INTERFACE TECNOLÓGICA
volume 10 - número 1 - 2013

CRIPTOGRAFIA: UMA APLICAÇÃO DA MATEMÁTICA DISCRETA ATRAVÉS DA IMPLEMENTAÇÃO DA CIFRA DE CÉSAR EM VISUALG

ENCRYPTION: AN APPLICATION OF DISCRETE MATHEMATICS THROUGH THE IMPLEMENTATION OF CAESAR CIPHER BY USING VISUALG

Douglas Francisco Ribeiro[1]
Patrícia Gonçalves Primo Lourençano[2]
Aparecido Doniseti da Costa[3]

RESUMO

A ideia deste artigo é descrever como desenvolver um algoritmo capaz de criptografar e descriptografar mensagens utilizando, para isso, formulações matemáticas do tipo criptografia RSA[4], que utiliza chaves públicas e privadas construídas com base na teoria dos números. Utilizar-se-á o software VisuAlg para descrever em linguagem computacional e, ao mesmo tempo, mostrar como criar um algoritmo capaz de fazer essas operações. Para a demonstração dos algoritmos escolhemos como base uma formulação básica: a cifra de César.

PALAVRAS-CHAVE: Algoritmo. Módulo n. Criptografia. Cifra de César.

ABSTRACT

The idea of this article is to describe how to develop an algorithm to encrypt and decrypt messages using, for this, mathematical formulations of type RSA encryption, built using public and private keys based on number theory. VisuAlg to describe the software in computer language and at the same time show how to create an algorithm capable of these operations will be-used. For the demonstration of the algorithms chosen based on a basic formulation: the Caesar cypher.

KEYWORDS: *Algorithm. n Module. Encryption. Caesar Cypher.*

[1] Graduando do curso Sistemas para Internet da FATEC- TQ. douglas.ribeiro@ig.com.br
[2] Professora Pleno da FATEC-TQ. patricia.lourencano@fatectq.edu.br
[3] Professor Coordenador do Curso de Sistemas para Internet da FATEC-TQ doniseti.costa@fatectq.edu.br
[4] O RSA é um algoritmo que possui este nome devido a seus inventores: Ron Rivest, Adi Shamir e Len Adleman, que o criaram em 1977 no MIT. (Oliveira, 2006)

INTRODUÇÃO

Esse trabalho mostra como usar a linguagem de programação VisuAlg na implementação do método da Cifra de César na resolução de sentenças criptografadas.

A Criptografia[5] é a ciência que estuda as formas de se escrever uma mensagem utilizando código. Trata-se de um conjunto de técnicas que permitem tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir que apenas o destinatário a decifre e compreenda (Cavalcante, 2004). De maneira geral, há um emissor que tenta enviar uma mensagem para um receptor. Existe também um adversário que deseja interceptar essa mensagem (Stein, 2011). O ato de criptografar é também conhecido como - encriptação e desencriptação. A encriptação é a conversão de dados para uma forma que não será compreendida facilmente por pessoas não autorizadas, com o objetivo de assegurar a privacidade, mantendo a informação escondida e ilegível mesmo para quem vê os dados. A desencriptação é o processo de converter dados encriptados de volta a sua forma original, para que a mensagem possa ser compreendida. Para que isso aconteça alguma informação secreta é requerida, usualmente denominada chave.

Apesar da criptografia ser bem antiga, originalmente utilizada para fins militares e diplomáticos ao longo dos séculos, atualmente percebe-se um grande interesse sobre o assunto, principalmente devido a utilização de vários serviços na Internet. O comércio eletrônico, por exemplo, precisa manter diversas informações confidenciais, como registros bancários, faturas de cartão de crédito, senhas e outras.

No campo da criptografia existem algumas denominações específicas:

- os códigos são denominados cifras;
- as mensagens não codificadas são textos comuns;
- as mensagens codificadas são textos cifrados ou criptogramas.

O processo de conversão de um texto comum em cifrado é chamado **cifrar** ou **criptografar** e o processo inverso de converter um texto cifrado em comum é chamado **decifrar** ou **descriptografar**. Os termos criptografar e descriptografar são os mais utilizados no meio científico.

As criptografias mais simples e também as mais fáceis de serem quebradas são as denominadas cifras de substituição, também chamadas de Código de César. No Código de César, cada letra do alfabeto é substituída por outra letra.

VISUALG

O VisuAlg foi criado em 1987 pelo professor Cláudio Morgado de Souza que atua na área de

[5] A palavra Criptografia é definida por dois termos gregos *kryptos* (kryptos secreto,escondido, oculto) e *grapho* (grapho – escrita, grafia).

desenvolvimento de software. O objetivo dessa ferramenta é permitir, aos iniciantes em programação, o exercício dos seus conhecimentos num ambiente próximo da realidade. VisuAlg possui as características de uma linguagem apropriada para a aprendizagem de programação. Segundo Almeida (2013) esta ferramenta é capaz de simular o que acontece na tela do computador com o uso dos famosos comandos "leia" e "escreva", bem como possibilitar a verificação dos valores das variáveis, o acompanhamento passo a passo da execução de um algoritmo e até mesmo suportar um modo simples de depuração.

O VisuAlg é um software simples, que não depende de DLLs[6], OCXs ou outros componentes. Sua instalação não copia arquivos para outra pasta a não ser aquela em que for instalado, e exige cerca de 1 MB de espaço em disco. Pode ser executado sob Windows 95 ou posterior, e tem melhor aparência com resolução de vídeo de 800x600 ou maior.

METODOLOGIA

O presente artigo tem como objetivo empregar conceitos e conhecimentos matemáticos algébricos, tais como aritmética módulo n, fundamentando dessa forma, a criptografia RSA[7].

Mostrar-se-á por meio deste trabalho que para chegar a uma mensagem criptografada, pode-se fazer uso de conhecimentos matemáticos fundamentados na aritmética módulo n e implementar um algoritmo utilizando o software VisuAlg.

Por meio de dois códigos, um de codificação e outro de decodificação de uma mensagem na linguagem de programação VisuAlg, mostraremos o uso prático e efetivo da matemática. Demonstrar-se-á ainda, que este programa é fácil de ser trabalhado por utilizar uma linguagem simplificada.

CIFRA DE CÉSAR

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. Ela substitui cada letra do texto por outra, que se apresenta no alfabeto abaixo dela um número fixo de vezes. Por exemplo, com uma troca de três posições, "D" seria substituído por "G", "E" se tornaria "H" e assim por diante. Este nome foi concedido em homenagem a Júlio César, que a usou para se comunicar com seus generais.

[6] As DLLs (Dynamic-link library) juntamente com as OCXs (OLE control extension) são arquivos com definições e recursos necessários para a execução de programas. Foram desenvolvidas pela Microsoft e são comumente chamadas de bibliotecas.

[7] O RSA é um algoritmo que possui este nome devido a seus inventores: Ron Rivest, Adi Shamir e Len Adleman, que o criaram em 1977 no MIT. (Oliveira, 2006)

A figura 1 ilustra a relação de letras de um Alfabeto Simples.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	W	Y	Z

Figura 1. Alfabeto Simples

Seguindo a ideia de deslocamento de três posições, a figura 2 pode ser criada:

D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	W	Y	Z	A	B	C

Figura 2. Alfabeto Cifrado

Uma mensagem como: "ALGORITMO" seria cifrado como "DOJRULXPR". A equivalência entre as letras pode ser facilmente identificada quando ambos os conjuntos de letras são sobrepostos, como na figura 3:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	W	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	W	Y	Z	A	B	C

Figura 3. Alfabeto simples e alfabeto cifrado

Poder-se-ia também representar essa cifra usando aritmética, transformando as letras em números, seguindo um esquema: A=0, B=1 até Z=25. Teríamos um total de 26 letras. A simples troca de uma letra x por uma fixa n pode ser descrita como:

$$E_n(x) = (x + n) \bmod 26$$

Já para a sua descriptografia teríamos que ter a inversa desta fórmula:

$$D_n(x) = (x - n) \bmod 26$$

Como o número encontrado precisa estar dentro da faixa das 26 posições definidas na tabela, utiliza-se o artifício do resto da divisão. Deste modo, tem-se a certeza de que este número estará no intervalo entre 0 e 25, ou seja, exatamente o esquema sugerido.

Pode-se verificar isso na prática através da frase "EU VOU".

Tabela 1. Alfabeto relacionado com número arábico.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
1	2	3	4	5	6	7	8	9	10	11	12	13
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**X**	**W**	**Y**	**Z**
14	15	16	17	18	19	20	21	22	23	24	25	26
<espaço>												
0												

Percebe-se que na tabela 1 há 26 letras e seus respectivos valores, mas há também a referência ao espaço identificado pelo número 0, ou seja, são 27 números, no intervalo de 0 a 26. Os caracteres acentuados não estão sendo considerados aqui. Se necessário, basta incluí-los e atualizar o novo total de caracteres no cálculo do Mod. Como a tabela 1 possui 27 posições, ou seja, as 26 letras mais o caractere espaço, a conta do resto da divisão deverá ser por 27. Caso haja interesse em aumentar a tabela, acrescentando os acentos, por exemplo, basta aumentar o valor 27 proporcionalmente também.

Exemplo 1: Para codificar a frase "*EU VOU*", usando como chave $a = 14$, ou seja, a fórmula matemática ficaria: $y = x + 14 \pmod{27}$.

Tabela 2. Codificação da frase "Eu vou"

Letra	Código	Cod+chave	Soma	Resto Div	Resultado	Posição/Resultado
E	5	5 + 14 =	19	19 mod 27	19	S
U	21	21 + 14 =	35	35 mod 27	8	H
<espaço>	0	0 + 14 =	14	14 mod 27	14	N
V	22	22 + 14 =	36	36 mod 27	9	I
O	15	15 + 14 =	29	29 mod 27	2	B
U	21	21 + 14 =	35	35 mod 27	8	H

Utilizando o esquema da tabela 2, o código para a frase "EU VOU" é " SHNIBH".

Para descriptografar " SHNIBH" pode-se utilizar a operação inversa: $y = x - 14 \pmod{27}$. No entanto, haveria um pequeno problema, que é o resto da divisão por números negativos. Esse problema pode ser contornado utilizando um artifício matemático chamado simétrico aditivo. Um simétrico aditivo é o número que somado a nossa chave daria o valor de nossa quantidade de letras. Por exemplo, qual é o simétrico aditivo de 14 módulo 27? A resposta é 13. Pois 14+13=27 e 27 mod 27 é igual a 0. Sendo assim, basta substituir a chave 14 pela chave 13 e teremos condição de reverter a mensagem. Veja a tabela 3 abaixo.

Tabela 3. Decodificação de uma frase

Letra	Código	Cod+chave	Soma	Resto Div	Resultado	Posição/Resultado
S	19	19 + 13 =	32	32 mod 27	5	E
H	8	8 + 13 =	21	21 mod 27	21	U
N	14	14 + 13 =	27	27 mod 27	0	<espaço>
I	9	9 + 13 =	22	22 mod 27	22	V
B	2	2 + 13 =	15	15 mod 27	15	O
H	8	8 + 13 =	21	21 mod 27	21	U

Pode-se observar que a utilização do simétrico aditivo permitiu que a operação realizada fosse exatamente a mesma da fórmula para criptografar. A única adequação foi a chave, que antes era 14 e passou a ser 13, mas que não causou perda alguma quando foi utilizado o aditivo simétrico.

IMPLEMENTAÇÃO DA CIFRA DE CÉSAR USANDO VISUALG

Utilizando o software VisuAlg é possível implementar o algoritmo Cifra de César, capaz de executar as tarefas de cifrar e decifrar mensagens de texto. Também na implementação do algoritmo é conveniente utilizar o simétrico aditivo de modo a evitar surpresas na fórmula com o resto da divisão por números negativos. A Listagem 1 mostra o código fonte para criptografar.

```
algoritmo "CIFRA DE CESAR"
// Declaração das variáveis que utilizaremos em nosso exemplo
var
  cFraseOriginal: Caractere              // Frase a ser criptografada
  cFraseCifrada: Caractere               // Frase já criptografada
  aTabela: Vetor[0..26] de Caracter      // Vetor das Letras
  nChave: inteiro                        // Chave de Segurança

// Procedimento para Montar a tabela de letras
// Aqui estamos utilizando um subterfugio da programação, com a
utilização
// da tabela ASCII, pois a letra "A" encontra-se na posição 65 e a
Letra
// "Z" na posição 90. Na posição 0 da tabela colocaremos o espaço e
nas
// posições de 1 a 26 colocaremos as letras de A a Z.
procedimento CarregaTabela
var x: inteiro
inicio
   aTabela[0]:= " "
   para x:=1 ate 26 faca
      aTabela[x]:= Carac(64+x)
   fimpara
fimprocedimento

// Função que retorna a posição da Letra na tabela
funcao LocalizaPosicaoTabela( cLetra: caracter ): inteiro
var x: inteiro
inicio
   x:= 0;
   repita
      x:=x+1;
   ate (x<27) e (cLetra<>aTabela[x]) faca
   retorne(x)
```

```
fimfuncao

// Função que efetua a criptografia da Frase através da operação
aritmética
// y = x + a (mod 27) e retorna a frase criptografada.
funcao Criptografa( cFrase: caracter; nSeguranca:inteiro ):
Caracter
var x: inteiro
    cLetra: caracter
    cCifra: caracter
    cRetorno: caracter
    nCodigo: inteiro
    nCodCifrado: inteiro
inicio
   cRetorno := ""
   para x:= 1 ate Compr(cFrase) faca
        cLetra :=  Copia(cFrase,x,1)
        nCodigo :=  LocalizaPosicaoTabela(cLetra)
        nCodCifrado :=  (nCodigo + nSeguranca ) mod 27
        cCifra :=  aTabela[ nCodCifrado ]
        cRetorno :=  cRetorno+cCifra
   fimpara
   retorne(cRetorno)
fimfuncao

// Inicio do programa
inicio
   CarregaTabela
   Escreva("Digite uma Frase: ")
   Leia(cFraseOriginal)
   Escreva("Informe a chave de segurança: ")
   Leia(nChave)
   cFraseCifrada := Criptografa(cFraseOriginal,nChave)
   Escreva("A Frase Criptografa é ",cFraseCifrada)
fimalgoritmo
```

Listagem 1. Algoritmo para a Cifra de César utilizando o VisuAlg

A seguir, o código para a inversão do processo de criptografia, ou seja, o de descriptografia.

```
// Declaração das variáveis que utilizaremos em nosso exemplo
var
  cFraseOriginal: Caractere              // Frase a ser criptografada
  cFraseCifrada: Caractere               // Frase ja criptografada
  aTabela: Vetor[0..26] de Caracter      // Vetor das Letras
  nChave: inteiro                        // Chave de Segurança

// Procedimento para montar a tabela de letras
// Aqui estamos utilizando um subterfugio da programação, com a
utilização
// da tabela ASCII, pois a letra "A" encontra-se na posição 65 e a
Letra
// "Z" na posição 90. Na posição 0 da tabela colocaremos o espaço e
nas
// posições de 1 a 26 colocaremos as letras de A a Z.
procedimento CarregaTabela
var x: inteiro
inicio
   aTabela[0] = " "
   para x:=1 ate 26 faca
      aTabela[x] =  Carac(64+x)
   fimpara
fimprocedimento

// Função que retorna a posição da letra na tabela
funcao LocalizaPosicaoTabela( cLetra: caracter ): inteiro
var x: inteiro
inicio
   x:= 0;
   repita
      x:=x+1;
   ate (x<27) e (cLetra<>aTabela[x]) faca
   retorne(x)
fimfuncao


// Função que efetua a descriptografia da frase através da operação
// aritmética y= x + a (mod 27) e retorna a frase descriptografada.
funcao Descriptografa( cFrase: caracter; nSeguranca:inteiro ):
```

```
Caracter
var x: inteiro
    cLetra: caracter
    cCifra: caracter
    cRetorno: caracter
    nCodigo: inteiro
    nCodCifrado: inteiro
inicio
   cRetorno = ""

// O simétrico aditivo é encontrado com a fórmula abaixo:
     NSeguranca =  (27 - nSeguranca)

   para x:= 1 ate Compr(cFrase) faca
         cLetra = Copia(cFrase,x,1)
         nCodigo = LocalizaPosicaoTabela(cLetra)
         nCodCifrado = (nCodigo + nSeguranca ) mod 27
         cCifra = aTabela[ nCodCifrado ]
         cRetorno = cRetorno+cCifra
   fimpara
   retorne(cRetorno)
fimfuncao

// Inicio do programa
inicio
   CarregaTabela
   Escreva("Digite uma Frase: ")
   Leia(cFraseOriginal)
   Escreva("Informe a chave de segurança: ")
   Leia(nChave)
   cFraseCifrada = Descriptografa(cFraseOriginal,nChave)
   Escreva("A Frase Descriptografa é ",cFraseCifrada)
fimalgoritmo
```

Listagem 2. Algoritmo da resolução de uma criptografia - Descriptografia

É importante ressaltar que a cifra de César é uma técnica de criptografia simples, porém fácil de ser interceptada, pois se fundamenta na troca básica de letras de acordo com uma tabela. Desta maneira, sua quebra pode ser realizada através de uma técnica chamada Análise de Frequência, processo em que se identifica a frequência com que determinados códigos aparecem e se repetem.

CONSIDERAÇÕES FINAIS

Este trabalho descreveu a criptografia e descriptografia através da Cifra de César. Foi elaborado um algoritmo no ambiente VisuAlg para a demonstração do funcionamento básico dos mecanismos de criptografia e descriptografia. Atenção especial foi dada ao processo de decifração, adotando-se recursos de matemática básica com a finalidade de eliminação de ocorrências de erros no processo.

Entende-se que a vontade investigativa do aluno para a Ciência possa ser estimulada pela utilização de exemplos simples e interessantes como os mecanismos de criptografia e descriptografia aqui demonstrados.

REFERÊNCIAS

ALMEIDA, R. S. **Aprendendo algoritmo com visualg**. Rio de Janeiro: Ciência Moderna, 2013.
CAVALCANTE, A.L.B. **Matemática I**. Notas de Aula. Brasília: UPIS, 2004.
FIGUEIREDO, L. M. S. **Números primos e criptografia de chave pública**. Rio de Janeiro: UFF/ CEP – EB, 2006.
OLIVEIRA, R. R.. **Criptografia tradicional simétrica de chave privada e criptografia assimétrica de chave pública**: análise das vantagens e desvantagens. Niterói: Trabalho da pós-graduação Criptografia e Segurança em Redes da UFF, 2006.
PEREIRA, J. C. R. **Análise de dados qualitativos**: Estratégias Metodológicas para as Ciências da Saúde, Humanas e Sociais. 3. ed 1ª.reimpr. São Paulo: Universidade de São Paulo, 2004.
PIVA, D.,..[et al]. **Algoritmos e programação de computadores** [recurso eletrônico]. Rio de Janeiro: Elsevier, 2011.
QUIERELLI, D. A. **Aprenda a programar**. Leme: Edição do Autor, 2012.
SCHEINERMAN, E. R. **Matemática discreta**: uma introdução. São Paulo: Cengage Learning, 2011.
SINGH, S. **O livro dos códigos**: as ciências do sigilo - do antigo egito à criptografia quântica. Rio de Janeiro: Record, 2003.
STEIN, C.; DRYSDALE R. L.; BOGART. K. **Discrete mathematics for computer scientists**. Boston, Massachusetts: Pearson Education, 2011.