‡;161;:188;‡?;
```

Tarefa: Crie um algoritmo (em qualquer linguagem ou pseudocódigo) que faça a criptoanálise do texto acima e descubra a mensagem original.