Implementação de Biblioteca de Processamento Algébrico para o Esquema de Criptografia de Chave Pública Rafaella

Rafael Kunst, Vinicius Gadis Ribeiro

Unilasalle - Centro Universitário La Salle, Av. Victor Barreto, 1288 - Canoas, RS, Brasil

rkunst@inf.lasalle.tche.br,vinicius@unilasalle.edu.br

Abstract. *This paper presents the software implementation of a recently proposed public-key cryptography scheme, called Rafaella. This project is based on the difficulty of getting the original function, given one which was translated over the complex plan. The article is organized as follows: first is presented a discussion about cryptography, focusing on public-key theory. Later, is reported a brief description of Rafaella algorithm such as its software implementation proposal.*

Keywords: Cryptography, Computer Security, Mathematics.

Resumo. *O presente artigo apresenta a implementação via software de um esquema de criptografia recentemente proposto, chamado Rafaella. Esse esquema baseia-se na dificuldade em se obter a função original, dada uma que fora translada no plano dos números complexos. Para tanto, são abordados aspectos básicos a respeito do tema, com maior foco em criptografia de chave pública. Por fim, é apresentado o referido algoritmo, bem como a implementação do mesmo, que está sendo realizada.*

Palavras-chave: Criptografia, Segurança Computacional, Matemática

1. Introdução

Criptografia é o emprego de técnicas matemáticas relacionadas a aspectos da segurança da informação, tais como: confiabilidade, integridade de dados, identificação de entidades - pessoas, máquinas, etc -, reconhecimento de origem e não-repúdio. É uma ciência que apresenta influência histórica há mais de dois mil anos (Piper, 2002). No entanto, têm-se registros de sua utilização, de forma limitada, há mais de 4000 anos (Menezes, 1996).

As técnicas modernas de criptografia (Mao, 2004), consistem em alterar uma mensagem original - também conhecida como texto pleno - de tal forma que o resultado gerado não seja compreensível para pessoas não autorizadas a conhecer tal conteúdo - texto cifrado -, ao passo que seja simples, ou seja, de complexidade computacional baixa para receptores autorizados, recuperar a mensagem original. A referida transformação é realizada a partir de uma série de procedimentos aplicados sobre a mensagem no formato original, que são conhecidos como algoritmo de cifragem ou de criptografia, e, geralmente, dependem da utilização de uma ou mais chaves para gerar o texto cifrado. O retorno à mensagem original segue o mesmo princípio, porém funciona através da aplicação da operação inversa à utilizada para codificar o texto, podendo para tanto ser necessária a utilização de chave diferente da aplicada na primeira etapa.

Existem dois tipos de algoritmos que são aplicados a nível de criptografia moderna com a utilização de chaves: os simétricos, também conhecidos como esquemas de chave secreta, os quais utilizam a mesma chave tanto para decifrar, quanto para crifrar as mensagens e, os assimétricos - esquemas de chave pública, quer serão detalhados neste artigo.

O esquema Rafaella (Ribeiro e Weber, 2004) enquadra-se ao contexto da criptografia de chave pública, apresentando como diferencial o fato de abordar um novo paradigma matemático para executar as operações de cifragem e decifragem de mensagens. Sendo assim, o presente trabalho visa, a partir da implementação em software do método criptográfico, realizar estudo de caso utilizando como unidade de análise o referido esquema, em comparação com outro método - a ser definido - que seja baseado em chave pública, com a finalidade de avaliar a nível de desempenho computacional e aplicabilidade o algoritmo proposto.

A próxima seção, abordará em maiores detalhes criptografia de chave pública. Em seguida, será apresentado o esquema Rafaella. A quarta seção apresentará considerações sobre a implementação em desenvolvimento, apresentando a metodologia a ser empregada para que sejam atingidos os objetivos propostos, bem como a arquitetura a ser utilizada na implementação sugerida e, na seqüência, serão apresentadas considerações finais e trabalhos futuros.

2. Criptografia de Chave Pública

A primeira proposta publicada na área dos algoritmos de criptografia assimétricos surgiu no ano de 1976, oportunidade na qual Whitfield Diffie e Martin E. Hellman tornaram público artigo intitulado *"New Directions in Cryptography"* (Diffie, 1976). Essa metodologia é baseada na utilização de duas chaves geradas por cada usuário, pertencentes a um conjunto finito K, denotado por {K}, que representa o espaço amostral de possíveis chaves. A primeira delas, conhecida como chave pública (representada por E_k, derivando-se do inglês *enciphering key*), como o próprio nome indica, deve ser deixada disponível publicamente - geralmente em um diretório de acesso livre, como uma página pessoal, por exemplo -, juntamente com os dados de identificação e de endereço do gerador da referida chave, tendo a finalidade de cifrar mensagens destinadas a quem a gerou. A transformação da mensagem original em texto cifrado pode ser representada pela seguinte equação (1), onde E_k é a função de cifragem, C é a mensagem criptografada e M a original:

$$C = E_k(M) \tag{1}$$

A segunda chave deve ser mantida em segredo, e é chamada de chave privada (D_k, a saber, *deciphering key*). Sua utilidade dentro do esquema proposto é a de decifrar textos que foram criptografados através da aplicação da chave pública da pessoa que a possui. Sendo que o retorno ao texto pleno pode ser representado pela equação abaixo (2), onde D_k é a função de decifragem:

$$M = D_k(E_k(C)) \tag{2}$$

Exemplo do funcionamento dessa classe de esquemas é demonstrado na figura 2, a seguir:

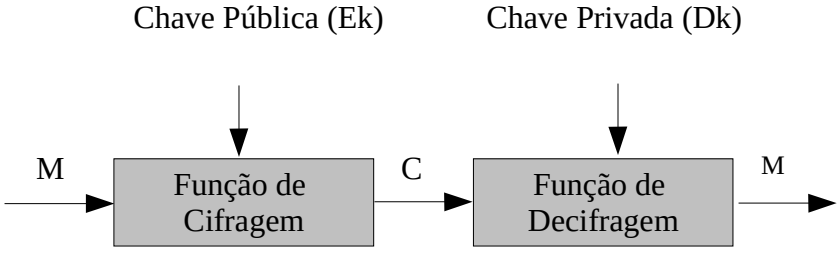

Figura 1. Funcionamento de esquemas de criptografia assimétricos

Diffie e Helmann (Diffie, 1976) propuseram quatro propriedades que qualquer esquema de criptografia de chave pública deve seguir, as quais serão listadas a seguir. Para melhor entendimento, assume-se que um criptosistema assimétrico é um par de famílias de algoritmos, tal que $\{Ek\}k \in \{K\} \wedge \{Dk\}k \in \{K\}$ representam, para um espaço finito de mensagens – $\{M\}$ – as transformações inversíveis a seguir:

$Ek : \{M\} \rightarrow \{M\}$

$Dk : \{M\} \rightarrow \{M\}$

Sendo assim:

I) $\forall K \in \{K\}, Ek = Dk^{-1}$

II) $\forall K \in \{K\} \wedge M \in \{M\}$, Ek e Dk são simples de computar.

III) Para praticamente todas as ocorrências de $K \in \{K\}$, computar Dk a partir de Ek deve ser computacionalmente inviável.

IV) $\forall K \in \{K\}$, não é factível computar o par Ek, Dk partin-se de K.

A propriedade I assegura que, independente das chaves geradas, a chave privada é o inverso da pública, sendo a recíproca verdadeira. A segunda assertiva dá conta de que, para qualquer conjunto de chaves utilizadas e de mensagens geradas, as chaves de cifragem e decifragem são fáceis de calcular computacionalmente. Na afirmativa III, é indicado que deve ser impossível chegar ao valor da chave privada, a partir da pública. Por fim, a quarta propriedade garante que, a partir do conjunto de possíveis chaves, não existe maneira simples de chegar ao par de chaves gerado inicialmente.

Para que esses objetivos sejam atingidos, devem ser aplicados problemas matemáticos fáceis de computar, mas que, no entanto, a operação inversa seja de difícil solução, buscando assim que o tempo necessário para quebrar a segurança de determinado esquema seja o suficiente para que as informações trafegadas já não tenham mais valor qualquer. Pode-se citar, dentre outros, a fatoração de números inteiros, o cálculo de raízes quadradas modulo *n*, o problema do logaritmo discreto, a soma de resíduos quadráticos e a soma subconjuntos de valores - também conhecidos como algoritmos baseados no problema da mochila (Mao, 2004).

Diversos algoritmos que empregam as técnicas acima citadas foram propostos, no entanto, o funcionamento desses foge ao escopo do presente trabalho. Entretanto, abaixo, o quadro 1 cita alguns dos mais importantes esquemas de chave pública encontrados na literatura, os relacionando aos problemas computacionais aplicados por cada um deles, conforme apresentado por Menezes (Menezes, 1996).

Esquemas	Problemas Computacionais
RSA	Fatoração de Inteiros
Rabin	Raízes quadradas modulo n e fatoração de inteiros
El Gamal	Logaritmo discreto
Chor-Rivest knapsacke Markle-Hellman knapsack	Problema da mochila

Quadro 1. Esquemas de criptografia de chave pública e problemas computacionais a eles relacionados.

A seção a seguir irá apresentar aspectos referentes ao esquema de criptografia de chave pública Rafaella, com a finalidade de familiarizar o leitor com o algoritmo, facilitando assim a compreensão da implementação em software que está sendo proposta.

3 O Esquema Rafaella

O esquema de criptografia de chave pública Rafaella foi proposto recentemente por Ribeiro e Weber (Ribeiro, 2004a; Ribeiro, 2004b), oferecendo serviços de cifragem e decifragem de mensagens. A sub-seção a seguir irá abordar aspectos matemáticos relavantes do esquema discutido.

3.1 Aspectos Matemáticos

O embasamento matemático do algoritmo não é focado na teoria do números, como grande parte dos exemplos que se encontra na literatura atual, ao invés disso, é baseado no emprego de operadores diferenciais. O esquema criptográfico consiste em efetuar operações de translação sobre funções de uma variável complexa, baseando-se na teoria dos grupos de Lie (Olver, 2000) - ao invés de grupos de Galois (Emil, 1998), como se verifica no caso de algoritmos baseados em matemática discreta. Os grupos de Lie são parte dos de Galois e, no contexto de equações diferenciais apoiam-se fortemente na utilização de simetrias, que nesse caso, são operações de transformação aplicadas sobre equações diferenciais, que alteram apenas os valores dos coeficientes das mesmas, sendo possível então a geração de equações diferentes da original, porém equivalentes a ela.

Assim, torna-se claro que a teoria citada se enquadra na exigência dos esquemas de criptografia de chave pública, uma vez que aplicar tais transformações é simples do ponto de vista computacional, ao passo que a operação inversa apresenta alto grau de complexidade para ser executada. No entanto, ao se propor o discutido esquema, o objetivo foi o de concebê-lo da maneira mais simples possível de implementar sendo que, para tal, ao invés de aplicar-se diretamente os grupos de Lie - o que exigiria grandes conhecimentos matemáticos -, utilizou-se uma das regras propostas pelo matemático em questão, a qual limitou o emprego direto dos operadores diferenciais.

As referidas simetrias quando aplicadas sobre funções, também geram mudanças nos argumentos das mesmas. Levando isso em consideração, foi escolhida uma transformação que realiza translações no plano complexo, gerando funções multivaloradas equivalentes à original,

atendendo aos requisitos da criptografia assimétrica, assim como ao desejo de simplicidade na proposta (Ribeiro, 2004a).

Posto isso, a implementação do esquema, proposta no presente trabalho, terá como base a criação de um processador algébrico (Mayr, 2000) que possibilite a execução computacional das operações matemáticas necessárias para realizar transformações, sobre funções de uma variável complexa. A variável que é aplicada sobre determinada função para a transladar no plano complexo ($\mathbb{C}$) é a chave privada do participante da sessão segura que está realizando a translação. Ela é composta por um número complexo - no formato $a + bi$ -, possuíndo a parte real e a imaginária não nulas, podendo ser representada no plano complexo de duas maneiras: cartesiana e polar (Soares, 2003).

As translações aplicadas sobre funções de uma variável complexa geram como resultados funções multivaloradas equivalentes à original. Essas possuem como propriedade infinitas raízes, sendo que apenas uma delas é a chave privada do participante que gerou a transformação. Então, para que um atacante comprometa o esquema, é necessário que ele descubra tal ponto ou coordenada do plano complexo, o que equivale a fazer uma varredura completa em $\mathbb{C}$, operação que possui alto custo computacional para ser executada. Há ainda a possibilidade de o atacante buscar, através da chave pública, chegar à privada, sendo necessário para tanto resolver equações algébricas ou diferenciais, ao invés de efetuar testes de primalidade, resolver logaritmo discreto ou definir o escalar em curvas elípticas, como ocorre em esquemas baseados na teoria dos números. Ou seja, a dificuldade está ligada ao fato de descobrir o valor de *a*, na fórmula 3, a seguir, que representa o operador A, o qual pode ser utilizado como chave pública do esquema proposto, operação que exigiria também um grande número de operações simbólicas.

$$A = \left(a \frac{\partial}{\partial_x} \right) \tag{3}$$

A partir de então, o esquema segue com a aplicação da exponencial do operador encontrado sobre uma função arbitrária, o que produz a transformação a seguir (4), que corresponde a uma translação no plano complexo, uma vez que é condição do algoritmo proposto que o número complexo utilizado como chave privada possua tanto parte real como imaginária, caso contrário, a operação equivaleria a uma translação na reta real.

$$\left[e^{A} \right] f(x) = f(x + a) \tag{4}$$

A seguir será apresentado o funcionamento do referido esquema de criptografia assimétrica, bem como algumas características do mesmo.

3.2 Funcionamento do Esquema Rafaella

O processo de cifragem e de decifragem de mensagens no referido esquema é baseado em transformações aplicadas em funções com a finalidade de gerar outra função - equivalente à inicial - que corresponde ao texto cifrado, assim como em transformações inversas com a finalidade de retornar ao texto original.

Suponha-se que Alice deseja criptografar uma mensagem com a fim de enviá-la para Bob. Para que a comunicação seja possível, eles devem seguir os passos apresentados no quadro 2, a seguir (Ribeiro, 2004a):

Alice	Bob
– Converte a mensagem original para valores numéricos, baseando-se no código ASCII dos caracteres que compõe o texto; – Escolhe uma função real *n* vezes derivável - $f_0(x)$ -, na qual a quantidade de coeficientes corresponde ao número de caracteres do texto pleno, sendo que as parcelas geradas devem ser distintas entre si;	
– Escolhe um número complexo que será sua chave privada (K_{dA}), a partir dele, gera a chave pública (K_{eA}), que é uma potência da privada;	– Escolhe um número complexo que será sua chave privada (K_{dB}), a partir dele, gera a chave pública (K_{eB}), que é uma potência da privada;
– Aplica K_{dA} sobre $f_0(x)$, gerando o deslocamento no plano complexo, tendo como resultado outra função, equivalente à primeira, que corresponde à mensagem crifrada, $f_1(x)$; – Envia $f_1(x)$ para Bob;	
	– Aplica K_{dB} sobre $f_1(x)$, obtendo a função translada $f_2(x)$; – Envia $f_2(x)$para Alice;
– Alice aplica o simétrico de K_{dA} sobre $f_2(x)$, gerando a função $f_3(x)$; – Envia a Bob t_A em comjunto com $f_3(x)$.	
	– Aplica o simétrico de sua chave privada em $f_3(x)$, obtendo a função $f_4(x)$, que corresponde a original - $f_0(x)$; – Extrai os coeficientes de $f_0(x)$, que correspondem à codificação ASCII dos caracteres que compunham a mensagem original enviada por Alice. Após, transforma os valores ASCII nos seus caracteres correspondentes, recuperando o texto pleno.

Quadro 2. Protocolo utilizado pelo algoritmo

O deslocamento no plano complexo deve ser definido conforme a mudança variável apresentada a seguir que contém tanto partes reais quanto imaginárias e mapeia a função f(x) em f (x+a+bi):

$$x \rightarrow x + a + bi$$

A transformação reversa consiste em outra mudança variável, expressa abaixo, e consiste em mapear a função f(x) em f(x-a-bi):

$$x \rightarrow x - a - bi$$

As chaves são definidas da seguinte forma: a privada é escolhida por cada participante, consistindo nos componentes real e imaginária do deslocamento aplicado sobre a função original, ou seja, é um número complexo. A chave pública é obtida a partir da chave privada e constitui-se de uma função, na qual pelo menos uma das raízes seja constituída pela chave privada do participante. Para tal, também pode ser aplicado um operador diferencial. Cabe salientar que, partindo-se da chave pública é exigido custo computacional extremamente elevado para se obter a chave privada, o que vem ao encontro com o que foi proposto por Diffie e Hellman em 1976 (Diffie, 1976).

A próxima seção apresentará a metodologia utilizada para tornar possível a implementação da biblioteca de processamento simbólico quer permita a utilização do esquema de critografia de chave pública Rafaella de maneira simplificada.

4. Considerações sobre a implementação

O fato de o esquema Rafaella exigir a implementação de sistema de processamento simbólico dificulta bastante seu emprego imediato em aplicações científicas ou comerciais. A prova de funcionamento do algoritmo apresentado foi desenvolvida empregando-se um programa proprietário - Maple -, entretanto, sem a possibilidade de aplicação prática de forma rápida em sistemas que necessitem de tráfego seguro de informações, tendo em vista as dificuldades de processamento apresentadas.

Então, está sendo criada biblioteca de processamento algébrico, com a finalidade de facilitar a utilização do algoritmo Rafaella em aplicações desenvolvidas tanto no meio acadêmico quanto comercial. O referido software está sendo implementado utilizando linguagem de programação C++, apresentando a propriedade da portabilidade, ou seja, não depende de um sistema operacional específico para ser executado, o que aumenta bastante a flexibilidade no seu emprego.

Um dos principais objetivos é criar interface de fácil utilização para que programadores possam utilizar o algoritmo em suas aplicações de maneira simples - através de invocações de métodos, que o dispensarão de desenvolver um sistema completo de processamento simbólico e de comunicação entre os participantes da sessão segura de troca de informações, bem como de preocupar-se com operações de ponto flutuante, ficando o mesmo apenas responsável por informar atributos relacionados aos deslocamentos no plano dos números complexos a serem aplicados sobre as funções.

Após concluída, a biblioteca computacional proposta será disponibilizada considerando-se os princípios do desenvolvimento de software livre (FSF, 2005), sob licença GPL(FSF,1991) para que possa ser livremente alterada por outros programadores, bem como utilizada sem custos no desenvolvimento de sistemas.

Assim que for finalizada a implementação, será realizado estudo comparativo, baseado em análise de desempenho, entre o esquema de criptografia Rafaella e um dos esquemas de criptografia assimétrica presentes na literatura atual - que seja baseado na teoria dos números. As métricas a serem avaliadas para tal experimentação serão utilização de memória do sistema operacional em determinados momentos do processamento e, em tempo de execução dos algoritmos a partir de arquivos de entrada idênticos, possibilitando assim a obtenção de conclusões a respeito das situações ideais nas quais a utilização de cada paradigma matemático é aconselhada. Também será realizada comparação do desempenho da implementação com os resultados obtidos em estudo conduzido com auxílio da ferramenta de processamento algébrico Maple.

A sub-sessão 4.1 irá apresentar a arquitetura que está sendo utilizada na construção da biblioteca de processamento algébrico, bem como explicações referentes às funções que cada módulo deverá executar.

4.1 Arquitetura

A arquitetura do sistema que está sendo implementado é baseada em quatro módulos: texto original, processador algébrico, gerenciador de comunicação e recuperação do texto original, quer serão detalhados a seguir. A figura 2, a seguir, os apresenta de forma gráfica.

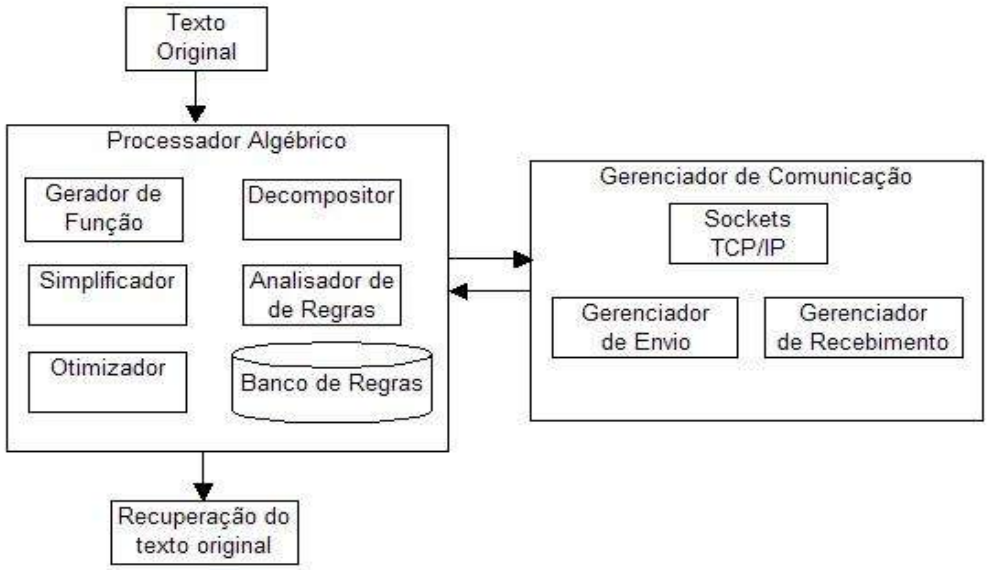

Figura 2. Arquitetura do Software

O primeiro passo apresentado pelo algoritmo é a obtenção do texto original, módulo que é responsável pela leitura do arquivo de entrada e pela inicialização do sistema como um todo,

colocando o texto lido em um formato no qual seja passível de utilização pelo método que irá gerar a função inicial ($f_0(x)$).

O processador algébrico é de grande importância, uma vez que é responsável pela execução das tarefas principais do algoritmo Rafaella, ou seja, as etapas que se referem aos processos de cifragem, decifragem das mensagens. Para tal, serão criados métodos a serem invocados pelo sistema de processamento simbólico a fim de executar operações matemáticas. Além disso, haverá o desenvolvimento de métodos que auxiliem na tomada de decisão referente a qual técnica deve ser utilizada em cada situação, baseado-se em consultas a um banco de regras previamente definido. Além da referida base de dados, o processador algébrico possui os seguintes métodos:

- Gerador de Função: responsável por gerar a função inicial utilizada no esquema criptográfico, chamada de $f_0(x)$. A sua criação é baseada no valor ASCII dos caracteres que compõe o texto original, os quais irão compor as parcelas (distintas entre si) de uma função real *n* vezes derivável;
- Decompositor: possui papel semelhantes ao exercido pelo analisador léxico no contexto dos compiladores (Aho, 1986), ou seja, no caso da implementação em questão, fazer a leitura de cada caracter das funções geradas, os transformando em uma seqüência de símbolos léxicos, também conhecidos como *tokens*, que serão utilizados posteriormente para resolução das mesmas;
- Analisador de regras: tendo como base o banco de regras, que possui definições previamente estabelecidas para suporte à tomada de decisões baseada nos tokens gerados, tem como função reconhecer o tipo de expressão e executar as operações matemáticas previstas pelo protocolo em questão;
- Simplificador: a este módulo é delegado o tratamento das funções geradas durante a execução do esquema Rafaella, tornando as mesmas matematicamente simples. A finalidade das referidas transformações é de facilitar tanto a visualização das mesmas durante execuções do software, quanto de simplificar futuras alterações que a função gerada deverá sofrer para correto funcionamento do algoritmo;
- Otimizador: visa otimizar a execução das operações simbólicas através da aplicação de diversas técnicas de otimização de processamento matemático (Mayr, 2000).

Outro mecanismo essencial ao sistema é a comunicação entre os participantes. Para tanto são utilizadas redes de computadores, haja vista necessidade de troca de funções e de argumentos auxiliares entre os participantes da sessão segura. Sendo assim, foi projetado módulo que é dividido em três métodos responsáveis pelo gerenciamento da referida comunicação. Tais elementos são baseados na utilização de Berkeley sockets (McKusick, 1996), com o emprego do protocolo TCP na camada de transporte, sobre IP (Tanenbaum, 1996), para transmissão de dados entre os participantes do protocolo de troca de informações seguras. Cada um dos participantes possui gerenciadores de envio e recebimento de mensagens, que são responsáveis por tratar os pacotes que são enviados e os que são recebidos, respectivamente.

O último passo na execução do sistema é aquele em que o receptor deve recuperar o texto original, com base nos valores ASCII dos caracteres, etapa cuja responsabilidade é delegada a um módulo específico.

A próxima seção apresentará as considerações finais, bem como perspectivas futuras a partir do trabalho que está sendo desenvolvido.

5. Considerações Finais e Perspectivas Futuras

Diversos são os esquemas de criptografia de chave pública conhecidos, assim como inúmeros são os problemas computacionais a eles relacionados. No entanto, é comum a todos os algoritmos a necessidade de utilizar problemas matemáticos que tenham simples solução para pessoas autorizadas a visualizarem determinada mensagem, enquanto são computacionalmente complexos para que resistam a tentativas de ataques com a finalidade de obter indevidamente o conteúdo das informações trafegadas em forma de texto cifrado.

Baseando-se nisso, o esquema de criptografia assimétrica intitulado Rafaella utiliza um paradigma matemático não antes empregado com essa finalidade, que utiliza deslocamentos de funções (texto original) no plano complexo, gerando funções equivalentes que representam o texto cifrado, sendo a tarefa de retornar a uma função que foi deslocada, sem possuir a chave privada, extremamente onerosa. O mesmo se observa para o caso de existirem tentativas de deduzir a chave privada a partir da chave pública. Entretanto, usuários autorizados poderão facilmente gerar, a partir de um texto pleno, funções de criptografia e enviá-las a seu destinatário que, somente se for a pessoa autorizada, poderá ler a mensagem. Isso ocorre graças ao processo de autenticação, que é baseado na utilização das chaves públicas de ambos participantes, assim como da chave privada do emissor, o que visa provar a identidade do receptor, através do método de prova de conhecimento zero, conforme anteriormente explanado.

Analisando-se o funcionamento do esquema, se percebe que há a vantagem de os participantes poderem escolher suas chaves privadas, o que não é apresentado em outros protocolos, quando essas são geradas a partir da pública. Outro ponto positivo é a autenticação, evitando que atacantes se passem por um dos participantes. Como desvantagem, tem-se o grande número de operações simbólicas exigidas para implementação do algoritmo, o que, devido à complexidade computacional, supostamente irá influenciar negativamente no desempenho do software. Outra fraqueza está ligada ao fato de haver necessidade de trocar três mensagens para que um texto enviado por Alice seja decifrado por Bob, o que exige que a comunicação seja síncrona. O número excessivo de pacotes trafegados deve tornar o protocolo lento, em comparação com os demais esquemas de criptofrafia de chave pública conhecidos, o que limita sua utilização.

A necessidade de processamento simbólico faz com que a utilização ampla do esquema proposto em aplicações científicas ou comerciais seja dependente da criação de uma interface amigável para que programadores possam acoplar o esquema de maneira ágil e simples a suas aplicações, objetivo que pretende-se alcançar através do desenvolvimento de biblioteca, em um primeiro momento na linguagem C++, no entanto com o projeto de ser estendida a para outras linguagens de programação de larga utilização, a partir da disponiblização da mesma como software livre.

Além disso, a partir da finalização da implementação da referida biblioteca, será realizado estudo comparativo entre o proposto esquema e os atualmente existentes, com a finalidade de verificar a possibilidade de operacionalização do algoritmo proposto, bem como de comparar, a partir de métricas definidas (utilização de memória e velocidade de processamento), o desempenho do esquema Rafaella quando avaliado em conjunto com outros sistemas criptográficos baseados em chave pública.

Referências Bibliográficas

Aho, A. V., Sethi, R., Ullman, J. D. (1986) "Compilers: Principles, Techniques and Tools", Addison-Wesley.

Diffie, W., Hellman, M. E. (1976) "New Directions in Cryptography", IEEE Transactions on Information Theory. IT 22, 644-654.

ElGamal, T. (1985) "A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms". IEEE Transactions on Information Theory, Vol.31, Nr.4, .469-472

Emil, A., Milgram, A. N. (1998) "Galois Theory". Dover Science.

FSF (1991) "GNU General Public License", http://www.gnu.org/licenses/gpl.html. Free Software Foundation. Acesso em 06/03/2005.

FSF (2005) "The Free Software Definition", http://www.fsf.org/licensing/essays/free-sw.html. Free Software Foundation. Acesso em 06/03/2005.

Mao, W. (2004) "Modern Cryptography: Theory and Practice". Prentice Hall.

Mayr, E. W., Vorozhtsov, E. V., Ganzha, V. G. (2000) "Computer Algebra in Scientific Computing". New York. Springer-Verlag.

McKusick, M. K.,Bostic, K., Karels, M. J., Quarterman J. S. (1996) "The Design and Implementation of the 4.4 BSD Operating System". Addison-Wesley.

Menezes, A., Oorschot, P., Vanstone, S. (1996) "Handbook of Applied Cryptography", CRC, Press.

Neto, A. L. (1993) "Funções de uma variável complexa". Rio de Janeiro, IMPA.

Nichols, R. K. (1999), "ICSA Guide to Cryptography", McGraw-Hill.

Olver, P. (200*0)* "Applications of Lie Groups to Differential Equations", 2nd Edition. New York. Springe.

Piper, F., Murphy (2002), "Cryptography: A Very Short Introduction". Oxford. New York.

Rabin M.O. (1979) "Digitalized Signatures and Public-key Functions as Intractible as Factorization". Technical Report TR-212. MIT Laboratory for Computer Science.

Ribeiro, V. G., Weber, R. F. (2004a) "Problemas Computacionais para Esquemas de Criptografia de Chave Pública". In: 22º Simpósio Brasileiro de Redes de Computadores. IV Workshop de Seguraça Computacional, 101-112.

Ribeiro, V. G. (2004b) "Rafaella: um esquema de criptografia de chave pública baseado em um novo paradigma matemático". Tese de doutorado, Programa de Pós-Graduação em Computação, Universidade Federal do Rio Grande do Sul.

Rivest, R. L., Shamir, A., Adleman, L. A. (1978) "A method for obtaining digital signatures and public-key cryptosystems". Communications of the ACM, Vol.21, Nr.2, 120-126.

Schneider, B. (1996) "Applied Cryptography", 2nd Edition. John Wiley & Sons.

Soares, M. G. (2003) "Cálculo em uma variável complexa", 3a.Edição. Instituto de Matemática Pura e Aplicada, Rio de Janeiro.

Tanenbaum, A. S. (1996) "Computer Networks", 3rd Edition. Prentice Hall.