Trabalho Sobre a Cifra de César

Arquitetura e Organização de Computadores – CC33B

Aluno Andrey Naligatski Dias

16 de novembro de 2019

• *Andrey Naligatski Dias, cursando Ciência da Computação na Universidade Técnológica Federeal do Paraná - UTFPR. E-mail: andreydias@alunos.utfpr.edu.br*

1 Introdução

A Cifra de César é uma técnica de criptografia extremamente arcaíca, utilizada a alguns séculos atrás pelo General Júlio César, que segundo Suetônio(Escritor látino da época) trocava três posições das letras para proteger dos seus inimigos a tática de guerra do seu exército. Não existem dados comprovando estatísticamente se tal técnica foi efetiva ou não, mas pode se dizer que funcionava, pois baseando-se na época ao qual esta foi inventada, muitos de seus inimigos eram analfabetos, e qualquer anagrama já bastaria para dificultar no entendimento de mensagens. O algoritmo funcionava da seguinte forma: Cada letra da mensagem enviada era trocada pela letra 3 casas a sua frente, por exemplo, uma mensagem de “ataque”, se criptografada ficaria como “DWDTXH”. Especificando um pouco mais sobre, o alfabeto era considerado como um circulo que se reiniciava a cada volta, ou seja, do Z, usando a cifra comum de César, com a cifra 3, seria substituído por C, e assim sucessivamente,

2 Desenvolvimento

2.1 Início do desenvolvimento

Como a linguagem de programação MIPS é bem mais baixo nível do que as linguagens que eu estou acostumado a programar, inicialmente comecei resolvendo o problema com a linguagem C, para ver se conseguiria encontrar semelhanças ou ideia para converter de uma para outra.

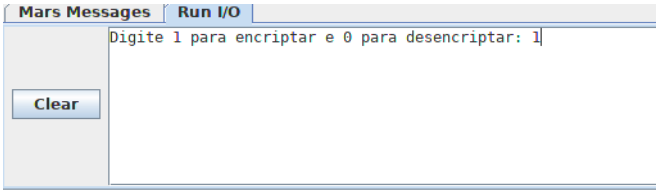
2.2 O código em si

Me baseando no que havia feito no passo anterior, percebi que a forma mais fácil de se alterar as letras da string era utilizando a tabela ASCII, visando olhar em sua parte decimal, e realizando operações aritméticas na mesma, assim então manipulando o alfabeto tanto para letras antecessoras como sucessoras, e depois “ convertendo “ novamente para o formato de string. O resto do código foi devidamente mais fácil, visto que a maioria das funções utilizadas foram vistas em sala de aula. Infelizmente ocorreu 2 bugs visuais aos quais eu não consegui arrumar de maneira alguma, e que serão vistos na parte de utilização do programa, que seriam símbolos logo após o print da frase encriptada ou descriptada.

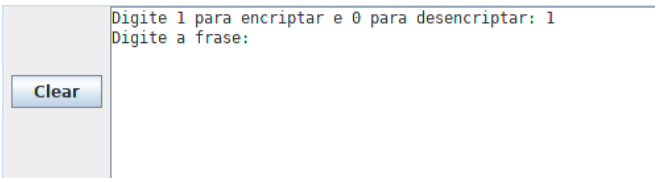
3 Utilização

O programa possui duas opções de uso, encriptar mensagens ou desencriptar, baseando-se em uma cifra pré-definida pelo usuário.

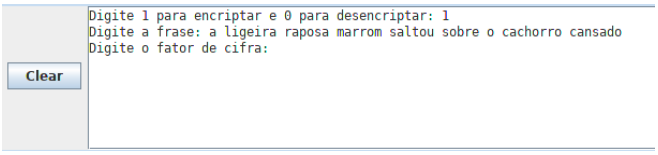
O primeiro passo é escolher, teclando 1 ou 0 se deseja encriptar ou desencriptar uma frase(Utilizarei a encriptação como exemplo):



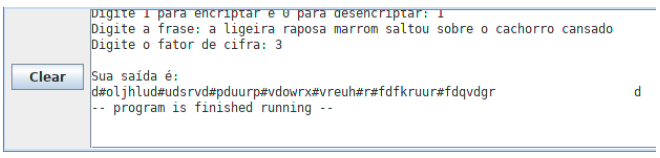
Logo após, será pedido para que se digite uma frase:



Com a frase já confirmada, será pedido o fator de cifra ao qual você deseja encriptar(ou desencriptar):



Por fim, será printado sua frase(o d logo após algumas tabulações da frase é o problema visual que eu não consegui arrumar, as vezes aparece outras letras)



4 RESULTADOS

Os códigos criptografados e descriptografados a seguir foram feitos pelo aluno Breno, e logo após, dois testes iguais, utilizando o meu programa:

Criptografando:

```
Olá, o que você deseja? Criptografar(C) ou Descriptografar (D)? C
Digite o texto a ser criptografado: codigo
Qual chave deseja usar? 1
dpejhp
-- program is finished running --
```

Descriptografando:

```
Olá, o que você deseja? Criptografar(C) ou Descriptografar (D)? D
Digite o texto a ser descriptografado: paopa
Qual chave deseja usar? 4
lwklw
-- program is finished running --
```

Criptografando:

```
Digite 1 para encriptar e 0 para desencriptar: 1
Digite a frase: a ligeira raposa marrom saltou sobre o cachorro cansado
Digite o fator de cifra: 3

Sua saída é:
d#oljhlud#udsrvd#pduurp#vdowrx#vreuh#r#fdfkruur#fdqvdgr d
-- program is finished running --
```

Descriptografando: (Novamente o problema de símbolos aleatórios aparecendo no fim da frase)

```
Digite a frase: Digite 1 para encriptar e 0 para desencriptar: 0
Digite a frase: D OLJHLUD UDSRVD PDUURP VDOWRX VREUH R FDFKRUUR FDQVDGR
Digite o fator de cifra: 3

Sua saída é:
A LIGEIRA RAPOSA MARROM SALTOU SOBRE O CACHORRO CANSADO ýýýýýýýýýýýýýýýýýýýýýýýýý
-- program is finished running --
```

5 REFERÊNCIAS

[1] Mars (mips assembler and runtime simulator). http://courses.missouristate.edu/kenvollmar/mars/index.htm

[2] Mars wiki (IDE, Debbuging, Tools, Limitations, Syscalls). http://courses.missouristate.edu/kenvollmar/mars/Help/MarsHelpIntro.html

[3] Fred Cohen, "A Short History of Cryptography", 1990, 1995.

[4] *Suetonius, "The Lives of the Caesars".*