

## Lista de Exercícios 07

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 caracteres “ABCDE”.

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

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

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

### Caso 5

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

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

### Caso 6

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.

- 6.1. Qual o conteúdo do texto cifrado?

### Caso 7

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.

- 7.1. Qual o conteúdo do texto cifrado (em hexadecimal)?
- 7.2. Compare o texto cifrado com aquele obtido no caso 4 e apresente uma conclusão desta comparação.



#### **Caso 8**

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.

8.1. Qual o conteúdo do texto cifrado?

8.2. Compare o texto cifrado com o que foi obtido no caso 7 e apresente conclusão sobre a comparação.

8.3. A partir do resultado de 8.2, decriptografe 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 9**

9.1. 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.