

## Exercícios de fixação 11 - Criptografia

Entrega	1 dez em 23:59	Pontos	1	Perguntas	4	Disponível até	1 dez em 23:59	Limite de tempo	Nenhum
---------	----------------	--------	---	-----------	---	----------------	----------------	-----------------	--------

## Instruções

Este questionário contém questões sobre métodos e técnicas de criptografia.

## Histórico de tentativas

	Tentativa	Tempo	Pontuação
MAIS RECENTE	Tentativa 1	5 minutos	0,5 de 1

Pontuação deste teste: **0,5** de 1  
Enviado 27 nov em 20:37  
Esta tentativa levou 5 minutos.

Você respondeu

Pergunta 1

0 / 0,25 pts

Qual é o resultado da cifraem por meio da Cifra de Vigenère para a seguinte mensagem:

PROVA NA SEGUNDA FEIRA

Observações:

- Mantenha os espaços como espaços (eles não devem ser cifraados e não devem ser considerados no processamento da chave)
- Considere a seguinte chave criptográfica: **NOTAS**

CFHS AO LEYHBWA XRWKA

Respostas corretas

cfhvs\_ao\_leyhbwa\_xrwka

CFHVS AO LEYHBWA XRWKA

cfhvs ao leyhbwaxrwka

cfhvsaoleyhbwxrwka

Usando a tabela passada nos slides, chegaremos ao seguinte resultado:

PROVA NA SEGUNDA FEIRA  
NOTAS NO TASNOTA SNOTA  
CFHVS AO LEYHBWA XRWKA

Você respondeu

Pergunta 2

0 / 0,25 pts

Qual é o resultado da cifraem por meio da Cifra das Colunas para a seguinte mensagem:

PROVA NA SEGUNDA FEIRA

Observações:

- Os espaços devem ser incluídos na cifraem, isto é, eles também mudarão de posição.
- Considere a seguinte chave criptográfica: **NOTAS**

VSDRPNFGRUAOVNIEAAEE

Respostas corretas

V NEP EARRNG AASDIOAUF

A seguinte tabela será construída:

2 3 5 1 4  
N O T A S  
-----  
P R O V A  
N A S  
E G U N D  
A F E I  
R A

O seguinte resultado será gerado:

V NEP EARRNG AASDIOAUF

Correto!

Pergunta 3

0,25 / 0,25 pts

O que é uma cifra de substituição polialfabética?

☐ É uma cifra que pode ser aplicada a dados de qualquer idioma, independentemente do seu conjunto de caracteres.

☐ É uma cifra em que um caráter passa pelo processo de substituição mais de uma vez.

☐ É uma cifra que considera todos os caracteres do alfabeto Unicode nas substituições.

☒ É uma cifra em que um caráter pode ser substituído por caracteres diferentes dependendo da sua posição.

Uma cifra monoalfabética faz sempre a mesma subsituição. Assim, se um 'A' é substituída por 'D', então todas as ocorrências de 'A' serão sempre substituídas por 'D'. Em uma cifra polialfabética, cada 'A' pode ser substituído por um símbolo diferente.

Correto!

Pergunta 4

0,25 / 0,25 pts

Qual algoritmo baseado no DES usa 2 chaves diferentes em três ciclos de cifraem/decifragem?

☒ 2TDES

☐ O próprio DES

☐ Twofish

☐ 3TDES

O algoritmo que trabalha com três ciclos de cifraem/decifragem DES é o TDES (Triple DES). Esse algoritmo pode trabalhar com 3 chaves diferentes (3TDES) ou com 2 chaves diferentes (2TDES). Nesse caso, a chave  $K_1$  será usada no primeiro e terceiro ciclos e a chave  $K_2$  será usada no segundo ciclo.

Pontuação do teste: **0,5** de 1

◀ Anterior

Próximo ▶

Detalhes do envio:	
Tempo:	5 minutos
Pontuação atual:	0,5 de 1
Pontuação mantida:	0,5 de 1