1. Vamos usar a criptografia simétrica pelo algoritmo elementar XOR, assim como pedido no trabalho
2. Escolhi o ASC II por ser o modelo padrão, e por ser o sistema que mais me identifiquei por sua praticidade e de fácil modelagem.
3. Identifiquei os números que faziam parte do meu RU, e notei, que alguns números se repetiam, assim sobrando só quatro: 3687, e esses são os números que vou usar como chave criptográfica, fazendo variações entre eles, formando assim diversos números.
4. Identifiquei o texto plano “CRIPTOGRAFIA”, por ter 12 letras, vou fazer a codificação com as variações do meu RU, ou seja, cada letra vai ser um número deixando assim mais forte a criptografia.

|  |  |  |
| --- | --- | --- |
| **C** | **067** | **01000011** |
| **R** | **082** | **01010010** |
| **I** | **073** | **01001001** |
| **P** | **080** | **01010000** |
| **T** | **084** | **01010100** |
| **O** | **079** | **01001111** |
| **G** | **071** | **01000111** |
| **R** | **082** | **01010010** |
| **A** | **065** | **01000001** |
| **F** | **070** | **01000110** |
| **I** | **073** | **01001001** |
| **A** | **065** | **01000001** |

1. Esses são os códigos da palavra “CRIPTOGRAFIA”:
2. A variações que eu usei do meu RU “3686783” e suas formas binarias são:

|  |  |
| --- | --- |
| **RU** | **3686783** |
| **36** | **0010 0100** |
| **38** | **0010 0110** |
| **37** | **0010 0101** |
| **63** | **0011 1111** |
| **68** | **0100 0100** |
| **67** | **0100 0011** |
| **83** | **0101 0011** |
| **86** | **0101 0110** |
| **78** | **0100 1110** |

1. O texto cifrado ou texto código ficou assim:

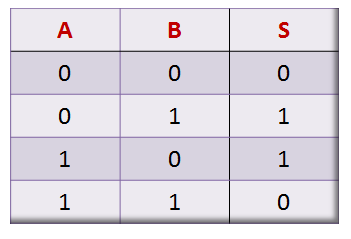
**0110 0111 0110 0111 0110 1100 0001 1110 0110 1011 0000 1011 0000 0100 0111 0100 0001 0010 0001 0000 0110 1100 0001 0010**

1. Como o algoritmo utilizado foi o XOR, e a criptografia usada foi a simétrica, ele só tem uma chave que é:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **C 0110 0111** | **R 0111 0100** | **I 0110 1100** | **P 0001 1110** | **T 0110 1011** | **O 0000 1011** |
| **G 0000 0100** | **R 0111 0100** | **A 0001 0010** | **F 0001 0000** | **I 0110 1100** | **A 0001 0010** |

1. Comprovando a reciprocidade:

Tabela XOR:



O C em negrito é o código criptografado, o sem é o código segundo o

ASC II, e o na ultima linha é a prova da reciprocidade.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| C 0100 0011 | R0101 0010 | I 0100 1001 | P 0101 0000 | T0101 0100 | O0100 1111 |
| **36 0010 0100** | **38 0010 0110** | **37 0010 0101** | **78 0100 1110** | **63 0011 1111** | **68 0100 0100** |
| **C 0110 0111** | **R 0111 0100** | **I 0110 1100** | **P 0001 1110** | **T 0110 1011** | **O 0000 1011** |
| **C: 0100 0011** | **R: 0101 0010** | **I: 0100 1001** | **P: 0101 0000** | **T: 0101 0100** | **O: 0100 1111** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| G0100 0111 | R0101 0010 | A0100 0001 | F0100 0110 | I0100 1001 | A0100 0001 |
| **67 0100 0011** | **38 0010 0110** | **83 0101 0011** | **86 0101 0110** | **37 0010 0101** | **83 0101 0011** |
| **G 0000 0100** | **R 0111 0100** | **A 0001 0010** | **F 0001 0000** | **I 0110 1100** | **A 0001 0010** |
| **G: 0100 0111** | **R: 0101 0010** | **A: 0100 0001** | **F: 0100 0110** | **I: 0100 1001** | **A: 0100 0001** |