Lista 07

João Henrique Cardoso Bragantino

**Caso 1**

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

Texto cifrado: 2513f7a5d3e00e8c

Extensão: 16

**Caso 2**

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

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

f34739ab7634c4efe50ff1b554856572

**2.2. Qual a extensão do texto cifrado?**

16 bytes

**2.3. Por que o texto cifrado tem tal tamanho?**

Porque na criptografia blowfish os blocos cifrados são formados sempre por 64 bits (8 bytes), o que significa que o tamanho do texto cifrado será um múltiplo de 8 bytes.

**Caso 3**

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

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

841091472604b96acdbc3e2fefa73bdd

**3.2. Qual a extensão do texto cifrado?**

16 bytes

**3.3. Por que o texto cifrado tem tal tamanho?**

Por que o esquema de preenchimento de bloco PKCS#5 adiciona mais 8 bytes para completar um bloco de 64 bits (8 bytes).

**Caso 4**

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

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

841091472604b96a841091472604b96a841091472604b96acdbc3e2fefa73bdd

**4.2. Qual a extensão do texto cifrado?**

32 bytes

**4.3. Avalie o conteúdo do texto cifrado. Que conclusão é possível obter a partir do texto cifrado e do texto simples?**

O esquema de preenchimento adicionou mais 8 bytes para formar o conjunto de blocos a serem criptografados

**Caso 5**

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

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

579d4e7333d43ab5

**5.2. Tente decifrar o texto cifrado, para recuperar o texto simples. O que acontece?**