CRIPTOGRAFIA APLICADA NA LINGUAGUEM C

**Kevin Noviski e Anderson Almeida**

Bacharelado em Sistemas de Informação/2° Período

*Sociedade Paranaense de Ensino e Informática*

***Resumo.*** *O presente artigo tem como objetivo mostrar como a criptografia vem sendo utilizada manualmente e computacionalmente ao longo do tempo até os dias atuais. Criptografia é a junção das palavras gregas "Kryptós" e "gráphein", que significam "oculto" e "escrever". Trata-se de um conjunto de regras que visa ocultar a informação de forma que somente quem envia e recebe a mensagem consiga decifrá-la. Para que isso aconteça vários métodos diferentes são usados, e ao passar do tempo são modificados permitindo assim o surgimento de técnicas mais seguras. E também ira apresentar como estudantes do curso de Bacharelado em Sistemas de Informação desenvolveram um software que utiliza criptografia para codificar arquivos de texto, implementado na Linguagem C.*

***Abstract.*** *This article was written to show how Cryptography has been used throughout the years, while it was made by hand and by computers. The word Cryptography is made up of two Greek words, "Kryptós" and "gráphein", they mean to hide and to white. This is a method used to hide secret information, making it possible to send a message with its contents hidden within the text, only the people who send the message and the ones who receive the message will understand what’s written in there. Throughout the years they’ve developed a series of different methods to achieve perfection. This article will also show how students managed to create a software that encrypts messages using the C language.*

***Palavras-chave:*** *Criptografia, Ocultar, Decifrar, Manualmente e Computacionalmente.*

**1. INTRODUÇÃO**

Com a necessidade de proteger informações sigilosas, sendo elas de origem familiar, militar, religiosa ou governamental surgiram diferentes maneiras de ocultar tais informações, com esse intuito a criptografia foi criada para proteger, por exemplo, mensagens enviadas para bases militares, informando planos de ataque, localizações de bases, mensagens que não podiam ser desviadas de seu destinatário, e mesmo que a mensagem fosse interceptada, não houvesse nenhum perigo de perder o sigilo. A partir desta necessidade foram criadas técnicas para criptografar informações, ao passar do tempo essas técnicas foram aprimoradas.

**2. FORMULAÇÃO DO PROBLEMA.**

O objetivo inicial foi definido como: Desenvolver um programa em C que utiliza de alguma maneira operações de matrizes. A partir deste tema surgiu a idéia de criar um software que criptografa-se um texto, para isso utilizaria uma senha gerada através de operações matriciais. Antes de qualquer coisa foi necessário adquirir um amplo conhecimento sobre criptografia como um todo, para que a partir disso a técnica pudesse ser escolhida para que o programa fosse desenvolvido.

**3. ESTADO DA ARTE**

**HISTÓRIA DA CRIPTOGRAFIA.**

Segundo Kahn (1967), o primeiro exemplo documentado da escrita cifrada relaciona-se aproximadamente ao ano de 1900 a.C, quando o escriba de Khnumhotep II teve a idéia de substituir algumas palavras ou trechos de texto. Caso o documento fosse roubado, o ladrão não encontraria o caminho que o levaria ao tesouro e morreria de fome perdido nas catacumbas da pirâmide.

A criptografia ao longo do tempo se divide em três fases que são: criptografia manual, criptografia por máquinas e criptografia por rede.

**3.1. Criptografia manual**

-**Bastão de Licurgo:** Técnica criada e utilizada pelos Espartanos para ocultar mensagens enviadas de general a general, onde a mensagem era escrita em uma tira de couro, enrolada em um bastão com tamanho e diâmetro especifico, a mensagem era então enviada enrolada na cintura do mensageiro, a leitura da mensagem somente era possível com o uso do outro bastão com as mesmas medidas do bastão usado para escrever a mensagem.

-**Cifra de Cesar:** A utilização de algoritmos da criptografia foi vista pela primeira vez na Cifra de Cesar, que utilizava a cifra para se comunicar com seus generais. Com o passar do tempo esta técnica foi descoberta por seus inimigos, pois ela utiliza um deslocamento fixo, de três posições no alfabeto para a direita, ou seja, se uma palavra for decodificada a mensagem inteira também será, pois utiliza o mesmo deslocamento.

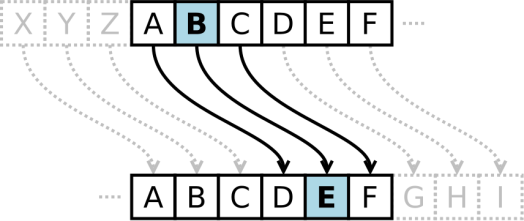


Figura 1. Cifra de Cesar

A cifra de Cesar pode ser gerada usando mais do que três Posições de deslocamento, porem sua limitação é o numero de deslocamento, que será sempre fixo.

-**Cifra de Vigenère:** A cifra de Vigenère criada por Giovan Battista Bellaso, porem erradamente atribuída a Blaise de Vigenère. Esta Cifra consiste da utilização de varias cifras de Cesar, a diferença esta nas posições de deslocamento, onde uma palavra chave é usada para definir as posições de deslocamento baseado na tabela de Vigenère.

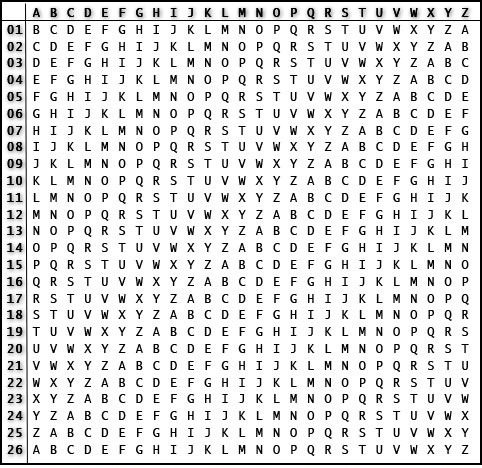


Figura 2. Tabela de Vigenère

Utilizando a palavra chave “ceu” as seguintes posições de deslocamento são adquiridas: 2, 3, 18 porque a letra ‘c’ na primeira coluna esta na linha 2, na segunda coluna a letra ‘e’ esta na linha 3, na terceira coluna a letra ‘u’ esta na linha 18. A partir desta chave é usado o mesmo conceito da cifra de Cesar, por exemplo, a palavra “ela” se transformaria em “gos” onde a primeira letra ‘e’ desloca duas casas para a direita torna-se ‘g’, a segunda letra ‘l’ desloca três casas torna-se ‘o’ e a terceira dezoito casas para a direita tornando-se ‘s’.

**3.2. Criptografia por Máquinas**

A criptografia evoluiu muito com o passar dos anos, deixou de ser feita diretamente a mão e passou a usar máquinas com complexidade e eficiência muito maiores que seus antecedentes, juntamente com novas formas de criptografar, surgiram também novos métodos para decodificar mensagens criptografadas.

**3.2.1 Código Morse**

O Código Morse foi inventado por Samuel Morse, o físico Joseph Henry e o inventor Alfred Vail. Trata-se de mensagens enviadas usando sinais elétricos, neste método utiliza-se uma variedade de sinais elétricos, onde uma voltagem-ligada longa significa um traço, voltagem-ligada curta significa um ponto, voltagem-desligada longa significa espaço entre caracteres e palavras e voltagem-desligada curta (espaço entre pontos e traços), para que seja possível decodificar este código sonoro, é necessário possuir uma tabela com todas as combinações de sinais e seus respectivos significados.

**3.2.2 Enigma**

Os inventores da máquina Enigma foram os alemães Arthur Scherbius e Richard Ritter, fundadores da empresa Scherbius & Ritter, eles inventaram a enigma usando rotores eletromecânicos, tentaram vender a máquina para a marinha alemã, porém a Marinha não achou ser necessário uso desta máquina, somente em 1926 após algumas alterações terem sido feitas na maquina, a Marinha Alemã aceitou comprar a máquina, então passou a ser usada pela marinha, exército e diplomacia alemã, aproximadamente 200mil máquinas foram produzidas. A Enigma foi muito usada durante a segunda guerra mundial.

**Criptografia em Redes**

Com a evolução tecnológica, os antigos métodos de criptografia foram aprimorados, inovados, reduzindo assim a margem de erro dos códigos e a chance de serem decifrados, a velocidade e complexidade computacional contribuiu para um avanço muito significativo em termos de eficácia, tanto para cifrar uma mensagem quanto para decifrá-la. Novos modos surgiram com uma vasta variedade de métodos e conceitos em criptografia, deixando de ser usada apenas em mensagens de texto, mas para fins mais complexos como certificados digitais. Na criptografia atual o uso de chaves é um ponto principal para o grau de segurança do código, seu nível de segurança pode ser obtido de acordo com o número de bits que a chave utiliza, quanto maior o número de bits utilizado na chave menor a chance de quebrar o código usando força bruta. Usando uma chave de oito bits é possível ter até 256 combinações de chaves, mesmo sendo um número grande ainda não é impossível de ser quebrado a força bruta(tentar todas as combinações possíveis até encontrar a verdadeira), já quando uma chave de mais de 8 bits é usada, a segurança aumenta significantemente, mesmo sendo mais segura e mais difícil de ser quebrada, ainda assim a chave pode ser rompida. A criptografia em redes é executada de duas formas, usando chaves Simétricas e chaves Assimétricas.

**Criptografia Simétrica**

A chave Simétrica também conhecida com “chave secreta” pode ser considerada como um método muito seguro, pois utiliza somente uma chave para codificação e decodificação, sendo assim existe apenas uma maneira para decodificar um arquivo criptografado, o ponto fraco deste método é na transmissão da chave, se o emissor enviar a chave ao receptor e esta por sua vez for interceptada, sua segurança é perdida completamente, sendo esta a única fraqueza deste método. A partir deste método surgiram-se novas técnicas de criptografia, como por exemplo:

**- DES** Data Encryption Standard, técnica que foi desenvolvida pelos pesquisadores da IBM (International Business Machines), ficou muito famosa nos Estados Unidos após ter sido aceita pelo governo americano em 1977 devido ao seu alto nível de segurança. Com isso, este método foi rapidamente adotado por outros setores como, por exemplo, o setor financeiro onde a necessidade de manter sigilo é muito grande. O DES é um cifrador de blocos, em outras palavras, ele não aplica a cifra em um bit de cada vez, mas sim em um bloco de informação por vez. Para criptografar um texto o DES agrupa blocos de 64-bits por vez, e aplica a chave no bloco, transformando assim em um bloco cifrado de 64-bits, usando permutações e substituições. O DES usa um sistema com uma chave de 64-bits, sendo que oito destes 64 não são realmente usados para a cifra, deixando assim a chave com 56-bits, isso leva a um numero muito alto de possíveis combinações de senhas igual a 2^56, porem esse numero não foi muito bem aceito, pois ainda era possível quebrar a senha usando força bruta, isso é, tentar todas as combinações possíveis para encontrar a senha correta, é uma tarefa muito difícil mas não é impossível. Com o passar do tempo a DES foi substituída pela AES(Advanced Encryption Standard), por sua alta segurança medida pelo tamanho da chave utilizada neste método, nele é possível usar três tipos diferentes de chaves, a de 128-bits, 192-bits ou a mais eficiente de 256-bits.

**Chaves Assimétricas**

O problema com chaves Simétricas esta na forma em que são transmitidas, seja pela internet ou meio físico, sempre existirá a possibilidade de esta chave cair nas mãos erradas, para resolver este problema a chave Assimétrica foi criada, também conhecida como “chave - publica”, esta técnica utiliza duas chaves, uma é publica, pode ser postada em qualquer lugar, a outra é chamada de chave-privada, a decodificação de um documento é dada através da junção das duas chaves. O lado ruim deste método é que requer muito mais processamento tanto para cifrar quanto para decifrar uma mensagem.

**DESCRIÇÃO**

O programa desenvolvido usa um conjunto de técnicas de criptografia, a princípio foi utilizado apenas a técnica de Cesar, porem com a avanço do projeto foi implementado não somente um número fixo de deslocamento, mas vários, cada letra recebe um número de deslocamento diferente, aumentando assim a segurança do código. Para que isso fosse possível foi utilizado uma função da linguagem C, esta função tem como objetivo gerar números pseudo aleatórios usando um número base chamado de “Seed” que significa "semente",em Português, a partir deste número é que são geradas as posições de deslocamento, se a Seed é modificada, todos os números gerados também serão. Para que a seed seja gerada, o usuário entra com uma senha de quinze dígitos (120-bits), todos os caracteres digitados na senha são lidos pelo programa em seu valor inteiro, e não como caractere, para que se possa fazer cálculos matriciais com estes números inteiros, gerando assim a seed. Neste programa foi utilizado o método de chave Simétrica, ou “chave secreta”. O Programa possui duas funções, a de Criptografar arquivos de texto e a de decodificar arquivos criptografados, a senha é inserida ao iniciar o programa, e pode ser alterada durante a execução se for necessário.

**IMPLEMENTAÇÃO**

A idéia central do algoritmo implementado em C é de usar todos os caracteres uteis da tabela ASCII em uma fita circular, usando está fita como base para a codificação. Assim que o arquivo de texto é aberto, um vetor recebe todos os caracteres do texto, para evitar o desperdício de memória, foi utilizado Alocação Dinâmica de memória, deixando assim o vetor com o tamanho exato do texto. As posições de deslocamento são definidas dentro de um vetor com o mesmo tamanho do texto. Para o processo de codificação, cada caractere é analisado e trocado de acordo com o numero de deslocamento armazenado no vetor chave, ou seja, vetor texto posição um é deslocado de acordo com o numero de vezes armazenado no vetor chave posição um, e assim por diante.



(1)

O processo inverso utiliza a mesma lógica, mas ao invés de deslocar a direita, desloca-se a esquerda.



(2)

Para evitar a perda do arquivo em caso de erro ao digitar a senha, um novo arquivo é aberto toda vez que uma decodificação é executada, assim se a senha estiver errada o arquivo criptografado não será substituído com informações erradas. O mesmo acontece com um arquivo em sua forma regular, com suas informações legíveis, ao passar este arquivo no programa, ele não é substituído, um novo arquivo é criado com suas informações criptografadas, a partir disto o usuário é que escolhe apagar ou manter o arquivo original.

**RESULTADOS**

Grandes arquivos podem ser codificados, o programa mostra não ter uma alta taxa de repetição de deslocamentos, a cada nova senha o resultado é sempre diferente. Textos escritos em português são reconhecidos pelo programa, mesmo com toda acentuação contida na linguagem Portuguesa, As únicas limitações deste programa são: O texto contido no arquivo a ser criptografado, não pode em momento algum pular uma linha, o texto tem que ser seqüencial, caso haja uma nova linha, o programa não reconhece o valor binário para “nova linha” e gera um erro, não finalizando a codificação. Outra limitação é que este programa consegue somente ler arquivos no formato .txt outros formatos não são reconhecidos.

**CONCLUSÃO**

Com a ajuda de todos os recursos e funções disponíveis na linguagem C, e com uma ampla pesquisa sobre os diversos métodos e técnicas de criptografia foi possível desenvolver um programa que codifica arquivos de texto, sendo eles em português ou inglês, a linguagem não é um item decisivo contanto que as letras do alfabeto constem na tabela ASCII. O uso de cálculos matriciais fez com que as senhas geradas, tenham um nível de dificuldade muito maior, pois a senha não é baseada em simples caracteres, mas sim operações matemáticas, a senha possui 15 bytes, sendo assim pode haver 2120 combinações isto é, 1.329228e36 combinações diferentes, isso torna mais difícil a quebra da senha a força bruta.

# Agradecimentos

Esta seção deve estar localizada entre o fim do corpo do texto e a lista de referências. Digite somente ***Agradecimentos*** em negrito e itálico, com alinhamento à esquerda, pule uma linha e digite o texto regularmente.

**4. REFERÊNCIAS**

As referências devem ser citadas no texto pelo nome do autor e número entre colchetes, na primeira vez, por exemplo: “Em um trabalho recente, Hunt *et al*. [Hunter-1983] propuseram..." A partir da segunda vez em que a mesma referência é citada, basta colocar [Hunter-1983], por exemplo: "em [Hunter-1983] comprova-se que..." Numere as citações de forma consecutiva, segundo a ordem de referência a elas no texto, entre colchetes [Hunter-1983]. Para a redação de cada referência observe os modelos a seguir:

Para citação de um artigo de periódico:

[Hunter-1983] HUNTER, J.S. e HUNG, J.C., “Development of low-cost Multifunction sensors for lightweight fire and forget antitank weapon system,” IEEE Trans. Industrial Electronics, vol. E-30, no. 1, Feb. 1983, pp. 7-10.

Para citação de um livro:

[Dubey-1989] DUBEY, G.K., Power Semiconductor Controlled Drives, Englewood Cliffs, NJ: 1989, p. 81.

Para citação de trabalho apresentado em um evento:

[Alqueres-1991] ALQUERES, J. L. e PRACA, J. C., “The Brazilian power system and the challenge of the Amazon transmission,” in Proceedings of the 1991 Power Engineering Society Transmission and Distribution Conference, 91CH3070-0, pp. 315-320.

<http://www.penta.ufrgs.br/gere96/segur2/des.htm>

acessado em 23/09

<http://www.ricardojcsouza.com.br/download/seguranca_redes_7.pdf>

acessado em 23/09

FECHINI, Joseana Macêdo. Segurança da Informação. Disponível em http://www.dsc.ufcg.edu.br/~joseana/Criptografia-SI.html .

BRAGA, Hugo Rodrigo. HISTÓRIA DA CRIPTOLOGIA – Antiguidade. Disponível em http://www.hu60.com.br/assuntos/criptologia.php .

STALLINGS, William. Criptografia e segurança de redes. 4. ed. São Paulo: Pearson Prentice Hall, 2008.

<https://support.microsoft.com/en-us/kb/246071>

acessodo em 23/09

<http://searchsecurity.techtarget.com/definition/asymmetric-cryptography>

acessado em 23/09