UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO

VINICIUS GADIS RIBEIRO

Rafaella: um esquema para um novo paradigma de criptografia de chave pública

Tese de Doutorado apresentada como requisito parcial para obtenção do grau de Doutor em Ciência da Computação

Prof. Dr. Raul F. Weber
Orientador

Porto Alegre, maio de 2005.

CIP – CATALOGAÇÃO NA PUBLICAÇÃO

Ribeiro, Vinicius Gadis
Rafaella: um esquema para um novo paradigma de criptografia de chave pública/ Vinicius Gadis Ribeiro – Porto Alegre: PPGC da UFRGS, 2005.
82 f.: il.
Tese (Doutorado) – Universidade Federal do Rio Grande do Sul. Programa de Pós-Graduação em Compitação, Porto Alegre, BR-RS, 2005. Orientador: Raul F. Weber
1. Criptografia. 2. Matemática. 3. Segurança computacional. I. Weber, Raul F. II. Título.

aos meus irmãos, **Rafael** e Daniel**la**. Estudem SEMPRE.

AGRADECIMENTOS

Seria proibitivo listar todas as pessoas que me ajudaram, cooperaram e participaram desse trabalho. A qualquer pessoa que esquecesse, eu estaria cometendo uma enorme injustiça. Contudo, arrisco, visto que maior injustiça seria não agradecer a determinadas pessoas, cujo trabalho, empenho, dedicação e amor possibilitaram - ainda que de forma indireta - , que fosse possível que meu trabalho chegasse a esse ponto.

Agradeço

ao meu Professor Orientador, Raul Fernando Weber, que tantas vezes chamei de MESTRE (como conceito carinhoso da relação Mestre-discípulo), apesar de possuir titulação maior. **Meu Mestre, muito obrigado**.

ao Professor Juergen Rochol, sempre incentivando e cobrando-me a escrita do volume. Grande amigo e padrinho de crisma, muito obrigado. O mesmo obrigado, à Vera.

ao apoio do Professor Dalcídio Cláudio que, mesmo jamais tendo ministrado aula em alguma turma que eu tenha me matriculado, sempre soube apoiar e incentivar mesmo as idéias mais mirabolantes. Professor Dalcídio, muito obrigado.

aos Professores Laira Toscani - pelas dicas sobre complexidade - e Paulo Werlang.

ao Professor Doutor Ricardo Dahab, pelas observações construtivas e altamente relevantes para o escopo matemático do presente trabalho.

ao Professor Jorge Zabadal, pelas suas originais aulas de Métodos Híbridos, bem como pela paciência em participar dos testes do esquema Rafaella, no papel de "Bob". Professor Jorge, muito obrigado.

à equipe do GSeg - em especial, pelo apoio dos colegas Rafael Campello e Vinicius Serafim.

às Instituições de Ensino Superior que bancaram horas-aula para que eu pudesse realizar o trabalho com mais tranqüilidade: Faculdade Cenecista Nossa Senhora dos Anjos (FACENSA), Universidade Luterana do Brasil (ULBRA) e Centro Universitário La Salle (UNILASALLE). Aos dirigentes da IES que me apoiaram, obrigado.

à equipe da biblioteca, em especial à Ida Rossi (sempre pacienciosamente dedicando o tempo que provavelmente era de seu lazer ou almoço, para corrigir as referências erradas), Beatriz Haro (igual dedicação). Valeu, pessoal.

a Fermat, Euler, Galois e, principalmente, a Marius Sophus Lie, matemático norueguês que concebeu as ferramentas necessárias para esse trabalho.

às minhas famílias, pois tenho a felicidade de ter mais de uma. Grato pela paciência.

A Deus, por tudo.

SUMÁRIO

LISTA DE ABREVIATURAS

ANSI	American National Standards Institute
CPU	Central Process Unit – Unidade Central de Processamento
DES	Data Encryption Standard
ECB	Electronic Code Book
ECC	Elliptic curve cryptography – Criptografia de Curvas Elípticas
ECDH	Elliptic curve Diffie-Hellman
ECDSA	Elliptic curve digital signature algorithm
ISO	International Standards Organization
NIST	National Institute of Standards and Technology
OEF	Optimal Extension Field
WAP	Wireless Application Protocol

LISTA DE SÍMBOLOS

$\approx$	Aproximadamente igual a
$\equiv$	Congruente a
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{N}$	Conjunto dos números naturais
$\mathbb{Z}^*$	Conjunto dos números inteiros - excluindo-se o ZERO
$\{\}, \varnothing$	Conjunto vazio
∂	Derivada Parcial
$\propto$	Infinito
Π	Problema
$\in$	Pertence a
$\leftrightarrow$	Se e somente se

LISTA DE QUADROS

LISTA DE FIGURAS

RESUMO

O presente trabalho apresenta um novo esquema de criptografia de chave pública baseado no emprego de funções para representar as mensagens original e cifrada. No esquema proposto – denominado Rafaella -, o processo de cifração consiste na aplicação de um deslocamento no argumento da função que representa a mensagem, de modo que se *f(x)* descreve a mensagem original, então *f(x+z)* representa a respectiva mensagem cifrada. O deslocamento *z* representa um número complexo que, no esquema proposto, representa a forma das chaves privadas dos participantes. A dificuldade da resolução do problema inversos concentra-se na obtenção das partes real e imaginária do deslocamento *z*, que pode ser efetuada através de método de força bruta, ou da resolução de um problema de contorno. A segunda alternativa envolve a resolução de equações diferenciais. Dentre os métodos disponíveis para a resolução de equações diferenciais, o emprego dos chamados grupos de Lie constitui, via de regra, a estratégia mais apropriada para a obtenção de soluções analíticas, que demandam menor tempo de processamento do que as formulações numéricas. Mesmo assim, a solução obtida através da utilização dos grupos de Lie requer elevado número de operações simbólicas.

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

Rafaella: a scheme to a new public-key cryptography paradigm

ABSTRACT

This work presents a new public key cryptography scheme based in functions to represents the plain and cipher text. In this scheme, called Rafaella, cipher process consists on the application of shifting a function by a complex argument z. Therefore, if f(x) stands for the function corresponding the original message, then f(x+z) represents the cipher message. In this scheme, private keys are complex numbers. The major difficult in solving the inverse problem e.g., finding the real and imaginary parts of the private keys can be carried out by brute force or by means of solving a boundary value problem. The second alternative requires solving differential equations. Among the available methods for solving differential equations, the use of Lie groups constitutes the most simple way to obtain analytical solutions – which demands a lower time processing than usual numerical formulations. Notwithstanding, the solutions obtained by using Lie groups often requires a great amount of symbolic operations.

Keywords: Computer Security, Cryptography, Public-key Cryptography, Applied Mathematics, Differential Equations.

1 INTRODUÇÃO

A Matemática assume um papel primordial na Criptografia. Desde a mais remota das épocas, onde quer que o ser humano desejasse manter privada a sua comunicação escrita, eram usados artifícios para torná-la ininteligível para pessoas não-autorizadas. Dados os métodos antigos de Criptografia, usando recursos simples, era possível reverter a situação e descobrir a informação oculta.

Contudo, essa Criptografia era calcada sobre a obscuridade do conhecimento de determinada informação ou algoritmo. Assim são trabalhados os algoritmos de Chave Simétrica - ou Chave Secreta -, visto que a segurança se baseia no conhecimento ou não da chave. Com o histórico trabalho de Diffie e Hellman, em 1976, um esquema relativamente simples permitiu uma revolução na Criptografia, graças a determinadas propriedades matemáticas. Essas propriedades - em sua maior parte, conhecidas desde eras remotas - eram concentradas em problemas como definir se um número é ou não primo, ou como calcular um logaritmo em uma operação de módulo aplicada a uma potência. Nos últimos anos, o foco tem-se colocado sobre a dificuldade em se definir por qual escalar foi multiplicado um ponto, tendo-se apenas um outro ponto. Destaca-se que todos os problemas se apresentam sob a forma numérica - isto é, é necessário definir o valor de um número que satisfaça determinadas propriedades, normalmente referidas na Teoria dos Números.

Com a descoberta de propriedades matemáticas e problemas de elevado grau de complexidade, aliados ao uso de computadores, permitiu o emprego de técnicas melhores e de difícil quebra. São os algoritmos de Chave Assimétrica, onde são públicos o algoritmo ou procedimentos para obtenção das chaves, e uma das chaves envolvidas. Esses algoritmos - ou esquemas - baseiam-se em dois problemas: um, simples - o qual é facilmente solucionável por participantes autorizados -; e um outro problema, de grande complexidade, na qual um adversário não teria condições de resolver – em tempo razoável - , sem algum conhecimento privado. Esses algoritmos são também chamados de Algoritmos ou Esquemas de Chave Pública, os quais possibilitam que sistemas possam munir-se de diversas funcionalidades, como troca de chaves, compartilhamento de segredo, votação digital, dinheiro eletrônico, etc. A base para a implementação de tais esquemas são os problemas matemáticos supra citados.

Esses problemas são conhecidos como problemas inversos e estão, normalmente, relacionados com problemas de origem matemática ou computacional. Pode-se entender

como o problema ao qual um atacante ou adversário é exposto, para tentar obter alguma informação sensível - ou mesmo a própria mensagem que se deseja proteger. É comum envolver a descoberta de informação secreta - no contexto de criptografia de chave pública, poderia ser a descoberta da chave privada. Tradicionalmente, esses problemas envolvem algumas características, tais como

1 - ser de rápida realização por usuários autorizados a participar do esquema; e

2 - ser de onerosa realização por outros usuários. Essa segunda característica é referida como inviável ou proibitiva: não é de impossível realização, mas o seu custo é elevado, em relação à primeira característica.

O presente trabalho propõe um novo paradigma para a construção de esquemas de Chave Pública - não baseado em Teoria dos Números. A codificação envolvida força o emprego de uma função, ao invés de apenas um - ou mais - números. O adversário, para quebrar o esquema proposto, é obrigado a tentar descobrir qual é a função original. Para tanto, é forçado a resolver problema em Teoria das Funções ou da área das Equações Diferenciais.

Diversos são os métodos de resolução de equações diferenciais. Estudos dos últimos quarenta anos têm permitido métodos de mais fácil resolução de equações diferenciais, empregando-se um método criado por Marius Sophus Lie - matemático norueguês do século XIX.

O esquema proposto no presente trabalho permite efetuar a criptografia de uma mensagem, bem como prova de conhecimento zero para autenticação das partes envolvidas em uma comunicação empregando, como problema inverso a solução de equações diferenciais. Ao adversário que tentar a quebra do esquema caberá uma das duas alternativas, pertencentes respectivamente a Teoria das Funções e as Equações Diferenciais:

1 - varredura do plano complexo, para descoberta de uma das chaves privadas - é um processo similar ao emprego de força bruta, nos problemas de teoria dos números.

2 - resolver equações diferenciais, para descobrir a mensagem original. Mesmo empregando-se o método de Lie, a solução é extremamente onerosa.

Para os matemáticos, descobrir qual função originou-se a partir de determinada transformação é tido como um problema de grande dificuldade - razão pela qual se emprega tal paradigma no esquema proposto - aqui chamado de Rafaella. Observam-se as mesmas características de algoritmos de Chave Pública que emprega os problemas relacionados à Teoria dos Números.

1.1 Objetivos do presente trabalho

O principal objetivo do presente trabalho é a apresentar a viabilidade do esquema Rafaella, do ponto de vista operacional. Para tanto, é efetuado um estudo de viabilidade e é apresentado, ao final desse trabalho, um conjunto de possíveis ataques relevantes à forma empregada para cifração. Dessa forma, buscou-se fornecer ao leitor uma estimativa do número de operações simbólicas envolvidas no processo de resolver o problema inverso. Outrossim, a descrição do processo de resolução do problema inverso é encontrado na literatura específica – principalmente, Olver(2000), Ibragimov(1995) e Bluman & Kumei(1989) -, sendo apresentado um estudo sobre a complexidade no Capítulo 5.

São objetivos específicos:

- introduzir o uso de funções como objetos matemáticos para fins criptográficos;
- descrever o processo de cifração e decifração baseado em operações simbólicas – para tanto, esse processo foi operacionalizado utilizando-se o software de processamento simbólico Maple V ®;
- apresentar as vantagens operacionais de efetuar a cifração/decifração utilizando translações no plano complexo. Entende-se por translações no plano complexo mudanças de variável efetuadas sobre a função que descreve a mensagem original ou codificada:

$$f(x) \rightarrow f(x+a),\ a = r + is,\ \text{sendo } r \text{ e } s \text{ reais não nulos.}$$

1.2 Estrutura do trabalho

No estudo que se segue tem-se a seguinte organização: o Capítulo 2 trata de conceitos de Criptografia, assim como as vantagens, desvantagens e algoritmos básicos de chave pública/chave privada. Ademais, é apresentado breve resumo da base para a fundamentação teórica desses algoritmos, englobando a Teoria dos Números, com especial destaque para o estudo da primalidade, a Geometria e uma tendência recente na Criptografia: curvas elípticas, além dos Fundamentos da Matemática, onde concentram-se os estudos sobre complexidade.

O Capítulo 3 aborda aspectos conceituais e métodos de resolução de equações diferenciais, que fornece os fundamentos teóricos nos quais se baseiam os possíveis métodos de ataque por parte de adversários. Esse capítulo apresenta o tratamento das mesmas, pelo emprego das simetrias de Lie. Por simetrias, entende-se mudanças de variável que não alteram a forma da equação diferencial sobre a qual são aplicadas.

A proposta para o novo esquema de Chave Pública é encontrada no Capítulo 4 - bem como um exemplo de aplicação. Essa proposta baseia-se no emprego de translações no plano complexo utilizadas nos processos de cifração e decifração. A análise do esquema proposto é realizada em capítulo imediatamente posterior.

Conclusões e sugestões possíveis trabalhos futuros são encontrados no sexto capítulo.

Foi definido um pequeno glossário, como apêndice, no intuito de facilitar o entendimento dos termos especializados da Matemática aqui empregados. Há ainda um apêndice que apresenta uma das formas de se realizar o problema inverso, quando a chave pública é uma equação diferencial, empregando-se os recursos **determine** e **autosimp** do sistema Maple V ®. O último apêndice apresenta um breve histórico da vida de Marius Sophus Lie.

2 CRIPTOGRAFIA

O presente capítulo apresenta uma revisão sobre a criptografia, os sistemas criptográficos, os tipos de criptografia. Especial enfoque é dada à Criptografia de Chave Pública - onde cada esquema de Chave Pública, baseados no paradigma matemático da Teoria dos Números são relatados. É também efetuada breve revisão sobre as características matemáticas dos problemas inversos, empregadas atualmente por tais esquemas.

2.1 Definições de criptografia

A criptografia baseia-se na cifração de alguma informação, conhecida como **texto claro**, tornando-a ininteligível, o **texto cifrado**, de modo que apenas as pessoas que tenham autorização possam decifrar e entender esta informação. Deste modo busca-se garantir o sigilo, ou seja, mesmo que alguém não autorizado venha a interceptar a informação, não conseguirá entendê-la. Numa comunicação, apenas o remetente e o destinatário devem ter acesso à informação transmitida, para tanto o texto da mensagem deve ser cifrado e só então remetido para o destinatário, que decifrará a mensagem, obtendo o texto normal original. Para isto seria usada uma chave (senha) para realizar a cifração e a decifração da informação.

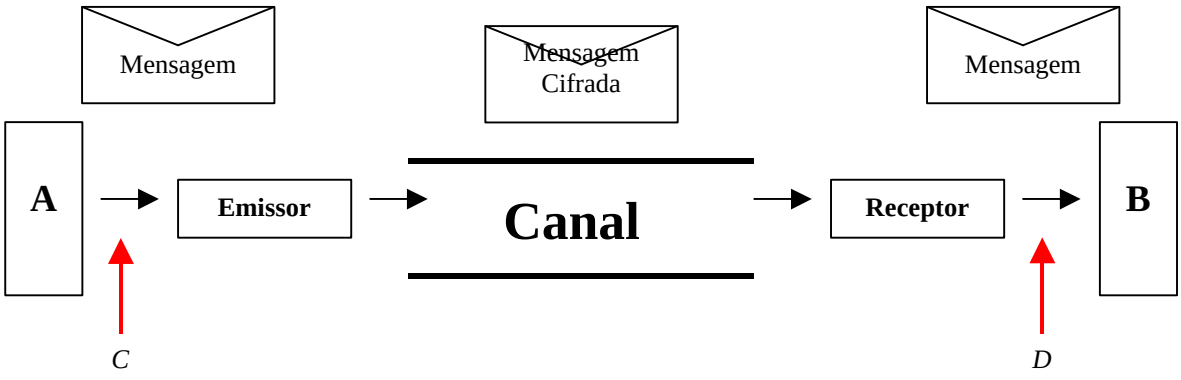


Figura 2. 1: Cifração (“C”) e Decifragem (“D”)de um texto

Segurança computacional ou segurança da informação é a parte da Ciência da Computação que se preocupa com os diversos aspectos que envolvem segurança. Para prover segurança, empregam-se serviços os quais atendem a determinadas necessidades de segurança. Alguns desses serviços podem ser providos, se o sistema em questão empregar mecanismos de criptografia.

Menezes (1996) define criptografia como "o estudo de técnicas matemáticas relacionadas a aspectos de segurança de informação – tais como confidencialidade, integridade de dados, autenticação de entidade e autenticação de origem de dados". Afirma, ainda, que não é o único meio de prover segurança da informação.

A criptografia atende a diversos desses serviços, considerando as características apresentadas no quadro a seguir:

Característica	Descrição
Privacidade ou confidencialidade	Manter a informação secreta de todos os não autorizados a ela
Integridade de dados	Garantir que a informação não seja alterada por meios desconhecidos ou não autorizados
Autenticação ou identificação de entidade	Corroborar a identidade de uma entidade
Autenticação de mensagem	Corroborar a origem de uma mensagem - ou autenticação da origem
Assinatura	Significa amarrar uma informação a uma entidade
Autorização	Exprimir, para outra entidade, de sanção oficial para ser ou fazer algo
Validação	Significa prover tempo de expiração de autorização de uso ou manipulação de recursos ou informações
Controle de acesso	Restringir acesso a recursos para entidades privilegiadas
Certificação	Endosso da informação por uma entidade confiável
Testemunhar	Verificação da criação ou existência de informação por outra entidade que não seja o criador da mesma
Confirmação	Conhecimento de que os serviços foram prestados
Recebimento	Conhecimento de que a informação foi recebida
Anonimato	Ocultar a identidade de alguma entidade envolvida em algum processo
Revocação	Retração de certificação ou autorização

Quadro 2. 1: Alguns objetivos da segurança da informação

Fonte: adaptado de Menezes (1996)

Dentre os objetivos - ou serviços - acima apresentados, Menezes (1996) destaca quatro para formar um esquema da qual originarão os outros, a saber:

Confidencialidade - é um serviço usado para manter o conteúdo de uma informação apenas aos autorizados a tanto. Pode-se obter confidencialidade por meio de uma série de técnicas, as quais podem variar desde proteção física, até algoritmos numéricos que tornam os dados ilegíveis.

Integridade de dados – é um serviço que se refere à alteração não–autorizada de dados. Para garantir integridade de dados, deve-se ter a habilidade de detectar essas alterações – as quais podem se referir à inclusão, exclusão ou substituição.

Autenticação – serviço relacionado à identificação, podendo-se referir a entidades ou mesmo à própria informação.

Não-repúdio – serviço que busca impossibilitar que um usuário negue a autoria legítima de mensagens ou outra informação, o que pode garantir que atos realizados pelas partes não possam ser negados.

Um sistema criptográfico - ou criptossistema - pode oferecer alguns dos serviços básicos de segurança: são eles a autenticação, a confidencialidade - também chamada de privacidade -, a integridade, a disponibilidade, o controle de acesso e o não repúdio (Stallings, 1998). Opondo-se aos serviços, têm-se os ataques: a interrupção é um ataque ao serviço da disponibilidade e, entre diversos exemplos, pode-se destacar o ataque de negação de serviço. Já a intercepção é um ataque à confidencialidade. A modificação é um ataque à integridade, e a fabricação, um ataque à autenticidade.

Para prover segurança da informação, são empregadas primitivas criptográficas. Uma taxinomia de primitivas criptográficas é apresentada a seguir:

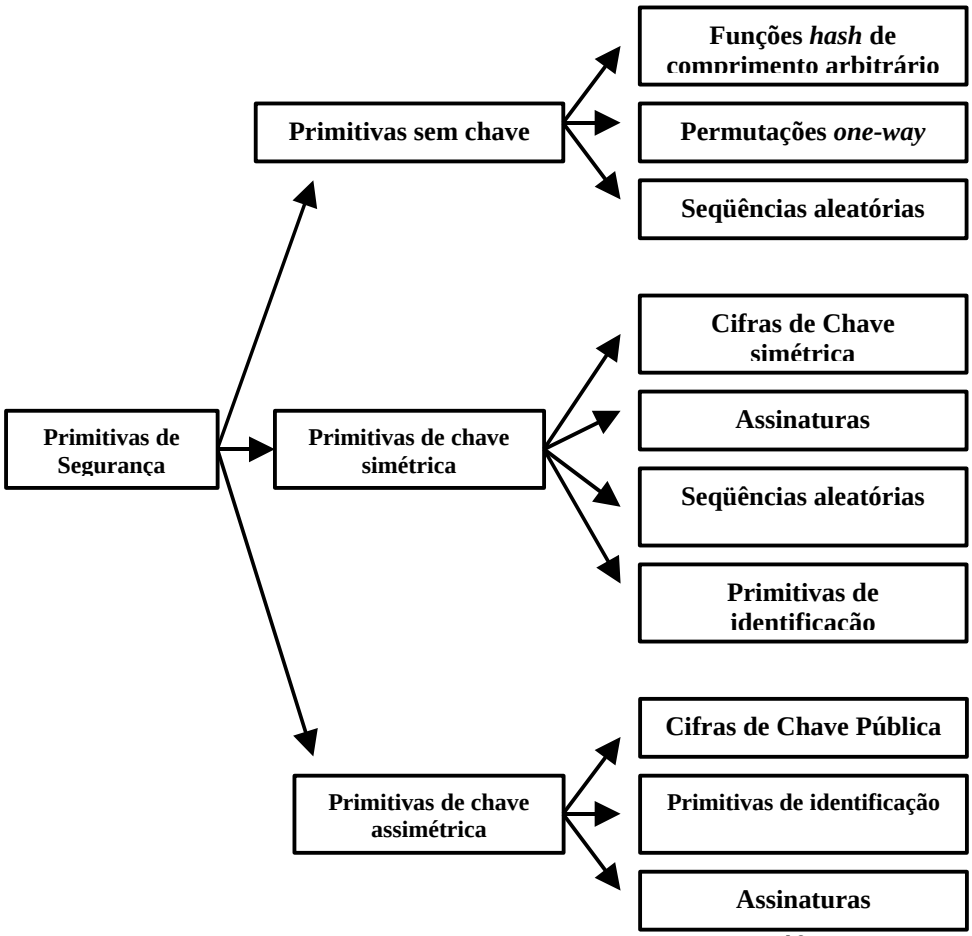


Figura 2. 2: Uma taxinomia de primitivas criptográficas
Fonte: traduzido de Menezes (Menezes, 1996)

Pode-se inferir da classificação acima que é possível empregar-se primitivas que não utilizam chaves ou voltadas ao uso de chaves. Dentre as últimas, pode-se ter aquelas que usam chaves simétricas - ou secreta ou simples -, ou chaves assimétricas - ou públicas.

Conforme diversos autores - Menezes (1996) e Stinson (1995) - , a diferença principal entre os sistemas simétricos e os sistemas assimétricos, como o próprio nome sugere, refere-se ao tipo das chaves nas operações de cifração e decifração. Nos sistemas simétricos, as duas chaves geralmente são iguais, ou seja, usa-se a mesma chave para realizar tanto a cifração quanto a decifração. Pode ser ainda que as chaves não sejam exatamente iguais, mas pelo menos elas devem estarem relacionadas, de tal forma que seja computacionalmente viável de se calcular a chave privada a partir da pública.

A partir de 1976, a criptografia apresenta novos conceitos, quando Whitfield Diffie e Martin Hellman escreveram um artigo chamado *New directions in cryptography* (Difie, 1976), onde foi apresentado um sistema criptográfico totalmente diferente: este novo sistema veio a ser conhecido como sistema de chave pública, que prometia ser mais seguro do que os sistemas de chave privada. Este sistema trouxe a noção de que as chaves poderiam ser duas, uma para cifração e outra para decifração, e que seria inviável descobrir a chave dita privada a partir da chave dita pública.

2.2 Sistemas criptográficos

Menezes (1996) define um criptossistema como sendo um termo geral, referindo-se a um conjunto de primitivas criptográficas – conforme as primitivas da figura 2.2 - usadas para prover serviços de segurança de informação. O termo mais freqüentemente utilizado em conjunto com primitivas se refere ao mecanismo que provê o serviço de confidencialidade – ou seja, criptografia. Já Schneier (1994) define criptossistema como o algoritmo – previamente por ele definido como transformações matemáticas para fins de criptografia e descriptografia -, além do modo como é implementado esse algoritmo. Stinson (1995) fornece uma definição mais formal, como é possível observar do quadro a seguir.

DEFINIÇÃO 1.1. Um criptossistema é uma penta-upla (P, C, K, E, D), onde são satisfeitas as seguintes condições:

1. P é um conjunto finito de textos claros
2. C é um conjunto finito de possíveis textos cifrados
3. K é o espaço de chaves - um conjunto finito de possíveis chaves k
4. Para cada $k \in K$, existe uma regra de cifração $e_k \in E$ e uma correspondente regra de decifração $d_k \in D$. Cada e_k mapeia de P para C - ou $\mathbf{e_k: P \rightarrow C}$ - e o d_k equivalente mapeia de D para C - ou $\mathbf{d_k: C \rightarrow P}$. Destaca-se que e_k e d_k são funções tais que $e_k(d_k(x)) = x$, para qualquer $x \in P$.

Quadro 2. 2: Definição de criptossistema.

Fonte: Traduzido de Stinson (1995)

Como se pode inferir do quadro acima, há objetos em um criptossistema - tais como textos claros, textos cifrados e chaves - e processos que realizam as transformações em alguns objetos gerando outros objetos - ou seja, as regras de cifração e decifração. Os esquemas de criptografia de chave pública normalmente diferem na lógica desses processos - ou seja, nas regras de transformação.

Os criptossistemas têm diferentes níveis de segurança, dependendo o quão difícil é a exposição de seu texto claro, ou de suas chaves - no caso da criptografia de chave pública, da exposição ou descoberta de sua chave privada. Diz-se então que foi realizada a "quebra" do criptossistema. Todo o algoritmo na qual se baseia um criptossistema pode ser "quebrável", dadas suficientes condições de tempo e recursos computacionais – contudo, esse fato pode ocorrer em uma quantidade de tempo bastante elevada; na prática, podem não o fazer em tempo hábil e, por isso, são ditos seguros. A tendência atual busca projetar algoritmos tal que a tentativa de quebra do algoritmo do criptossistema demande grande quantidade de tempo, o que torna o processo de quebra inviável. Diz-se que um algoritmo é incondicionalmente seguro, se não importa a quantidade de texto cifrado que se disponha, não possui informação suficiente para recuperar o texto original.

Um modelo matemático preciso de um criptossistema seguro é apresentado por Shannon (*apud* Schneier, 1994), e teoriza que é possível atingir um nível de "perfeito sigilo", contanto que o número de possíveis chaves para se obter um texto legível seja tão grande quanto o número de possíveis mensagens. Ou seja, em outras palavras, a chave deve ser aleatória e tão grande quanto o texto, e nenhuma chave pode ser reusada.

Define-se a entropia de um criptossistema como sendo a medida do tamanho do espaço de chaves. Essa definição é aproximadamente igual à relação

$$H(k) \approx \log_2 n$$

onde:

H é a entropia; e
n é o número de chaves.

De forma geral, quanto maior a entropia, mais difícil é a quebra do criptossistema.

Diferente de protocolos genéricos de comunicação, os criptossistemas são projetados para resistir a ataques. Quando falham, pode-se identificar os pontos fracos como sendo em uma ou ambas as categorias: no próprio algoritmo de cifração, ou no ambiente operacional.

Algumas das principais funções que podem ser implementadas com o uso da criptografia computacional são:

Sigilo: entende-se que somente os usuários ou processos autorizados possam ter acesso à informação, ou torná-la inteligível.

Integridade da informação: é conseguida se há uma garantia para o usuário de que a informação permanece correta e não foi alterada, acidentalmente ou não.

Autenticação de usuário: é o processo que permite ao sistema verificar se a pessoa ou processo, com quem está sendo realizada a comunicação, é de fato a pessoa ou processo que alega ser.

Autenticação de remetente: ou assinatura digital, é o processo que permite a um determinado usuário certificar-se de que a mensagem foi realmente enviada pelo usuário que alega tê-la enviado.

Autenticação de destinatário: consiste de conseguir uma prova de que a mensagem enviada para um determinado usuário foi de fato recebida por ele, sem nenhuma alteração no seu conteúdo.

Autenticação de atualidade: consiste em provar que a mensagem recebida é uma mensagem atual, e não alguma mensagem antiga que está sendo reenviada. Isto pode prevenir o "ataque da meia-noite", onde mensagens enviadas anteriormente foram gravadas e são repetidas, tentando iludir o destinatário.

Os sistemas criptográficos podem ser simétricos ou assimétricos. Diz-se que um sistema criptográfico é simétrico se a chave de decifração é igual a chave de cifração ou uma função computacionalmente viável desta, este sistema também é conhecido como sistema de chave secreta. Já o sistema assimétrico - foco do presente trabalho -, também conhecido como sistema de chave pública, é aquele onde as chaves de cifração e decifração são diferentes e não se pode facilmente computar a chave privada partir da pública (sendo uma pessoa não autorizada). Conforme Stinson (1995), pode-se assumir, em um sistema assimétrico, que $e_k <> d_k$.

Com relação ao desempenho dos algoritmos, os simétricos são mais rápidos, sendo recomendados para situações onde a velocidade de cifração ou decifração é um fator importante. A grande vantagem dos sistemas assimétricos é que em momento algum, durante a operação com este tipo de algoritmo, é necessário enviar a chave secreta pelo canal de comunicação, evitando que ela seja capturada por algum adversário monitorando a linha. Os dois tipos de sistemas podem ser considerados seguros - a escolha de um ou outro depende da preferência do usuário e do tipo de aplicação desejada. Caso o usuário desejar maior segurança, pode aumentar o tamanho das chaves até um nível que ele considere seguro. Contudo, a velocidade de processamento das operações envolvidas pode tornar o tempo de processamento proibitivo para a operação.

O maior problema em empregar a criptografia de chave pública como um método de segurança é que a distribuição, armazenagem e eventual revogação das chaves introduz uma carga administrativa cara e onerosa (Menezes, 1996). Essas dificuldades limitaram, durante algum tempo, o uso em larga escala de muitos produtos de criptografia.

Considerando-se as situações existentes vida real, especialmente no que tange à aplicações que devem ser dotadas de serviços de privacidade, observa-se a ocorrência de diversos problemas. Na vida real, os seres humanos se comunicam – porém nem sempre suas intenções são claras. Diferente de computadores, pode haver interesses em jogo, tais como burlar uma eleição, ou o desvio de recursos monetários – o que altera o comportamento dos envolvidos na comunicação. Para buscar uma solução para esses problemas, surgiram os protocolos criptográficos - nos quais a maioria emprega, em algum passo, criptografia de Chave Pública.

2.3 Criptografia de Chave Pública

Com o trabalho publicado por Whitfield Diffie e Martin E. Hellman, foram apresentados conceitos de relevância para o emprego de esquemas de chaves públicas para possibilitar seu emprego em criptossistemas. Dentre esses conceitos, destacam-se o emprego de duas chaves diferentes: uma, chamada de pública - pois pode ser amplamente divulgada - e a outra, privada - a qual deve manter-se secreta (Diffie, 1976). Emprega-se uma dessas chaves para realizar a cifração da mensagem, e a outra, para a decifração da mesma. Essas chaves, embora tenham sido calculadas a partir de origens comuns, têm o seu

cálculo proibitivo, a partir de uma delas. Em outras palavras, tendo-se uma delas - a pública, por exemplo -, não se pode calcular a outra - a privada - em tempo tal que a informação por elas oculta ainda tenha valor. Na verdade, cita-se como unidade de tempo para efetuar esse cálculo a ordem de milhares de anos (Schneier, 1994; Stallings, 1998).

Com o emprego desse conceito, resolveu-se o problema da distribuição de chaves - visto que as chaves públicas podem estar disponíveis em qualquer lugar, circulando livremente.

Sendo K_e e K_d as chaves pública e privada, M a mensagem, E, a operação de cifração e D, a operação de decifração, pode-se afirmar que

se $C = E(M, K_e)$, então $M = D(C, K_d)$, para qualquer M.

é computacionalmente intratável deduzir K_d, partindo-se de K_e.

é computacionalmente tratável, para o possuidor das chaves, calcular o par de chaves K_e e K_d, satisfazendo-se os requisitos acima.

A seguir, são apresentadas as características gerais do principais algoritmos de chave pública.

2.4 Características Gerais dos Principais Algoritmos de Chave Pública

A partir do artigo de Diffie e Hellman, diversos outros passaram a ser apresentados. Dentre as diversas propostas de algoritmos de chaves públicas, nem todos os algoritmos de chave pública se ocuparam em trocar chaves: diversos esquemas buscam a funcionalidade de criptografar mensagens; alguns preocupam-se em gerar assinaturas, e realizar a verificação das mesma; outros, contudo buscam realizar identificação das partes, com conhecimento zero; há os que se preocupam em garantir uma assinatura não falsificável , e verificável publicamente; existem aqueles esquemas em que se preocupam em evitar ataques de personificação, de fabricação de conteúdo, ou mesmo em garantir a integridade da informação que circula.

As operações para realizar criptografia de chave pública podem ser relacionadas com um problema de difícil solução – podendo o mesmo ser computacional ou matemático. Esse problema, via de regra, deve ter duas características básicas: ser de rápida execução, para usuários autorizados, e o problema inverso deve ser de difícil resolução – o que inviabilizaria a exposição da informação sensível a adversários.

Entende-se como problema inverso ao trabalho ao qual um adversário é submetido, para tentar obter a informação sensível ou texto legível . Normalmente, envolve a descoberta da chave privada. Os esquemas de chave pública tipicamente implementam operações que são rápidas para um usuário autorizado efetuar, mas resolver o problema inverso é extremamente oneroso. Dentre aqueles que são atualmente implementados, observa-se que a maioria dos esquemas determinísticos baseados em problemas matemáticos são calcados nos problemas de fatorização de números compostos, mochilas ou logaritmos discretos. Assume-se, então, que a resolução de tais problemas é computacionalmente inviável, visto a não existência - ou o não conhecimento - de algoritmo que o resolva em tempo polinomial.

Assim, para fins de estudo, os problemas inversos podem ser agrupados por famílias de problemas. A base que os relaciona é a Matemática - cuja abordagem segue na seção seguinte, bem como breve levantamento dos problemas inversos.

2.6 Criptografia de chave pública e o problema inverso

A Matemática é a ciência que investiga as relações entre entidades definidas abstrata e logicamente, ou ainda, o ciência que tem por objeto o estudo da grandeza mensurável e calculável .

Esta seção apresenta, baseada nas divisões da Matemática, breve estudo dos problemas inversos que viabilizam os esquemas de criptografia de chave pública. Destaca-se que o tema não constitui novidade, pois observa-se que o conhecimento desses problemas já era maduro o suficiente há bastante tempo. Por exemplo, desde os tempos de Euler[1], têm-se as condições suficientes para a elaboração de algoritmos do tipo RSA - embora tenha-se esperado cerca de duzentos anos para que essa implementação se tornasse real, com o advento do computador.

Para fins de facilidade de estudos da participação dessa ciência, a Matemática pode ser particionada em suas divisões principais, a saber:

- Fundamentos da Matemática
- Álgebra
- Análise Combinatória
- Análise Matemática
- Geometria
- Teoria dos Números
- Topologia

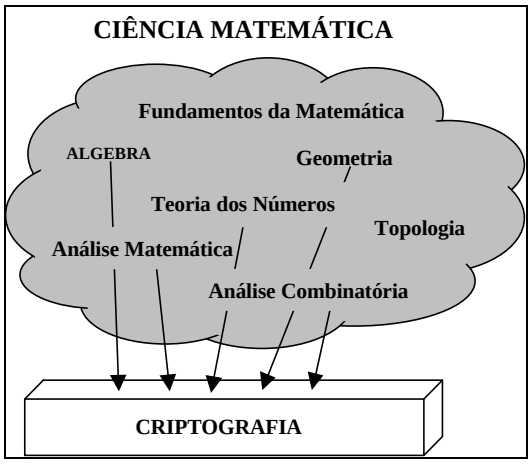


Figura 2. 3: Divisões da Matemática e relação com a criptografia

[1] Leonard Euler, Matemático, 1707-1783.

A figura anterior apresenta as diversas divisões da Matemática que têm alguma contribuição para a Criptografia. É relevante citar que nem todas as áreas contribuem diretamente para elaboração de esquemas de Chave Pública. A seguir, serão apresentados breves aspectos matemáticos dos principais problemas inversos do esquema de criptografia de chave pública atualmente empregados.

Considerando-se esses problemas inversos, é possível agrupar os esquemas em grupos: assim, há o grupo de esquemas cujo problema inverso refere-se à fatoração de um número grande, o grupo cujos esquemas referem-se ao problema do logaritmo discreto, etc. A área da matemática que apresenta problemas inversos aplicados na maior parte dos esquemas de criptografia de chave pública é a Teoria dos Números. Destaca-se, contudo, que esses esquemas não são limitados a apenas problemas dessa área.

Posteriormente, são apresentadas considerações referentes à área de Fundamentos da Matemática. Essa área incorpora os estudos de complexidade. Tais estudos possibilitam, por exemplo, estimar-se o esforço de resolução do problema inverso de um algoritmo de criptografia de chave pública. Ao final, é apresentado um modelo matemático dos sistemas criptográficos de chave pública.

2.6.1 Fatoração de números

Essa família emprega números naturais. Assume-se que grandes números inteiros podem ser primos - cujos únicos divisores são 1 e eles próprios - ou compostos - assim chamados por terem números primos como fatores. Dois grandes problemas dominavam essa área da Teoria dos Números: determinar se um número é ou não primo, e quais são os fatores de um grande número composto.

Até recentemente, determinar eficientemente se um número seria ou não primo constituía um problema de relativa dificuldade. Em agosto de 2002, Agrawwal, Kayal e Saxena publicaram um artigo contendo um algoritmo que define de forma eficiente e determinística, se um dado número é primo ou composto - em tempo proporcional ao número de dígitos do dado número.

O processo de determinar os fatores de um número é chamado de fatoração desse número - ou ainda decomposição desse número em fatores primos. Existem diversos algoritmos que possibilitam fatorar um número primo. A questão é o tempo para realizar essa fatoração. Assume-se ser a fatoração um problema difícil, mas ainda não provado.

Alguns dos algoritmos de fatoração são conhecidos desde os tempos da Grécia antiga - contudo, tais algoritmos nem sempre foram eficientes. Os mais recentes incluem o algoritmo proposto por Fermat - nem sempre utilizado, a não ser que se saiba que o número a ser fatorado tem dois fatores próximos da raiz quadrada do número. Contudo, esse algoritmo constitui a base para o algoritmos utilizados hoje para fatoração de números grandes, tais como o crivo quadrático e o das frações continuadas (Bressoud, 1989).

Os esquemas baseados em problemas de fatoração de números inteiros podem ser resumidas na seguinte situação: tendo-se dois números primos, é fácil calcular o produto desses. Contudo, dado o produto resultante, não é um problema fácil determinar os seus números primos compostos. Assim, diz-se que o problema inverso é a fatoração de dado número público. Dentre os esquemas de criptografia de chave pública baseados no problema da fatoração de números inteiros, considerando-se algoritmos determinísticos,

encontram-se o RSA proposto por Rivest, Shamir e Adleman, em 1978 e Rabin, além do esquema Williams - uma melhoria sobre o esquema Rabin (Menezes, 1996). Dentre os esquemas probabilísticos, Menezes (1996) cita o esquema Blum-Goldwasser. Stallings (1999), Menezes (1996) e Stinson (1995) listam os principais ataques efetuados contra esse esquemas baseados nesse problema - focando principalmente o RSA -, destacando ataques matemáticos e relacionados com tempo.

No que tange ao algoritmo RSA, um dos possíveis ataques se refere à determinação dos chamados números primos geradores (p e q), pela fatoração de n (n = p * q). De posse desses números, é possível calcular os seus anteriores (ou seja, p-1 e q-1) e, de posse de uma das suas chaves - pública -, determinar a outra - a chave privada. Esse ataque é de possível implementação; contudo, não há algoritmo eficiente conhecido para resolver esse problema (Menezes, 1996). Na realidade, o problema de se fatorar um número e o problema de calcular a chave privada a partir da pública e do conhecimento do produto dos números primos geradores são problemas equivalentes.

2.6.2 Logaritmo discreto

Essa família também emprega números naturais. Dado um elemento *g*, de um grupo *G* de ordem *t* e outro elemento *y* - também de *G*, o problema é determinar *x* - onde $0 < x < t-1$ tal que *y* seja resultante da aplicação de *g* com *g*, *x* vezes. Em alguns grupos há elementos que podem gerar todos os elementos de *G* por exponenciação, com todos os números inteiros entre *0* e *t-1*: nesse caso, tal número é chamado de gerador e o grupo é dito cíclico.

Os esquemas de chave pública baseados em problemas de logaritmos discretos restringem-se ao problema de logaritmos discretos em grupos cíclicos. Tais problemas podem ser apresentados do seguinte modo: dados um número primo p, um número g e o número *y*, resultante do cálculo $y = g^a \bmod p$, não é um problema fácil determinar o expoente a. O esquema mais conhecido é o ElGamal – embora tenha sido projetado para assinaturas digitais, pode ser também empregado para criptografia de dados (Menezes, 1996;). O esquema Diffie-Hellman também pode ser aqui enquadrado, com algumas reservas – visto constituir problema próprio. Outros exemplos são *Digital Signature Algorithm*, Massey-Omura e Nyberg-Rueppel - todos algoritmos determinísticos (Stinson, 1995; Menezes, 1996).

Ainda nesse âmbito, há um esquema proposto por William Raike, que não é baseado explicitamente em um problema matemático, mas é baseado em características específicas de uma máquina de estados que são equivalentes ao problema do logaritmo discreto (Nichols, 1999). Nesse esquema, determinados estados da máquina são suas chaves, e o número de estados entre eles é a chave privada. Considerando que as seqüências de estados podem representar laços, a determinação do número de estados entre eles não é problema de fácil resolução.

Menezes (Menezes, 1996) destaca, além dos desses problemas, o problema da residuosidade quadrática - tendo, como representante, o esquema probabilístico Goldwasser-Micali - e o problema da raiz quadrada módulo n

Assim, pode-se observar que grande parte dos problemas inversos na qual são baseados os esquemas supra mencionados têm ao menos um aspecto em comum: baseiam-se em problemas da Teoria dos Números – habitualmente, esforços computacionais com o intuito de efetuar a determinação de um número, que pode ser a chave privada, por exemplo. Contudo, esquemas baseados na Teoria dos Números não constituem exclusividade, conforme relatado a seguir.

2.6.3 Outros problemas inversos

Há outras áreas da Matemática que podem apresentar problemas de difícil solução e constituir a base para elaboração de esquemas de criptografia de chave pública. Comumente, seus problemas inversos são baseados em problemas do tipo NP-completos.

Uma família desses esquemas são baseados em problemas de mochilas. Tais problemas podem ser descritos da seguinte forma simplificada: determinar os valores de sub-conjuntos de números inteiros que, somados, resultaram em um determinado valor dado. A soma desses pesos é de realização eficiente; contudo, o problema inverso não é de fácil resolução. Destacam-se aqui os esquemas Merkle-Hellman e Chor-Rivest (Stinson, 1995; Schneier,1994). Esses problemas inversos são considerados como pertencentes à àrea da Análise Combinatória (Koblitz, 1999).

Jacques Patarin sugeriu, em 1993, um esquema cujo problema matemático de dificuldade é a resolução de um sistema de equações polinomiais multivariáveis. Sabe-se que sistemas de equações podem gerar zero, uma ou um indeterminado número de soluções. Patarin mostrou como quebrar esquema similar proposto anteriormente, em 1983 por Matsumoto e Imai, e apresentou sua proposta de melhoria nesse sistema cujo problema inverso pertence à área da Álgebra Linear (Koblitz, 1999).

Há outros esquemas que empregam propriedades da Álgebra Linear. Um exemplo é o esquema McEliece, de 1978, o qual emprega um caso especial de problema NP, para fins de decifração da mensagem cifrada. O problema em questão é a decodificação de um código de detecção de erros linear. A sugestão de McEliece para códigos lineares foi o emprego de códigos Goppa. O objeto que se trabalha, tipicamente, são matrizes para os quais a mensagem deve ser codificada. O algoritmo que realiza essas operações é citado na literatura como sendo de duas a três vezes mais rápido do que o RSA. Um dos problemas tipicamente relatados nesse esquema é a considerável expansão de dados na transformação para o texto codificado. (Stinson, 1995; Blake, 1999).

Menezes (Menezes, 1996) destaca algumas generalizações dos problemas já citados nessa subseção.

A seção a seguir apresenta algumas considerações sobre a complexidade e sua relevância para o estudo dos problemas inversos.

2.7 Complexidade

Um problema pode ser de dois tipos: solucionável ou não solucionável (Toscani, 2000). Em se havendo um procedimento efetivo que sempre pára - ou seja, um algoritmo que resolve esse problema -, diz-se que o problema é solucionável.

Um problema de decisão não solucionável pode ser parcialmente solucionável, se há um procedimento efetivo que, sempre que a resposta é afirmativa pára, e para respostas negativas, pode ou não parar.

Programas cujo procedimento efetivo sempre pára são ditos algorítmicos.

Contudo, pode ocorrer que, para algumas entradas, os programas podem não parar - isto é, contém laços infinitos. Assim, iterações indefinidas podem gerar execuções infinitas. Uma iteração indefinida pára se e somente se existe - associada a sua execução - uma cadeia decrescente infinita - ou limitada -, de forma que, a cada iteração, corresponda um elemento da cadeia. Sendo essa cadeia finita, e não repetindo elementos, ela tende a ser decrescente e a execução da iteração tem que parar. Essa cadeia, na verdade, determina a proximidade da condição de parada - isto é, a cada iteração, a execução tem que estar mais próxima da parada. Se não há evidência dessa cadeia, não se pode afirmar que o procedimento é um algoritmo.

Um algoritmo, apesar de parar, pode ser tão demorado, que não tenha utilização prática (Toscani, 2000). Entende-se por complexidade de um algoritmo o esforço despendido para resolvê-lo. A complexidade de tempo é medido em número de operações necessárias à execução do algoritmo, e é função do tamanho da entrada - ou volume de dados.

Tamanho da entrada é um número natural associado à dificuldade do problema para a entrada - entretanto, sem particularizar essa entrada. Por exemplo, no problema de classificação de uma lista, é o número de elementos da lista - nada sendo afirmado sobre a organização original dos elementos da lista. O tamanho da entrada varia com o problema, podendo ser

- o número de elementos de um vetor;
- dimensões de uma matriz;
- o número de símbolos de um texto;
- o número de vértices de um grafo;
- o número de operações de uma expressão;
- o número de bits de representação de um número;
- o número de termos de uma série, etc.

Definição
Dada uma função f(n), onde n é o tamanho da entrada, define-se que

f(n) = O(g(n)) é definido como limite superior assintótico, se

$$\exists\, \mathbf{c, k} \in \mathbf{N} \mid \mathbf{0} \leq \mathbf{f(n)} \leq \mathbf{cg(n)}\,, \forall\, \mathbf{n} \geq \mathbf{k}$$

f(n) = W(g(n)) é definido como limite inferior assintótico, se

$$\exists\, \mathbf{c, k} \in \mathbf{N} \mid \mathbf{0} \leq \mathbf{cg(n)} \leq \mathbf{f(n)}\,, \forall\, \mathbf{n} \geq \mathbf{k}$$

f(n) = Q(g(n)) é definido como limite exato assintótico, se

$$\exists\, \mathbf{c_1, c_2, k} \in \mathbf{N} \mid \mathbf{c_1 g(n)} \leq \mathbf{f(n)} \leq \mathbf{c_2 g(n)}\,, \forall\, \mathbf{k} \geq \mathbf{n}$$

A notação definida acima é chamada de notação de ordem (Menezes, 1996).

Assim, a ordem de complexidade de algumas funções pode ser estimada como

Funções polinomiais, se o grau de um polinômio de ordem n, sendo m $\in$ N^* e o seu coeficiente de maior grau um número positivo, então $f(n) = Q(n^m)$;

Funções logarítmicas, se para qualquer valor constante m, então $log_m (n) = Q(ln(n))$;

Fatoriais, $n! = W(2^n)$;

Função logaritmo de um fatorial, $ln (n!) = Q(n\ ln(n))$.

Definição

Dada uma função f(n), onde n é o tamanho da entrada, e k, um valor constante define-se que a ordem do algoritmo é de complexidade de tempo

- **linear**, se para o pior caso, o tempo de execução é da ordem $O(n)$;
- **polinomial**, se para o pior caso de execução é da ordem $O(n^k)$; ou
- **exponencial**, se não for possível limitar dessa forma o seu tempo de execução.

Observa-se que pode haver ainda uma outra ordem, sub-exponencial, se para o pior caso de execução é da ordem $e^{Q(n)}$ (Menezes, 1996). Há autores que definem a complexidade de tempo exponencial se o seu pior tempo de execução é de ordem $O(k^{f(n)})$, k constante.

Considerável simplificação de notação pode ser empregada, caso se reduza o problema da identificação da complexidade a um problema de decisão; assim, um algoritmo poderia ser considerado uma forma de se definir se determinado problema concreto pode ter uma resposta do tipo sim ou não.

Definição

A classe de complexidade P é o conjunto de todos os problemas de decisão para os podem ser resolvidos em tempo polinomial.

A classe de complexidade NP é o conjunto de todos os problemas para os quais uma resposta afirmativa pode ser obtida em tempo polinomial, empregando-se alguma informação extra - normalmente, chamado de certificado.

A classe de complexidade co-NP é o conjunto de todos os problemas para os quais uma resposta negativa pode ser obtida em tempo polinomial, empregando-se alguma informação extra - normalmente, chamado de certificado.

Caso, ao se tentar resolver um problema, ocorre a geração de um novo problema do mesmo tipo do original, diz-se ter um problema de função recursiva (Manna, 2003). Para um algoritmo de função recursiva, a complexidade depende fortemente do tamanho do subproblema - isto é, da velocidade como a recursão se aproxima da parada - ou base (Toscani, 2000). Como no caso da iteração, é preciso a cada iteração estar mais próximo da base para ser solucionável. Se essa aproximação dá-se a passos constantes, diz-se ser a complexidade exponencial - sendo exponencial, o algoritmo é ineficiente e, para entradas grandes, impraticável.

Se, dentre todos os algoritmos que buscam resolver o problema, não há um algoritmo polinomial - ou seja, só há algoritmos exponenciais -, então o problema não é tratável. Diz-se, então, que o problema é intratável (Toscani, 2000).

O próximo capítulo apresenta as Equações Diferenciais - visto ser a área do problema inverso do esquema de criptografia de chave pública que é proposto no capítulo posterior.

3 INTRODUÇÃO ÀS EQUAÇÕES DIFERENCIAIS E AOS GRUPOS DE LIE

O presente capítulo apresenta as equações diferenciais, a sua dificuldade de trabalho, bem como os grupos de Lie. Esse capítulo apresenta fundamentos teóricos do trabalho a ser desenvolvido na tese.

Equações diferenciais são um problema do tipo

$$Af = g,$$

sendo f e g funções de classe C^n, e

A, um operador diferencial de ordem n.

Em outras palavras, equações diferenciais são equações que estabelecem propriedades geométricas para funções de uma ou mais variáveis. Essas propriedades geométricas são, via de regra, representadas pela amplitude, inclinação e concavidade da função, denotadas, respectivamente, pelas derivadas de ordem 0 , 1 e 2.

Por ordem de equação diferencial, entende-se a maior ordem de derivação encontrada entre todas as parcelas da equação.

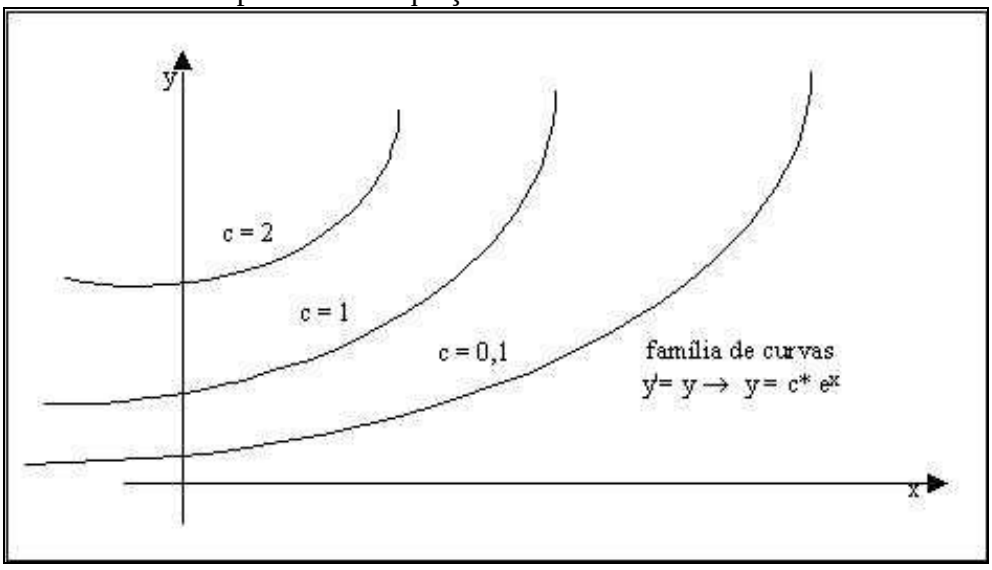


Figura 3. 1: Família de soluções de $y' = y$.

O objetivo da resolução de uma equação diferencial consiste em encontrar famílias de curvas – funções - que possuam propriedades geométricas prescritas, em termos de suas derivadas. Um exemplo dessas famílias se encontra na figura 3.1 - sendo solução de $y' = y$.

Podem ser classificadas conforme o número de variáveis, dependência na função incógnita, a existência ou não de funções fonte e o tipo de coeficientes que multiplicam a função e as derivadas dessa última.

Com o emprego do critério de dependência na função incógnita, podem ser classificadas em lineares e não-lineares (Boyce, 1999; Kreider, 1972; Ayres, 1974).

Pelo critério da existência de funções fonte, podem ser classificadas em homogêneas, e não homogêneas.

Considerando como critério o tipo de coeficientes que multiplicam a função e suas derivadas, podem ser classificados em coeficientes constantes ou coeficientes variáveis. Caso os coeficientes sejam variáveis, a equação ainda pode ser classificada como linear ou não-linear. Nas equações lineares, os coeficientes dependem apenas das variáveis independentes, enquanto que nas equações não-lineares, os coeficientes dependem também da função incógnita e/ou de suas derivadas.

Como exemplo, considere-se a equação diferencial ordinária linear de segunda ordem dada por

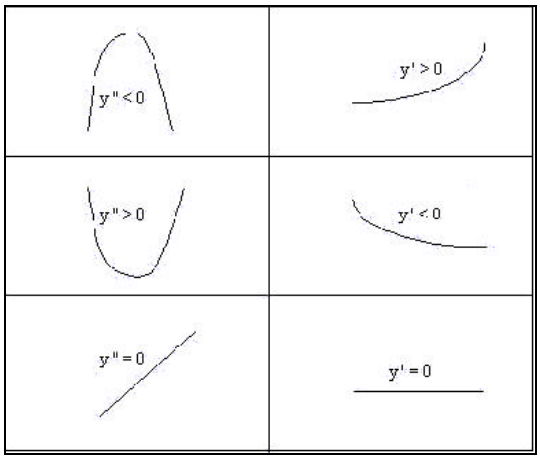
$$y'' + y' - y = 0.$$

Essa equação informa que uma determinada função $y(x)$, quando derivada duas vezes, somada a sua derivada primeira e subtraindo ela própria, se anula, para qualquer valor de x.

Do ponto de vista geométrico, isso equivale a formular a seguinte questão: quais são as possíveis funções $y(x)$ cuja amplitude é igual a sua concavidade somada a sua inclinação, em qualquer ponto?

$$y = y'' + y'.$$

y'' associada com a concavidade
y' associada com o crescimento da função – a inclinação
conforme o quadro a seguir:



Quadro 3. 1: Possibilidades para y" e para y'.

A fim de ilustrar o processo de resolução da equação acima apresentada, toma-se um ponto arbitrário P_0, de coordenadas (x_0, y_0).

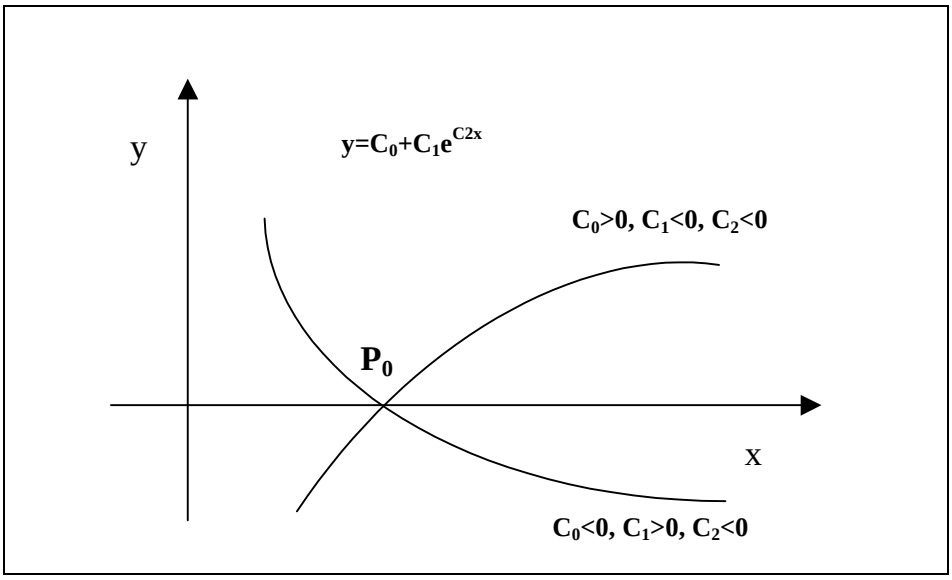


Figura 3. 2: Vizinhança do ponto P_0 para a função $y = C_0+C_1e^{C2x}$

Assuma-se o valor 0 para y_0, e 1 para x_0. Analisando o comportamento da equação nas vizinhanças de x_0, observa-se que as equações diferenciais ordinárias assumem localmente a forma

$$y'' + y' = 0,$$

ou seja, a concavidade da curva nas vizinhanças do ponto (1,0) é igual a sua inclinação, com o sinal oposto. Conforme a figura 3.2, têm-se duas possibilidades: ou a função original y(x) é crescente, sendo a sua concavidade negativa, ou y(x) é decrescente, sendo a concavidade positiva.

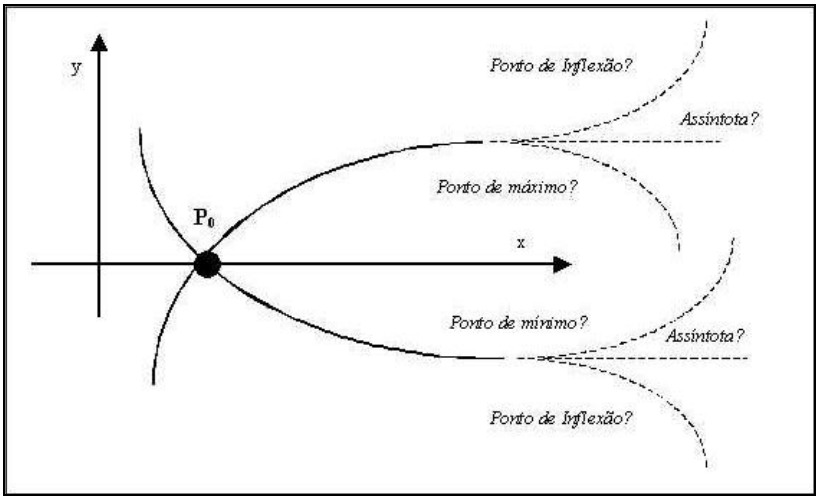


Figura 3. 3: Possibilidades para a função y(x)

Destaca-se que esse comportamento é válido apenas nas vizinhanças do ponto P_0 (1,0). Surge, então , a seguinte questão:

Como se comporta a função, a partir da abscissa x, suficientemente distante de x_0? Seria esse ponto, um ponto de máximo local da função ou mínimo local da função? Ou a forma da curva continua mantendo a tendência assintótica? Ou ainda, o ponto poderia ser um ponto de inflexão, invertendo a concavidade?

A fim de responder a essas questões, tome-se novamente a equação diferencial ordinária na forma

$$y'' - y = - y',$$

para verificar a validade das três hipóteses.

Procedendo-se a análise, suponha-se que exista um ponto de máximo ou mínimo local. Neste caso, y´ seria nulo, a equação se reduziria a

$$y'' = y,$$

o que incorre que a concavidade é igual ao próprio valor local da função. Constata-se que essa hipótese é inconsistente com a premissa, visto que a concavidade deveria sofrer uma mudança de sinal, caso existisse um ponto de máximo – conforme a figura 3.3.

Poderia continuar a tendência assintótica? Nesse caso, a conseqüência é a mesma da primeira hipótese. Uma vez que y´= 0, a equação se reduziria a

$$y'' = y$$

ou seja, que a concavidade teria o mesmo sinal da função, o que não é verdade.

Testando-se, finalmente, a hipótese da existência de um ponto de inflexão à direita de P_0, conclui-se que, uma vez que y ´´ = 0, a equação se reduziria a

$$y = y' ,$$

ou seja, a inclinação local é igual à própria função. Essa conseqüência é consistente com a premissa assumida, de modo que o comportamento da curva, ilustrado pela figura 3.4, constitui um esboço da função y(x) em uma vizinhança de maior extensão em torno de P_0.

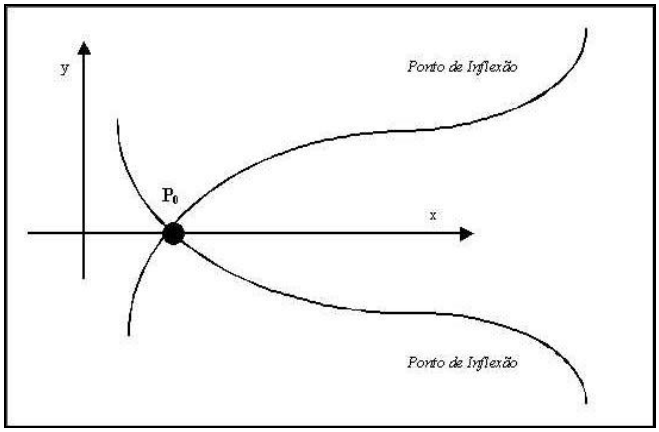


Figura 3. 4: Comportamento da curva f = y(x)

O próximo passo no estudo do comportamento de y(x) segue naturalmente da análise já efetuada – o que levaria a uma questão subseqüente: continuaria a curva crescendo, após o ponto de inflexão? Existiriam novos máximos ou mínimos locais, ou novos pontos de inflexão?

Utilizando-se argumentos semelhantes aos já apresentados, pode-se testar as hipóteses a cada região adjacente determinando, dessa forma, o comportamento qualitativo da solução da equações diferenciais ordinárias.

Naturalmente, o processo qualitativo apresentado visa tão somente compreender o comportamento da família de curvas que constitui a solução da equações diferenciais ordinárias. A fim de obter resultados quantitativos, ou seja, especificar a família de curvas com dada precisão, é necessário recorrer a métodos de resolução de equações diferenciais. Esses métodos são divididos em três grandes classes:

1 – métodos analíticos – esses métodos fornecem soluções em forma fechada para a família de curvas – ou seja, a partir deles, são obtidas expressões algébricas para a função incógnita. Nessa classe de métodos se destacam o método da separação de variáveis, transformadas integrais, método das características, método dos coeficientes a determinar, métodos perturbativos, e o método de Lie – este último, baseado na análise de grupos contínuos (Ayres, 1974).

2 – métodos numéricos – esses métodos fornecem soluções discretas – ou seja, são obtidos vetores, cujos valores numéricos correspondem a amostragem da solução em determinados pontos escolhidos. Nesta classe de métodos, encontram-se diversas formulações em diferenças finitas, elementos finitos, elementos de contorno, volumes finitos, além de alguns métodos variacionais baseados em colocação.

3 – métodos híbridos - esses métodos fornecem, em geral, soluções em forma fechada – embora utilizem recursos analíticos e numéricos. A principal diferença entre os métodos analíticos e métodos híbridos reside no fato de que as soluções em forma fechada fornecidas pelos últimos não serem exatas, embora possam ser refinadas até a exatidão desejada. Essa classe de métodos é consideravelmente mais ampla que as outras, pois pode ser baseada em quaisquer dos métodos já mencionados, além de empregar recursos adicionais – tais como ajuste de curvas, interpoladores, otimizadores, sistemas de cálculo

de raízes, transformadas discretas, e diversas aproximações. Nessa classe se encontram os métodos espectrais, e os métodos nodais, bem como o método dos painéis(Polyanin,2004).

Nos métodos analíticos, a obtenção de soluções envolve a aplicação de operadores integrais, mudanças de variável e mapeamentos. A necessidade de aplicar recursivamente essas operações analíticas torna o método bastante dispendioso – mesmo dispondo de programas de computação algébrica. Já nos métodos híbridos resultam, em geral, na obtenção de sistemas lineares de ordem elevada cuja resolução é igualmente dispendiosa, do ponto de vista computacional, uma vez que requerem a aplicação de algoritmos de inversão de matrizes, triangularização ou fatorações. Os métodos híbridos, por sua vez, tendem a reduzir o esforço computacional exigido pelos métodos analíticos e numéricos, pelo fato de empregarem recursos específicos para os quais determinadas formulações são mais eficientes. Ainda assim, o resultado das formulações híbridas envolvem essencialmente as mesmas operações exigidas para obtenção de soluções via métodos numéricos e analíticos – de modo que resultam em grande esforço computacional.

3.1 Mapeamento de soluções

Mapeamento entre soluções de uma equação diferencial consiste na transformação de uma dada solução f em uma nova solução g. Esse mapeamento pode ser efetuado de duas formas.

A primeira realiza-se através de mudanças de variável sobre a função f e seus argumentos. Outra forma é através da aplicação de operadores diferenciais sobre a solução f. Operadores diferenciais são transformações efetuadas sobre funções que envolvem o cálculo de suas derivadas. Como exemplo, o operador

$$A = \frac{\partial^2}{\partial x^2} + \frac{\partial}{\partial y}$$

é uma instrução que informa o processo de obtenção da função g: a função g é obtida ao derivar duas vezes a função f em relação a x, e somada com a sua derivada primeira em relação a y. Esse processo é definido da seguinte forma:

$$Af = g.$$

A fim de ilustrar o procedimento, considere-se a seguinte equação diferencial parcial a coeficientes variáveis

$$\frac{\partial f}{\partial x} = y\frac{\partial f}{\partial y} \qquad (1)$$

Essa equação admite a seguinte solução particular:

$$f = c_1(x + \ln y) + c_2 \qquad (2)$$

Uma nova solução pode ser obtida impondo a condição

$$f = c_1(a(x,y) + \ln b(x,y)) + c_2$$

onde a(x,y) e b(x,y) são funções a determinar.

A fim de determinar as soluções a(x,y) e b(x,y) a função resultante pode ser novamente substituída na equação diferencial original, dada por (1), fornecendo uma nova equação diferencial parcial:

$$\frac{\partial a}{\partial x} - y\frac{\partial a}{\partial y} + \frac{1}{b}\left(\frac{\partial b}{\partial x} - y\frac{\partial b}{\partial y}\right) = 0.$$

Para que a nova função satisfaça a equação original, a nova equação obtida deve ser idêntica à equação original. Essa condição implica as seguintes restrições, para as soluções a e b:

$$\frac{\partial a}{\partial x} - y\frac{\partial a}{\partial y} = Q \qquad (3) \text{ e}$$

$$\frac{\partial \ln b}{\partial x} - y\frac{\partial \ln b}{\partial y} = Q \qquad (4),$$

onde Q representa uma função fonte.

Qualquer solução particular desse sistema constitui uma possível mudança de variável que produz uma nova solução para a equação diferencial original. Como exemplo, as mudanças de variável

$$x \to c_1(x + \ln y) + c_2 \qquad (5) \text{ e}$$

$$y \to c_3 e^{c_4 x} \qquad (6) \text{ ,}$$

que transformam a solução dada pela equação (2) na nova solução,

$$f = c_1 + \left(c_1(x + \ln y) + \ln\left(c_3 e^{c_4 x}\right)\right) + c_2$$

constituem uma simetria de Lie admitida pela equação original. Assim, uma simetria de Lie admitida por uma dada equação diferencial, nada mais é do que um conjunto de mudanças de variável que transformam soluções particulares em novas soluções particulares da mesma equação dada.

Definição:

Uma simetria de Lie pode ser formalmente definida como uma transformação

$$(x_1, x_2, ..., x_n) \rightarrow (\wp_1, \wp_2, ..., \wp_n)$$

onde

$$\wp_i = \wp_i(x_1, x_2, ..., x_n)$$

tal que, se

$$A\ f(x_1, x_2, ..., x_n) = g(x_1, x_2, ..., x_n)$$

então

$$Af(\wp_1, \wp_2, ..., \wp_n) = g(\wp_1, \wp_2, ..., \wp_n).$$

A principal aplicação das simetrias de Lie consiste na construção de soluções gerais a partir de soluções particulares de uma certa equação diferencial. Durante o processo de construção uma ou mais simetrias são aplicadas sucessivamente sobre uma determinada solução particular, obtida por inspeção direta, métodos analíticos convencionais, métodos espectrais, transformadas integrais ou quaisquer métodos que forneçam soluções analíticas para formas analíticas particulares da equação original.

3.2 Mapeamentos que preservam a estrutura das equações diferenciais

A fim de garantir que as mudanças de variável transformem soluções particulares em novas soluções de uma mesma equação diferencial, é preciso impor condições que assegurem a invariância da equação diferencial em relação a essas mudanças de variável. As mudanças de variável definidas dessa forma são simetrias de Lie admitidas pela equação diferencial. No exemplo anterior, as mudanças de variável dadas pelas equações (5) e (6) não alteram a forma da equação diferencial (1), alterando entretanto a forma da solução dada por (2). Essas mudanças de variável constituem soluções particulares das equações diferenciais (3) e (4), que representam os critérios de invariância da equação diferencial. Dessa forma, qualquer solução das equações (3) e (4) constituem mudanças de variável que não alteram a equação diferencial original, isto é, constituem **simetrias admitidas** pela equação diferencial (1).

Existem mapeamentos que não preservam a forma da equação diferencial, ou seja, não obedecem a condições de invariância. Ao contrário das simetrias de Lie, esse mapeamento não visa transformar soluções particulares em novas soluções de uma mesma equação diferencial, mas tão somente converter soluções de determinadas equações originais em soluções de uma dada *equação alvo* (Bluman, 1989). A fim de ilustrar o argumento, suponha-se que se deseja obter soluções da equação

$$\frac{df}{dx} - f = 1.$$

Caso sejam conhecidas soluções de outra equação diferencial, tal como

$$\frac{df}{dx} - f = 0,$$

para a qual uma solução particular dada por

$$f = e^{x},$$

é possível impor a seguinte condição restritiva para a respectiva solução mapeada: a função

$$f = e^{a}$$

deve satisfazer à equação alvo, dada por

$$\frac{df}{da} - f = 1.$$

Esse mapeamento define possíveis mudanças de variável que transformam a solução de uma determinada equação em soluções de uma equação de interesse. Existem, entretanto, soluções que não mudam a sua forma em relação a determinadas simetrias de Lie. Essas soluções, denominadas invariantes, são estudadas na seção seguinte.

3.3 O conceito de invariante

Existem determinados mapeamentos que, além de preservar a forma da equação diferencial, preservam também determinadas soluções desta. Quando isso ocorre, diz-se que a solução é **invariante** com respeito a essas mudanças de variável. Essa situação pode ser ilustrada calculando soluções particulares para a equação

$$\frac{df}{dx} = f \qquad (7).$$

Sabendo que a função

$$f = e^{x}$$

é uma solução particular da equação, pode ser construída a solução geral, a partir da seguinte mudança de variável

$$x \to a(x).$$

Efetuando a substituição, e aplicando a regra da cadeia[2], resulta

$$\frac{df}{da}\frac{da}{dx} = f \ .$$

Impondo a condição de invariância da equação diferencial, obtém-se

$$\frac{df}{da} = f \ ,$$

o que implica

$$\frac{da}{dx} = 1$$

que constitui uma equação diferencial auxiliar a ser resolvida. Nesse caso, a solução da equação auxiliar é obtida diretamente, via integração:

$$a = x + c_0 \ .$$

Assim, a mudança de variável

$$x \to x + c_0 \qquad (8)$$

define uma nova solução para a equação diferencial. Uma vez que

$$e^x \qquad (9)$$

é solução de $\frac{df}{da} = f$, a função

$$e^{x+c_0} \qquad (10),$$

obtida pela substituição de (8) em (9), também é solução da mesma equação diferencial. Nesse caso, diz-se que a equação diferencial (7) admite uma simetria do tipo **translacional** – isto é, através da translação da variável independente por um fator constante, obtém-se uma nova solução para a equação diferencial (7) a partir de uma solução particular. A nova solução obtida, dada pela equação (10), é invariante em relação a translações, uma vez que novas substituições do tipo

$$x \to x + c_1 \ ,$$

[2] Por "regra da cadeia" entende-se a aplicação do conceito de derivada a funções compostas, a fim de avaliar, em seqüência, as variações de cada função em relação a suas variáveis independentes.

não alteram a forma da solução obtida. Isto ocorre porque os parâmetros c_0 e c_1 são arbitrários.

Soluções invariantes são, portanto, funções que não têm sua estrutura alterada frente a determinadas mudanças de variável. Em seções posteriores, será demonstrado que as soluções são invariantes com respeito a determinadas mudanças de variável quando se mantiverem inalteradas frente a aplicação de determinados operadores presentes na solução formal da equação diferencial em estudo. Esses operadores são exponenciais dos chamados **geradores infinitesimais do grupo de simetria** admitido pela equação diferencial. O conceito de gerador infinitesimal é introduzido a seguir.

3.4 Reconsiderando o conceito de simetria: geradores infinitesimais

O conceito geométrico de simetria é bastante familiar para a maioria das pessoas não versadas em Matemática. Por exemplo, sabe-se que o corpo humano possui simetria bilateral – isto é, traçando-se um eixo vertical ao longo do corpo, é possível secioná-lo em duas regiões cuja geometria é essencialmente a mesma, a menos de uma reflexão. Em termos analíticos, a geometria bilateral do corpo humano se traduz como segue. Supondo-se que o corpo esteja centrado num sistema de eixo cartesianos, como na figura a seguir:

Figura 3. 5: O corpo humano: exemplo de simetria bilateral.

Caso seja tomado um ponto com coordenadas (x,y), pertencente ao interior do corpo, existirá sempre um ponto com coordenadas (-x, y), que corresponde a sua imagem especular. Ou seja, pontos da seção "A" da figura tem seu simétrico na seção "B". Assim, simetria bilateral consiste na invariância de um determinado objeto em relação à troca de sinal da sua abscissa.

O conceito geométrico de simetria pode ser generalizado tomando como exemplo o caso da simetria bilateral. Assim como o corpo humano permanece invariante em relação à operação $x \rightarrow -x$ - ou seja, em relação ao rebatimento em torno do eixo y -, pode-se redefinir o conceito de simetria como a invariância em relação à aplicação de determinadas transformações. Um exemplo da generalização do conceito pode ser obtido através da observação de manchas de poluente na superfície de corpos hídricos.

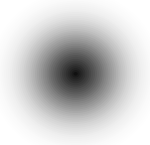


Figura 3. 6: Uma mancha concêntrica: exemplo de simetria rotacional.

Considere-se uma mancha cujo mapa de densidade de concentração cujas isolinhas consistem em círculos concêntricos – isto é, que a concentração do poluente decaia a partir do ponto central, apenas com a variável radial. Essa mancha possui simetria rotacional, ou seja, permanece invariante em relação às operações de rotação em torno do eixo perpendicular à superfície do corpo hídrico, e que atravessa o seu centro. Note-se que, ao girar a mancha em torno desse eixo, a distribuição de concentração correspondente não sofre alterações. Esse exemplo ilustra uma generalização do conceito de simetria, denominado simetria operacional – invariância em relação a aplicação de transformações efetuadas por operadores.

Tal como no exemplo da mancha, é possível definir simetrias operacionais para funções contínuas. Essas simetrias consistem na invariância das funções em relação à aplicação de determinados operadores diferenciais. Por exemplo, a função

$$f(x,y) = x^2 + y^2$$

é invariante em relação a rotações em torno da origem. O mapa de densidade dessa função é mostrado na figura anterior.

Quando uma determinada função é invariante em relação à aplicação de um determinado operador diferencial, diz-se que ela é um **ponto fixo** desse operador. Torna-se possível agora generalizar ainda mais o conceito de simetria, através de sua definição segundo o ponto de vista de Lie. Ao invés de definir simetria como sendo a invariância de uma função em relação a aplicação de determinado operador diferencial, Marius Sophus Lie estendeu esse conceito para denotar não a invariância, mas a **conservação de determinada propriedade específica da função**.

Essa propriedade decorre do fato da função ser uma solução particular de determinada equação diferencial. Dessa forma, a simetria de Lie pode ser definida de maneira mais precisa, como

" uma solução particular de uma determinada equação se transforma em outra solução particular da mesma equação, através da aplicação da exponencial de determinado operador diferencial".

Um exemplo típico de simetria com aplicações em Física Matemática consiste na terna de operações dada por

$$\left(x + 2et, t, u.\exp\left(-ex - e^2 t\right)\right),$$

válida para a equação diferencial que descreve a transferência de calor por condução na forma

$$\frac{\partial^2 u}{\partial x^2} = \frac{\partial u}{\partial t} \quad .$$

A ação dessas operações de simetria tem o seguinte significado matemático: se uma dada função u(x,t) é a solução da equação dada acima, então a função

$$u_1(x, y) = \exp(-ex - e^2 t) * u(x + 2et,\ t)$$

também é solução da mesma equação diferencial. Note-se que determinadas transformações nos argumentos de uma função que satisfaz uma equação diferencial preservam o seu caráter fundamental, do ponto de vista de Lie: o fato de ser solução dessa equação diferencial.

Os operadores diferenciais que transformam soluções particulares de uma equação diferencial em novas funções que também são soluções particulares da mesma equação são as **exponenciais dos geradores infinitesimais do grupo de simetria** (Bozicevic, 2000; Dattolli, 1998; Ibragimov, 1995).

Definição:

Grupo de simetria é definido como o conjunto $\{v_1, v_2,...,v_m\}$ de operadores diferenciais lineares de 1ª ordem, provido da operação binária [,], definida como $[v_i,v_j] = v_i v_j - v_j v_i$.

Em outras palavras, os geradores infinitesimais são operadores diferenciais lineares de primeira ordem com coeficientes constantes ou variáveis, que constituem os elementos do grupo de simetria - também conhecidos como grupo de Lie, associado àquela equação diferencial. No trabalho proposto, esses operadores constituem incógnitas no problema inverso.

Dentre os exemplos mais freqüentes de geradores infinitesimais de grupos de simetria aplicados a problemas físicos, destacam-se os exemplos apresentados no seguinte quadro:

$v_1 = l\frac{\partial}{\partial x} - k\frac{\partial}{\partial y}$
$v_2 = y\frac{\partial}{\partial x} - x\frac{\partial}{\partial y}$
$v_3 = y\frac{\partial}{\partial x} + x\frac{\partial}{\partial y}$
$v_4 = x\frac{\partial}{\partial x} + y\frac{\partial}{\partial y}$

Quadro 3. 2: Geradores infinitesimais de grupos de simetria mais empregados em Física Matemática.

O emprego de simetrias de Lie na conversão de soluções particulares de equações diferenciais é utilizado, basicamente, para **evitar o processo de inversão de operadores diferenciais**, que constitui uma tarefa extremamente onerosa, do ponto de vista computacional - seja por via numérica, seja por via analítica (Chari, 1995; Ibragimov, 1995; Olver, 2000).

Do ponto de vista operacional, a grande dificuldade encontrada na resolução de equações diferenciais consiste na aplicação de operadores inversos. Como exemplo, suponha-se que sobre a função

$$f(x, y) = x.\cos(y) + e^{-x^2} - 3.x.y + 2.x - y,$$

seja aplicado o operador diferencial

$$\frac{\partial^2}{\partial_x^2} + \frac{\partial^2}{\partial_y^2} - e^{(x-y)}\frac{\partial}{\partial_x} - x\frac{\partial}{\partial_y}.$$

Esse operador transforma a função f(x,y) em

$$g(x, y) = -2e^{-x^2} + 4x^2e^{-x^2} - x.\cos(y) + e^{x-y}.(\cos(y) - 2xe^{-x^2} - 3y + 2) + x.(-x.\text{sen}(y) - 3.x - 1).$$

Essa operação é facilmente aplicável em qualquer dos sistemas aplicativos simbólicos mencionados acima. Entretanto, o respectivo problema inverso, que consiste em restaurar a função f(x,y), tendo-se a função g(x,y) é extremamente oneroso – tanto do ponto de vista numérico, quanto analítico. Esse procedimento consiste na resolução da equação diferencial

$$\frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2} - e^{(x-y)}\frac{\partial f}{\partial x} - x\frac{\partial f}{\partial y} = g(x,y).$$

Assim como a operação de derivação pode ser aplicada facilmente sobre quaisquer funções, sendo a operação inversa - ou seja, a integração - extremamente difícil (Davenport,

1988), a aplicação de operadores diferenciais inversos constitui uma tarefa consideravelmente mais complexa do que a aplicação dos próprios operadores (Ayres, 1974; Greenspan, 1988; Ortega, 1981; Strang,1980).

Observando novamente o quadro 3.2, uma questão surge naturalmente: como determinar todos os geradores infinitesimais admitidos por uma determinada equação diferencial? A fim de responder a essa pergunta, torna-se necessário introduzir o conceito de **grupo de Lie**.

3.5 Grupos de Lie

O grupo de Lie de uma equação diferencial consiste no conjunto de todos os geradores infinitesimais por ela admitidos. Esse conjunto é provido de uma operação binária denominado **comutador** ou *Lie bracket*, definido como

$$[v_1,v_2] = v_1v_2 - v_2v_1,$$

onde $\mathbf{v_1}$ e $\mathbf{v_2}$ são geradores infinitesimais admitidos pela equação diferencial. O termo grupo decorre do fato do conjunto acima definido possuir também as propriedades básicas dos grupos convencionais, a saber:

1 – associatividade

$$[v_1,[v_2, v_3]] = [[v_1,v_2], v_3]$$

2 – existência de um elemento neutro

$$v_0 = I$$

3 – existência de elemento inverso para cada gerador

$$v_{1i} = v_1^{-1}$$

4 – fechamento em relação à operação binária

$$v_1, v_2 \in G \Rightarrow [v_1,v_2] \in G.$$

Além das propriedades básicas de grupo, os grupos de Lie são anti-comutativos, isto é

$$[v_2,v_1] = - [v_1,v_2] ,$$

e obedecem à identidade de Jacobi:

$$[v_1,[v_2, v_3]] + [v_2 ,[v_1,v_3]] + [v_3 ,[v_1,v_2]] = 0.$$

Como exemplo, o grupo de Lie da equação do calor unidimensional, transiente, para difusividade térmica unitária dada por

$$\frac{\partial u}{\partial t} = \frac{\partial^2 u}{\partial x^2}$$

tem a seguinte estrutura (Olver, 2000):

$[\,,\,]$	v_1	v_2	v_3	v_4	v_5	v_6	v_a
v_1	0	0	0	v_1	$-v_3$	$2v_5$	v_{ax}
v_2	0	0	0	$2v_2$	$-2v_1$	$4v_4 - 2v_3$	v_{at}
v_3	0	0	0	0	0	0	$-v_a$
v_4	v_1	$-2v_2$	0	0	v_5	$2v_6$	v_a'
v_5	v_3	$-2v_1$	0	$-v_5$	0	0	v_a''
v_6	$-2v_5$	$2v_3 - 4v_4$	0	$-2v_6$	0	0	v_a'''
v_a	$-v_{ax}$	$-v_{at}$	v_a	$-v_a'$	$-v_a''$	$-v_a'''$	0

Quadro 3. 1: grupo de Lie da equação do calor

Fonte: Olver (Olver, 2000)

Na tabela 3.1 , os elementos do grupo de simetria são dados por:

$$v_1 = \frac{\partial}{\partial x}$$

$$v_2 = \frac{\partial}{\partial t}$$

$$v_3 = u\frac{\partial}{\partial u}$$

$$v_4 = x\frac{\partial}{\partial x} + 2t\frac{\partial}{\partial t}$$

$$v_5 = 2t\frac{\partial}{\partial x} - xu\frac{\partial}{\partial u}$$

$$v_6 = 4tx\frac{\partial}{\partial x} + 4t^2\frac{\partial}{\partial t} - \left(x^2 + 2t\right)u\frac{\partial}{\partial u}$$

$$v_a = a(x,t)u\frac{\partial}{\partial u}$$

sendo v_a, uma sub-álgebra de dimensão infinita[3].

Estabelecidas as propriedades dos grupos de Lie, torna-se possível, então, responder à pergunta “como determinar todos os geradores infinitesimais admitidos por uma

[3] Uma sub-álgebra de dimensão infinita é um conjunto infinito de geradores infinitesimais que compõe um grupo de Lie.

determinada equação diferencial?". Note-se que as propriedades do grupo de Lie fornecem, implicitamente, estratégias para a obtenção de geradores infinitesimais. Supondo-se conhecidos dois geradores infinitesimais do grupo de simetria - v_1 e v_2, que não comutam entre si - torna-se possível obter um terceiro gerador - v_3 -, aplicando o comutador ou a propriedade de fechamento, uma vez que

$$v_3 = [v_1, v_2].$$

Uma vez obtido o terceiro gerador infinitesimal, pode-se então aplicar a identidade de Jacobi a fim de determinar mais três elementos do grupo:

$$[v_1,[v_2, v_4]] + [v_2 ,[v_1,v_4]] + [v_4 ,[v_1,v_2]] = 0$$

$$[v_1,[v_3, v_5]] + [v_3 ,[v_1, v_5]] + [v_5,[v_1, v_3]] = 0$$

$$[v_2,[v_3, v_6]] + [v_3 ,[v_2,v_6]] + [v_6,[v_2,v_3]] = 0.$$

De posse de seis geradores infinitesimais, é possível aplicar novamente as propriedades de anti-comutatividade e identidade de Jacobi sobre todas as outras combinações não utilizadas anteriormente. Esse processo conduz, em geral, à obtenção de todo o grupo de simetria da equação diferencial, a menos que ocorram duas situações:

1 – o processo leve à construção de um sub-grupo; ou

2 – o grupo tenha um número infinito de geradores.

Além dessas duas situações adversas, uma dificuldade adicional surge na determinação do grupo de simetria: é preciso conhecer, ao menos, dois geradores infinitesimais admitidos pela equação diferencial. Ademais, esses dois operadores não podem comutar entre si, pois produziriam um terceiro operador nulo, o que encerraria o processo.

Será mostrado posteriormente que essas últimas são as principais dificuldades envolvidas na resolução do problema inverso em cifração, isto é, na decodificação de mensagens originadas a partir de equações diferenciais. Dessa forma, qualquer técnica que explore essas situações adversas constitui, a princípio, um possível método de cifração baseado nas simetrias admitidas por equações diferenciais.

Entretanto, é necessário conhecer previamente os geradores infinitesimais, a fim de que a solução da equação seja obtida em forma fechada[4]. Caso seja necessário calcular os geradores infinitesimais, o processo pode ser tornar tão oneroso quanto o requerido pelos métodos numéricos e analíticos convencionais.

O próximo capítulo apresenta o esquema de criptografia de chave pública proposto.

[4] Uma forma fechada consiste em uma expressão algébrica – em suma, uma fórmula ou função explícita.

4 PARADIGMA PROPOSTO: DESCRIÇÃO DO MÉTODO RAFAELLA E ANÁLISE DE VIABILIDADE

Considerando-se as características descritas no capítulo anterior, é proposto um novo paradigma para esquemas de Chave Pública em Criptografia, baseado em grupos contínuos – grupos de Lie - ao invés de grupos discretos – grupos de Galois. Nesse novo paradigma, a mensagem original é expressa em termos de uma função e as chaves privadas consiste em um número complexo – arbitrados pelos participantes. O processo de cifração consiste na transformação da mensagem original em uma nova função. Essa nova função não revela os elementos, torna mais complexo o problema inverso a ser resolvido pelo adversário: torna-se necessário resolver uma equação diferencial que descreve a transformação da função original na nova função **e** aplicar as respectivas condições restritivas sobre a solução obtida – condições iniciais, de contorno ou de passagem por pontos -, ao invés de efetuar fatoração, resolver logaritmo discreto, ou outro problema cuja solução é objeto de estudo da Teoria dos Números. O esquema proposto, denominado Rafaella, utiliza mudanças de variável no plano complexo, a fim de efetuar a cifração da mensagem original.

A dificuldade associada à resolução do problema inverso reside, em primeiro lugar, na ausência de um processo sistemático para a determinação das condições de contorno. Além disso, reside também na elevada quantidade de operações com ponto flutuante - para soluções numéricas -, ou operações simbólicas - para soluções analíticas. Isso ocorre porque os métodos analíticos requerem o emprego de operadores integrais, mudanças de variável e mapeamentos, enquanto que os métodos numéricos resultam na obtenção de sistemas lineares de ordem elevada – exigindo o uso de algoritmos de inversão de matrizes, fatorações e triangularização.

No presente capítulo é apresentado um esquema simbólico baseado no novo paradigma. As seções iniciais desse capítulo – de 4.1 a 4.4 - fornecem a descrição do método proposto, ao passo que a seção 4.5 constitui uma análise de viabilidade do método proposto, perante o ataque de um adversário. Considerações sobre a complexidade do problema inverso são apresentadas no Capítulo 5. A seção 4.6 apresenta um exemplo de aplicação do método.

4.1 Descrição formal do esquema Rafaella

O processo pode ser formalmente descrito, de modo análogo aos modelos apresentados por Stinson e Brawley e Gao (Stinson, 1995; Brawley, 1999).

Definições:

Seja $z \hat{I} P$, sendo P o espaço das chaves privadas, tal que P $\subset V$, onde V é o conjunto dos números complexos.

Seja $C_p \hat{I} P_n$, sendo P_n o espaço de chaves públicas e definido como o conjunto das funções de variável complexa, definida como $C_p = f(z)$ sendo que z $\in V$, onde V é o conjunto dos números complexos.

Seja $f_0 \hat{I} F$, sendo F o espaço de funções contínuas e infinitamente diferenciáveis em uma região $a_1 < x < a_2$, $b_1 < y < b_2$ no plano complexo. Assim, f_0 representa a forma codificada da mensagem original .

Sejam $C, D \hat{I} J$, onde J representa o conjunto dos operadores diferenciais lineares. Definem-se os operadores diferenciais C e D, que mapeiam funções de variável complexa em funções de variável complexa, de modo que $C(f_0(x)) = f_0(x+z)$. Em outras palavras, pode-se dizer que $\$ C \mid C(f(x)) = f(x+z))$. Esse operador efetua a transformação da mensagem original f_0 em mensagem cifrada. Os operadores podem ser definidos matematicamente como $C = e^{z\frac{\partial}{\partial x}}$, e $D = e^{-z\frac{\partial}{\partial x}}$.

Destaca-se que os operadores de cifração - C - e decifração - D - são formalmente definidos, mas não empregados diretamente em sua forma original para efetuar as operações de cifração/decifração. No esquema proposto, essas operações são efetuadas diretamente através da translação da função.

Uma vez apresentado formalmente o esquema, resta apresentar as possíveis estruturas das chaves.

4.2 Estruturas das Chaves Privada e Pública

No esquema proposto, as chaves privadas não necessariamente são obtidas a partir de uma chave pública[5], que consiste em uma função contínua[6] para a qual uma das raízes complexas é a chave privada. Como exemplo, considere-se a função

$$f(x) = (x-z_1)(x-z_2).$$

A equação algébrica $f(x) = 0$ possui duas soluções no plano complexo, z_1 e z_2.

A primeira delas constitui a chave privada de Alice. Dessa forma, o processo de geração da chave privadas a partir da chave pública consiste na obtenção das respectivas raízes.

---

[5] Embora seja possível. Por questões de praticidade, a Chave Privada é utilizada para a geração da Chave Pública.

[6] Pode também ser construído, como Chave Pública, um operador diferencial que efetua a própria translação no plano complexo.

Uma possível alternativa ao uso de funções contínuas como Chaves Públicas consiste no emprego de operadores diferenciais. Tradicionalmente, empregam-se letras maiúsculas para representar operadores. Nesse caso, o operador A - utilizado como Chave Pública -, e definido como

$$A = \left(a_1 \frac{\partial}{\partial x} + a_2 \frac{\partial}{\partial y} \right),$$

possui a seguinte propriedade: a exponencial desse operador, quando aplicada sobre uma função arbitrária, produz a seguinte transformação

$$\left[e^A \right] f(x, y) = f(x + a_1, y + a_2) .$$

Essa transformação corresponde a uma translação na reta real ou no plano complexo, dependendo da natureza dos coeficientes a_1 e a_2. No esquema proposto, os coeficientes a_1 e a_2 possuem partes real e imaginária caracterizando, portanto, uma operação de translação no plano complexo. A equação acima define, portanto, a origem das chaves privadas – ou seja, o processo de geração das chaves privadas a partir de uma chave pública. Uma vez que a exponenciação do operador A produz uma série infinita de potências desse operador, o processo correspondente à avaliação do membro esquerdo da equação acima é extremamente oneroso, ao passo que o mesmo efeito obtido através de translação direta – pelo emprego de números complexos, correspondente ao membro direito da mesma equação - constitui uma operação trivial.

A próxima seção descreve o processo de autenticação.

4.3 O processo de autenticação

No esquema proposto , o processo de autenticação é realizado através de uma prova de conhecimento zero. Basicamente, é construída uma função de duas variáveis, empregando-se as chaves públicas de cada participante, e a chave privada de participante verificador. Propõe-se um desafio e, verificada determinada condição, aceita-se ou não a outra parte como legítima.

Definição

Seja aa uma função contínua, formada por uma combinação linear das chaves públicas dos participantes. Infere-se que aa pertence ao mesmo espaço de funções que o espaço das chaves públicas. O argumento aa representa o argumento criado por Alice, o qual será transformado por Bob - a fim de posteriormente identificar Bob.

Seja ta uma função contínua. consiste no resultado da aplicação da função sobre a chave privada de Bob – a chave privada serve como argumento da função.

Seja va um número complexo, resultante da aplicação da função ta sobre a chave privada de Alice. Condição de aceitação da identidade de Bob por Alice consiste na obtenção de um zero da função ta. Caso a aplicação da chave privada de Alice gere um número complexo

não nulo, então pode-se afirmar que o participante não é Bob – impedindo que o protocolo prossiga.

Em outras palavras, o cálculo do chamado *argumento de autenticação* - ou *aa* - consiste em uma função contínua, formado por uma função, cujos argumentos correspondes às chaves públicas de ambos os participantes, somados com uma função cuja raiz é a sua própria chave privada. Por exemplo,

$$aa = g(C_{pub}A, C_{pub}B) + (y - C_{priv}A)^n$$

onde g representa qualquer função que assuma o valor nulo caso um de seus argumentos seja nulo.

Sobre essa função, o receptor deve aplicar sua chave privada, a fim de reduzi-la a uma expressão cuja validação final será efetuada pelo verificador. Assim, o receptor - Bob - retira o fator das chaves públicas, ao aplicar a sua chave privada

$$ta = aa(C_{priv}B) = g(C_{pub}A,0) + (y - C_{priv}A)^n = (y - C_{priv}A)^n$$

, resultará a expressão ta - que nada mais é senão uma função cuja raiz é a chave privada de Alice.

A nova função obtida é, então, utilizada por parte do emissor, para verificar a autenticidade do receptor, através de um simples teste de autenticidade: ao aplicar na função resultante a chave privada, deverá resultar no valor zero. Essa prova reconhece que o receptor realmente é quem afirma ser, por ter aplicado no argumento de autenticação a correta chave privada. Ou seja,

$$ta = 0.$$

Caso o número resulte nulo, a autenticidade do receptor é constatada; caso contrário, o esquema adultera a informação, não permitindo que a mensagem final seja conhecida. Dessa forma, apenas o receptor autorizado poderá, ao final do processo, recuperar a mensagem original.

A simplicidade dos processos de cifração, decifração e da autenticação, permite construir um algoritmo conciso, e de fácil implementação computacional – desde que empregado um software de processamento simbólico, como o *Derive*, *SimbMath*, *Mathematica* ou *Maple V*. As etapas do algoritmo proposto – que compõe o esquema Rafaella - são apresentadas a seguir.

4.4 Descrição esquemática do processo

A partir de uma mensagem dada, o processo de cifração consiste na aplicação dos seguintes passos básicos:

1. Converter a mensagem original para valores numéricos empregando a codificação desejada (ASC, por exemplo) e compondo os coeficientes da função correspondente à mensagem original - m_0 - de tal forma que a cada coeficiente da função corresponda um

caracter da mensagem original;

2.Escolha de uma função real e contínua, contendo um número de parcelas igual ao número de coeficientes numéricos resultantes – sendo que todas as parcelas devem ser distintas entre si – seguida da soma da Chave Pública do participante receptor da mensagem. Por simplicidade, no presente esquema são usados polinômios de grau "n". Ou seja,

$$g(x) = c_n.x^n + c_{(n-1)}.\ x^{(n-1)} + ... + c_{0.}$$

3.Produção de argumentos de autenticação, que contém o produto entre potências inteiras da Chaves Pública, por cada participante. Sendo C_{prA} a chave privada de um dos participantes, sua chave pública será $C_{pubA} = (x - C_{prA})^k$, sendo k um inteiro positivo não nulo qualquer – desejável que seja elevado.

4.Aplicação, por parte do emissor, de deslocamento da função mensagem no plano complexo, com componentes real e imaginária – essa operação corresponde à cifração da função original, vindo a compor a mensagem a ser remetida; assim sendo, tem-se

$g_1(x) = g(x + a),\ a\ \hat{I}\ V$, sendo V o conjunto dos números complexos .

5.Envio da mensagem cifrada para o receptor autorizado;

6.Aplicação, por parte do receptor, de um novo deslocamento – de modo similar ao aplicado no passo 4 -, com componentes real e imaginário e geração de um argumento auxiliar, que consiste em uma nova função contínua; ou seja,

$$g_2(x) = g_1(x + b),\ b\ \hat{I}\ V.$$

7.Envio da mensagem mapeada, e do argumento auxiliar, ao emissor;

8.Aplicação, por parte do emissor, da mudança inversa e verificação da autenticidade do argumento auxiliar do receptor através da geração de um novo argumento – denominado de argumento de verificação (o novo argumento é utilizado para deturpar a mensagem cifrada, caso não se constate a autenticidade do receptor); assim, para a operação de mudança inversa,

$$g_3(x) = g_2(x - a).$$

continuando o processo apenas se a verificação de autenticidade retornar nulo; ou seja, se

$$ta(C_{prA}) = 0,$$

então pode-se efetuar os passos restantes.

9.Envio, ao receptor, da mensagem mapeada e do argumento auxiliar gerado pelo emissor;

10.Aplicação da mudança inversa por parte do receptor, verificação da autenticidade do argumento auxiliar do emissor, e subtração da chave pública do receptor – essa operação corresponde à decifração da mensagem, através da qual a função original é recuperada;

$$g_4(x) = g_3(x - b) = g.$$

11.Recuperação dos caracteres originais - os quais são os coeficientes da função original.

Como referido anteriormente, a codificação prévia da mensagem consiste na determinação dos códigos ASC II de cada caracter envolvido, os quais constituirão os coeficientes da função f_0. Contudo, algumas restrições devem ser respeitadas, em relação à forma da função associada à mensagem original:

1 – não é permitido repetir parcelas na construção da função correspondente à mensagem;
2 – não é permitido incluir combinações lineares de funções já inseridas na construção da função correspondente à mensagem;
3 – é recomendável o emprego de coeficientes inteiros como fatores multiplicativos das funções empregadas; e
4 – não é permitida a utilização de termos independentes nos argumentos de funções exponenciais.

A função f(x) pode ser obtida através da combinação linear de funções de base, de composições entre funções, ou da aplicação de ambos os recursos. Como exemplo, a função

$$c_1 e^x + c_2 \operatorname{sen} x + c_3 x^2 + c_4 x^6 \tan x + e^{x^2}$$

- onde c1, c2, c3 e c4 são coeficientes numéricos, que representam os códigos ASC II da mensagem original -, contém composições e combinações lineares aplicadas alternadamente.

A aplicação de um deslocamento composto de partes real e imaginária consiste na seguinte mudança de variável

$$x \text{ ® } x + z,$$

onde z é da forma a + ib.

Essa mudança mapeia a função f(x) na função f(x + a + ib).

A aplicação da operação inversa consiste na mudança de variável que atua em sentido contrário, ou seja,

$$x \to x - a - ib\ ,$$

que mapeia f(x) em f(x - a - ib).

Salienta-se que as chaves privadas de cada participante do esquema são as componentes real e imaginária do deslocamento aplicado sobre a função f. Dessa forma, cada participante arbitra um número complexo, que é empregado unicamente para efetuar a cifração e a **decifração da função**.

Existem diversas formas de construir Chaves Públicas a partir de números complexos. Todas elas, contudo, resultam na obtenção de funções ou de operadores diferenciais. Entretanto, a escolha de uma chave na forma de um operador diferencial

fornece uma contra-informação ao adversário, induzindo-o a concluir que se trata de um operador presente na própria equação diferencial satisfeita por f_0 – o que, não necessariamente, é verdade. Formulações anteriores do método proposto vinham utilizando, como chaves públicas, as próprias equações diferenciais satisfeitas pela função f0. Nesse caso, a implementação de simetrias de Lie-Bäcklund[7] (Bluman, 1989) constituiria um fator de segurança extra a ser empregado, uma vez que tornariam inviáveis as tentativas de determinação dos geradores infinitesimais do grupo de simetria associado àquela equação diferencial. Essa formulação foi abandonada em favor do esquema proposto, pelo fato de não haver necessidade de relacionar o operador diferencial utilizado (como Chave Pública) e a equação diferencial satisfeita pela equação f_0. Em outras palavras, a omissão da equação diferencial como medida extra de segurança foi considerado mais eficaz do que sua utilização em conjunto com as simetrias de Lie-Bäcklund.

4.5 Análise de viabilidade do esquema – o trabalho do atacante

A presente seção aborda questões sobre o problema inverso, que consiste na operação de decifração por parte de um atacante. Essa operação, para um usuário não autorizado, exige a resolução de equações diferenciais, tarefa consideravelmente dispendiosa do ponto de vista computacional.

Existem, basicamente, dois fatores que justificam a viabilidade do método do ponto de vista da dificuldade de tratamento do problema inverso: o primeiro reside no elevado número de operações simbólicas necessárias para que um adversário possa restaurar a mensagem original a partir da mensagem cifrada. O segundo fator se refere às dificuldades encontradas na execução desse processo. Na ausência das chaves privadas, o adversário deve proceder da seguinte maneira, para decodificar a mensagem:

I) inferir a forma do operador diferencial presente na equação diferencial satisfeita por $f_0(x)$ - conforme Olver (Olver, 2000).

II) resolver a respectiva equação diferencial;

III) inferir e aplicar as condições iniciais de contorno – ou de passagem por pontos - , que estabelecem a unicidade da solução;

IV) recuperação da mensagem original, aplicando o comando ASC sobre os códigos ASCII da função obtida.

Destaca-se que os itens I e III constituem etapas limitantes no processo, uma vez que não existem procedimentos sistemáticos para obtenção da equação diferencial e das respectivas condições iniciais de contorno. Embora seja sabido que a estrutura da equação diferencial é dada por

$$\frac{\partial F}{\partial a} = \frac{\partial F}{\partial x},$$

pelo fato de sua solução ser obtida pelo emprego da regra de translação

[7] Simetrias de Lie-Bäcklund são aquelas cujos coeficientes dos geradores infinitesimais dependem não apenas das variáveis independentes, mas também da função incógnita e de suas derivadas.

$$Af = g.$$

Destaca-se que o coeficiente complexo a é desconhecido – uma vez que constitui a chave privada. A princípio, o atacante, ao realizar a procura direta de chaves privadas por meio de varredura do plano complexo – que, nos problemas pertinentes à Teoria dos Números eqüivaleria a processos de tentativa e erro – obtém um problema consideravelmente mais oneroso no âmbito do novo paradigma, uma vez que o conjunto pesquisado tem potência de contínuo - ao contrário, por exemplo, do conjunto dos primos, que é numerável.

Além disso, o item II, que envolve o emprego dos grupos de Lie, pode ser decomposto em quatro passos – cada um dos quais computacionalmente dispendioso:

A - encontrar o sistema correspondente de equações determinantes (Olver, 2000), empregadas na obtenção dos coeficientes variáveis presentes nos geradores infinitesimais dos grupos de simetria. Nessa etapa, são obtidas as equações diferenciais cuja resolução fornecem os grupos de Lie da equação original;

B - resolver o sistema obtido, empregando bibliotecas de mapeamento e resolução de equações diferenciais parciais;

C - encontrar uma solução particular da equação diferencial, para dar início ao processo de mapeamento;

D - mapear a solução particular, utilizando a exponencial de uma combinação linear dos geradores infinitesimais obtidos (Dattolli, 1998);

Foi constatado, a partir de testes de equações diferenciais de segunda ordem que a construção das equações determinantes - conforme a etapa A - requer, em média, cerca de 250 operações simbólicas, para equações bidimensionais parciais de segunda ordem com coeficientes variáveis. Isso ocorre porque se faz necessário calcular os prolongamentos[8] de segunda ordem dos geradores infinitesimais do grupo de simetria e, em seguida, aplicar o critério de variância infinitesimal (Olver, 2000). É importante salientar que o número de operações simbólicas requeridas para a obtenção das equações determinantes **cresce exponencialmente** com o aumento da ordem do prolongamento utilizado – que é a mesma ordem da equação diferencial a solucionar. Considerações sobre a complexidade são apresentadas no Capítulo 5.

O número de operações simbólicas exigidas para a resolução do sistema de equações determinantes varia, essencialmente, com o grau de acoplamento do sistema obtido. Em geral, o número de operações simbólicas necessárias para resolver um sistema de equações determinantes produzidas por equações bidimensionais parciais de segunda ordem com coeficientes variáveis é da ordem de 500 – considerando que o número médio de equações determinantes situe-se em torno de 10. Ocorre que o número de operações simbólicas cresce com o quadrado do número de equações que, por sua vez, cresce linearmente com a ordem da equação diferencial a solucionar.

[8] Por prolongamento, entende-se o domínio estendido composto pelas variáveis independentes, pelas funções incógnitas e por suas derivadas.

A obtenção de uma solução particular para a equação diferencial pode ser resultado de dois modos de trabalho: utilizando comandos que efetuam a resolução direta da equação em formas especiais, ou encontrando as equações determinantes para a forma especial estabelecida. No primeiro caso, a solução pode ser obtida imediatamente, em uma única linha de comando. Caso a resolução direta não seja possível, deve-se retornar ao passo I), e efetuar todas as etapas do roteiro estabelecido para a forma especial da equação diferencial.

O mapeamento da solução também pode ser obtido de três formas: através do emprego de regras de manipulação para exponenciais de operadores, através do uso de expansões desses operadores em séries de Taylor, ou da resolução de equações diferenciais auxiliares. Caso existam regras disponíveis para a manipulação das exponenciais dos geradores infinitesimais obtidos, o número de operações resultantes é bastante reduzido – sendo freqüentemente da ordem do número de geradores infinitesimais[9]. O número de operações exigidas para obtenção das expansões da série de Taylor depende unicamente do raio de convergência da série, sendo proporcional ao número de termos utilizados. Já a resolução de equações auxiliares – a exemplo do cálculo para encontrar as equações determinantes para a forma especial estabelecida -, também requer a execução do algoritmo por completo.

A aplicação das condições iniciais de contorno – ou de passagem por pontos -, consistem, basicamente, na determinação de funções arbitrárias contidas na solução mapeada, através da resolução de equações algébricas ou diferenciais de 1ª ordem – recaindo, portanto, no mesmo problema do passo anterior.

Os demais passos são essencialmente numéricos e não exigem o emprego de operações simbólicas – mas apenas um pequeno número de operações com ponto flutuante.

Embora o crescimento exponencial do número de operações simbólicas requeridas com o aumento da ordem da equação diferencial seja suficiente para justificar a viabilidade do método, existem dificuldades adicionais na execução do próprio processo supra apresentado – de tentativa de quebra da cifração por um adversário. Em primeiro lugar, a própria equação diferencial a solucionar não é fornecida como chave pública – de modo que se torna necessário inferir sua estrutura a partir de um processo de tentativa e erro. Além disso, as condições iniciais de contorno e passagem por pontos também não são fornecidas. Na hipótese extremamente improvável do adversário encontrar a solução geral da equação, torna-se necessário, ainda, escolher dentre as diversas famílias de superfícies que a representam, uma superfície que obedeça às **condições de contorno implicitamente aplicadas**. Isso implica a execução de um novo processo de tentativa e erro semelhante ao aplicado na determinação da forma da equação diferencial – portanto, extremamente oneroso. Ademais, não existe nenhum procedimento sistemático para orientar o processo de tentativa e erro em ambos os casos apresentados. Outrossim, a solução de problemas auxiliares que surgem durante a execução dos passos do algoritmo exigem, com freqüência, a reaplicação recursiva dos quatro passos do item II do algoritmo proposto. Esse procedimento efetuado em laço aumenta significativamente o número de operações simbólicas requeridas, uma vez que a cada aplicação recursiva desdobra exponencialmente esse número de operações.

[9] Ou seja, da dimensão do grupo de Lie correspondente.

4.6 Exemplo de aplicação

Na presente seção, é apresentado um exemplo de aplicação do esquema proposto, bem como dados sobre o desempenho computacional do mesmo.

Exemplo 1: Partindo-se da mensagem original “RAFAELLA”, produz-se os respectivos códigos ASCII dos caracteres componentes:

114 097 102 097 101 108 108 097

A função m0 será a função correspondente à mensagem original. Os coeficientes de seus termos correspondem aos códigos ASCII dos caracteres originais da mensagem. Os expoentes podem ser arbitrados.

$$m0 := 114\,\mathbf{e}^{(8.7564x)} + 97\,\mathbf{e}^{(3.456x)} + 102\,\mathbf{e}^{(2.45x)} + 97\,\mathbf{e}^{(.456x)} + 101\,\mathbf{e}^{(9.04x)} + 108\,\mathbf{e}^{(2.709x)} + 108\,\mathbf{e}^{(8.06x)} + 97\,\mathbf{e}^{(4.14x)}$$

$$ca := 27 - 9\,I$$

$$cpa := 14880348\,x^2 + 6429780\,x^3 - 459270\,x^4 - 189\,x^6 + 13608\,x^5 + 391849164\,I\,x^2 + 9527674248 + 11746971864\,I + x^7 + 63\,I\,x^6 - 22044960\,I\,x^3 + 663390\,I\,x^4 - 10206\,I\,x^5 - 3482001432\,I\,x - 1309470624\,x$$

O valor ca é a Chave PRIVADA de Alice, sendo cpa sua respectiva chave pública. Deve ser da forma ca = A + Bi, onde "i" é a unidade imaginária. A e B têm que ser números inteiros, diferentes de ZERO (não serão empregados números com ponto flutuante, em razão do erro de arredondamento envolvido nas operações de cifração e decifração)[10].

.

$$cb := 9 + 4\,I$$

O número complexo "cb" é a chave PRIVADA de Bob.

$$cpb := -20615140\,x^2 + 2579976\,x^3 - 67130\,x^4 + 1820\,x^6 - 16632\,x^5 - 72\,x^7 + 70269624\,x + x^8 + 655200\,I\,x^4 - 50848\,I\,x^5 - 86689919 - 17952480\,I + 2016\,I\,x^6 - 4502624\,I\,x^3 - 15273184\,I\,x + 15101856\,I\,x^2 - 32\,I\,x^7$$

A expressão cpb é a chave PÚBLICA de Bob. É obtida da seguinte maneira: define-se uma função para a qual UMA de suas raízes constitui a chave PRIVADA de Bob Essa função pode apresentar raízes reais e complexas - desde que, ao menos , uma delas corresponda à chave PRIVADA do usuário.

[10] No MAPLE, sempre o "i" é grafado em letra maiúscula. O efeito de aplicar-se um número complexo como deslocamento no argumento de uma função é equivalente a aplicar-se um determinado operador diferencial

$$f0 := 114\,e^{(8.7564\,x)} + 97\,e^{(3.456\,x)} + 102\,e^{(2.45\,x)} + 97\,e^{(.456\,x)} + 101\,e^{(9.04\,x)} + 108\,e^{(2.709\,x)}$$
$$+ 108\,e^{(8.06\,x)} + 97\,e^{(4.14\,x)} - 20615140\,x^2 + 2579976\,x^3 - 67130\,x^4 + 1820\,x^6$$
$$- 16632\,x^5 - 72\,x^7 + 70269624\,x + x^8 + 655200\,I\,x^4 - 50848\,I\,x^5$$
$$- 86689919 - 17952480\,I + 2016\,I\,x^6 - 4502624\,I\,x^3 - 15273184\,I\,x + 15101856\,I\,x^2$$
$$- 32\,I\,x^7$$

A função f0 é uma função construída por Alice, a partir da função correspondente à mensagem original, e da chave pública de Bob. Destaca-se que f0 deve ficar mantida com Alice.

$$f1 := -.5227106382\,10^{105}\,e^{(8.7564\,x)} + .3091566704\,10^{43}\,e^{(3.456\,x)}$$
$$- .5450390611\,10^{31}\,e^{(2.45\,x)} - .1232698233\,10^{8}\,e^{(.456\,x)} + .3082617877\,10^{51}\,e^{(4.14\,x)}$$
$$+ .4598813352\,10^{34}\,e^{(2.709\,x)} - .3364449005\,10^{97}\,e^{(8.06\,x)} + .9640269817\,10^{108}\,e^{(9.04\,x)}$$
$$- 2747423980\,x^2 - 302177232\,x^3 - 13649930\,x^4 + 4340\,x^6 - 184464\,x^5 + 144\,x^7$$
$$- 6977307312\,x + x^8 + .9797457705\,10^{96}\,I\,e^{(8.06\,x)} + .1434179443\,10^{105}\,I\,e^{(8.7564\,x)}$$
$$+ .9968850719\,10^{42}\,I\,e^{(3.456\,x)} + .3211340874\,10^{30}\,I\,e^{(2.45\,x)}$$
$$+ .1769786809\,10^{8}\,I\,e^{(.456\,x)} - 104\,I\,x^7 + .1447893216\,10^{51}\,I\,e^{(4.14\,x)}$$
$$+ .3209765087\,10^{108}\,I\,e^{(9.04\,x)} + .4299219701\,10^{34}\,I\,e^{(2.709\,x)}$$
$$+ 16976403601 + 56580909840\,I - 13104\,I\,x^6 - 584584\,I\,x^5 - 10155600\,I\,x^4$$
$$+ 20107904648\,I\,x - 4281368\,I\,x^3 + 1925619696\,I\,x^2$$

A partir de f0, Alice produz a FUNÇÃO cifrada f1, deslocando f0 de SUA (de ALICE) chave privada .

$$aa := 94\,I\,x^{21} + 5212321104520591305048\,x^9 + 2384872084262537931355949376 0\,I\,x$$
$$+ 5197540704161170646003635584\,I\,x^3 - 1414125746594424629707034419 2\,I\,x^2$$
$$- 3903651147474985781444774 4\,I\,x^6 - 8984742768898344\,I\,x^{14}$$
$$+ 233847538098440\,I\,x^{15} + 77270676700\,I\,x^{17} + 4735766673643490304231744\,I\,x^7$$
$$- 1338797174595017731917178464\,I\,x^4 + 2585491254695757131734328 64\,I\,x^5$$
$$+ 150235687251251633304\,I\,x^{11} + 279338945316881310\,I\,x^{13}$$
$$- 2637056457709318951488\,I\,x^{10} - 7121497964463430002\,I\,x^{12}$$
$$+ 385903277956407765662 64\,I\,x^9 - 4700058056368317640862 64\,I\,x^8$$
$$- 4833815568372\,I\,x^{16} - 11395944\,x^{19} + 92036\,x^{20} + 957677266\,x^{18}$$
$$- 57883279356\,x^{17} + 2592086395724\,x^{16} - 86741664973488\,x^{15}$$
$$- 2536184231825035133 16\,x^{10} - 450\,x^{21} + x^{22}$$
$$+ 8111575273225687367111520768 - 1855727832009380947836181977 6\,I$$

$$+ 5915647537630340328\,x^{11} + 247267129974509736\,x^{12} - 35283092367942090\,x^{13}$$
$$+ 208465300430229843194859705 6\,x^{2} - 918218952\,I\,x^{18}$$
$$- 232975282185266349624803712\,x^{3} - 480092826550401355214004 48\,x^{4}$$
$$+ 7612976\,I\,x^{19} + 2129640864123913\,x^{14} - 530614401242495257905940 8\,x^{6}$$
$$- 39186\,I\,x^{20} + 248231188847243989542012 48\,x^{5}$$
$$+ 736874504494613653497408\,x^{7} - 65710638981032218151693356 80\,x$$
$$- 72920563092134325870048\,x^{8}$$

A função "aa" é a função de AUTENTICAÇÃO DE ALICE. Pode ser o produto de uma potência da chave pública da Alice por uma potência da Chave Pública de Bob. A função aa deve ser enviada a Bob, juntamente com f1.

$$f2 := .9797457705\,10^{96}\,I\,\mathbf{e}^{(8.06\,x + 72.54 + 32.24\,I)}$$
$$+ .1434179443\,10^{105}\,I\,\mathbf{e}^{(8.7564\,x + 78.8076 + 35.0256\,I)}$$
$$+ .9968850719\,10^{42}\,I\,\mathbf{e}^{(3.456\,x + 31.104 + 13.824\,I)} + .3211340874\,10^{30}\,I\,\mathbf{e}^{(2.45\,x + 22.05 + 9.80\,I)}$$
$$+ .1769786809\,10^{8}\,I\,\mathbf{e}^{(.456\,x + 4.104 + 1.824\,I)} - 104\,I\,(x + 9 + 4\,I)^{7}$$
$$+ .1447893216\,10^{51}\,I\,\mathbf{e}^{(4.14\,x + 37.26 + 16.56\,I)} + .3209765087\,10^{108}\,I\,\mathbf{e}^{(9.04\,x + 81.36 + 36.16\,I)}$$
$$+ .4299219701\,10^{34}\,I\,\mathbf{e}^{(2.709\,x + 24.381 + 10.836\,I)} - 13104\,I\,(x + 9 + 4\,I)^{6}$$
$$- 584584\,I\,(x + 9 + 4\,I)^{5} - 10155600\,I\,(x + 9 + 4\,I)^{4} + 20107904648\,I\,(x + 9 + 4\,I)$$
$$- 4281368\,I\,(x + 9 + 4\,I)^{3} + 1925619696\,I\,(x + 9 + 4\,I)^{2}$$
$$- 45819362207 + 28671680592\,I - .5227106382\,10^{105}\,\mathbf{e}^{(8.7564\,x + 78.8076 + 35.0256\,I)}$$
$$+ .3091566704\,10^{43}\,\mathbf{e}^{(3.456\,x + 31.104 + 13.824\,I)} - .5450390611\,10^{31}\,\mathbf{e}^{(2.45\,x + 22.05 + 9.80\,I)}$$
$$- .1232698233\,10^{8}\,\mathbf{e}^{(.456\,x + 4.104 + 1.824\,I)} + .3082617877\,10^{51}\,\mathbf{e}^{(4.14\,x + 37.26 + 16.56\,I)}$$
$$+ .4598813352\,10^{34}\,\mathbf{e}^{(2.709\,x + 24.381 + 10.836\,I)} - .3364449005\,10^{97}\,\mathbf{e}^{(8.06\,x + 72.54 + 32.24\,I)}$$
$$+ .9640269817\,10^{108}\,\mathbf{e}^{(9.04\,x + 81.36 + 36.16\,I)} - 2747423980\,(x + 9 + 4\,I)^{2}$$
$$- 302177232\,(x + 9 + 4\,I)^{3} - 13649930\,(x + 9 + 4\,I)^{4} + 4340\,(x + 9 + 4\,I)^{6}$$
$$- 184464\,(x + 9 + 4\,I)^{5} + 144\,(x + 9 + 4\,I)^{7} + (x + 9 + 4\,I)^{8} - 6977307312\,x$$

Bob recebe f1, aplica um deslocamento de sua própria chave PRIVADA, gerando a f2.

$$tb := y^{5} - 135\,y^{4} + 45\,I\,y^{4} + 6480\,y^{3} - 4860\,I\,y^{3} - 131220\,y^{2} + 189540\,I\,y^{2} + 918540\,y$$
$$- 3149280\,I\,y + 708588 + 18659484\,I$$

Argumento auxiliar, gerado por Bob, com o objetivo de autenticar a mensagem. A função gb é resultado de aplicação da chave privada de Bob em uma expressão envolvendo o argumento aa, somado com uma potência da função aa. Pode-se afirmar que tb = aa(Cb), devendo retornar uma expressão em y.

$$ab := 94\,I\,x^{21} + 5212321104520591305048\,x^{9} + 2384872084262537931355949376 0\,I\,x$$
$$+ 519754070416117064600363558 4\,I\,x^{3} - 1414125746594424629707034419 2\,I\,x^{2}$$
$$- 3903651147474985781444774 4\,I\,x^{6} - 8984742768898344\,I\,x^{14}$$
$$+ 233847538098440\,I\,x^{15} + 77270676700\,I\,x^{17} + 4735766673643490304231744\,I\,x^{7}$$
$$- 1338797174595017731917178464\,I\,x^{4} + 2585491254695757131734328 64\,I\,x^{5}$$
$$+ 150235687251251633304\,I\,x^{11} + 279338945316881310\,I\,x^{13}$$
$$- 2637056457709318951488\,I\,x^{10} - 7121497964463430002\,I\,x^{12}$$
$$+ 38590327795640776566264\,I\,x^{9} - 4700058056368317640862 64\,I\,x^{8}$$
$$- 4833815568372\,I\,x^{16} - 11395944\,x^{19} + 92036\,x^{20} + 957677266\,x^{18}$$
$$- 57883279356\,x^{17} + 2592086395724\,x^{16} - 86741664973488\,x^{15}$$
$$- 2536184231825035133 16\,x^{10} - 450\,x^{21} + x^{22}$$
$$+ 81115752732256873671115207 68 - 1855727832009380947836181977 6\,I$$
$$+ 5915647537630340328\,x^{11} + 247267129974509736\,x^{12} - 35283092367942090\,x^{13}$$
$$+ 20846530043022984319485970 56\,x^{2} - 918218952\,I\,x^{18}$$
$$- 2329752821852663496248037 12\,x^{3} - 4800928265504013552140044 8\,x^{4}$$
$$+ 7612976\,I\,x^{19} + 2129640864123913\,x^{14} - 5306144012424952579059408\,x^{6}$$
$$- 39186\,I\,x^{20} + 2482311888472439895420124 8\,x^{5}$$
$$+ 7368745044946136534974 08\,x^{7} - 6571063898103221815169335680\,x$$
$$- 7292056309213432587004 8\,x^{8}$$

A função "ab" é a função de autenticação de Bob. De modo similar ao passo onde se definiu "aa", pode ser o produto das potências de cada chave pública dos participantes. Bob deve remeter ab para Alice, juntamente com f2 e gb.

$$vb := 0$$

vb é a operação de verificação da autenticidade de Bob, por Alice. Se for igual a ZERO, confirma-se a autenticidade do receptor da mensagem. Por essa prova de conhecimento zero - $tb(C_{privA}) = 0$ -, Alice pode certificar-se que está contatando com Bob.

$$ta := 276426\,y - 736255 + 539352\,I - 14385\,y^{2} - 5940\,y^{3} + 975\,y^{4} - 54\,y^{5} + 1080\,I\,y^{4} + y^{6}$$
$$- 18160\,I\,y^{3} + 140400\,I\,y^{2} - 482424\,I\,y - 24\,I\,y^{5}$$

Argumento auxiliar, gerado por Alice, com o objetivo de verificar a autenticidade da mensagem. Se o argumento for realmente emitido por Bob, resultará NULO ($ta(C_{privB})=0$).

$$f3 := .9797457705\,10^{96}\,I\,e^{(8.06x - 145.08 + 104.78I)} + .1434179443\,10^{105}\,I\,e^{(8.7564x - 157.6152 + 113.8332I)} + .9968850719\,10^{42}\,I\,e^{(3.456x - 62.208 + 44.928I)} + .3211340874\,10^{30}\,I\,e^{(2.45x - 44.10 + 31.85I)} + .1769786809\,10^{8}\,I\,e^{(.456x - 8.208 + 5.928I)} - 104\,I\,(x - 18 + 13\,I)^7 + .1447893216\,10^{51}\,I\,e^{(4.14x - 74.52 + 53.82I)} + .3209765087\,10^{108}\,I\,e^{(9.04x - 162.72 + 117.52I)} + .4299219701\,10^{34}\,I\,e^{(2.709x - 48.762 + 35.217I)} - 13104\,I\,(x - 18 + 13\,I)^6 - 584584\,I\,(x - 18 + 13\,I)^5 - 10155600\,I\,(x - 18 + 13\,I)^4 + 20107904648\,I\,(x - 18 + 13\,I) - 4281368\,I\,(x - 18 + 13\,I)^3 + 1925619696\,I\,(x - 18 + 13\,I)^2 - .3364449005\,10^{97}\,e^{(8.06x - 145.08 + 104.78I)} - .5227106382\,10^{105}\,e^{(8.7564x - 157.6152 + 113.8332I)} + .3091566704\,10^{43}\,e^{(3.456x - 62.208 + 44.928I)} - .5450390611\,10^{31}\,e^{(2.45x - 44.10 + 31.85I)} - .1232698233\,10^{8}\,e^{(.456x - 8.208 + 5.928I)} + .3082617877\,10^{51}\,e^{(4.14x - 74.52 + 53.82I)} + .9640269817\,10^{108}\,e^{(9.04x - 162.72 + 117.52I)} + .4598813352\,10^{34}\,e^{(2.709x - 48.762 + 35.217I)} - 2747423980\,(x - 18 + 13\,I)^2 - 302177232\,(x - 18 + 13\,I)^3 - 13649930\,(x - 18 + 13\,I)^4 + 4340\,(x - 18 + 13\,I)^6 - 184464\,(x - 18 + 13\,I)^5 + 144\,(x - 18 + 13\,I)^7 + (x - 18 + 13\,I)^8 + 142567935217 - 34124085216\,I - 6977307312\,x$$

Alice desloca f2 do simétrico de sua chave privada, gerando f3. A função f3 é a função de onde Alice retira o seu deslocamento. Alice envia f3 para Bob.

$$va := 0$$

vb é a operação de verificação da autenticidade de Alice, por Bob. Se for igual a ZERO, confirma-se a autenticidade do receptor da mensagem. Assim, caso ($ta(C_{privB})=0$), Bob confirma que está tratando com Alice.

$$f4 := 114.0000000\,e^{(8.7564x)} + 97.00000000\,e^{(3.456x)} + 102.0000000\,e^{(2.45x)} + 97.00000001\,e^{(.456x)} + 97.00000000\,e^{(4.14x)} + 108.0000000\,e^{(2.709x)} + 108.0000000\,e^{(8.06x)} + 101.0000000\,e^{(9.04x)}$$

Finalmente, Bob desloca f3 do simétrico de sua própria chave privada, e subtrai sua própria chave pública, restaurando a função (mensagem) original.

Caso o adversário não disponha das respectivas chaves privadas, a restauração da mensagem torna-se um processo de tentativa e erro computacionalmente inviável, pois deverá tentar encontrar diretamente os componentes real e imaginário dessa chave privada; para tanto, deverá obrigatoriamente recorrer a um processo de varredura no plano complexo sem conhecer, a *priori*, os próprios limites da região de busca correspondente. Esse forma de proceder constitui um processo de força bruta.

É importante recordar que, nos métodos baseados em grupos de Galois, a varredura se limitaria a um subconjunto finito dos números inteiros constituído pelos números primos – que é um conjunto numerável. Já o conjunto dos números complexos tem potência de contínuo, de modo que o processo de varredura cobriria uma região do plano complexo que possui uma infinidade de elementos, para cada subintervalo de varredura. Dessa forma, os participantes podem escolher suas chaves privadas de maneira independente, escolhendo dois inteiros longos quaisquer para representar as partes real e imaginária do número complexo que compõe essas chaves, a fim de garantir privacidade do esquema proposto. Tal procedimento constitui, ao mesmo tempo, um elemento de segurança, e uma vantagem considerável do ponto de vista operacional.

Finalmente, com respeito ao desempenho, percebe-se que uma mensagem relativamente simples produz um volume de dados consideravelmente elevado, que constitui um aspecto negativo do esquema proposto.

A fim de amenizar esse problema, é recomendável que a mensagem seja enviada em blocos, afim de reduzir o volume de informação transmitida a cada etapa do processo. Caso o usuário julgue necessário podem ser utilizadas combinações lineares entre diferentes funções em cada bloco.

5 RESULTADOS OBTIDOS

O presente capítulo apresenta os resultados obtidos e a descrição de possíveis estratégias de quebra do esquema. Ressalta-se que o paradigma na qual o esquema aqui apresentado se baseia permite novas implementações, sendo o esquema Rafaella apenas uma sugestão. Assim, também são apresentadas sugestões para trabalhos futuros, bem como breve estudo sobre a sua complexidade computacional.

5.1 Considerações Gerais

O emprego de translações no plano complexo apresenta duas vantagens fundamentais sobre os algoritmos baseados na formulação direta de equações diferenciais: a primeira reside na simplicidade das expressões obtidas; a segunda e principal vantagem consiste na dificuldade de resolução do problema inverso associado - isto é, o processo de decifração. Caso o adversário não disponha das respectivas chaves privadas, a restauração da mensagem torna-se um processo de tentativa e erro computacionalmente inviável, **mesmo quando utilizados os grupos de Lie na resolução das equações diferenciais produzidas**. É importante ressaltar que o adversário não conhece o problema de contorno satisfeito pela função que constitui a mensagem original – o que torna a resolução do problema do atacante ainda mais onerosa. Observa-se que o problema de contorno é constituído pela equação diferencial e por suas respectivas condições iniciais e de contorno.

O tempo médio de processamento[11] requerido em 40 execuções foi de dois minutos, e a quantidade de memória secundária requerida para o armazenamento da mensagem cifrada foi aproximadamente 25 % superior à do arquivo original. Em todas as simulações efetuadas, não houve, até o presente momento, quebra do código via algoritmos baseados em álgebra de Lie. As tentativas de decifração consistem no emprego de bibliotecas (*liesymm*, *pdetools* e *detools*) do sistema Maple V, que têm por objetivo calcular os coeficientes dos geradores infinitesimais do grupo de simetria de equações diferenciais obtidas a partir das funções transladadas e do vetor de codificação.

[11] Os experimentos foram conduzidos em uma máquina Pentium MMX 233 MHz, com 128 MB de memória RAM.

As principais dificuldades encontradas no processo de decifração recaem na ausência de condições de contorno para iniciar o processo, bem como da necessidade de recorrer a processos recursivos envolvendo a síntese de equações determinantes (Olver, 2000), e à resolução das mesmas através do uso de simetrias disponíveis. O apêndice B apresenta um exemplo no qual o processo de decifração conduz a um esquema recursivo, a partir do qual são produzidas diversas equações diferenciais auxiliares a serem resolvidas. O processo foi encerrado devido à necessidade de efetuar novas etapas de recursão. Essa característica exemplifica claramente o crescimento exponencial do número de operações simbólicas requeridas por cada aplicação recursiva.

5.2 Possíveis tentativas de obtenção das chaves privadas

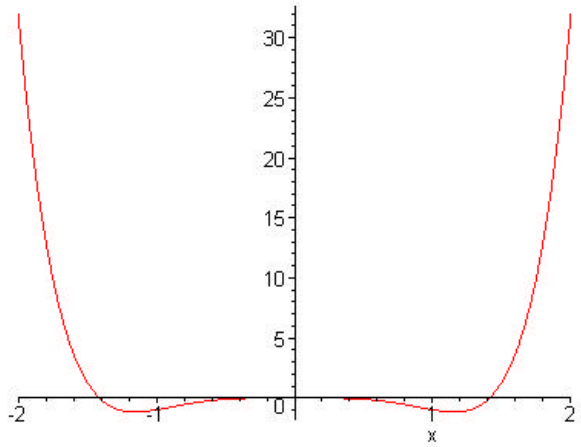
Alguns possíveis ataques podem ser inferidos, dentre os quais podem ser salientados os seguintes:

a - ataque das chaves: por intermédio da chaves pública de algum participante do esquema, poder-se-ia tentar obter-se a chave privada, visto ser essa apenas uma raiz complexa. Tal ataque, não é possível, visto que não há algoritmo para determinar raízes de equações cujo grau seja maior do que quatro - fato demonstrado por Galois no século XIX.

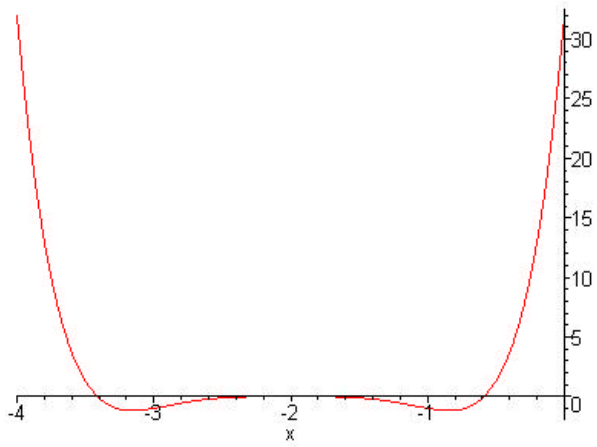
A tentativa mais próxima seria a determinação através de algum método de obtenção de raízes - sendo o mais promissor o método numérico chamado Newton-Bairstow, o qual guarda similaridade com o método Briot-Rufinni, mas aplicável para raízes complexas.

Ainda assim, para que esse método possa ser empregado, é necessário ter-se, no mínimo, uma raiz para iniciar o processo - o que é uma situação desconsiderada, em modelos de chave pública, a posse de uma chave privada.

b - tentativa de determinação da chave privada pela análise do deslocamento efetuado: tal método pode ser empregado em situações que envolvam deslocamentos puramente reais. O efeito do deslocamento pode ser verificado pelo conjunto de figuras abaixo apresentadas.



Comportamento da curva $f(x) = x^6-2x^4$ antes do deslocamento



Comportamento da curva após o deslocamento f(x) := f(x+a)

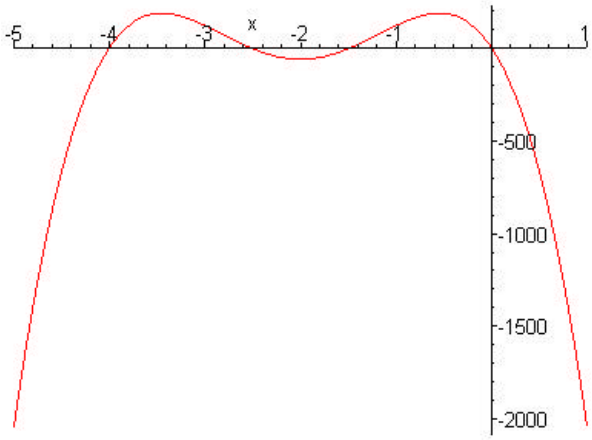
Figura 5. 1: Comportamento de curvas, antes e após aplicação de deslocamento real.

Observa-se que o deslocamento realizou apenas uma alteração na fase da função. O eixo de simetria, anteriormente coincidindo com a origem, passa a ser centrado no eixo x = -2.

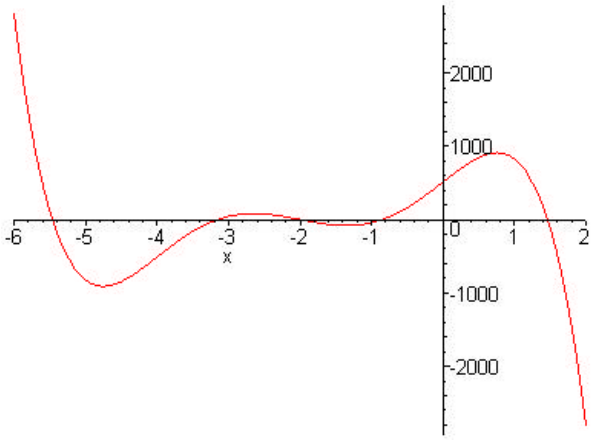
Não se observa alteração no formato da curva, ou mesmo na disposição das raízes, em relação ao eixo de simetria.

Contudo, tal efeito não se verifica ao se empregar variável complexa. A função passa a ser tratada como duas: uma, que contém a parte real e a outra, a parte imaginária.

Ao se observar o formato da curva no plano complexo, pode-se observar o comportamento completamente irregular, como no exemplo do conjunto das figuras a seguir, onde foi realizado um deslocamento sobre a mesma curva inicial acima apresentada:



Comportamento da componente real da curva $f(x) = x^6-2x^4$ após o deslocamento f(x) := f(x+2-2i)



Comportamento da componente imaginária da curva $f(x) = x^6-2x^4$ após o deslocamento f(x) := f(x+2-2i)

Figura 5. 2: Comportamento das curvas após empregado deslocamento de número complexo

Observa-se, na curva representativa da componente real da mesma curva apenas uma simples reflexão sobre o eixo x. Contudo, o comportamento da curva resultante da componente imaginária apresenta um aspecto diverso da original, ou mesmo das outras curvas resultantes do deslocamento.

c – obtenção de v através da resolução de equações determinantes: tendo-se f1 e f2, pode-se tentar determinar uma equação diferencial para o qual ambas as funções são soluções – e, posteriormente, tentar obter f0. Tal procedimento é inviável, visto que incorrerá na obtenção de equação diferencial de ordem infinita. Ordem infinita, pois resulta da aplicação da exponencial de um operador de 1ª ordem sobre uma das funções.

d – obtenção do gerador infinitesimal através da aplicação do logaritmo natural sobre a respectiva exponencial: parte-se do princípio que o atacante conhece a regra empregada pelo esquema Rafaella. Assim, seria natural que o mesmo tentasse obter a informação empregando o logaritmo natural. Esse procedimento não é cabível, visto que não existem regras para aplicação de logaritmos sobre operadores, mas apenas para números ou funções.

Ainda que fosse utilizada série de Taylor relativa ao logaritmo natural, a fim de produzir tais regras, o procedimento esbarraria em dificuldade prática proibitiva: o raio de convergência da série de Taylor para a função ln(x) é extremamente pequeno – o que inviabiliza qualquer tentativa de aplicação da regra para o caso de operadores.

e – ataque da regra da cadeia: consiste em calcular derivadas da função f1 a fim de sintetizar equações diferenciais para os quais a própria função seja a solução. Em seguida, utilizando a regra da cadeia, o atacante sintetiza uma nova equação diferencial que deva ser satisfeita por f2. O atacante procura, então, uma mudança de variável que converta a primeira equação diferencial na segunda, na tentativa de encontrar simetrias de Lie relativas à transformação de f1 em f2. Esse processo também não é viável, visto que é preciso encontrar uma mudança de variável específica que torne ambas as equações invariantes.

5.3 Complexidade do esquema Rafaella

O estudo da complexidade do problema inverso - tratado por complexidade de algoritmos, por alguns autores - demanda certas considerações, por se tratar de problema diferente dos tradicionais problemas da área da Teoria dos Números.

As abordagens mais comuns enfocam no esforço computacional despendido, na tentativa de solucionar o problema. Esse construto torna o estudo de complexidade realizável, visto que a medida de esforço propriamente dito normalmente não é mensurável - mas tão somente alguns de seus fatores de influência, como o número de operações, laços, repetições, etc.

Para que o atacante obtenha a mensagem original a partir da função transladada no plano complexo, dois caminhos podem ser tomados: um, a varredura do plano complexo – o que eqüivale a um ataque de força bruta - e outro, obtenção da solução formal da equação diferencial correspondente.

Considerando-se que o problema inverso correspondente ao esquema proposto baseia-se na resolução de equações diferenciais, então a complexidade do problema inverso é a complexidade da resolução de equações diferenciais. A análise de complexidade referente a obtenção de soluções exatas e aproximadas para equações diferenciais é discutido em Werschulz (Werschulz, 1991), que apresenta um levantamento bibliográfico, considerando-se o número de operações envolvidas nos métodos clássicos – diferenças finitas, métodos variacionais e soluções numéricas em geral. Uma vez que se torna necessário obter a solução exata da equação a fim de restaurar a mensagem original – sem que haja perda de informação -, o emprego de métodos numéricos não constitui uma estratégia apropriada de ataque – ou seja, a tentativa de decifração por parte de um adversário. Desse modo, somente a complexidade de métodos analíticos pode ser considerada na análise.

Dentre os métodos analíticos desenvolvidos para resolução de equações diferenciais ordinárias e parciais, o algoritmo mais eficiente consiste no emprego de simetrias de Lie (Zwillinger, 1992).

A fim de obter soluções analíticas para equações diferenciais, são aplicadas exponenciais de operadores diferenciais sobre a função que descreve o estado inicial do esquema, ou que prescreve o comportamento da função em alguma interface específica. A solução formal de uma equação diferencial genérica

$$\frac{\partial F}{\partial t} = AF \qquad (1)$$

é dada por

$$F = \left[e^{tA} \right] f \quad (2)$$

onde ϕ - phi(x) - representa o estado inicial do sistema. Nessa equação, A representa um operador diferencial ou uma matriz contendo operadores diferenciais. Para o segundo caso, encontra-se um interessante estudo de complexidade desenvolvido por Celledoni (Celledoni, 2002).

No esquema Rafaella, a complexidade associada ao processo de resolução de equação diferencial é avaliada estimando-se o número de operações simbólicas necessárias para avaliar a exponencial presente na equação (2). Expandindo-se a exponencial em série de Taylor, e truncando no termo de ordem k, obtém-se

$$e^{tA} = I + tA + \frac{t^2 A^2}{2!} + \ldots + \frac{t^k A^k}{k!} \quad (3).$$

Essa aproximação, que contém, k + 1 termos, deve produzir um erro equivalente à precisão de máquina – caso contrário, a mensagem original não poderá ser integralmente restaurada.

Resta, portanto, avaliar o número de operações envolvidas no cálculo de sucessivas potências do operador A. Para o esquema proposto, o operador A assume a forma

$$A = a_1 \frac{\partial}{\partial x} + a_2 \frac{\partial}{\partial y} + a_3 \frac{\partial}{\partial z} + \ldots \quad (4).$$

Suas sucessivas potências são obtidas através do emprego do binômio de Newton.

A fim de estimar o número de operações simbólicas envolvidas no cálculo do exponencial do operador A, presente na equação diferencial, é preciso calcular o número de operações requeridas para a obtenção de uma potência genérica do operador – A^k - , que representa a complexidade associada à obtenção de uma parcela da serie de Taylor, e então somar as contribuições correspondentes a cada uma das parcelas até a ordem de truncamento considerada.

Para calcular o parâmetro pk, basta avaliar o número de termos do multinômio de Newton correspondente. Uma vez que A possui n termos e a série é truncada no termo de ordem k, são necessárias n^k operações simbólicas para avaliar uma potência genérica do operador A – que corresponde a uma parcela da série. Para o cálculo de todas as parcelas, o número de operações simbólicas correspondentes é dada por

$$m = \sum_{\nu=0}^{k} n^{\nu} \quad (5).$$

Assim, m representa o número total de derivadas a serem aplicadas sobre a função ϕ. Resta, portanto, estimar o número de operações simbólicas necessárias para calcular as derivadas ordem inteira de uma função arbitrária ϕ.

5.3.1 Número de operações requeridas para a derivação de funções arbitrárias

Seja uma f função genérica composta e g(x), seu argumento. Tomando a derivada primeira dessa função, obtém-se

$$\frac{dF}{dx} = \frac{dg}{dx}\frac{dF}{dg} \qquad (6),$$

resultado obtido através do emprego da regra da cadeia. Derivando a equação (6) resulta

$$\frac{d^2F}{dx^2} = \frac{d^2g}{dx^2}\frac{dF}{dg} + \left(\frac{dg}{dx}\right)^2 \frac{d^2F}{dg^2} \qquad (7).$$

A última equação é obtida através do emprego das regras do produto e da cadeia. Derivando esse resultado, obtém-se

$$\frac{d^3F}{dx^3} = \frac{d^3g}{dx^3}\frac{dF}{dg} + \frac{d^2g}{dx^2}\frac{dg}{dx}\frac{d^2F}{dg^2} + 2\frac{dg}{dx}\frac{d^2g}{dx^2}\frac{d^2F}{dg^2} + \left(\frac{dg}{dx}\right)^3 \frac{d^3F}{dg^3} \qquad (8).$$

É importante observar que a aplicação da regra do produto induz à produção do dobro do número de termos da derivada de ordem imediatamente inferior.

A derivada de ordem m – que representa a maior derivada presente na série de Taylor definida pela equação 3 - contém, portanto, $2^{(m-1)}$ parcelas – sendo m definido pela equação (5).

A complexidade otimista resulta, portanto, em

$$\Omega = \mathrm{O}\left(2^{\sum_{v=0}^{k} n^v - 1}\right) = \mathrm{O}\left(2^{\frac{n^{2v}-1}{2}}\right) \qquad (9).$$

Ou seja, a complexidade é da ordem **exponencial**.

É importante observar que não foram consideradas os possíveis produtos surgidos através da derivação da própria função g. Ademais, a própria função phi(x) - que representa o estado inicial do sistema – é desconhecida, uma vez que a condição inicial não é publicada. Finalmente, a possibilidade de auto-simplificação por parte do sistemas de processamento algébrico não deve ser incluída na análise, visto que esses sistemas não efetuam automaticamente a simplificação das expressões derivadas. Caso o próprio usuário venha a eventualmente a fazer uso de rotinas de simplificação ao longo do processo, a

complexidade total resultante torna-se consideravelmente superior. Isso ocorre porque essas rotinas envolvem, em geral, o emprego de algoritmos cujo número de operações simbólicas varia com o quadrado do número de termos envolvidos na expressão simplificada.

É relevante salientar que, para a forma mais geral das chaves públicas – equações diferenciais ou funções de variável complexa – não existem procedimentos sistemáticos para efetuar o caminho inverso, ou seja, a determinação da chave privada. Isso ocorre porque no caso em que a chave pública é uma equação diferencial, a ausência das respectivas condições de contorno inviabiliza qualquer processo de resolução – seja por via numérica ou analítica; no caso em que a chave pública é uma função de variável complexa, o ataque poderia ser efetuado através de duas estratégias básicas:

1. Inversão da função
2. Cálculo de raízes

Uma vez que podem ser escolhidas como chaves públicas funções multivaloradas no plano complexo, não existe a possibilidade de inversão da função – a não ser por ramos. Nesse caso, o atacante deveria escolher um ramo da função a fim de obter um possível valor para a função inversa.

Para o cálculo de raízes, o emprego de funções oscilantes de alta freqüência torna o ataque inviável, uma vez que o elevado número de raízes mascara a chave privada.

O capítulo seguinte apresenta as conclusões do presente trabalho, assim como alternativas sugeridas para trabalhos futuros.

6 CONCLUSÕES E TRABALHOS FUTUROS

O presente capítulo apresenta as conclusões e a propostas de possíveis melhorias. Ressalta-se que o paradigma na qual o esquema aqui apresentado se baseia permite novas implementações, sendo o esquema Rafaella apenas uma sugestão. Assim, também são apresentadas sugestões para trabalhos futuros, bem como breve estudo sobre a sua complexidade computacional.

6.1 Considerações Gerais

O emprego de translações no plano complexo apresenta duas vantagens fundamentais sobre os algoritmos baseados na formulação direta de equações diferenciais: a primeira reside na simplicidade das expressões obtidas; a segunda e principal vantagem consiste na dificuldade de resolução do problema inverso associado - isto é, o processo de decifração. Caso o adversário não disponha das respectivas chaves privadas, a restauração da mensagem torna-se um processo de tentativa e erro computacionalmente inviável, **mesmo quando utilizados os grupos de Lie na resolução das equações diferenciais produzidas**. É importante ressaltar que o adversário não conhece o problema de contorno satisfeito pela função que constitui a mensagem original – o que torna a resolução do problema do atacante ainda mais onerosa. Observa-se que o problema de contorno é constituído pela equação diferencial e por suas respectivas condições iniciais e de contorno.

O tempo médio de processamento[12] requerido em 40 execuções foi de dois minutos, e a quantidade de memória secundária requerida para o armazenamento da mensagem cifrada foi aproximadamente 25 % superior à do arquivo original. Em todas as simulações efetuadas, não houve, até o presente momento, quebra do código via algoritmos baseados em álgebra de Lie. As tentativas de decifração consistem no emprego de bibliotecas (*liesymm*, *pdetools* e *detools*) do sistema Maple V, que têm por objetivo calcular os coeficientes dos geradores infinitesimais do grupo de simetria de equações diferenciais obtidas a partir das funções transladadas e do vetor de codificação.

[12] Os experimentos foram conduzidos em uma máquina Pentium MMX 233 MHz, com 128 MB de memória RAM.

As principais dificuldades encontradas no processo de decifração recaem na ausência de uma equação diferencial para iniciar o processo, bem como da necessidade de recorrer a processos recursivos envolvendo a síntese de equações determinantes (Olver,

2000), e à resolução das mesmas através do uso de simetrias disponíveis. O apêndice B apresenta um exemplo no qual o processo de decifração conduz a um esquema recursivo, a partir do qual são produzidas diversas equações diferenciais auxiliares a serem resolvidas. O processo foi encerrado devido à necessidade de efetuar novas etapas de recursão. Essa característica exemplifica claramente o crescimento exponencial do número de operações simbólicas requeridas por cada aplicação recursiva.

6.2 Aplicações do esquema Rafaella

A criptografia procura aplicar características mais confiáveis à informação, através de seus algoritmos e métodos. Busca-se, com relação aos dados sensíveis, uma forma na qual só possam ser processados por pessoas autorizadas.

Porém, usados isoladamente, esses algoritmos têm uma utilidade bastante restrita. Por essa razão, quando se utiliza um protocolo criptográfico, a quantidade de aplicações torna-se maior, dadas as novas funcionalidades que podem ser incorporadas quando de seu emprego – agregando serviços como autenticação, definição de chave comum, dividir ou compartilhar segredos, votar, realizar uma transação comercial, jogar, assinar contratos .

Basicamente, um protocolo criptográfico é um protocolo que usa criptografia em alguma de suas camadas ou de seus passos (Schneier, 1994). Diversas podem ser as características das partes envolvidas: podem ser amigas e se confiarem mutuamente, ou podem ser adversárias e não confiarem na outra parte – podendo ou não empregar uma terceira parte confiável a ambos.

Na verdade, qualquer protocolo criptográfico já proposto pode vir a ser usado, empregando o esquema Rafaella.

6.3 Sugestões para trabalhos futuros

Embora o esquema proposto tenha se mostrado eficaz e seguro, algumas melhorias adicionais podem ser implementadas com o intuito de tornar ainda mais oneroso o processo inverso - ou de decifração por parte de um elemento não autorizado. Algumas dessas melhorias dizem respeito a aspectos matemáticos e outras, a recursos computacionais.

Do ponto de vista matemático, as melhorias que podem ser incorporadas são as seguintes:

1) O emprego de simetrias de Lie-Backlund. As simetrias de Lie-Backlund apresentam infinitesimais dependentes das derivadas da função incógnita. Os infinitesimais constituem os coeficientes dos geradores infinitesimais do grupo de simetria da equação diferencial cuja solução é a função que representa a mensagem original. Assim, mesmo dispondo dos geradores do grupo de simetria, a aplicação da exponencial desses operadores sobre soluções particulares produz novas soluções que resultam implícitas.

2) Formulação de simetrias baseadas em derivadas fracionárias. Essas simetrias dificultam não apenas a quebra do código, mas a própria determinação de eventuais soluções particulares para dar início ao processo. Essa dificuldade reside basicamente nas definições de derivada fracionária, expressas como somatórios, produtórios ou operadores integrais.

3) Mapeamentos utilizando operadores não-lineares. Consistem na transformação da equação diferencial original em uma nova equação, cujas simetrias de Lie são completamente diferentes, mas cuja solução é exatamente a mesma. Desse modo, a

mensagem original é preservada, mas o processo de obtenção das simetrias se torna consideravelmente mais complexo.

4) Emprego de funções oscilantes, tais como funções de Bessel de ordem ν - $J_\nu(x)$, onde ν representa a chave privada. O emprego de tais funções se justifica, dada seu elevado número de raízes, o que proporciona dificuldade extra ao ataque por via numérica. Uma vez que funções dessa natureza não permitem o ataque por via analítica, as possíveis alternativas numéricas - tais como o método do passo descendente, gradientes conjugados, Lanczos – e demais algoritmos utilizados em Pesquisa Operacional para a obtenção de raízes, máximos e mínimos de funções se tornariam ineficazes para a determinação da chave privada.

5) Emprego de soluções particulares como chave privada, ao invés de um dos geradores do grupo de simetria admitido pela equação diferencial. Esse procedimento exige sempre o conhecimento prévio das respectivas condições de contorno por parte do atacante, o que inviabiliza o processo de obtenção da chave privada, uma vez que os próprios participantes não detém o conhecimento das condições de contorno.

Do ponto de vista computacional, uma possível melhoria explora a simplicidade do esquema proposto, quando do emprego de um sistema de processamento simbólico ou algébrico, como os citados anteriormente; como o processo de cifração e decifração é efetuado de modo simples, torna-se possível efetuar laços múltiplos de cifração - nos quais dois ou mais números complexos são utilizados para efetuar sucessivas translações no plano z.

Outra possibilidade do ponto de vista computacional seria a implementação de um sistema de processamento simbólico que possibilitasse o eficiente reconhecimento de padrões e reagrupamento de expressões algébricas. Tal sistema possibilitaria a simplificação de diversas expressões geradas pelo esquema Rafaella.

Uma outra melhoria do ponto de vista computacional seria o remapeamento automático da função a intervalos regulares de tempo; esse recurso permite que as chaves privadas sejam periodicamente alteradas através de uma função definida pelo usuário, sem que o mesmo tome parte no processo. Essa medida proporciona um item extra de segurança, uma vez que torna dinâmico o processo de produção de chaves privadas – não exigindo do usuário qualquer esforço adicional no sentido de produzir chaves alternativas.

Na verdade, diversas melhorias podem ser implementadas no esquema original visando dificultar ainda mais o processo de decifração da mensagem por indivíduos não-autorizados. Uma nova característica emergiu naturalmente ao longo de desenvolvimento do esquema e condução dos experimentos: a razão custo-benefício. O benefício obtido em relação à segurança do esquema suplanta o custo de implementação do método - ou seja, o emprego de um processador simbólico ou algébrico.

Por fim, pode-se concluir que há um novo paradigma que atende aos requisitos de Chave Pública. O paradigma que viabiliza o esquema Rafaella sai do domínio tradicional dos esquemas que empregam teoria dos números, devido à potência do conjunto de Chaves Privadas envolvidas, graças ao trabalho de Marius Sophus Lie.

REFERÊNCIAS

ADLEMAN, L. M.; McCURLEY, K. S. Open Problems in Numeric Theoretic Complexity, II. In: ANTS 1,[199?]. **Proceedings...** Disponível em: <*http://citeseer.nj.nec.com/ 168265.html*>. Acesso em: 12fev.2001.

AYRES JÚNIOR, F. **Equações Diferenciais**. 2. ed. São Paulo: Makron Books, 1994. 406 p.

BLAKE, I.; SEROUSSI, G.; SMART, N. **Elliptic Curves in Cryptography**. London: Cambridge Press, 2000. 210 p.

BLUMAN, G.W.; KUMEI, S. **Symmetries and differential equations**. New York: Springer-Verlag, 1989. 420 p.

BOYCE, W.; DiPRIMA, R. **Equações Diferenciais e Problemas de Valores de Contorno**. 6. ed. Rio de Janeiro: LTC, 1994. 534 p.

BOZICEVIC, M. A Property of Lie Group Orbits. **Canadian Mathematical Bulletin**, Ottawa, v. 43, n. 1, p. 47-50, 2000.

BRAWLEY, J.; GAO, S. **Mathematical Models in Public-Key Cryptology**. 1999. Disponível em: <*http://citeseer.nj.nec.com/ /brawley99mathematical.html*>. Acesso em: 25 abr.2001.

BRESSOUD, D. **Factorization and primality test**. New York: Springer Verlag, 1989. 246 p.

CHARI, V. **A Guide to Quantum Groups**. London: Cambridge Press,1995. 651 p.

CELLEDONI, E. et al. Complexity theory for Lie-group solvers. **Journal of Complexity**, [S.l.], v. 18, n. 1, p. 242-286, Mar. 2002.

COUTINHO, S. C. **Mathematics of Ciphers - Number Theory and RSA Cryptography**. Natick, MA: A. K. Peteres, 1998. 190 p.

DALEY, M. J. **Algorithmic Primality Testing**. 1997. Disponível em: <*http://citeseer.nj.nec.com/270620.html*>. Acesso em: 13 mar.2001.

DATTOLLI, G. et al. Exponential operators, operational rules and evolution problems. **Il Nuovo Cimento**, Bologna, v. 113 B, n. 6, p. 699-710, 1998.

DAVENPORT, J. H.; SIRET, Y. TOURNIER. E**. Computer Algebra**: Systems and Algoritms for Algebraic Computation. London: Harcourt Brace Jovanovich, 1988. 272 p.

DIFFIE, W.; HELLMAN, M. E. New directions in cryptography. **IEEE Trans. Inform. Theory**, New York, v. IT-22, n. 6, p. 644-654, 1976. Disponível em: <*http://citeseer.nj.nec.com/diffie76new.html*> . Acesso em 25 abr.2001.

GAREFALAKIS, T. **Primality Testing, Integer Factorization and Discrete logarithms**. 1998. Disponível em: <*http://citeseer.nj.nec.com/ garefalakis98primality.html*>. Acesso em: 13 mar.2001.

GREENSPAN, D.; CASULLI, V. **Numerical Analysis for Applied Mathematics, Science and Engineering**. Redwood City, CA: Addison Wesley, 1988. 346 p.

IBRAGIMOV, N. **CRC Handbook of Lie Group Analisys of Differential Equations**. 2 nd ed. Boca Ratón: CRC, 1995. v. 2.

KOBLITZ, N. **Algebraic Aspects of Cryptography**. 2 nd ed. Berlin: Springer-Verlag, 1999. 210 p. (Algorithms and Computation in Mathematics, v.3).

KREIDER, D. L.; KULLER, R. G.; OSTBERG, D. **Equações Diferenciais**. São Paulo: E. Blucher, 1972. 490 p.

MANNA, Zohar. **Mathematical Theory of Computation**. Mineola, New York: Dover, 2003.

MENEZES, A. J.; OORSCHOT, P. C. van; VANSTONE, S. A. **Handbook of Applied Cryptography**. Boca Raton: CRC Press, 1996. 786 p.

NATIONAL COUNCIL OF TEACHERS OF MATHEMATICS. **Historical Topics for the Mathematics Classroom**. Washington: National Council of Teachers of Mathematics, 1969. 530 p.

NICHOLS, R. K. **ICSA guide to Cryptography**. New York: McGraw-Hill, 1999. 840 p.

O'CONNOR, J. J; ROBERTSON, E. F. **Biography of Marius Sophus Lie**. Scotland: University of Saint Andrews, 2000. Disponível em: <*http://www-history.mcs.st-andrews.ac.uk/hystory/Mathematicians/Lie.html*> . Acesso em: 13 maio2001.

OLVER, P. **Applications of Lie Groups to Differential Equations**. 2 nd ed. New York: Springer, 2000. 513 p.

ORTEGA, J. M.; POOLE JÚNIOR, W. G. **Numerical Methods for Differential Equations**. Massachusetts: Pitman, 1981. 334 p.

POLYANIN, A. **Handbook of Non-linear Partial Differential Equations**. Moscou: Nauka, 2004.

REDDY, J. N. **Applied Functional Analysis and Variational Methods in Engineering**. New York: McGraw-Hill, 1986. 550 p.

RIBEIRO, V. G. **Um estudo sobre a Matemática empregada em Criptografia**. 2001. 86 p. Trabalho individual (Doutorado em Ciência da Computação) - Instituto de Informática, Universidade Federal do Rio Grande do Sul, Porto Alegre.

RIVEST, R.; SHAMIR, A. ; ADLEMAN, L. A. A method for obtaining digital signatures and public-key cryptosystems. **Communications of the ACM**, New York, v. 21, n. 2, p.

120-126, 1978. Disponível em: <*http://citeseer.nj.nec.com/ rivest78method.html*>. Acesso em: 8 jun.2000.

ROSING, M. **Implementing Elliptic Curve Cryptography**. Greenwich: Manning, 1999. 322 p.

SCHNEIER, B. **Applied Cryptography – Protocols, Algorithms and Source code in C**. 2 nd ed. New York: John Wiley, 1994. 624 p.

SCHROEDER, M. R. **Number Theory in Science and Communication – with applications in Cryptography, Physics, Digital Information, Computing and Self Similarity**. Berlin: Springer-Verlag, 1999. 368 p.

SHAMIR, A. Polinomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem. **IEEE Found. on Theory of Computing**, New York, p. 145-152, 1982.

SINKOV, A. **Elementary Cryptanalysis**: A Mathematical Approach. New York: Yale University, 1966. 198 p. (New Mathematical Library, v.22).

STALLINGS, W. **Cryptography and network security**: principles and practice. 2 nd ed. Upper Saddle River: Prentice-Hall, 1998. 574 p.

STINSON, D. R. **Cryptography**: theory and practice. New York: CRC, 1995. (Discrete mathematics and its applications).

STRANG, G. **Linear Algebra and Its Applications**. San Diego: Harcourt Brace Jovanovich, 1980. 420 p.

SZWARCFITER, J. L. **Grafos e algoritmos computacionais**. 2 ed. Rio de Janeiro: Campus, 1988. 222 p.

TERADA, R. **Segurança de Dados - Criptografia em redes de computador**. São Paulo: E. Blücher, 2000. 246 p.

TIKHONOV, A. et al. **Numerical methods for ill-posed problems**. Moscou: Nauka, 1990. 287 p.

TOSCANI, L. V.; VELOSO, P. A. S. **Complexidade de Algoritmos**: análise, projeto e métodos. Porto Alegre: Instituto de Informática da UFRGS: Sagra Luzzatto, 2001. (Série Livros Didáticos, n.13).

WEBER, R. F. Criptografia Contemporânea. In: SIMPÓSIO DE COMPUTADORES TOLERANTES A FALHAS, 6., 1995, Canela. **Anais...** Porto Alegre: Instituto de Informática da UFRGS, 1995. p. 7-32.

WERSCHULZ, A. G. **The computational complexity of differential and integral equations - an information-based approach**. New York: Oxford, 1991.

ZWILLINGER, D. **Handbook of Differential Equations**. 2 nd ed. Boston: Academic Press, 1992. 792 p.

APÊNDICE A GLOSSÁRIO DE TERMOS MATEMÁTICOS

Amplitude: intervalo de valores da coordenada y que uma função pode assumir.
Anel: assume-se ser um anel, um conjunto com duas operações binárias definidas - soma e produto -, definidas sobre um grupo G, tal que se verificam as propriedades de adição comutativa(soma), existência de identidade(produto), comutatividade(produto), distributividade(produto e soma) e associatividade(produto).
Característica: diz-se de dois textos, S e TST^{-1}, que têm a mesma decomposição cíclica.
Chi: Ou teste Chi, é um teste aplicado às distribuições dos elementos de dois textos cifrados, para determinar se os resultados da distribuição formam a cifração por alfabetos de cifração idênticos, ou para determinar se há alguma relação entre os alfabetos de cifração envolvidos.
Coordenadas projetivas: Sistemas de coordenadas obtidas através da supressão de componentes de uma n-upla: $(x_1,x_2,x_3,...,x_n) \rightarrow (x_1,x_2,x_3,...,x_{n-k})$.
Curvas de Koblitz: Também chamadas de curvas binárias anômalas sobre $GF(2^n)$.
Elemento de identidade: Chama-se ao elemento "e" de um conjunto ou grupo, tal que um elemento, operado com o elemento de identidade, fornece o mesmo elemento original.
Espaço de chaves: Um grande conjunto de possíveis chaves.
GIMPS: Organização composta de matemáticos que estudam primalidade, usando números de Mersenne. Sigla originada de **G**reat **I**nternet **M**ersenne **P**rime **S**earch. Página na WEB, em 21 de abril de 2001: http://www.loria.fr/~zimmerma/records/primes.html.
Grupos: Conjunto (finito ou não) de elementos onde, ao se operar quaisquer dois elementos a ele pertencentes, resulta em um elemento do mesmo conjunto. Ademais, um grupo tem que satisfazer as operações de associatividade, ter um elemento de identidade e possuir um inverso. Se além dessas operações, ainda possuir a propriedade de comutatividade, diz-se que o grupo é dito abeliano.
Grupos abelianos: Têm esse nome em homenagem a Abel[13], o qual contribuiu para diversas áreas da Matemática. A teoria das integrais elípticas foram radicalmente transformadas graças a seus estudos, os quais abrangem grupos e integrais abelianas, da forma $\int \Re(z,u)dz$, onde $\Re$ (z,u) é uma função racional de "z" e de "u", sendo "z" e "u" ligados por uma relação algébrica qualquer.
Inverso: Diz-se do elemento que detém a propriedade de, ao operar com um elemento, gera o elemento de identidade.

[13] Matemático norueguês Niels Abel, 1802-1829.

Jacobiano (... de uma transformação de coordenadas): definido como o determinante $\begin{vmatrix} \frac{\partial u_1}{\partial x_1} & \frac{\partial u_1}{\partial x_2} & \cdots & \frac{\partial u_1}{\partial x_n} \\ \frac{\partial u_2}{\partial x_1} & \frac{\partial u_2}{\partial x_2} & \cdots & \frac{\partial u_2}{\partial x_n} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\partial u_n}{\partial x_1} & \frac{\partial u_n}{\partial x_2} & \cdots & \frac{\partial u_n}{\partial x_n} \end{vmatrix}$, onde $(x_1,x_2,x_3,...,x_n)$ e $(u_1,u_2,u_3,...,u_n)$ representam os sistemas de coordenadas envolvidos na transformação.

Kappa IC: A razão de coincidências observadas ao se comparar duas seqüências de textos superimpostas - além do que seria esperado, se fosse considerada aleatoriedade.

Operador lagrangeano: Operador que descreve a propagação de corpos ao longo de uma determinada trajetória, considerando os fenômenos de dispersão e advecção.

Pseudoprimos: diz-se do número n, se n é ímpar e composto, e satisfaz $2^p-1 \equiv 1 \pmod n$, então n é um pseudoprimo Não há muitos pseudoprimos: menores do que mil, há 3 (341, 561 e 645); e menores do que um milhão, existem 245 – em contrapartida, há nesse intervalo exatos 78.498 números primos. Assim, um número na forma $\mathbf{2^{p-1} \equiv 1 \pmod n}$ for determinado, ele terá grande probabilidade e ser um primo.

Redução Polinomial: São reduções que preservam a complexidade polinomial - o que é de especial interesse no estudo da complexidade.

APÊNDICE B UM EXEMPLO DE EQUAÇÕES DETERMINANTES

O exemplo a seguir pode facilmente ser verificado, empregando-se o software Maple V ®.

```
> restart:
> with(liesymm):
> with(PDEtools):
```

Operador que define a equação - no exemplo, é a equação da condução do calor para difusividade térmica unitária

```
> A:=f->diff(f,x$2)-diff(f,t);
```

Equação diferencial parcial produzida

```
> edp:=A(f(x,t))=0;
```

$$edp := \left(\frac{\partial^2}{\partial x^2} \mathrm{f}(x, t)\right) - \left(\frac{\partial}{\partial t} \mathrm{f}(x, t)\right) = 0$$

Equações a partir das quais são determinados os infinitesimais(fazem parte da biblioteca de simetrias de Lie)

```
> d:=determine(edp,V,f(x,t),k);
```

$$d := \{\frac{\partial}{\partial x} \mathrm{V2}(x, t, f) = 0, \frac{\partial}{\partial f} \mathrm{V2}(x, t, f) = 0, \frac{\partial^2}{\partial f^2} \mathrm{V1}(x, t, f) = 0,$$
$$\frac{\partial}{\partial f} \mathrm{V1}(x, t, f) = -\left(\frac{\partial^2}{\partial x\, \partial f} \mathrm{V2}(x, t, f)\right), \frac{\partial^2}{\partial f^2} \mathrm{V2}(x, t, f) = 0, \frac{\partial}{\partial t} \mathrm{V3}(x, t, f) = \frac{\partial^2}{\partial x^2} \mathrm{V3}(x, t, f),$$
$$\frac{\partial^2}{\partial f^2} \mathrm{V3}(x, t, f) = 2\left(\frac{\partial^2}{\partial x\, \partial f} \mathrm{V1}(x, t, f)\right),$$
$$\frac{\partial^2}{\partial x^2} \mathrm{V2}(x, t, f) = -2\left(\frac{\partial}{\partial x} \mathrm{V1}(x, t, f)\right) + \left(\frac{\partial}{\partial t} \mathrm{V2}(x, t, f)\right),$$
$$\frac{\partial}{\partial t} \mathrm{V1}(x, t, f) = \left(\frac{\partial^2}{\partial x^2} \mathrm{V1}(x, t, f)\right) - 2\left(\frac{\partial^2}{\partial x\, \partial f} \mathrm{V3}(x, t, f)\right)\}$$

Sistema de auto-simplficação das equações

```
> a:=autosimp(d);
```

$$a := \{\frac{\partial}{\partial t} \mathrm{V1\_4}(t) = -x\left(\frac{\partial}{\partial t} \mathrm{V1\_3}(t)\right) - 2\left(\frac{\partial}{\partial x} \mathrm{V3\_1}(x, t)\right), \frac{\partial^2}{\partial x^2} \mathrm{V3\_1}(x, t) = \frac{\partial}{\partial t} \mathrm{V3\_1}(x, t),$$
$$\frac{\partial^2}{\partial x^2} \mathrm{V3\_2}(x, t) = \frac{\partial}{\partial t} \mathrm{V3\_2}(x, t), \frac{\partial}{\partial t} \mathrm{V2\_2}(t) = 2\ \mathrm{V1\_3}(t)\} \ \&\mathrm{where}\ \{$$
$$\mathrm{V2}(x, t, f) = \mathrm{V2\_2}(t), \mathrm{V1}(x, t, f) = x\ \mathrm{V1\_3}(t) + \mathrm{V1\_4}(t),$$
$$\mathrm{V3}(x, t, f) = f\ \mathrm{V3\_1}(x, t) + \mathrm{V3\_2}(x, t)\}$$

Soluções invariantes em relação a elementos do grupo - o operador v, aplicado à função zera a mesma

```
> ed2:=diff(V3_1(x,t),`$`(x,2)) = diff(V3_1(x,t),t);
```

$$ed2 := \frac{\partial^2}{\partial x^2} \mathrm{V3\_1}(x,t) = \frac{\partial}{\partial t} \mathrm{V3\_1}(x,t)$$

Obtenção de uma solução invariante em reação a um dos geradores - no caso, v3.
Definição do infinitesimal:

```
> v31:=rhs(pdsolve(ed2,V3_1(x,t),build));
```

$$v31 := \_C3\, \mathbf{e}^{(\_c_1\, t)}\, \_C1\, \mathbf{e}^{(\sqrt{\_c_1}\, x)} + \frac{\_C3\, \mathbf{e}^{(\_c_1\, t)}\, \_C2}{\mathbf{e}^{(\sqrt{\_c_1}\, x)}}$$

Definição do gerador

```
> V:=C->(f*v31+x^2+2*t)*diff(C,f)+k*diff(C,x);
```

Equação que define uma solução invariante em relação a um dos geradores - se aplicar esse operador sobre uma determinada função e a mesma resultar zero, então essa função é uma solução particular da equação original. E essa solução é chamada de solução invariante em relação ao gerador usado.
Observa-se que a forma mais geral é a aquela invariante em relação a *todos* **os geradores.**

```
> ea:=V(C(x,t,f))=0;
```

$$ea := \left(f \left(\_C3\, \mathbf{e}^{(\_c_1\, t)}\, \_C1\, \mathbf{e}^{(\sqrt{\_c_1}\, x)} + \frac{\_C3\, \mathbf{e}^{(\_c_1\, t)}\, \_C2}{\mathbf{e}^{(\sqrt{\_c_1}\, x)}} \right) + x^2 + 2\,t \right) \left(\frac{\partial}{\partial f} \mathrm{C}(x,t,f) \right) + k \left(\frac{\partial}{\partial x} \mathrm{C}(x,t,f) \right) = 0$$

Emprego do comando pdsolve para obter a solução invariante em relação a esse gerador particular

```
> pdsolve(ea,C(x,t,f),build);
```

$$\mathrm{C}(x,t,f) = \_\mathrm{F1}\left(t, \left(f - \mathbf{e}^{\left(-\frac{\left(\_C1\, \mathbf{e}^{(2\sqrt{\_c_1}\, x)} + \_C2 \right) \_C3\, \mathbf{e}^{(\_c_1\, t - \sqrt{\_c_1}\, x)}}{\sqrt{\_c_1}\, k} \right)} \right) \int \frac{\mathbf{e}^{\left(\frac{\left(\_C1\, \mathbf{e}^{(2\sqrt{\_c_1}\, x)} + \_C2 \right) \_C3\, \mathbf{e}^{(\_c_1\, t - \sqrt{\_c_1}\, x)}}{\sqrt{\_c_1}\, k} \right)} (x^2 + 2\,t)}{k}\, dx \right) \mathbf{e}^{\left(\frac{\left(\_C1\, \mathbf{e}^{(2\sqrt{\_c_1}\, x)} + \_C2 \right) \_C3\, \mathbf{e}^{(\_c_1\, t - \sqrt{\_c_1}\, x)}}{\sqrt{\_c_1}\, k} \right)}$$

```
> ed:= diff(f(x,a),a) = diff(f(x,a),x);
```

$$ed := \frac{\partial}{\partial a} f(x, a) = \frac{\partial}{\partial x} f(x, a)$$

Equação diferencial associada à regra do deslocamento.

```
> pdsolve(ed,f(x,a),build);
```

$$f(x, a) = \_F1(a + x)$$

APÊNDICE C BREVE HISTÓRICO DE LIE

A seguir, apresenta-se a biografia de Lie , conforme O'Connor (O´Connor, 2000):

Marius Sophus Lie nasceu em 17 de dezembro de 1842, em Nordfjordeide, na Noruega. Foi o mais jovem dos seis filhos do pastor luterano Johann Herman Lie. Embora desejasse seguir a carreira militar, a sua pouca acuidade visual o impediu - e ele cursou Ciências na Universidade de Christiania (posteriormente, Kristiania - atual Oslo -, também na Noruega).

Em seu curso de graduação, assistiu a diversas palestras sobre Matemática e, embora tenha se graduado em 1865, não aparentava ter grandes habilidades nessa ciência. Durante algum tempo, ficou indeciso sobre qual objetivo seguir, tendo se inclinado para Astronomia - embora tenha se impressionado com a Mecânica, a Botânica e a Zoologia. Contudo, os registros da biblioteca da Universidade de Christiania revelam que, por volta de 1866, seu interesse começara a se concentrar em Matemática.

Figura C. 1: Marius Sophus Lie, matemático norueguês.

Em 1869, Lie publicou um pequeno artigo por suas próprias expensas, que havia sido escrito em 1867. A razão: a Academia de Ciências de Christiania estava relutante em aceitar certas noções revolucionárias de Lie, tendo causado certa insegurança no mesmo. Seu amigo

Motzfeldt o encorajou a publicar, tendo sido aceito no *Crelle's Journal* - da antiga Prússia - e passado um período em Göttingen e em Berlin.

Durante a primavera de 1870, Lie e seu novo amigo Felix Klein - que seguiam a linha de Plücker - conheceram Camille Jourdan, em Paris. Jourdan mostrara o quão importante o trabalho de teoria dos grupos era para a Geometria. Lie iniciou a desenvolver idéias que apareceriam posteriormente em seu trabalho de grupos de transformação. Contudo, ocorreu um contratempo: tendo sido deterioradas as relações entre a França e a Prússia, Klein retornara a Prússia; Lie, considerando-se um cidadão norueguês, ignorou qualquer perigo, permanecendo na França. Resultado: Lie foi preso como espião da Prússia, e suas anotações matemáticas foram confiscadas, tendo sido consideradas como mensagens codificadas altamente secretas. Durante a intervenção de Darboux, Lie foi solto, tendo se dirigido para a Itália e, de lá, retornado para Christiania via Prússia.

Em 1872, tendo-se tornado professor assistente em Christiania, submeteu a tese intitulada *On a class of geometric transformations* - escrita em norueguês. A tese continha idéias de resultados de seu primeiro artigo, bem como do trabalho em transformações de contato - um caso especial dessas transformações era uma transformação na qual mapas poderiam ser alinhados em uma esfera.

Casou-se em 1874 com Anna Birch, tendo uma filha e dois filhos. Desde 1873, contudo, Lie examinou suas transformações de contato, considerando o efeito como elas afetavam um processo, devido a geração de soluções de equações diferenciais a partir de uma equação dada, conforme Jacobi. Esse exame levou a combinar as transformações de um modo que Lie as chamou de "grupo infinitesimal" - embora não seja um grupo por definição, tornou-se, mais tarde, "Álgebra de Lie". Por volta do verão europeu de 1874, Lie começou a desenvolver sistematicamente o que veio a se tornar sua teoria dos grupos de transformação contínuos - a qual foi chamada mais tarde de "Grupos de Lie", o que levou-o a abandonar sua idéia inicial de examinar apenas as equações diferenciais parciais.

Embora Lie tenha produzido grandes inovações matemáticas, começou a desmotivar-se, devido ao pouco reconhecimento que recebeu no mundo matemático. Uma provável razão era o seu isolamento em Christiania; contudo, outra razão era a complexidade de seus artigos - em parte, devido ao seu estilo de escrita, e parte, devido a seu alto grau de abstração geométrica, que excedia a compreensão da maioria dos matemáticos da época. Assim, seu amigo Klein enviou Friedrich Engel para Christiania, para ajudar Lie, tendo trabalhado juntos durante nove meses. Posteriormente, Klein deixou a sua cadeira para Lie, tendo esse se mudado para Leipzig, continuando a trabalhar com Engel. Juntos publicaram, entre 1888 e 1893, a sua maior obra: *Theorie der Transformationsgruppen*, em três volumes. Esse foi o maior trabalho de Lie, em transformação de grupos contínuos.

Por razões não claramente documentadas, Lie termina suas relações com Engel em 1880, e com Klein, em 1892. Retornou a Christiania em 1898, tendo a sua saúde deteriorado e vindo a falecer em 18 de fevereiro de 1899.