**Exercício 1**

**a)**

C = 10010111

K = 01100111

------------------

M = 11110000

**b)**

K = C1 xor M1 = 1010 (encontraremos a chave)

M2 = K xor C2 = 0111

**c)**

Fazendo com que a chave tenha um comportamento pseudo aleatório, mudando assim a chave para cada mensagem.

**Exercício 2**

**a)**

Pode acertar e errar = ½

Possui 128 combinações possíveis , logo:

**b)**

**Exercício 3**

**a)**

A mensagem possui 48 caracteres.

Codificação da mensagem é de 8 bits

O tamanho do bloco é de 128 bits.

Mensagem codificada = 48 \* 8 bits

**b)**

48 caracteres / 3 blocos = 16 caracteres por bloco.

N.1 Pagar o Saul, 10, para White 10000000 reais,

**c)**

A mensagem mesmo embaralhada pelo atacante não teria problema pois dependeria do bloco anterior, sendo assim a mensagem não poderia ser descriptografada pois os blocos foram bagunçados.

**Exercício 4**

**a)**

N-1 (não podemos trocar chaves com nós mesmos por isso do -1)

**b)**

**c)**

**KDC - Distribuição de Chaves**

Existem uma chave mestra para cada um dos usuários no KDC. Quando queremos efetuar a comunicação entre dois usuários, usr1 quer se comunicar com usr2.

Usr1 manda um pedido de comunicação para o KDC, para se comunicar com o usr 2 e com a mensagem.

Uma nova chave aleatória é criada. Essa chave para comunicação é codificada com a chave mestra do usr1 e enviada para ele, da mesma forma a nova chave é codificada com a chave mestra do usr2 e enviada para ele