

UNIP – UNIVERSIDADE PAULISTA

Curso de Engenharia da Computação

**ATIVIDADES PRÁTICAS SUPERVISIONADAS - APS**

**AS TÉCNICAS CRIPTOGRÁFICAS, CONCEITOS, USOS E APLICAÇÕES**

Igor Gabriel Mariano Mendonça - RA – D71386-8

Yan Gabriel Furlan - RA – N30662-9

Bruno Lassakoski - RA – D51Igb0

Samuel Ribeiro Pereira - RA – N190086

São José dos Campos, 28 de Abril de 2020.

UNIP – UNIVERSIDADE PAULISTA

Curso de Engenharia da Computação

**ATIVIDADES PRÁTICAS SUPERVISIONADAS - APS**

**AS TÉCNICAS CRIPTOGRÁFICAS, CONCEITOS, USOS E APLICAÇÕES**

Atividades Práticas Supervisionadas do 4º/5º Semestres do Curso de Engenharia da Computação da **Universidade Paulista – UNIP**.

Coordenador: Prof. Élcio Hideiti Shiguemori

Prof Responsável: André Yoshimi Kusumoto

São José dos Campos, 28 de abril 2020.

Resumo

O uso e compreensão da criptografia data-se de muito tempo antes dos primeiros computadores surgirem, tendo sido utilizada por diversos povos como espartanos e romanos visando codificar acordos entre líderes ou até mesmo estratégias de guerra. Seu significado é tão antigo quanto sua utilização, sendo um derivado das palavras “*Kriptós”*e *“Gráfein”* sendo traduzidas respectivamente como “secreto” e “escrita”. Os métodos de codificação de informações podem ser divididos em dois períodos sendo eles a criptografia clássica e moderna. Com o decorrer dos anos a utilização de recursos para proteção de informações foi aperfeiçoando-se e o que antes utilizado por reis e generais de guerra com objetivos diplomáticos agora, tem seu propósito voltado a proteger informações de grandes empresas e até mesmo de pessoas comuns em suas casas. Notoriamente o uso de tais métodos foram refinados e são constantemente atualizados em busca de padrões cada vez mais complexos para proteção de dados e todos hoje, tem ao menos um contato com a criptografia. No desenvolvimento de tais proteções diversas áreas acabaram sendo abrangidas tais como redes sem fio com padrões simples de codificação até as mais complexas como sites de compras que tem como proteção chaves assimétricas (El Gamal e RSA(Rivest, Shamir and Adleman).

Palavras-chave: Criptografia. Aperfeiçoamento

ABSTRACT

The use and understanding of data encryption is very fast before the first surgeons, having been used by several peoples, such as Spartans and Romans, to codify the agreements or their aimed at codifying agreements between leaders or even war strategies. it meaning is as old as it's used the derivative of the words "Kriptós" and "Gráfein" being translated respectively as "secret" and "written". The methods of encoding information can be divided into two periods of resources for information protection has been improved and what has been used before kings and generators of war for the purposes of plomatics now, its aim is to protect information methods to refine and are constantly being shown in search of more and more patterns During the development of protections diverse finished areas being covered, such as fanless networks coding comas asia, coding ass wing, christ asia keys the symmetric (El Gamal and RSA (Rivest, Shamir and Adleman).

Key worlds: Encryption. Improvement.

Sumário

[1 Introdução 2](#_Toc39140227)

[2 DESENVOLVIMENTO 3](#_Toc39140228)

[2.1 CRIPTOGRAFIA 3](#_Toc39140229)

[2.2 CRIPTOGRAFIA SIMÉTRICA E ASSIMÉTRICA 4](#_Toc39140230)

[3 TÉCNICAS CRIPTOGRÁFICAS 5](#_Toc39140231)

[3.1 RSA 5](#_Toc39140232)

[3.1.1 FUNCIONAMENTO 5](#_Toc39140233)

[3.2 CIFRA DE VIGENÈRE 6](#_Toc39140234)

[3.2.1 FUNCIONAMENTO 6](#_Toc39140235)

[4 projeto 7](#_Toc39140236)

[5 RELATÓRIOS COM LINHAS DE CÓDIGO 8](#_Toc39140237)

[REFERÊNCIAS 15](#_Toc39140238)

[REFERÊNCIA BIBLIOGRÁFICA 15](#_Toc39140239)

1 Introdução

Para a realização da APS (Atividade Pratica Supervisionada), na Universidade Paulista – UNIP, o aprimoramento e compreensão de estilos de programação são essenciais. Colocou-se em prática os elementos até então adquiridos durante as aulas em conjunto com a busca de um maior aprofundamento, para conseguir desta forma desenvolver técnicas básicas de criptografia.

A criptografia tem como função básica a proteção de dados e informações em diversas áreas e segmentos, e é de competência de engenheiros a realização de programas para dificultar o acesso a tais dados por meio de terceiros. Determinada noção levou os membros a empenharem-se na formação de vários protótipos de criptografia para buscar a que melhor pudesse adequar-se as necessidades do mercado atual.

Tendo tais aspectos como base, as necessidades de um programa simples, mas eficaz tornaram as buscas e aprimoramentos o pilar principal para a realização de um trabalho voltado aos aspectos essenciais dos programas atuais ou o mais próximo possível. Foram necessários várias horas de pesquisa e testes para atingir o resultado atual, necessariamente desta forma adquiriu-se uma carga de conhecimento notável referente a criptografia, sendo dissertada neste trabalho.

2 DESENVOLVIMENTO

2.1 CRIPTOGRAFIA

A criptografia tem uma função primordial nos dias atuais, mas seu surgimento data de muito antes do esperado, sendo utilizada por povos antigos como romanos e gregos. O motivo principal da criptografia não mudou mesmo com o passar das eras, tendo como função principal proteger informações. Segundo Tamarozzi (2004, p. 69): “a criptografia é tão antiga quanto a própria escrita; já estava presente no sistema de escrita hieroglífica dos egípcios”. Tendo isso como base funções primárias como a matemática tomam papéis fundamentais no desenvolvimento de programas para proteção de dados. Os modelos criptográficos variam-se de uma forma muito grande como a escrita na madeira com cera por cima até a máquina enigma utilizada pelos alemães durante a segunda guerra mundial.

Sendo datada de tempos antigos ela vem sendo aprimorada e está presente desde antes de Cristo, e seu desenvolvimento tem três grandes fases: artesanal, mecânica e digital (SINGH, 2005).

A criptografia artesanal surge juntamente com a escrita sendo necessário apenas lápis e papel, consecutivamente seu método de quebra não era complexo e tendo como seu maior exemplo o código de César.

Durante a revolução industrial surge a criptografia mecânica, onde com o domino das máquinas em grande parte do mundo fez surgir métodos de criptografias mais avançados como alavanca a segunda guerra mundial, tendo notoriedade assim o Disco de Cifras, o código morse e a máquina enigma sendo os dois últimos os mais famosos. Segundo Diffie e Hellman (2007, p. 39): “Antes deste século, sistemas de criptografia foram limitados a cálculos que poderiam ser realizados à mão ou com dispositivos simples”.

A criptografia digital, usada nos dias atuais veio com o surgimento dos computadores alavancando notoriamente a complexidade dos códigos, por meio de cálculos extremamente grandes, podendo-se observar a criptografia simétrica e assimétrica como principais.

2.2 CRIPTOGRAFIA SIMÉTRICA E ASSIMÉTRICA

Os primeiros sistemas de criptografia eram do tipo simétricos, ou chave secreta. São sistemas que tem apenas uma chave de cifração, e o exemplo mais claro e simples é o algoritmo de Júlio César, que dependia apenas de somar ou subtrair três ao código numérico de cada letra do alfabeto. O principal ponto forte de tal método é que ambas as partes que trocam mensagens podem encriptar e decriptar a mensagem independente de qual seja seu conteúdo através da chave que ambos compartilham. Claramente por tratar-se de um sistema simples sua quebra também não é complexa e a ciência que busca analisar tais algoritmos em busca de “quebra-los” é chamada de Criptoanálise. Por tal método sem simples a necessidade de desenvolvimento de métodos mais complexos deu origem ao mais utilizado dos métodos que é a criptografia assimétrica.

A criptografia assimétrica tem com pilar duas chaves (pública e privada), logo se uma pessoa tiver a chave pública ela não poderá decodificar a mensagem sem a chave privada, tornando assim muito mais segura e com um grau de quebra muito menor do que a simétrica tendo em vista a redução no número de chaves possíveis: n x ( n – 1) / 2 para simétricos e 2\*n para assimétricos.

3 TÉCNICAS CRIPTOGRÁFICAS

3.1 RSA

É o sistema mais comumente usado para criptografia, segundo Coutinho (2011, p.3):

Este código foi inventado em 1978 por R. L. Rivest, A. Shamir e L. Adleman, que na época trabalhavam no Massachussets Institute or Technology (M.I.T). As letras RSA correspondem às iniciais dos inventores do código. Há vários outros códigos de chave pública, mas o RSA é, atualmente, o mais usado em aplicações comerciais. Este é o método utilizado, por exemplo, no *Netscape*, o mais popular dos softwares de navegação da *Internet* (COUTINHO, 2011, p.3).

3.1.1 FUNCIONAMENTO

1. Obter dois números primos *p* e *q*;

2. Calcular *n* = *pq*;

3. Calcular *Φ(n)* = *(p-1)(q-1)*;

4. Escolher *e* | Máximo Divisor Comum – MDC entre *e* e *Φ(n)* seja igual a *1*, ou seja, *e* e *Φ(n)* são coprimos (primos relativos);

5. Calcular *d* | *de*≡*1 (mod Φ(n))*, ou seja, *de mod Φ(n) = 1*;

6. Chave pública: *(e, n)*; chave privada: *(d, n)*;

7. Função para cifrar uma mensagem *m*: *C(m) = me mod n = c*;

8. Função para decifrar uma mensagem *c*: *D(c) = cd mod n = m*;

9. *D(C(m)) = m*.

O RSA surgiu sobre uma dar áreas mais conhecidas da matemática sendo ela, a Teoria dos números. Ele utiliza do método da divisão por números primos (Divisíveis por eles mesmo e por um).

Quando tratamos de números pequenos como três ou onze a fatoração torna-se fácil, mas o grande problema é quando surgem números grandes e complexos.

O RSA aproveita-se desses números e as chaves são geradas com a multiplicação de dois desses números primos. O resultado será público, mas caso o número seja muito grande tentar descobrir os números que geraram os resultados tende-se a ser uma tarefa inviável. Seu método pode ser quebrado, mas levaria muito tempo o que não seria rentável já que ao descobrir uma solução das chaves outra já poderia ter sido gerada durante todo o processo.

3.2 CIFRA DE VIGENÈRE

Esse método de criptografia foi descrito originalmente pelo criptologista italiano Giovan Battista Bellaso em um livro de 1553 de nome “La cifra del. Sig. Giovan Battista Bellaso”. Posteriormente foi atribuído erroneamente a [Blaise de Vigenère](https://en.wikipedia.org/wiki/Blaise_de_Vigen%C3%A8re" \t "_blank) no século XIX, tendo então recebido a atribuição de “Cifra de Vigenère”.

3.2.1 FUNCIONAMENTO

Tem com base várias cifras de César usadas em sequência, obtidos através de uma chave (palavra-chave). É realizada através de uma tabela alfabética que é denominada “tabula recta” ou “quadrado de Vigenère”, que em sintaxe é o alfabeto escrito 26 vezes em linhas diferentes, desta forma correspondendo às 26 cifras de César.

**Ci=Pi+Ki**

**Seguindo a fórmula apresentada o “Ci” representará o texto cifrado, o “P” o texto puro, o “K” a chave de Criptografia e o “i” referindo-se ao índice. Automaticamente a fórmula de descriptografia torna-se:**

**P=C-K+26**

**Tomando como modelo a fórmula as variáveis são as mesmas que o da fórmula anterior.**

4 projeto

A criptografia escolhida no projeto foi a Cifra de Vigenère por ter um padrão mais complexo do que a Cifra de César, já que, foi baseada na mesma. Para escolha da linguagem de programação a ser utilizada, pensou-se na habilidade de cada integrante visando a melhor opção de desenvolvimento do programa que deveria abranger os tópicos pressupostos sendo eles, a codificação a inserção da chave e a decodificação do programa.

Durante a execução dividiu-se o grupo em dois para testar as linguagens plausíveis que poderiam ser utilizadas, sendo elas linguagem C e Python. Apresentado os aspectos a linguagem escolhida foi a “C”, que assim poderia realizar todos os métodos necessários através do conhecimento dos membros na linguagem.

A linguagem Python não foi utilizada pois, a maioria dos membros do grupo não contém uma base tão profunda na mesma para a realização do trabalho, sendo assim o mais plausível tornou-se a linguagem C.

Durante as reuniões discutiu-se os tipos de criptografia existentes e as que melhor seriam capazes de adequarem-se as necessidades. Analisou-se as criptografias: RSA, Cifras de César e Cifra de Vigenère, e adequando um grau de complexibilidade com as competências do grupo chegou-se ao consenso na utilização da Cifra de Vigenère.

5 RELATÓRIOS COM LINHAS DE CÓDIGO

#include<stdio.h>

#include<stdlib.h>

#include<string.h>

// Redefinição de dados

typedef struct sDados

{

char chave[200];

char texto[200];

char cifrado[200];

}

Dados;

/\* Tirar espaços em branco, jogando tudo uma casa pra frente no vetor. \*/

int verificar(Dados \* info)

{

/\* strcpy Realiza a cópia do conteúdo de uma variável a outra. \*/

strcpy(info->chave,"");

int c, i = 0;

printf("-- Chave --:\n");

setbuf(stdin,NULL);

scanf("%[^\n]",info->chave);

/\* strlen retornar o tamanho da string como long int \*/

for(i=0;i<strlen(info->chave);i++)

{

if(info->chave[i] == ' ')

{

for(c=i;c<strlen(info->chave);c++)

{

info->chave[c] = info->chave[c+1];

}

}

else

{

info->chave[i] = info->chave[i];

}

}

}

int verificar\_texto(Dados \* info)

{

printf("-- Texto a ser cifrado: --\n");

setbuf(stdin,NULL);

scanf("%[^\n]",info->texto);

}

int cifrar(Dados \* info)

{

int i,caracter, c=0, t=strlen(info->chave);

/\* Repetição da chave até igualar-se ao tamanho do texto a ser cifrado \*/

for(i=strlen(info->chave);i<strlen(info->texto)+1;i++)

{

info->chave[i] = info->chave[c];

c++;

if(c==t)

{

c=0;

}

}

/\*I= strings C = Chave. \*/

for(i=0,c=0;i<strlen(info->texto);i++,c++)

{

if(info->texto[i] == ' ')

{

info->cifrado[i] = ' ';

c--;

}

else

{

caracter=(int)info->texto[i]+info->chave[c]-97;

if(caracter > 122)

{

caracter = caracter - 26;

info->cifrado[i] = caracter;

}

else

{

info->cifrado[i] = caracter;

}

}

}

}

void em\_tela(Dados \* info)

{

printf("\n Chave: %s \n \n",info->chave);

printf("Texto informado: %s \n \n",info->texto);

printf("Texto Cifrado em Vigenère: %s \n \n",info->cifrado);

}

int menu(Dados \* info)

{

int op;

int i = 0;

do

{

printf("-- 1\* Informe a chave: --\n");

printf("-- 2\* Informe o texto a ser cifrado: --\n");

printf("-- 3\* Cifrar o texto --\n");

printf("-- 4\* Apresenta-lo em tela --\n");

scanf("%d",&op);

switch(op)

{

case 1:

{

verificar(info);

break;

}

case 2:

{

verificar\_texto(info);

break;

}

case 3:

{

cifrar(info);

break;

}

case 4:

{

em\_tela(info);

break;

}

}

}

while(op != 0);

}

int main()

{

/\* sizeof = este operador permite saber o número de bytes ocupado por um determinado tipo de variáve \*/

Dados \* info = (Dados \*)malloc(sizeof(Dados));

menu(info);

free(info);

}

REFERÊNCIAS

Tipos de Criptografia conheça os 10 mais usados e como funciona cada um: https://cryptoid.com.br/valid/tipos-de-criptografia-conheca-os-10-mais-usados-e-como-funciona-cada-um/

Uma breve história sobre criptografia (06/07/2015). Disponível em: https://cryptoid.com.br/banco-de-noticias/a-historia-da-criptografia/

Redefinição de tipos com typedef. Disponível em: http://linguagemc.com.br/redefinicao-de-tipos-com-typedef/

LADEIRA. Ricardo. Instituto Federal Catarinense. Uma análise da complexidade do algoritmo RSA implementado com o teste probabilístico de Miller-Rabin. Disponível em: https://seer.imed.edu.br/index.php/revistasi/article/view/1639/1296.

REFERÊNCIA BIBLIOGRÁFICA

DAHAB, Ricardo. Professor da Faculdade UNICAMP. Disponível em: https://www.ic.unicamp.br/~rdahab/cursos/inf541/09/Welcome\_files/material\_didatico/Dahab-Lopez-JAI2007.pdf. Acesso em: 28 abril. 2020.

SANTOS, José. Dissertação de Mestrado pela Faculdade Federal da Bahia – UFBA Instituto de Matemática. Disponível em: https://repositorio.ufba.br/ri/bitstream/ri/22928/1/Disserta%C3%A7%C3%A3o%20-%20Jos%C3%A9%20Luiz.pdf. Acesso em: 28 abril. 2020.

BOMFIOM. Daniele. Dissertação Apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP. Disponível em: https://teses.usp.br/teses/disponiveis/55/55136/tde-06042017-164507/publico/DanieleHelenaBonfim\_revisada.pdf. Acesso em: 28 abril. 2020.

QUARESMA.Pedro. Departamento de Matemática, Universidade de Coimbra. Disponível em: https://www.mat.uc.pt/~pedro/lectivos/CodigosCriptografia1011/artigo-gazeta08.pdf. Acesso em: 28 abril. 2020.