Implementação do Esquema de Criptografia de Chave Pública Rafaella

Rafael Kunst[1], Vinicius Gadis Ribeiro[1,2]

[1,2]Centro universitário La Salle (UNILASALLE), Av. Victor Barreto, 2288 – Canoas, RS, Brasil
rkunst@inf.lasalle.tche.br
[2]Instituto de Informática – Universidade Federal do Rio Grande do Sul (UFRGS), Caixa Postal 15.064, 91.501-970 – Porto Alegre, RS, Brasil
vribeiro@inf.ufrgs.br

Resumo – O presente artigo apresentar a implementação via software de um esquema de chave pública recentemente proposto, chamado Rafaella. Esse esquema baseia-se na dificuldade de se obter a função original, dada uma função que fora transladada. Para tanto, são colocados aspectos básicos a respeito do tema, com foco maior em criptografia de chave pública. Por fim, é apresentado o referido algoritmo, bem como proposta de implementação do mesmo.

Palavras-chave: Criptografia de Chave Pública, Segurança Computacional, Matemática.

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 a translated one. To make it possible, first it is presented a discussion about cryptography, focusing on public key theory, later it is reported a brief description of Rafaella algorithm such as its software implementation proposal.

Key-words: Public Key Cryptography, Computer Security, Mathematics.

Introdução

A utilização de esquemas de criptografia tem se tornado ferramenta crucial para garantir comunicação segura em diversas situações. Transações bancárias, operações militares, troca de mensagens corporativas, garantia de autenticidade de pessoas e mensagem enviadas e recebidas e de não-repúdio à combinações, entre outros, fazem uso de diversas técnicas para criar canais de transmissão seguros, bem como garantir confiabilidade na troca de mensagens. Além disso, tem elevado grau de aplicabilidade na segurança de sistemas de informação, uma vez que, em muitos casos, é necessária a garantia de tráfego seguro de dados, assim como pode ser crucial para determinadas aplicações ter um mecanismo de reconhecimento de identidade dos participantes, como é o caso de aplicações de e-commerce.

Posto isso, o presente trabalho visa introduzir conceitos básicos referentes a esta ciência, focando em criptografia moderna. A finalidade na abordagem do referido tema é de situar o leitor para a apresentação de um esquema de criptografia de chave pública recentemente proposto, chamado Rafaella, assim como de proposta de implementação em software – já em desenvolvimento – do mesmo.

Para tanto, a próxima seção, intitulada Criptografia, irá apresentar os aspectos básicos da criptografia moderna, iniciando-se por técnicas que utilizam cifragem por fluxo e por blocos e, culminando em uma introdução a criptografia de chave pública, assunto abordado em maiores detalhes na terceira seção. A quarta parte do presente artigo apresenta o esquema Rafaella, sob o ponto de vista das dificuldades matemáticas envolvidas na implementação da proposta, dos passos necessários para cifrar e decifrar uma mensagem e do mecanismo de autenticação implementado no referido esquema. Em seguida, é apresentado exemplo da aplicação prática do algoritmo. Na sexta seção, é proposto sistema computacional para implementar o citado algoritmo, o qual encontra-se em fase de desenvolvimento. O trabalho encerra-se apresentando considerações finais, bem como perspectivas futuras relativas ao algoritmo desenvolvido, assim como ao processo de implementação computacional do mesmo.

Criptografia

Criptografia é o emprego de técnicas matemáticas relacionadas a aspectos da segurança da informação, tais como: confidencialidade, integridade de dados,

identificação de entidades (pessoas, máquinas, etc), reconhecimento de origem e não repúdio [1]. É considerada uma ciência bem estabelecida que apresenta significativa influência histórica há mais de 2.000 anos [2]. No entanto, têm-se registros de sua utilização pelos Egípcios – de forma limitada – há cerca de 4.000 anos [1]. Desde então, técnicas criptográficas vêm sendo utilizadas para diversos fins, principalmente em operações militares, tanto atuais quanto antigas, como exemplo pode-se citar as grandes guerras mundiais. Além disso, apresenta aplicações em diversas áreas, como na transmissão de dados sensíveis, principalmente em transações comerciais, mas também em trocas de mensagens corporativas e pessoais através de correio eletrônico, dentre outros.

Basicamente, as técnicas modernas [3] consistem em alterar uma mensagem original – também chamada de texto pleno – de tal forma que o resultado gerado não seja compreensível para pessoas não autorizadas a conhecer o conteúdo original da mesma – sendo o resultado gerado conhecido como texto cifrado. 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 chave para gerar o texto cifrado. O retorno à mensagem original segue o mesmo princípio, no entanto, aplicando a operação inversa à utilizada para codificar, podendo para isso ser necessária a utilização de uma chave diferente da aplicada na cifragem – no caso de esquemas de criptografia assimétricos.

Existem dois tipos de algoritmos que podem ser utilizados a fim de criptografia com a utilização de chaves: os simétricos, também conhecidos como esquemas de chave secreta e, os assimétricos – esquemas de chave pública.

Os esquemas de criptografia simétrica, ou seja, que utilizam chave secreta como base para codificar e decodificar mensagens, dividem-se em dois grupos: os de fluxo e os de bloco [1]. O primeiro deles trata o texto de entrada caracter a caracter – byte a byte –, ou ainda bit a bit; enquanto, o segundo, consiste na criação de blocos de bits [2], podendo esses ter tamanhos variados. Ambos cifram cada ocorrência – caracter ou bit e bloco de bits, respectivamente – a partir de funções baseadas na utilização de uma variável, chamada de chave secreta. A decifração consiste em submeter o texto cifrado a uma função de decifragem, aplicando a ele a mesma chave utilizada para criptografar. Cabe salientar que a chave deve ser mantida em segredo exigindo, assim, privacidade no seu transporte de um lado a outro da comunicação [3], o que pode ser garantido através da utilização de canal seguro, ou então de algoritmos de chave pública, com a finalidade de garantir a transmissão da chave de maneira segura através de canais públicos, ou seja, considerados inseguros. A figura a seguir apresenta um exemplo de funcionamento desse tipo de esquema de cifragem.

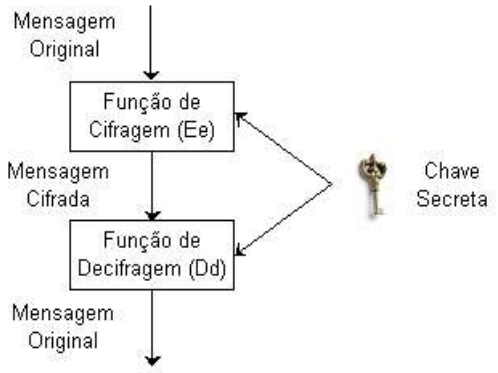

Figura 1. Funcionamento de esquemas de criptografia simétricos

Esquemas de criptografia assimétricos são baseados na utilização de duas chaves, geradas concomitantemente, uma pública, que é utilizada para cifrar mensagens endereçadas ao gerador da mesma, e uma privada, cuja utilidade é de decifrar o texto criptografado. Ambas as chaves se relacionam através de um problema de fácil e rápida solução direta, mas difícil solução inversa. A figura abaixo apresenta o emprego desse tipo de esquema.

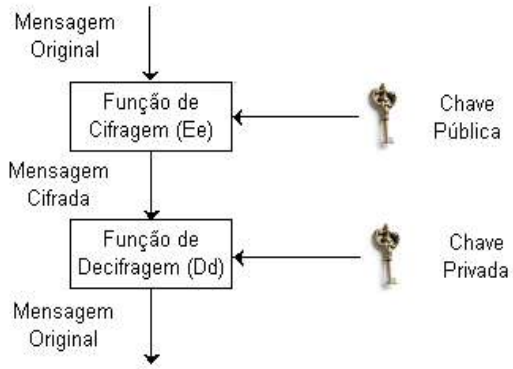

Figura 2. Funcionamento de esquemas de criptografia assimétricos

Maiores detalhes serão apresentados na próxima seção, intitulada Criptografia de Chave Pública.

Criptografia de Chave Pública

O histórico dos algoritmos de criptografia assimétricos iniciou-se em 1976, oportunidade na qual Whitfield Diffie e Martin E. Hellman

publicaram artigo intitulado "*New Directions in Cryptography*".

Esta 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 Ek, 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:

$C = Ek(M)$, onde C é a mensagem criptografada e M a original.

A segunda chave deve ser mantida em segredo, e é chamada de chave privada (Dk, 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:

$$M = Dk(Ek(C))$$

Diffie e Helmann [4] 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 familias de algoritmos, tal que $\{\mathrm{Ek}\}\mathrm{k} \in \{\mathrm{K}\} \wedge \{\mathrm{Dk}\}\mathrm{k} \in \{\mathrm{K}\}$ representam, para um espaço finito de mensagens – $\{\mathrm{M}\}$ – as transformações inversíveis a seguir:

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

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

Sendo assim:

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

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

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

IV) $\forall \mathrm{K} \in \{\mathrm{K}\}$, não é factível computar o par Ek, Dk partindo-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, salvo em casos especiais – raras exceções causadas pela utilização de chaves consideradas fracas –, deve ser impossível chegar ao valor da chave privada, partindo-se 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. 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[1].

O problema da fatoração de números inteiros pode ser utilizado em esquemas de criptografia, uma vez que, partindo-se de dois ou mais valores primos (suficientemente grandes), é computacionalmente simples calcular o produto resultante entre eles, enquanto, dado um número inteiro, torna-se uma tarefa extremamente complexa determinar os primos que o compõe.

A utilização de raízes quadradas modulo *n* se justifica pelo fato de ser pouco custoso chegar ao resultado quando se trabalha com números primos; no entanto, é complexo, do ponto de vista computacional, obter uma resposta correta quando trabalha-se com valores compostos de fatores desconhecidos [1].

O problema do logaritmo discreto está dividido em dois grupos: problemas de logaritmos discretos em campo finito e em dificuldades ligadas à utilização de curvas elípticas [5]. O primeiro tipo baseia-se na dificuldade em determinar o expoente (*a*) de uma equação do tipo: $y = g^a \bmod p$, onde *p* é um número primo e *y* e *g* são números quaisquer. Enquanto, no segundo grupo, a complexidade pode ser expressa pelo fato de: selecionando um ponto P (x,y) e somando-se P com suas próprias coordenadas *n* vezes, obtém-se um ponto resultante R(xr,yr), a partir do qual, torna-se extremamente difícil determinar as coordenadas originais – do ponto P.

A dificuldade em somar resíduos quadráticos reside no fato de os operadores de módulo apresentarem a propriedade da ciclicidade, o que dificulta o reconhecimento dos valores utilizados.

O problema da mochila é baseado no fato de ser computacionalmente oneroso obter-se os elementos que compõe a soma que resulta em um valor N, enquanto realizar a soma de diversos valores para gerar N é trivial.

Diversos algoritmos que empregam as técnicas acima discutidas foram propostos, no entanto, o funcionamento desses foge ao escopo do presente trabalho. Entretanto, abaixo, apresenta-se tabela citando 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 [1].

Esquemas	***Problemas computacionais***
RSA	Fatoração de inteiros
Rabin	Raízes quadradas módulo *n* e fatoração de inteiros
ElGamal	Logaritmo discreto
Chor-Rivest knapsack e Markle-Hellman knapsack	Mochila
Goldwasser-Micali probabilistic	Resíduos quadráticos

Tabela 1. Esquemas de criptografia de chave pública e problemas matemáticos relacionados.

O esquema Rafaella

O esquema de criptografia de chave pública Rafaella foi proposto recentemente por Ribeiro e Weber [5, 6], oferecendo tanto serviços de cifragem e decifragem de mensagens, quanto de autenticação da origem das mesmas – por prova de conhecimento zero.

O embasamento matemático por trás do algoritmo não é focado em teoria do números, como grande parte dos exemplos que se encontram na literatura atual, ao invés disso, se baseia no emprego de equações diferenciais. O esquema criptográfico consiste em efetuar operações de translação sobre funções, baseando-se na teoria dos grupos de Lie [7] – ao invés de grupos de Galois, no caso de algoritmos baseados em matemática discreta – que, por sua vez, no contexto de equações diferenciais – ao qual o discutido algoritmo se enquadra – é fortemente apoiada na utilização de simetrias. Simetrias, 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 equivalentes à original.

Posto isso, 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, ao passo que a operação inversa é extremamente complexa de 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 alto grau de conhecimento matemático –, utilizou-se uma das regras de Lie, o qual limitou o emprego direto dos operadores diferenciais. Tais 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, atendendo aos requisitos da criptografia assimétrica, assim como ao desejo de simplicidade na proposta [5].

A principal vantagem ligada à utilização do esquema em discussão está no fato de os participantes da troca de mensagens poderem escolher suas chaves privadas, ao contrário dos algoritmos propostos até o presente, nos quais, a chave privada é obtida a partir da chave pública – o que também é possível no proposto. Demais vantagens poderão ser discutidas a partir da implementação computacional que está sendo proposta, oportunidade na qual será possível fazer comparações com outros esquemas propostos na literatura.

O **processo de cifragem** de mensagens no referido esquema é baseado em transformações aplicadas em funções com a finalidade de gerar outra função que corresponde ao texto cifrado. Para isso, são aplicados dez passos básicos, conforme proposto por Ribeiro e Weber [5]. Supondo que Alice deseja criptografar uma mensagem com a finalidade de enviá-la para Bob, ela deve seguir os seguintes passos:

I) Converter a mensagem original para valores numéricos, baseando-se no código ASCII dos caracteres que compõe o texto pleno -ou outra forma de codificação), os quais irão compor os coeficientes da função correspondente à mensagem;
II) Escolher uma função real *n* vezes derivável, na qual a quantidade de coeficientes corresponde ao número de caracteres da mensagem a ser enviada, sendo que as parcelas geradas devem ser distintas entre si. A seguir, Alice e Bob devem obter suas chaves públicas e privadas, cujo procedimento será explicado na próxima seção;
III) Alice aplica o deslocamento no plano complexo, com a finalidade de gerar a função correspondente ao texto cifrado e gera um argumento auxiliar,

conhecido como argumento de autenticação;

IV) Alice envia a mensagem criptografada e o argumento auxiliar para Bob;

V) Bob aplica o deslocamento sobre a função recebida e gera uma função contínua – ou seja, uma função variável baseada em funções básicas, tais como: ln(x), exp(x), etc - que servirá como argumento auxiliar para reconhecimento de sua identidade;

VI) Bob envia a mensagem gerada após o deslocamento por ele aplicado e o argumento auxiliar por ele criado para Alice;

VII) Alice aplica a operação inversa sobre a função recebida e verifica a autenticidade do argumento recebido, através da geração de um argumento de autenticação, que, caso constate-se que o receptor não é o esperado, será utilizado para deturpar a mensagem;

VIII) Alice envia a Bob a mensagem, em conjunto com o argumento gerado;

IX) Bob aplica a mudança reversa sobre a função recebida, verifica a autenticidade da origem e extrai sua chave pública da mensagem, obtendo assim a mensagem original, gerada por Alice.

X) Bob recupera os caracteres originais, que estão representados nos coeficientes da mensagem original.

O deslocamento no plano complexo – aplicado por Alice no passo III e por Bob no V - deve ser definido conforme a mudança variável apresentada a seguir:

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

Essa transformação contém tanto partes reais quanto imaginarias e mapeia a função f(x) em f(x+a+bi).

A transformação reversa - aplicada por Alice no passo VII e por Bob no IX, consiste em outra mudança variável, expressa por:

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

A aplicação da apresentada simetria inversa consiste em mapear a função f(x) em f(x-a-bi).

As chaves são definidas da seguinte forma: a privada é escolhida por cada participante, consistindo as componentes real e imaginaria do deslocamento aplicado sobre a função original, ou seja, é um número complexo. A chave pública é obtida partindo-se da chave privada e constitui-se de uma função. Para tal, pode ser aplicado um operador diferencial. Cabe salientar que, partindo-se da chave pública exige-se custo computacional extremamente alto para se obter a chave privada, o que vem ao encontro com o que foi proposto por Diffie e Hellman em 1976 [4].

O **processo de autenticação** é baseado na geração de dois argumentos auxiliares, sendo o primeiro uma função continua - conforme já explanado no presente trabalho - formada por combinações lineares entre potências das chaves públicas dos participantes. Sobre essa função, deve ser aplicada a chave privada do receptor, gerando uma nova função que será utilizada por parte do emissor para verificar a autenticidade do receptor. O segundo argumento, é um número complexo.

De posse da função gerada, o emissor substitui sua chave privada sobre a mesma, verificando o número complexo gerado. Se o resultado for nulo, o receptor é o esperado. Caso contrário, o resultado deve ser multiplicado pela derivada da função gerada, com a finalidade de deturpar o seu conteúdo. Sendo assim, apenas o receptor autorizado poderá ler o conteúdo da mensagem original. Tal mecanismo de autenticação é baseado no emprego de uma prova de conhecimento zero [5].

A **dificuldade matemática** que determinado atacante irá enfrentar para quebrar o esquema proposto está ligada ao fato de apresentar custo extremamente elevado o trabalho de descobrir a raiz da função gerada que corresponde á chave privada de um dos participantes da comunicação. Para tanto, seria necessário resolver equações algébricas ou diferenciais, ao invés de efetuar testes de primalidade, resolver logaritmo discreto ou definir o escalar em curvas elípticas.

Ou seja, a dificuldade está ligada ao fato de descobrir o valor de a, na fórmula a seguir, que representa o operador A que pode ser utilizado como chave pública do esquema proposto.

$$A = \left(a \frac{\partial}{\partial_x} \right) \qquad (1)$$

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 (2), 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.

$$\left[e^{A} \right] f(x) = f(x + a) \qquad (2)$$

Cabe salientar que a equação (2) define a origem das chaves privadas no esquema proposto, comprovando que as mesmas podem

ser geradas a partir das chaves públicas, bem como que as chaves públicas podem ser geradas a partir das privadas, conforme demonstrado na equação (1).

Posto isso, como a exponenciação do operador A produz uma séria infinita de potências desse operador, o processo correspondente à avaliação do membro esquerdo de (2) é bastante oneroso, enquanto o mesmo efeito, quando obtido através da translação direta, ou seja, com a utilização de números complexos, constitui uma operação trivial.

Exemplo de aplicação do algoritmo

A seguir, com a finalidade de facilitar o entendimento do esquema Rafaella, será apresentado exemplo de utilização do algoritmo, através da demonstração dos passos necessários para que Alice transmita uma mensagem a Bob e este a decifre e reconheça a identidade de quem a enviou.

Supondo que Alice quer enviar a Bob mensagem cujo conteúdo é a palavra "rafaella", o primeiro passo que ela deve executar é a transformação dos caracteres que compõe o texto nos seus respectivos valores ASCII, sendo assim, a mesma obteria o resultado apresentado na tabela que segue:

Caracter	***Valor ASCII***
r	114
a	97
f	102
a	97
e	101
l	108
l	108
a	97

Tabela 2. Valores ASCII para a palavra rafaella.

O passo II consiste na escolha de uma função – $f_0(x)$ - real, *n* vezes derivável, cujos coeficientes são formados pelos valores ASCII dos caracteres que formam o texto a ser enviado. Exemplo dessa função para os caracteres acima mencionados pode ser deste tipo:

$$f_0(x) = 114e^{(8,7564x)} + 97e^{(3,456x)} + 102e^{(2,45x)} + 97e^{(0,456x)} + 101e^{(9,04x)} + 108e^{(2,709x)} + 108e^{(8,064x)} + 97e^{(4,14x)}$$

A seguir, Alice e Bob devem escolher suas chaves privadas e, a partir delas, gerar as respectivas chaves públicas. As chaves de decifragem devem ser do tipo c = A + Bi, onde *i* é a unidade imaginária e tanto A quanto B devem ser números inteiros maiores que zero. O fato de não serem empregados números de ponto flutuante está ligado ao erro de arredondamento presente nas operações de cifragem e decifragem.

As chaves públicas são obtidas a partir das privadas, sendo constituídas por uma função na qual pelo menos uma das raízes corresponde à chave privada de quem a está gerando. A referida função pode conter qualquer número de raízes, podendo ser tanto reais quanto imaginárias.

Exemplificando o mecanismo acima explanado, pode-se chegar a uma situação como a demonstrada a seguir:

ca = 27 - 9i, onde ca é a chave privada escolhida por Alice. A partir de então, ela deve definir função em que pelo menos uma das raízes constitua "ca". Isso pode ser alcançado, por exemplo, expandindo-se a expressão $(x\text{-}ca)^2$, cujo resultado obtido seria o seguinte:

$cpa = x^2 - 54x + 18ix + 648 – 486i$, que é a chave pública de Alice.

Bob aplica o mesmo procedimento, ou seja, se o mesmo escolhesse como sua chave privada o número complexo cb = 9 + 4i, ao expandir $(x\text{-}cb)^2$, obteria como sua chave pública $cpb = x^2 – 18x – 8ix + 65 + 72i$.

O passo III do algoritmo consiste na aplicação, por parte de Alice, do deslocamento no plano complexo – baseado em sua chave privada - sobre a função $f_0(x)$, o que consiste em gerar uma nova função do tipo $f_1(x) = f_0(x+ca)$, que representa o texto cifrado e deve ser enviada para Bob em conjunto com seu argumento de autenticação(etapa IV). A geração do referido argumento (chamado neste exemplo de "aa") poderá ser obtida através do produto das chaves publicas dos participantes, somado a uma potência da chave privada dela – Alice -, apresentando como restrição o fato de essa potência necessariamente precisar ser maior que 4.

A quinta etapa do algoritmo consiste no fato de Bob gerar nova função $f_2(x) = f_1(x+cb)$, que representa o deslocamento no plano complexo a partir da chave privada do mesmo. Além disso, ele constrói um argumento auxiliar ("ab" – gerado seguindo as mesmas regras que Alice seguiu quando criou "aa") que servirá como apoio para o reconhecimento da identidade dele por Alice. Para finalizar a etapa, Bob gera outro argumento, "tb", que consiste na aplicação de sua chave privada sobre o argumento "aa", que fora enviado por Alice. O passo seguinte (VI) consiste no envio – de Bob para Alice – da função $f_2(x)$, e dos argumentos "ab" e "tb".

Ao receber "tb" (etapa VII), Alice tem condições de confirmar a identidade de Bob, ou

seja, de saber se ele realmente é quem afirma ser. Para tanto, é necessário o cálculo de "vb" que consiste no fato de ela retirar de "tb" sua chave privada. Se o resultado for zero, existe a garantia de que apenas Bob poderia ter gerado "tb", portanto, sua identidade está reconhecida, sendo que, a partir de então, Alice aplicará o simétrico de sua chave sobre a função $f_2(x)$ – criando uma função do tipo $f_3(x) = f_2(x - ca)$ – e gerará um argumento "ta", da mesma maneira que Bob gerou "tb", ou seja, através da aplicação de sua chave privada sobre o argumento de autenticação de Bob ("ab"). Tanto "ta" quanto "$f_3(x)$" são encaminhados para Bob. Caso o valor de vb seja diferente de zero, a identidade de Bob não será reconhecida e o resultado obtido servirá para deturpar a mensagem, uma vez que Alice multiplicará o número complexo resultante pela derivada primeira da função cifrada, ou seja, uma operação do tipo $f_3(x) = vb * f_2'(x)$.

O passo VIII consiste no envio, por parte de Alice, da mensagem mapeada – f_3 – e do argumento "ta" para Bob. A seguir (IX), ele verifica a autenticidade de Alice, através do cálculo de "va'' - retira de "ta" sua chave privada -, que a exemplo de "vb", deve resultar em zero para que a identidade seja confirmada. Em seguida, ele extrai sua chave pública de $f_3(x)$ gerando $f_4(x) = f_3(x\text{-}cb)$, obtendo como retorno a função original (f_0), ou seja, ao retirar os coeficientes de f_0, ele terá o valor ASCII dos caracteres que compunham o texto pleno (passo X).

Implementação proposta

O fato de o esquema Rafaella exigir a implementação de sistema de processamento simbólico dificulta bastante seu emprego imediato em aplicações comerciais. Até recentemente. A implementação apresentada fora desenvolvida empregando-se um programa proprietário – Maple V.

Assim, está-se desenvolvendo biblioteca que consiste em classes, a princípio, sendo implementadas em linguagem C++, com a finalidade de criar interface amigável para que programadores possam utilizar o algoritmo em suas aplicações de maneira simples – através de simples invocações de métodos, que dispensarão o programador de implementar um sistema completo de processamento simbólico e de preocupar-se com operações de ponto flutuante, ficando o mesmo apenas responsável por informar atributos relacionados aos deslocamentos.

A referida biblioteca está em estágio avançado de desenvolvimento e será validada através da criação de software que permita gerar informações estatísticas, tanto a respeito de desempenho, quanto de perturbação da mensagem criptografada gerada. Tais dados poderão ser utilizados futuramente como subsídio para comparações do esquema proposto com os demais esquemas de criptografia de chave pública propostos na literatura e amplamente utilizados atualmente.

Embora a idéia inicial consista no desenvolvimento da interface em linguagem C++, tem-se também a intenção de disponibilizar interfaces em outras linguagens de programação de larga utilização, como é o caso de Java.

Perspectivas Futuras e Considerações Finais

Diversos são os esquemas de criptografia de chave pública conhecidos, assim como 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 a mensagem, enquanto são computacionalmente complexos no caso de tentativas de ataques com a finalidade de obter indevidamente o conteúdo do texto cifrado.

Baseando-se nisso, o esquema de criptografia assimétrica intitulado Rafaella utiliza um paradigma matemático não antes empregado com essa finalidade, que se baseia em 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, é extremamente onerosa. O mesmo se observa para o caso de haver 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 envia-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.

O fato de necessitar de processamento simbólico faz com que a utilização ampla do esquema proposto em aplicações comerciais seja dependente da criação de uma interface amigável para que programadores possam acoplar o esquema de maneira ágil e simples à 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 implementação para outras linguagens de grande utilização.

No que tange a trabalhos futuros, a partir da finalização da implementação da referida biblioteca, pretende-se desenvolver estudo comparativo entre o proposto esquema e os

atualmente existentes, com a finalidade de verificar a possibilidade de aplicação prática do algoritmo proposto.

Referências

1. Menezes, A., Oorschot, P., and Vanstone, S.: *Handbook of Applied Cryptography*. CRC, Press (1996)
2. Piper, F., Murphy, S.: *Cryptography: A Very Short Introduction*. Oxford. New York (2002)
3. Schneider, B.: *Applied Cryptography*. 2nd Edition. John Wiley & Sons (1996)
4. Diffie, W., Hellman, M. E.: *New Directions in Cryptography.*IEEE Transactions on Information Theory. IT 22, 6 (1976) 644 - 654
5. Ribeiro, V. G., Weber, R. F.: *Problemas Computacionais para Esquemas de Criptografia de Chave Pública*. In: 22º Simpósio Brasileiro de Redes de Computadores . IV Workshop de Segurança Computacional (2004) 101 – 112
6. Ribeiro, V. G.: *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 (2004)
7. Olver, P.: *Applications of Lie Groups to Differential Equations*. 2nd Edition. New York. Springer (2000)