Relatório de Arquitetura e organização de coputadores I

Nome: Luiz Ronny Acácio da Penha Matrícula: 417349
Professor: Roberto Cabral. Data: 14/06/2019

Trabalho 2: Cifra de Vigenère.

Introdução:

A criptografia é um conceito técnico usado para codificar informações, de tal forma que somente o seu destinatário e o emissor consigam acessá-la. O objetivo é evitar que terceiros interceptem e desvendem a mensagem.

A disciplina de Arquitetura e organização de computadores I é um excelente local para se implementar algorítimos de encriptação, e nesse trabalho foi usado a cifra de Vigenène que é uma encriptação bastante robusta de difícil quebra.

Apresentação das funções:

Todo o trabalho foi implementado em um só arquivo chamado ‘main.asm’, porém a encriptação é feita em cima de arquivos de texto, um de entrada, que é colocada a mensagem, um de chave para a cifra e outro de saída, que é essa mensagem encriptada. O trabalho ainda conta com um arquivo Makefile para facilitar usabilidade.

Desenvolvimento do trabalho:

Comecei o trabalho junto ao relatório no dia 06 de junho, implementando as funções básicas de leitura e escrita em arquivos, logo depois dei início a lógica de encriptar e decriptar, com a ajuda do monitor David consegui concluir essa parte facilmente, como o trabalho não é tão complexo consegui terminar todas as funções básicas rapidamente, porém, ainda existia vários erros por conta da falta de tratamento das exceções e de um menu para dar ao usuário total controle sobre o programa. No dia 13 de junho consegui completar todo o trabalho e todas as suas exceções.

Desenvolvimento das funções:

O programa faz uso de duas funções, cifrar e decifrar uma mensagem, toda vez que o arquivo ‘entrada.txt’ é cifrado, um arquivo ‘saidaCrip.txt’ é criado contendo a mensagem criptografada. Toda vez que o usuário desejar decifrar uma informação tal arquivo cifrado deve estar nesse arquivo ‘saidaCrip.txt’, quando ele for decifrado um arquivo chamado ‘saidaDescri.txt’ será criado contendo a informação decifrada.

A cifra de Vigenère ultiliza tal lógica de encriptação: Valor do caractere de entrada somado ao caractere correspondente na chave menos 130 mod 26 e por fim somando mais 65, fazendo isso em cada caractere e salvando o resultado no arquivo de saída a mensagem será cifrada.

Para decifrar, fiz o processo inverso, e coloquei em outro arquivo.

Outra preocupação que deve-se ter para cifrar é com o tamanho da chave, ou seja, caso a chave seja menor do que a informação, em relação à número de caracteres ela deve ser replicada até ser igual ao tamanho da entrada, uma forma de implementar isso no *assembly* é zerando o iterador que "anda" dentro do vetor da chave toda vez que ele for maior do que a quantidade de caracteres da chave. Quando lemos o arquivo 'chave.txt', a quantidade de caracteres é guardada no registrador EAX, assim, podemos salvar esse número e utilizarmos para comparar dentro do loop de cifra, e toda vez que o iterador do buffer de chave ultrapassar esse valor salvo, zeramos o iterador, assim a chave será replicada.

Por fim, também me preocupei com as exceções e mensagens de erro que o programa passa ao usuário e implementei cada uma delas co mensagens para todos os tipos de erro sendo imprimidos no console.

Dificuldades:

O principal impasse foi no começo, pois não estava ambientado em programar *assembly* fora de uma IDE, além disso, não tinha estudado quase nada sobre interrupções e arquivos.

Conclusão:

A fomentação desse trabalho foi de bastante ajuda para entender melhor criptografia e todas as suas usabilidades, também ajudou no meu crescimento co programador, pois esse trabalho foi muito mais usual, ou seja, mais aplicável ao cotidiano. E por fim, consegui estudar e entender todos os conceitos finais da disciplina e adquirindo diversos novos conhecimentos na área da tecnologia.