PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL

ESCOLA POLITÉCNICA

Curso de BACHARELADO EM ENGENHARIA DE SOFTWARE

SEGURANÇA DE SISTEMAS

ANDRÉ LUIZ MARQUES MACRINI LEITE

TRABALHO 1

CIFRA DE VIGèNERE

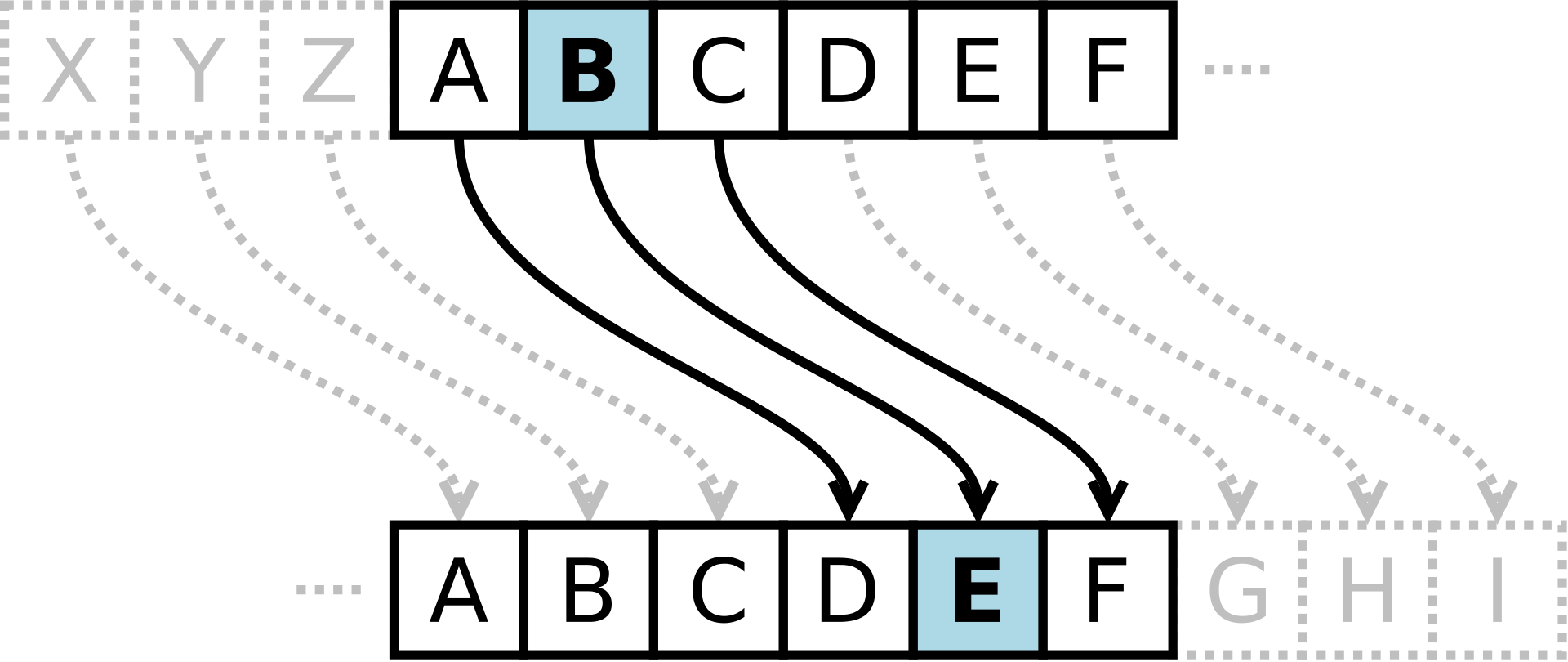
Porto Alegre

2021

### Introdução

No presente relatório é apresentada a solução desenvolvida para o primeiro trabalho proposta na disciplina de Segurança de Sistemas. O Objetivo do trabalho é criar um programa que seja capaz de encontrar um texto claro, sendo dado somente um texto cifrado. Para a implementação do programa foi utilizada a linguagem de programação Java, e neste relatório contém instruções para execução dele. Para explicar o que é a cifra de Vigenère precisamos inicialmente entender o que é a cifra de César.

### Cifra de César

Também conhecida como cifra de troca, é uma das mais conhecidas técnicas de criptográfica, além de ser uma das mais fáceis de utilizar. A cifra funciona de forma em que cada caractere do texto claro é substituído por outro caractere. Por exemplo, com uma troca de três posições, A seria substituído por D, B se tornaria E, e assim sucessivamente.

**Exemplo de substituição de caracteres**

### Cifra de Vigenère

Uma vez sendo visto o funcionamento da cifra de César, podemos entender como funciona a cifra de Viginère. A cifra de Viginère é uma técnica de criptografia por substituição polialfabética que utiliza uma série de cifras de César diferentes, baseadas nas letras de uma palavra-chave. É considerada uma cifra fácil de se entender, implementar e de decifrar, e mesmo assim durante 3 séculos foi considerada como “A Cifra Indecifrável”. O funcionamento da cifra é bem simples, consiste basicamente em pegar uma palavra-chave e aplicar a cifra de César diversas vezes obedecendo os caracteres da palavra-chave para fazer os deslocamentos.

### Solução

Para decifrar uma mensagem criptografada utilizando a cifra de Viginère precisamos descobrir o tamanho da chave, descobrir a melhor chave e decifrar a mensagem.

### Descobrir o Tamanho da Chave

Para achar o tamanho da chave, foi utilizado o método de Índice de Coincidência.

Primeiramente foi definido o tamanho máximo de chave como 20. Para cada tamanho possível de chave, até o tamanho máximo definido, é extraído da mensagem conjuntos de caracteres das posições obtidas com base em um salto, sendo este definido pelo tamanho atual da possível chave. Por exemplo, se definirmos o tamanho máximo de chave como 3 e tivermos uma mensagem criptografada “cyyzvmgurwbszxmehace” teremos que fazer um loop até 3 e para cada iteração desse loop pegaremos conjuntos de caracteres respeitando a chave da iteração atual:

Chave atual: 1

Conjuntos:

“cyyzvmgurwbszxmehace”

Chave atual: 2

Conjuntos:

“cyvgrbzmhc”

“yzmuwsxeae”

Chave atual: 3

Conjuntos:

“czgwzec”

“yvubxhe”

“ymrsma”

Para cada um dos conjuntos obtidos, é feito o cálculo do índice de coincidência para o conjunto e quando termina de calcular para todos os conjuntos encontrados para o tamanho da chave atual, é feita a média dos índices de coincidência calculados. Com base na média dos índices para cada tamanho de chave, podemos percorrer essas medias para encontrar qual delas fica mais próxima ao índice de coincidência da língua. Ao encontrar isso, conseguimos saber o tamanho provável da chave.

### Descobrir a Melhor Chave

Para descobrir a melhor chave, precisamos primeiramente do tamanho provável da chave e da mensagem cifrada. Vamos montar conjuntos de caracteres novamente, porém dessa vez cada conjunto vai ter o tamanho da melhor chave encontrada.

Se tomarmos como exemplo um melhor tamanho de chave encontrado como 2, basicamente, de 2 em 2 caracteres iremos pegar um e adicionar no conjunto atual. Por exemplo, com a mensagem cifrada “cyyzvmgurwbszxmehace” e tamanho da melhor chave encontrada 2:

Conjuntos:

“cyvgrbzmhc”

“yzmuwsxeae”

Para cada um dos conjuntos encontrados, calculamos a frequência das letras e pegamos a distância entre as 3 letras mais frequente da mensagem e as 3 letras mais frequentes da língua. Cada conjunto vai ter um caractere da chave, assim conseguimos descobrir todos os caracteres que compõem a chave

### Decifrar

Para decifrar a mensagem precisamos da mensagem cifrada e da melhor chave descoberta. Percorremos então a mensagem cifrada e para cada caractere deslocamos o mesmo para o caractere respectivo da chave. Por exemplo, tendo uma mensagem cifrada “cyyzvmgurwbszxmehace” e a melhor chave encontrada “meunome” iremos deslocar cada letra da mensagem por uma letra da chave:

Mensagem cifrada: c y y z v m g u r w b s z x m e h a c e

Chave: m e u n o m e m e u n o m e m e u n o m

Mensagem decifrada: q u e m h a c i n c o e n t a a n n o s

### Instruções de Execução

Para rodar a aplicação é necessário ter instalada um JDK 8 ou maior. Para compilar a aplicação basta executar o comando “make” em um terminal aberto na pasta da entrega do trabalho.

Para executar a aplicação, no terminal, deve ser digitado o comando:

java App <filename.txt>

Onde <filename.txt> é o caminho completo de onde o arquivo com o texto cifrado se encontra.

### Testes

Para os testes foram utilizados os arquivos disponibilizados no moodle da disciplina pelo professor.

A aplicação testa automaticamente para português e para inglês, devolvendo o resultado para as duas tentativas.

Ao executar o teste utilizando o arquivo “texto-cifrado-portugues.txt” podemos perceber que o resultado da tentativa de decifrar em português teve um resultado legível, já a tentativa de decifrar em inglês teve um texto completamente ilegível, logo pode-se perceber que o texto claro, de fato era em português.

Texto

Descrição gerada automaticamente

Ao executar o teste novamente, mas utilizando o arquivo “texto-cifrado-ingles.txt” podemos ver que o resultado é diferente. Neste caso, a tentativa de decifrar em português não obteve sucesso, tendo em vista que o texto não está legível. Já a tentativa de decifrar em inglês, nessa ocasião, funcionou corretamente e obtivemos o texto claro com sucesso.

Texto

Descrição gerada automaticamente

### Conclusão

O desenvolvimento do trabalho contribuiu demais com meu conhecimento sobre o mundo da criptoanálise e despertou interesses muito grandes no assunto. Com tudo, pude ter um entendimento maior sobre a Cifra de Vigenère e as suas fraquezas, o que contribui para saber quais tipos de criptografia devem ser evitados para obter uma maior segurança. O objetivo proposto foi atendido satisfatoriamente, tendo em vista que foi possível achar a chave e decifrar a mensagem com sucesso tanto em português quanto em inglês.

REFERÊNCIAS

Cifra de César. Cifra de César. Disponível em: <https://pt.wikipedia.org/wiki/Cifra\_de\_C%C3%A9sar>. Acesso em: 26/09/2021

Criptografia – Cifra de César. Cifra de César. Disponível em:<<http://www.bosontreinamentos.com.br/seguranca/criptografia-cifra-de-cesar/>> Acesso em: 26/09/2021

Cifra de Vigenère. Cifra de Vigenère. Disponível em: <https://pt.wikipedia.org/wiki/Cifra\_de\_Vigen%C3%A8re> Acesso em: 26/09/2021