Exercícios de fixação 12 - Algoritmos criptográficos

- Entrega 26 mai em 23:59
- Pontos 1
- Perguntas 4
- Disponível até 26 mai em 23:59
- Limite de tempo Nenhum

Instruções

Este questionário contém questões sobre os algoritmos de criptografia.

Este teste foi travado 26 mai em 23:59.

Histórico de tentativas

	Tentativa	Tempo	Pontuação
MAIS RECENTE	Tentativa 1	17 minutos	1 de 1

ⓘ As respostas corretas não estão mais disponíveis.

Pontuação deste teste: 1 de 1
Enviado 26 mai em 18:14
Esta tentativa levou 17 minutos.

Pergunta 1
0,25 / 0,25 pts

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

- O próprio DES
- Twofish
- 3TDES
- 2TDES

O algoritmo que trabalha com três ciclos de cifragem/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.

Pergunta 2
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

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.

Pergunta 3
0,25 / 0,25 pts

Indique qual é o algoritmo a que corresponde a característica apresentada.

O número de rodadas é variável, de acordo com o número de bits na chave.

AES

Usa 16 rodadas de cifragem em todo o processo.

DES

Repete três vezes o ciclo de rodadas.

TDES

As rodadas dos algoritmos apenas repetem um processo de cifragem que é considerado o seu núcleo. No DES, há 16 rodadas usando a estrutura de Feistel. No TDES, aplica-se três vezes o DES, na sequência de cifragem, decifragem e recifragem, cada uma com uma chave específica. Já o AES faz um número variável de rodadas (em função do número de bits da chave) e, em cada rodada, aplica uma variante da cifragem de blocos de Rijndael.

Pergunta 4
0,25 / 0,25 pts

Qual o tamanho da chave de rodada do AES?

- 256 bits
- Tamanho variável
- 64 bits
- 192 bits
- 32 bits
- 128 bits

O AES usa, em cada rodada, uma chave de 128 bits, composta por 4 palavras de 32 bits. Como ele trabalha sempre com bytes, podemos dizer que a chave de rodada tem 4 palavras de 4 bytes.

Pontuação do teste: 1 de 1