

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	103 minutos	0,75 de 1

Pontuação deste teste: **0,75** de 1
Enviado 1 dez em 22:36
Esta tentativa levou 103 minutos.

Correto!

Pergunta 1

0,25 / 0,25 pts

Qual das seguintes características se aplica às cifras de bloco?

☐ Vulnerabilidade a modificações.

☒ Baixa velocidade.

☐ Baixa difusão.

☐ Baixa propagação de erros.

Pergunta 2

0 / 0,25 pts

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

PROVA NA SEGUNDA FEIRA

Observações:

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

Você respondeu

VSERP NGFRAUIAEARO N A

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

Pergunta 3

0,25 / 0,25 pts

O que é uma cifra de substituição polialfabética?

Correto!

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

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

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

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

Uma cifra monoalfabética faz sempre a mesma substituição. 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.

Pergunta 4

0,25 / 0,25 pts

Qual dos seguintes algoritmos criptográficos de chave simétrica trabalha com a manipulação (substituição, permutação, ...) de bytes ao invés de bits?

☐ 3TDES

☐ DES

☒ AES

☐ 2TDES

Correto!

Entre os algoritmos listados, apenas o AES trabalha com bytes inteiros. Os demais, todos baseados no DES, fazem substituições e permutações bit a bit. O AES organiza cada bloco de 128 bits como uma matrix 4x4 de bytes.

Detalhes do envio:	
Tempo:	103 minutos
Pontuação atual:	0,75 de 1
Pontuação mantida:	0,75 de 1

Pontuação do teste: **0,75** de 1