

Lista de Exercícios 6

Nesta lista, iremos exercitar a utilização de um algoritmo de criptografia. Utilizaremos o algoritmo “Blowfish”. Este algoritmo utiliza cifragem de bloco de 64 bits. Nestes exercícios, utilize o esquema de preenchimento de bloco “PKCS#5” para todos os casos desta lista. Utilize também como chave a sequência de bytes [65, 66, 67, 68, 69].

As questões pedem para você exibir o conteúdo do texto cifrado. Apresente o conteúdo em formato hexadecimal e separando cada byte por um espaço em branco, além de quebrar a saída a cada 8 bytes. Exemplo de saída:

```
10 98 1F E3 00 9F 1F E0
AB 75 92 17 9C 36 1C C7
AF 8E B3 90 B7 9E BC 8E
```

Crie um programa para as questões abaixo. Submeta no AVA o programa que você construiu, bem como as respostas às perguntas das questões.

Caso 1

Criptografe o texto “FURB” usando o modo de operação “ECB”.

- 1.1. Qual o conteúdo do texto cifrado (em hexadecimal)?
- 1.2. Qual a extensão (quantidade de caracteres) do texto cifrado?

Caso 2

Criptografe “COMPUTADOR” e o modo de operação “ECB”.

- 2.1. Qual o conteúdo do texto cifrado (em hexadecimal)?
- 2.2. Qual a extensão do texto cifrado?
- 2.3. Por que o texto cifrado tem tal tamanho?

Caso 3

Criptografe “SABONETE” e utilize o modo de operação “ECB”.

- 3.1. Qual o conteúdo do texto cifrado (em hexadecimal)?
- 3.2. Qual a extensão do texto cifrado?
- 3.3. Por que o texto cifrado tem tal tamanho?

Caso 4

Criptografe a sequência de bytes [8, 8, 8, 8, 8, 8, 8, 8] utilizando o modo de operação ECB.

- 4.1. Qual o conteúdo do texto cifrado?
- 4.2. Compare os primeiros 8 bytes do texto cifrado com o último bloco cifrado da questão anterior. Que conclusão é possível obter?

Caso 5

Criptografe o texto “SABONETESABONETESABONETE” e utilize o modo de operação “ECB”.

- 5.1. Qual o conteúdo do texto cifrado (em hexadecimal)?
- 5.2. Qual a extensão do texto cifrado?
- 5.3. Avalie o conteúdo do texto cifrado. Que conclusão é possível obter a partir do texto cifrado e do texto simples?

Caso 6

Criptografe o texto “FURB” e agora utilize o modo de operação “CBC”.

- 6.1. Qual o conteúdo do texto cifrado (em hexadecimal)?
- 6.2. Tente decifrar o texto cifrado, para recuperar o texto simples. O que acontece?

Caso 7

Criptografe o texto “FURB”, utilizando o modo de operação “CBC”. Estabeleça que o vetor de inicialização seja constituído dos bytes: 1, 1, 2, 2, 3, 3, 4, 4.

7.1. Qual o conteúdo do texto cifrado?

Caso 8

Criptografe o texto "SABONETESABONETESABONETE" e utilize o modo de operação "CBC". Defina o vetor de inicialização constituído dos bytes 1, 1, 2, 2, 3, 3, 4, 4.

8.1. Qual o conteúdo do texto cifrado (em hexadecimal)?

8.2. Compare o texto cifrado com aquele obtido no caso 5 e apresente uma conclusão desta comparação.

Caso 9

Criptografe o texto "SABONETESABONETESABONETE" e utilize o modo de operação "CBC". Defina o vetor de inicialização constituído dos bytes 10,20,30,40,50,60,70,80.

9.1. Qual o conteúdo do texto cifrado?

9.2. Compare o texto cifrado com o que foi obtido no caso 8 e apresente conclusão sobre a comparação.

9.3. A partir do resultado de 9.2, descriptografe a mensagem usando o vetor de inicialização constituído dos bytes 1, 1, 2, 2, 3, 3, 4, 4. Qual a conclusão que você atinge?

Caso 10

Criptografe o texto "FURB" usando o modo de operação "ECB". A partir do texto cifrado obtido, tente decifrá-lo utilizando a chave "11111". Explique o resultado.

Caso 11

Utilizando a chave "ABCDE", criptografe o arquivo PDF que foi publicado para este exercício, salvando-o em disco com o nome "saida.bin". Utilize o modo de operação ECB.

11.1. Qual o tamanho em bytes dos dois arquivos?

Caso 12

Descriptografe o arquivo saida.bin, que você gerou anteriormente. Utilize a chave "ABCDE" e o modo de operação ECB. Salve o arquivo com o nome "descriptografado.pdf". Tente abrir o arquivo.