Código M: Componente Java para Criptografia

Carlos Peixoto, Oziel Carneiro
Laboratório de Computação Natural (LCN)
Área de Ciências Exatas e Tecnologia (ACET), Centro Universitário do Pará (CESUPA) Av. Gov. José Malcher, 1963 - 66.060-230 - Belém,PA,Brasil.
E-mail: {carlosrapeixoto,ozielcarneiro}@gmail.com

Otávio Noura Teixeira, Igor Ruiz Gomes
Laboratório de Computação Natural (LCN)
Área de Ciências Exatas e Tecnologia (ACET), Centro Universitário do Pará (CESUPA) Av. Gov. José Malcher, 1963 - 66.060-230 - Belém,PA,Brasil.
E-mail: {onoura,ruiz.igor}@gmail.com

RESUMO

O tráfego de dados em banda larga crescerá 8 vezes até 2012 [5]. Manter os dados seguros é essencial para uma organização. O processo de codificar um dado geralmente é muito trabalhoso. Existem várias bibliotecas para criptografia, implementadas em diversas linguagens de programação como, por exemplo, a *Application Programming Interface* (API) de criptografia do Java (Java Security), porém alguns métodos criptográficos acabam por gerar muitas linhas de código, o que o deixa com uma complexidade bem elevada. Este trabalho apresenta um componente para criptografia, utilizando um novo método criptográfico, chamado de *Código M*.

A criptografia estuda os métodos utilizados para codificar uma mensagem de modo que só o seu destinatário legítimo consiga interpretá-la [2]. A ciência de escrever em códigos pode ser dividida em dois ramos, transposição e substituição. Na transposição, as letras originais do texto são preservadas, ou seja, existe apenas uma troca em suas posições. Já na substituição, as letras do texto são trocadas por outras letras, números ou símbolos [1].

A engenharia de software baseada em componentes é um processo que enfatiza a construção de sistemas baseados em computador, usando componentes de software reutilizáveis [4].

A opção pela linguagem de programação Java baseou-se em sua popularidade, portabilidade, orientação a objetos, livre distribuição, além da facilidade de importação e exportação do componente.

O componente é constituído por várias classes e uma interface de acesso, a classe I*Mcode* herda da classe *TabelaVerdade* e a classe *IIMcode* implementa a interface. Desta forma é possível codificar e decodificar um texto apenas com o uso da interface, gerando assim, poucas linhas de código, conforme a figura 1 onde encontra-se o diagrama de classes de acordo com a notação da *Unifield Modelling Language* (UML) 2.0[3].

Para codificar é preciso passar o texto e a chave criptográfica como parâmetros, a chave é composta por dois caracteres, e ao final do processo de codificação, todo o texto criptografado vai se tornar um texto binário, ou seja, os dois caracteres fornecidos como chave representarão todo o texto, o que torna o ato de decifrar por contagem de caracteres inviável. Para decodificar, basta passar como parâmetros o texto criptografado, mais a chave criptográfica. Caso nenhuma chave seja informada, os caracteres "."(ponto) e "-"(traço) serão adotados por padrão.

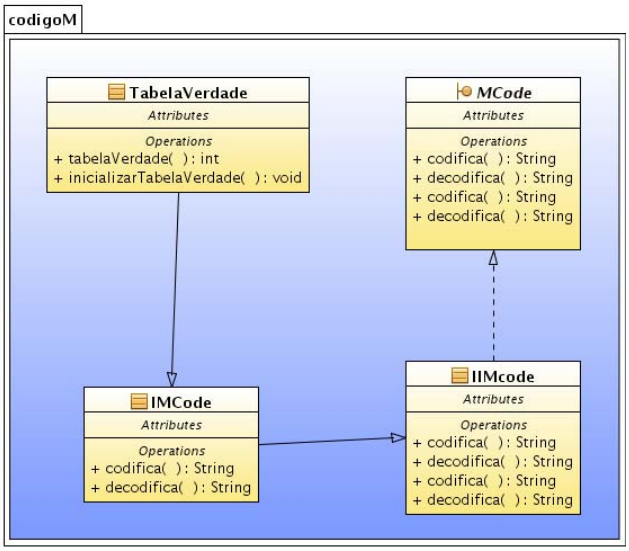

Figura 1 - Diagrama de Classes do *Código M*.

Características importantes implementadas foram a automatização do dicionário de caracteres, ao invés de definir os caracteres um a um, eles são gerados automaticamente através da classe *TabelaVerdade*, e a utilização do componente, através da interface. Desta forma sempre que for preciso codificar e decodificar um texto, não é necessário reescrever o código, basta escolher a operação desejada e passar os parâmetros requeridos.

O *Código M* mantém-se em desenvolvimento contínuo. Novas abordagens de sua utilização surgem constantemente, a criptografia de imagens utilizando o *Código M* é uma idéia a ser implementada futuramente, assim como a compressão de dados.

Palavras-chave*: Criptografia, componente, Java.*

Referências

[1] G. Almeida, Appelt. R. Escrita escondida Disponível em http://www.ajc.pt/cienciaj/n32/escrita.php, Acesso em: 03/04/2009.

[2] S.C. Coutinho, "*Números Inteiros e criptografia RSA*", IMPA (Inst. de Matemática Pura e Aplicada), 2003.

[3] Object Management Group. Disponível em http://www.omg.org/. Acesso em 05/04/2009.

[4] R.S. Pressman, "*Engenharia de Software*" , Addison Wesley, 2007.

[5] Reuters. Tráfego de dados em banda larga crescerá 8 vezes até 2012. Disponível em http://www.vsp.com.br/noticias.php?id=4542. Acesso em: 03/042009.