

ATIVIDADE PRÁTICA DE MATEMÁTICA COMPUTACIONAL

Isac da Fonseca Santos

RU: 3752111

Análise e Desenvolvimento de Sistemas

Resumo:

Este trabalho consiste na Atividade Prática de Matemática Computacional com o enunciado: *Codificar as 8 primeiras letras de seu nome por criptografia simétrica pelo algoritmo elementar XOR utilizando uma chave criptográfica baseada em seu RU. Após a obtenção da cifra decodificá-la comprovando a reciprocidade do processo.*

Introdução Teórica:

A técnica criptográfica utilizada no trabalho será a do algoritmo XOR, na qual primeiramente iremos converter os 8 primeiros caracteres do meu nome ('Isac San') para uma sequência de bits.

Utilizaremos como base o meu RU acrescido de um '0' como chave criptográfica, também convertido para uma sequência de bits.

A utilização do zero facilitará as posteriores conversões pois com isso o número de caracteres do nome e da chave criptográfica será igual (8).

De posse dos dois conjuntos de bits, realizaremos a operação XOR entre os dois, obtendo assim os dados criptografados.

Demonstraremos a criptografia convertendo a sequência cifrada para texto, atestando assim a ilegibilidade da mesma.

Após esse processo, faremos o caminho reverso, utilizando a chave criptográfica conhecida e a sequência cifrada, aplicaremos novamente o algoritmo XOR para decifrar a mensagem.

O ajuste necessário na chave criptográfica para aumentar a sua efetividade será exposto no decorrer do exercício.

Desenvolvimento:

Passo 1: Conversão da sequência de 8 caracteres do meu nome e de meu RU para seus valores correspondentes ASCII:

Isac San = 073 115 097 099 032 083 097 110

03752111 = 048 051 055 053 050 049 049 049

Passo 2: Conversão dos valores ASCII para binário:

Isac San = 0100 1001 0111 0011 0110 0001 0110 0011 0010 0000 0101 0011 0110 0001 0110 1110

03752111=0011 0000 0011 0011 0011 0111 0011 0101 0011 0010 0011 0001 0011 0001 0011 0001

Como o segundo conjunto de bytes do RU apresenta uma sequência de zeros, para melhorar a chave utilizaremos a sequência 1010 ao invés de 0000, resultando na nova chave criptográfica:

03752111=0011 1010 0011 0011 0011 0111 0011 0101 0011 0010 0011 0001 0011 0001 0011 0001

Passo 3: Realizar a operação XOR bit a bit para obter a sequência cifrada:

Isac San = 0100 1001 0111 0011 0110 0001 0110 0011 0010 0000 0101 0011 0110 0001 0110 1110



03752111=0011 1010 0011 0011 0011 0111 0011 0101 0011 0010 0011 0001 0011 0001 0011 0001



Cifra = 0111 0011 0100 0000 0101 0110 0101 0110 0001 0010 0110 0010 0101 0000 0101 1111

Passo 3: Atestando a efetividade da cifra:

Convertendo a cifra novamente para texto, temos o resultado ilegível "s@VV bP_"

Input data

```
0111 0011 0100 0000 0101 0110 0101 0110 0001 0010 0110 0010 0101
0000 0101 1111
```

Convert

Output:

binary numbers to text

s@VV bP_

Passo 4: Decifrando utilizando o algoritmo XOR e a chave de criptografia conhecida:

Cifra= 0111 0011 0100 0000 0101 0110 0101 0110 0001 0010 0110 0010 0101 0000 0101 1111



Chave= 0011 1010 0011 0011 0011 0111 0011 0101 0011 0010 0011 0001 0011 0001 0011 0001



Resultado=0100 1001 0111 0011 0110 0001 0110 0011 0010 0000 0101 0011 0110 0001 0110 1110

Passo 5: Atestando a eficácia da decriptação:

Para atestar a eficácia da decriptação, basta convertermos novamente a nossa sequência de bits para texto plano, temos assim a mensagem original "Isac San":

Input data	<pre>0100 1001 0111 0011 0110 0001 0110 0011 0010 0000 0101 0011 0110 0001 0110 1110</pre>
Convert	<div>binary numbers to text</div>
Output:	<pre>Isac San</pre>

Conclusão:

Fica demonstrado que utilizando o algoritmo XOR, podemos cifrar e decifrar um conjunto de dados e que esse processo é reversível utilizando o mesmo algoritmo e a chave de criptografia conhecida sem que haja perda de dados ou informações

Referências Bibliográficas:

<https://www.ime.usp.br/~pf/algoritmos/apend/ascii.html>

<https://pt.stackoverflow.com/questions/205163/como-funciona-o-xor-para-dois-bin%C3%A1rios-com-mais-de-um-d%C3%ADgito>

<http://www.unit-conversion.info/texttools/ascii/>

<https://codebeautify.org/xor-calculator>

Vídeo: Atividade Prática, Criptografia, Matemática Computacional, Prof. ME. Gian Carlo Bustolin.