

**Universidade Paulista – UNIP**

**Ciência da Computação**

**Atividades Práticas Supervisionadas**

**Tema: “AS TÉCNICAS CRIPTOGRÁFICAS, CONCEITOS, USOS E APLICAÇÕES”**

**Aluno: Matheus Rodrigues Martins Pereira / RA: B73ABD-5**

**Aluno: Matheus Gonçalves Brandão / RA: B67712-0**

**Aluno: Johnny Amancio Santos / RA: B633FF-8**

**Índice**

|  |  |
| --- | --- |
| Página | Conteúdo |
| 03 | **Introdução - Criptografia (Conceitos Gerais)** |
| 03 | **Técnicas criptográficas mais utilizadas e conhecidas** |
| 07 | **Estruturação, conceitos e fundamentação** |
| 08 | **Benefícios em relação às técnicas anteriores** |
| 08 | **Aplicações que fazem/fizeram uso da técnica** |
| 08 | **Discussão comparativa entre esta técnica e outras conhecidas /**  **Utilizadas** |
| 08 | **Vulnerabilidades e falhas** |
| 09 | **Melhorias propostas e/ou implementadas** |
| 10 | **Relatório de linhas de código do programa** |
| 15 | **Apresentação do programa em funcionamento em um computador, apresentando todas as funcionalidades pedidas e extras.** |
| 17 | **Bibliografia** |
| 18 | **Ficha de Atividades Práticas Supervisionadas** |

**Introdução - Criptografia (Conceitos Gerais)**

A criptografia nada mais é que um conjunto de técnicas para esconder informação de acesso não autorizado.

O objetivo da criptografia é transformar um conjunto de informação legível, como um e-mail, por exemplo, em um emaranhado de caracteres impossível de ser compreendido. O conceito chave é que apenas quem tem a chave de decriptação seja capaz de recuperar o e-mail em formato legível. Mesmo conhecendo todo o processo para esconder e recuperar os dados, a pessoa não autorizada não consegue descobrir a informação sem a chave de decriptação.

O primeiro uso documentado da Criptogria é datado em torno de 1900 a.C no Egito, quando um escriba usou hieróglifos fora do padrão numa inscrição.

Entre 600 a.c. e 500 a.c., os hebreus utilizavam a cifra de substituição simples (de fácil reversão e fazendo uso de cifragem dupla para obter o texto original), sendo monoalfabético e monogrâmica (os caracteres são trocados um a um por outros), e com ela escreveram o Livro de Jeremias.

Hoje dia a Criptografia vem sendo usada para vários meios de segurança ( O que é indispensavel nos dias de hoje caso queiro ter um sistema seguro e protegido. A criptografia fornece técnicas que permitem a codificação e decodificação dos dados, onde os mesmos podem ser transmitidos e armazenados sem que haja alterações ou a sua exposição a entidade não autorizada. O objetivo da criptografia é prover uma comunicação segura, garantindo aos serviços a confidencialidade, autenticidade, integridade e a não-repudiação.

**Técnicas criptográficas mais utilizadas e conhecidas**

A primeira tecnica de criptografia a ser conhecida foi o chamado "cifra de César" ou "códificador de Júlio Cesar, que apresentava uma das técnicas mais clássicas de criptografia, é um exemplo de substituição que, simplesmente, substitui as letras do alfabeto avançando três casas. O autor da cifragem trocava cada letra por outra situada a três posições à frente no alfabeto. Segundo o autor, esse algoritmo foi responsável por enganar muitos inimigos do Império Romano; no entanto, após ter sido descoberta a chave, como todas, perdeu sua funcionalidade.

Atualmente existem alguns tipos de tecnicas criptograficas bastante utilizadas uma delas são a de chave **simetrica** e **assimetrica,** alem destas tem a criptografia em **redes sem fio** a de **assinatura digital** e a **criptogradia quântica.**

**Chave simetrica**

É o tipo de chave mais simples e a mesma chave é utilizada tanto pelo emissor quanto por quem recebe a informação. Ou seja, a mesma chave é utilizada para codificação e para a decodificação dos dados.

Vários algoritmos de criptografia foram desenvolvidos a partir de chaves simétricas. Dentre os mais comuns estão o DES, o IDEA e o RC.

DES (Data Encryption Standard): criado pela IBM em 1977, o DES usa chaves de 56 bits, permitindo até 72 quatrilhões de combinações. Apesar disso, foi ‘quebrado’ ou desvendado utilizando-se as chamadas técnicas de "força bruta" (tentativa e erro) em um desafio promovido na internet.

IDEA (International Data Encryption Algorithm): criado em 1991 por James Massey e Xuejia Lai, o IDEA é um algoritmo que usa chaves de 128 bits e tem estrutura semelhante ao DES.

RC (Ron's Code ou Rivest Cipher): criado por Ron Rivest na empresa RSA Data Security, esse algoritmo é muito utilizado em e-mails e usa chaves de 8 a 1;024 bits. Há várias versões: RC2, RC4, RC5 e RC6. Cada uma delas difere da outra por trabalhar com chaves de maior complexidade.

Existem ainda outros algoritmos, como o AES (Advanced Encryption Standard), baseado no DES; 3DES; o Twofish; e a sua variante, o Blowfish. O uso de chaves simétricas tem desvantagens, e não é indicado para casos que envolvem informações muito valiosas.

**Chave Assimetrica**

Também conhecida como "chave pública", a chave assimétrica trabalha com duas chaves: uma privada e outra pública.

Nesse método, uma pessoa deve criar uma chave de codificação e enviá-la a quem for lhe mandar informações. Essa é a chave pública. Uma outra chave deve ser criada para a decodificação. Esta, a chave privada, é secreta.

Conheça alguns algoritmos que usam chaves assimétricas:

RSA (Rivest, Shamir and Adleman): criado em 1977 nos laboratórios do Massachusetts Institute of Technology (MIT), é um dos algoritmos de chave assimétrica mais usados. Nele, números primos são utilizados da seguinte forma: dois números primos são multiplicados para se obter um terceiro valor. A chave privada são os números multiplicados e a chave pública é o valor obtido.

**Criptografia nas redes sem fio**

As redes wireless abriram uma brecha enorme na segurança dos dados. Isso porque os dados podem ser facilmente interceptados com algum conhecimento técnico.

Isso obrigou o desenvolvimento de técnicas de criptografia para tornar esse tipo de comunicação viável, não só para empresas que decidem conectar seus usuários por meio de redes sem fio, mas também para que os usuários domésticos possam realizar suas transações financeiras com mais segurança e privacidade.

Os tipos de criptografia mais usados nas redes wireless são:

WEP: esta técnica usa uma chave secreta compartilhada e o algoritmo de criptografia RC4. O roteador wireless ou ponto de acesso, bem como todas as estações que se conectam a ele devem usar a mesma chave compartilhada. Para cada pacote de dados enviado em qualquer direção, o transmissor combina o conteúdo do pacote com uma soma de verificação desse pacote. O padrão WEP pede então que o transmissor crie um IV (Initialization Vector, vetor de inicialização) específico para o pacote, que é combinado com a chave e usado para criptografar o pacote. O receptor gera seu próprio pacote correspondente e o usa para decodificar o pacote. Em teoria, essa abordagem é melhor do que a tática óbvia de usar apenas a chave secreta compartilhada, pois inclui um bit de dado específico para o pacote que dificulta sua violação. Entretanto, se uma chave compartilhada estiver comprometida, um invasor poderá bisbilhotar o tráfego de informações ou entrar na rede.

WPA e WPA2: estes certificados de segurança são baseadas no padrão da Wi-Fi Alliance para redes locais sem fio e utilizados por muitas empresas e até em redes domésticas. Eles permitem autenticação mútua para verificação de usuários individuais e criptografia avançada. A WPA fornece criptografia para empresas, e a WPA2 – considerada a próxima geração de segurança Wi-Fi – vem sendo usada por muitos órgãos governamentais em todo o mundo. “O WPA2 com AES é a novidade, tanto para o uso corporativo quanto para o pessoal. Ao usuário residencial, ele garante um excelente padrão de segurança e, aos usuários corporativos, permite agregar um servidor de autenticação para controle dos usuários em conjunto com a criptografia”, avalia Diogo Superbi, engenheiro de vendas da Linksys no Brasil.

**Assinatura Digital**

Um recurso conhecido por Assinatura Digital é muito usado com chaves públicas. Trata-se de um meio que permite provar que um determinado documento eletrônico é de procedência verdadeira.

Quem recebe um documento assinado digitalmente usa a chave pública fornecida pelo emissor para se certificar da origem. Além disso, a chave é integrada ao documento – isso implica que qualquer alteração realizada nas informações vai invalidar o documento.

**Criptografia Quântica**

Este tipo de codificação de informação difere dos demais métodos criptográficos porque não precisa do segredo nem do contato prévio entre as partes.

A criptografia quântica permite a detecção de intrusos e é incondicionalmente segura mesmo que o intruso tenha poder computacional ilimitado. Mas o seu custo de implantação é muito elevado.

Outro fato limitante para a adoção dessa técnica é a taxa de erros na transmissão dos fótons, seja por ondas de rádio ou fibra ótica. Até agora, os melhores resultados foram obtidos por meio de fibras de altíssima pureza, abrangendo uma distância de aproximadamente 70 km.

**Dissertação**

Em [criptografia](http://pt.wikipedia.org/wiki/Criptografia), a **Cifra de César**, também conhecida como **cifra de troca**, **código de César** ou **troca de César**, é uma das mais simples e conhecidas técnicas de [criptografia](http://pt.wikipedia.org/wiki/Criptografia). É um tipo de [cifra de substituição](http://pt.wikipedia.org/wiki/Cifra_de_substituição) na qual cada letra do texto é substituída por outra, que se apresenta no [alfabeto](http://pt.wikipedia.org/wiki/Alfabeto) abaixo dela um número fixo de vezes. Por exemplo, com uma troca de três posições, A seria substituído por D, B se tornaria E, e assim por diante. O nome do método é em homenagem a [Júlio César](http://pt.wikipedia.org/wiki/Júlio_César), que o usou para se comunicar com os seus [generais](http://pt.wikipedia.org/wiki/General).

O processo de criptografia de uma cifra de César é frequentemente incorporado como parte de esquemas mais complexos, como a [cifra de Vigenère](http://pt.wikipedia.org/wiki/Cifra_de_Vigenère), e continua tendo aplicações modernas, como no sistema [ROT13](http://pt.wikipedia.org/wiki/ROT13). Como todas as [cifras de substituição monoalfabéticas](http://pt.wikipedia.org/wiki/Cifra_de_substituição_monoalfabética), a cifra de César é facilmente decifrada e na prática não oferece essencialmente nenhuma segurança na comunicação.

**Estruturação, conceitos e fundamentação**

Apesar de a criptologia estar bastante avançada na época, em 50 a.C. César usava um sistema bastante simples de substituição. Suetônio, escritor romano que viveu no início da era cristã (69 d.C.), em Vida dos Césares, escreveu a biografia dos imperadores romanos, de Júlio César a Domiciano.  
Conta que Júlio César usava na sua correspondência particular um código de substituição no qual cada letra da mensagem original era substituída pela letra que a seguia em três posições no alfabeto: a letra A era substituída por D, a B por E, e assim sucessivamente.  
Hoje em dia, porém, a denominação de Código de César é utilizada para qualquer cifra na qual cada letra da mensagem clara seja substituída por outra deslocada um número fixo de posições, não necessariamente três. Um exemplo é o código que, ainda segundo Suetônio, era usado por Augusto, onde a letra A era substituída por B, a B por C e assim sucessivamente.  
Como o alfabeto romano possui 26 letras, é possível obter 26 alfabetos cifrantes diferentes, dos quais um (o do deslocamento zero) não altera a mensagem original. Cada um destes alfabetos cifrantes é conhecido como Alfabeto de César.  
Características:  
\* Origem: Usada pelo imperador romano Júlio César em 50 a.C.  
\* Classe: Substituição Simples.  
\* Tipo: Monoalfabética (porque usa apenas UM alfabeto cifrante) Monogrâmica (porque trata cada UM dos caracteres individualmente).  
\* Segurança: Baixíssima  
\* Uso: Aplicável apenas em textos muito curtos.  
\* Criptoanálise: Uma simples criptoanálise baseada na característica estatística da língua é suficiente para decifrar o texto.  
A substituição original do código de César encontra-se na tabela abaixo:  
  
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C  
  
O Código de César original tem um deslocamento de 3 posições, porém é possível usar qualquer deslocamento. O deslocamento zero mantém a mensagem original.

**Benefícios em relação às técnicas anteriores**

As técnicas anteriores usavam o mesmo método substituição, como o método usado pelos hebreus, entre 600 a.C. e 500 a.C. onde escreveram o livro de Jeremias utilizando uma cifra de substituição simples o Atbash. Onde consiste na substituição do Aleph (a primeira letra) pela tav (a última), beth (a segunda) pela shin (a penúltima), e assim por diante, invertendo o alfabeto usual. Desta forma concluímos que a técnica utilizada por César era razoavelmente segura, ainda mais porque a maioria dos inimigos de César eram analfabetos.

**Aplicações que fazem/fizeram uso da técnica**

A cifra de César segundo Suetónio era usava com uma troca de três posições para proteger mensagens de significado militar. Como todas as cifras de substituição monoalfabéticas, a cifra de César é facilmente decifrada e na prática não oferece essencialmente nenhuma segurança na comunicação, assim ela não é muito utilizada.

**Discussão comparativa entre esta técnica e outras conhecidas /**

**Utilizadas**

A **cifra de Vigenère** é um método de [criptografia](http://pt.wikipedia.org/wiki/Criptografia) que usa uma série de diferentes [cifras de César](http://pt.wikipedia.org/wiki/Cifra_de_César) baseadas em letras de uma senha. Trata-se de uma versão simplificada de uma mais geral cifra de [substituição polialfabética](http://pt.wikipedia.org/w/index.php?title=Substituição_polialfabética&action=edit&redlink=1), inventada por Leone Battista Alberti cerca de [1465](http://pt.wikipedia.org/wiki/1465).

A invenção da cifra de Vigenère é erradamente atribuída a [Blaise de Vigenère](http://pt.wikipedia.org/wiki/Blaise_de_Vigenère); encontra-se originalmente descrita por Giovan Batista Belaso no seu livro datado de [1553](http://pt.wikipedia.org/wiki/1553) com o título *La cifra del. Sig. Giovan Batista Belaso*.

Esta [cifra](http://pt.wikipedia.org/wiki/Cifra) é muito conhecida porque é fácil de perceber e de pôr em prática, parecendo, a quem tem pouca prática, que é inquebrável (indecifrável). Consequentemente, muitos programadores implementaram esquemas de criptografia nas suas aplicações que são no essencial cifras de Vigenère, e que são facilmente quebradas por qualquer criptanalista.

**Vulnerabilidades e falhas**

O problema envolvido nessa cifra estava no procedimento lento, sobretudo na circulação, onde os emissários demoravam a enviar as mensagens da capital as demais cidades, bases militares e regiões sob conflito por conta das distancias percorridas, correndo também o grande risco do próprio ser morto no trajeto ou ser capturado e este possivelmente entregar o conceito (a chave) da descriptografia da mensagem, com o desenvolvimento cientifico se viu necessária a criação de uma nova lógica criptográfica, conhecida como a fórmula de Sator, que trazia por sua vez uma lógica mais avançada e logo depois substituída pelo teorema do Papiro de Leiden.  
Visto no plano contemporâneo globalizado e formal, que sustenta se nos meios de comunicação e a circulação da informação, a cifra de César perdeu seu valor em seus antigos planos, sua lógica fraca deu lugar a outras lógicas criptográficas, isso devido ao “encolhimento” das distancias no globo e no progresso matemático nos algoritmos, na lógica e contemporaneamente na informática, assim, em relação a cifra de César podemos concluir que, tais métodos algoritmos usualmente chamados de cifras de” lápis e papel ”estão muito distantes dos Algoritmos criptográficos modernos assimétricos que são projetados para serem executados por computadores ou por dispositivos especializados de hardware e assegurar a informação de bancos, governos, instituições privadas, multinacionais entre outras empresas, a cifra se césar entrou apara a historia e foi substituída por códigos complexos como os das funções Hash.

**Melhorias propostas e/ou implementadas.**

Entramos com um sistema interativo da cifra de César onde o usuário digita o valor de casa que ele irá deslocar. A partir deste temos também uma adição de um caractere especial entre cada caractere do arquivo original, e esse vária caso o numero do caractere do arquivo for par ou ímpar.

**Relatório de linhas de código do programa**

**using** System;

using System.Collections.Generic;

using System.Linq;

using System.Text;

namespace Sistema\_de\_Criptografia

{

class Program

{

static void Main(string[] args)

{

//declaração de variáveis

string p, encrypt;

int i, opcao, crypt, codigo;

bool b1;

//do..while para repetição do programa até que seja escolhida a opção sair

do

{

//menu do programa

Console.WriteLine("CRIPTOGRAFIA - CIFRA DE CESAR\n");

Console.WriteLine("1 para Criptografar");

Console.WriteLine("2 para Descriptografar");

Console.WriteLine("0 para Sair\n");

Console.Write("Digite a opção: ");

//do..while para repetição até que o usuário digite uma opção válida

do

{

encrypt = "";

p = "";

//usando uma variável boleana para verificar se o que o usuário digitar é um valor do tipo inteiro

b1 = int.TryParse(Console.ReadLine(), out opcao);

//se a opção for falsa, mostrar a mensagem abaixo

if (((opcao != 1) && (opcao != 0) && (opcao != 2)) || (b1 == false))

{

Console.Write("Opção inválida, por favor digite novamente: ");

}

}

while (((opcao != 1) && (opcao != 0) && (opcao != 2)) || (b1 == false));

//usando o comando switch..case para a escolha da opção

switch (opcao)

{

//caso a opção digitada seja '1'..

case 1: Console.Write("\nEntre com a mensagem para ser criptografada: ");

//do..while para consistir até que o usuário digite algo

do

{

//recebe o valor digitado pelo usuário, atribui à variável 'p' e em letra minúscula com o comando .ToLower()

p = Console.ReadLine().ToLower();

//se não for digitado nada, mostre a mensagem abaixo

if (p == "")

{

Console.Write("Por favor, não deixe este campo em branco. Digite novamente: ");

}

//se nao(se for digitado algo) então faça..

else

{

//estrutura de repetição 'for', para criptografar letra por letra digitadas pelo usuário

for (i = 0; i < p.Length; i++)

{

//a variável crypt recebe a primeira letra digitada pelo usuário, e com o laço de repetição ela recebe as outras em seguida, até a ultima

crypt = p[i];

//para a letra digitada, é acrescentado 3 na tabela ASCII

codigo = crypt + 3;

/\*atribui a variável encrypt a letra que foi criptografada, sendo assim, depois de todas as

letras da palavra digitada pelo usuário serem criptografadas e adicionadas à variável,

formará um código da palavra digitada, que será o conteúdo da variável encrypt\*/

encrypt += Convert.ToChar(codigo);

}

//mostra o resultado da criptografia

Console.Write("\nMensagem criptografada: " + encrypt);

fim();

}

}

while (p == "");

break;

/\*lcaso a opção digitada seja '2', acontecerá o mesmo processo que no primeiro caso, porém na hora da criptografia

ao invés de ser acrescentado 3 casas na tabela ASCII será decrementado, fazendo o processo de descriptografia\*/

case 2: Console.Write("\nEntre com a mensagem para ser descriptografada: ");

do

{

p = Console.ReadLine().ToLower();

if (p == "")

{

Console.Write("Por favor, não deixe este campo em branco. Digite novamente: ");

}

else

{

for (i = 0; i < p.Length; ++i)

{

crypt = p[i];

codigo = crypt - 3;

encrypt += Convert.ToChar(codigo);

}

Console.Write("\nMensagem descriptografada: " + encrypt);

fim();

}

}

while (p == "");

break;

}

}

while (opcao != 0);

}

public static void fim()

{

Console.Write("\n\n\n-------TECLE ENTER PARA CRIPTOGRAFAR OU DESCRIPTOGRAFAR OUTRA MENSAGEM.-------\n\n");

Console.ReadKey();

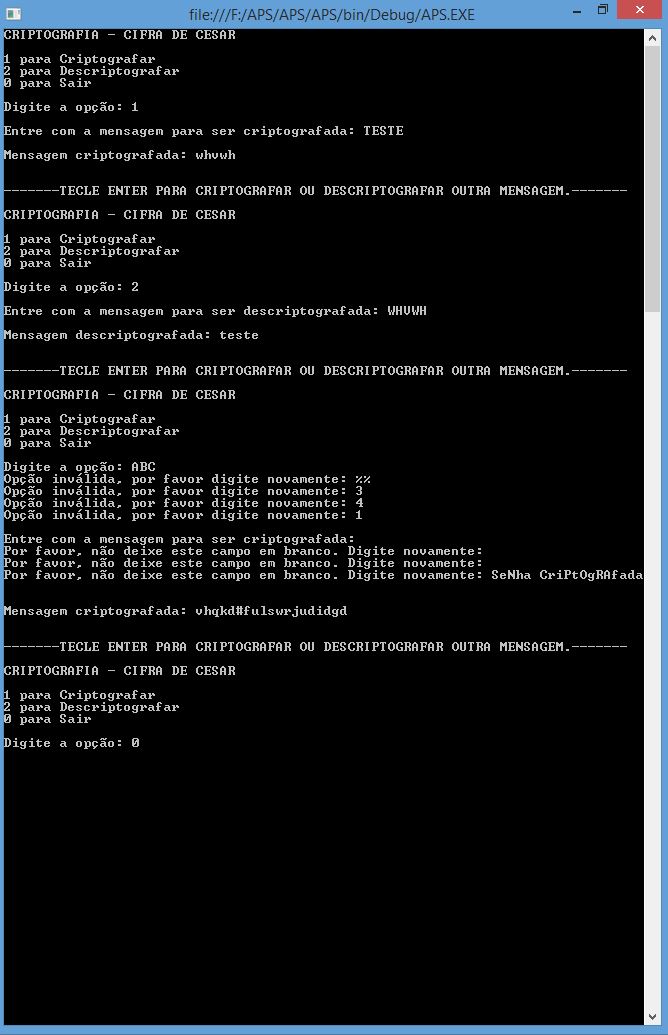
}

}

}

**Apresentação do programa em funcionamento em um computador, apresentando todas as funcionalidades pedidas e extras. (Próxima**

**página**



**Bibliografia**

* [**http://pt.wikipedia.org/wiki/Criptografia**](http://pt.wikipedia.org/wiki/Criptografia)
* [**http://cartilha.cert.br/criptografia/**](http://cartilha.cert.br/criptografia/)
* [**http://www.techtudo.com.br/artigos/noticia/2012/06/o-que-e-criptografia.html**](http://www.techtudo.com.br/artigos/noticia/2012/06/o-que-e-criptografia.html)
* [**http://informatica.hsw.uol.com.br/criptografia.htm**](http://informatica.hsw.uol.com.br/criptografia.htm)
* [**http://olhardigital.uol.com.br/video/o-que-e-criptografia/32637**](http://olhardigital.uol.com.br/video/o-que-e-criptografia/32637)
* [**http://pt.wikipedia.org/wiki/Cifra\_de\_C%C3%A9sar**](http://pt.wikipedia.org/wiki/Cifra_de_César)
* [**http://cmup.fc.up.pt/cmup/ajmachia/html/slide\_2.html**](http://cmup.fc.up.pt/cmup/ajmachia/html/slide_2.html)
* [**http://setesys.com.br/blog/como-produzir-senhas-criativas-utilizando-a-cifra-de-cesar/**](http://setesys.com.br/blog/como-produzir-senhas-criativas-utilizando-a-cifra-de-cesar/)
* [**http://www.mcsesolution.com/Seguran%C3%A7a/a-matematica-da-cifra-de-cesar.html**](http://www.mcsesolution.com/Segurança/a-matematica-da-cifra-de-cesar.html)
* [**http://pt.wikipedia.org/wiki/Cifra\_de\_substitui%C3%A7%C3%A3o**](http://pt.wikipedia.org/wiki/Cifra_de_substituição)

**Ficha de Atividades Práticas Supervisionadas**

