UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE COMPUTAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

PROTOCOLO PARA EMISSÃO DE ASSINATURA DIGITAL UTILIZANDO COMPARTILHAMENTO DE SEGREDO

WINICIUS PEREIRA

Uberlândia - Minas Gerais
2011

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE COMPUTAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

WINICIUS PEREIRA

PROTOCOLO PARA EMISSÃO DE ASSINATURA DIGITAL UTILIZANDO COMPARTILHAMENTO DE SEGREDO

Dissertação de Mestrado apresentada à Faculdade de Computação da Universidade Federal de Uberlândia, Minas Gerais, como parte dos requisitos exigidos para obtenção do título de Mestre em Ciência da Computação.

Área de concentração: Banco de Dados.

Orientador:
Prof. Dr. João Nunes de Souza

Uberlândia, Minas Gerais
2011

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE COMPUTAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Os abaixo assinados, por meio deste, certificam que leram e recomendam para a Faculdade de Computação a aceitação da dissertação intitulada "**Protocolo para Emissão de Assinatura Digital utilizando Compartilhamento de Segredo**" por **Winicius Pereira** como parte dos requisitos exigidos para a obtenção do título de **Mestre em Ciência da Computação**.

Uberlândia, 8 de agosto de 2011

Orientador: _____

Prof. Dr. João Nunes de Souza
Universidade Federal de Uberlândia

Banca Examinadora:

_____

Prof. Dr. Daniel Gomes Mesquita
Universidade Federal de Uberlândia

_____

Prof. Dr. Pedro Frosi Rosa
Universidade Federal de Uberlândia

_____

Prof. Dr. Edward David Moreno Ordonez
Universidade Federal de Sergipe

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE COMPUTAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Data: agosto de 2011

Autor:	**Winicius Pereira**
Título:	**Protocolo para Emissão de Assinatura Digital utilizando Compartilhamento de Segredo**
Faculdade:	**Faculdade de Computação**
Grau:	**Mestrado**

Fica garantido à Universidade Federal de Uberlândia o direito de circulação e impressão de cópias deste documento para propósitos exclusivamente acadêmicos, desde que o autor seja devidamente informado.

_____

Autor

Dedicatória

Aos meus pais e irmãos, à minha esposa Karla pelo incentivo, apoio e carinho, às minhas filhas pela paciência e compreensão nos momentos de ausência.

Agradecimentos

A conclusão de uma dissertação é fruto do envolvimento e comprometimento de várias pessoas, apesar de parecer um trabalho solitário. Portanto, fica aqui, o meu agradecimento àqueles que colaboraram para o êxito desse projeto.

Primeiramente agradeço a *Deus*, pela vida, saúde e por me ajudar a vencer cada obstáculo que parecia intransponível.

À minha esposa *Karla*, por compreender minha ausência em alguns momentos, incentivando-me e não me deixando desistir frente às dificuldades.

Às minhas filhas *Thalita*, *Thalissa* e *Thaiza*, cuja existência, me enche de forças para seguir adiante. Também ao meu filho *Pedro Henrique*, que, mesmo ausente, dá-me esperança e orgulho em suas conquistas.

Agradeço, ainda, a meu pai, *José Geraldo*, à minha mãe *Neusa*, aos meus irmãos *Leonardo* e *Graziella*, ao meu sogro, *Ovídio*, minha sogra *Málida*, aos meus cunhados *Denísio*, *Silas* e *Ovídio Júnior* e cunhadas *Milene*, *Gisele* e *Fabiana*. Enfim, a toda minha família por sempre estar ao meu lado.

Ao meu orientador, Prof. Dr. *João Nunes de Souza* pelo comprometimento, oportunidade, amizade e confiança oferecidos.

Aos amigos de verdade *Denis*, *José Otávio*, *Ricardo Chenche* e *Alexsandro*, com quem sei que posso contar.

Aos colegas *Gabriel*, *Marques*, *Cíntia*, *Daniele*, e em especial ao *Humberto*, companheiro das incansáveis viagens, pelo apoio e ajuda durante o mestrado.

Ao Centro Universitário do Planalto de Araxá, pela oportunidade e apoio financeiro, em particular ao *Prof. Me. Pedro Ashidani*, pelos conselhos e auxílio, e ao *prof. Marco Aurélio Moreira* pela preocupação e ajuda.

Viver no mundo sem tomar consciência do significado do mundo é como vagar por uma imensa biblioteca sem tocar os livros.

Os Ensinamentos Secretos de Todos os Tempos *[Brown 2009]*

Resumo

A internet possibilitou a criação de inúmeros serviços virtuais em prol da agilidade, comodidade e facilidade para o cidadão brasileiro. É um ambiente público, no qual centenas de milhares de dados são transmitidas a todo instante. Porém, alguns desses serviços requerem que as informações transmitidas atendam a determinados requisitos de segurança, como: a autenticidade, sigilo, integridade e irretratabilidade, como é o caso dos serviços prestados por cartórios digitais no Brasil.

A assinatura digital garante que esses requisitos sejam cumpridos mesmo em um ambiente complexo como a internet. Contudo, possui vulnerabilidades que podem ser exploradas, como o armazenamento da mesma em um único dispositivo. Se o dispositivo que armazena a chave secreta do usuário for roubado ou corrompido por um invasor, esse consegue emitir uma assinatura válida se passando pelo dono da assinatura. Em função desse tipo de problema, os cartórios digitais, não disponibilizam o análogo digital de vários procedimentos, como é o caso do reconhecimento de firma com autenticidade, em um documento eletrônico.

Essa dissertação, portanto, propõe um protocolo para emissão de uma assinatura digital compartilhada, em que a chave secreta é dividida em partes e armazenada em dispositivos distintos. Para exemplificar seu uso, é considerado o problema da emissão de uma assinatura digital em uma escritura de compra e venda de um imóvel com reconhecimento de firma e autenticação.

O esquema de assinatura digital utilizado foi RSA, no qual é feito a divisão da chave secreta do usuário, utilizando o conceito de compartilhamento de segredos por limiar. O protocolo se baseia na ideia de que a chave secreta não deve ser armazenada em um único dispositivo do usuário. Para aumentar sua segurança, somente uma parte da chave privada é armazenada no dispositivo do usuário. A parte da chave secreta de posse do usuário deve ser essencial para formação da totalidade da chave privada, mas não deve ser capaz de formar uma assinatura válida sozinha. Além do mais, como os cartórios são órgãos públicos que reconhecem firmas e autenticam documentos, eles devem também ter sua parcela de responsabilidade na emissão de uma assinatura digital, por autenticidade, e no armazenamento da chave privada. Também é considerada a assinatura das testemunhas no documento, pois elas atestam a existência do negócio.

Palavras chave: criptografia, compartilhamento de segredos, assinatura digital, criptografia de limiar

Abstract

The Internet has enabled the creation of many virtual services in favor of agility, comfort and ease for Brazilian citizens. It is a public environment, in which hundreds of thousands of data are transmitted at all times. But some of these services require that the information provided meet certain safety requirements, such as: the authenticity, confidentiality, integrity and denial, as is the case of digital services provided by notaries in Brazil.

The digital signature ensures that these requirements are met even in a complex environment like the Internet. However, it has vulnerabilities that can be explored, such as storing the same in a single device. If the device that stores the user's secret key is stolen or corrupted by an attacker, that can issue a valid subscription like the owner of the signature. Due to this type of problem, the notary digital, does not provide the digital analogue of several procedures, such as the notarization with authenticity in an electronic document.

This thesis, therefore, proposes a protocol for issuing a shared digital signature, in which the secret key is divided into parts and stored in different devices. To illustrate its use is considered the problem of issuing a digital signature on a deed of purchase and sale of a property with notarization and authentication.

The digital signature scheme RSA was used, dividing the user's secret key using the concept of sharing secrets threshold. The protocol is based on the idea that the secret key should not be stored in a single user device. To increase your safety, only a portion of the private key is stored in the user's device. It is also considered the signature of the witnesses in the document, that they attest to the existence of the business. But, should not be able to form a valid signature alone. Moreover, as the agencies of notary public are organ that recognize and authenticate documents, they should also have their share of responsibility in issuing a digital signature by authenticity and the private key storage.

Keywords: encryption, shared secrets, digital signature, threshold cryptography

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

ACs	Autoridades Certificadoras subordinadas à ICP-Brasil
AR	Autoridades de Registros subordinadas às ACs
e-CPF	Versão eletrônica do CPF
e-CNPJ	Versão eletrônica do CNPJ
e-CAC	Centro Virtual de Acesso ao Contribuinte
EDF	Escrituração Fiscal Digital
ICP-Brasil	Infraestrutura de chaves Públicas Brasileiras
IETF	*Internet Engineering Task Force*
ITI	Instituto Nacional de Tecnologia da Informação
SIDOF	Serviço de Documentos Oficiais
SPB	Sistema de Pagamento Brasileiro
SPED	Sistema Público de Escrituração Digital
RFC	*Request for Comments*
RSA	Criptosistema criado por *Ronald Rivest*, *Adi Shamir* e *Leonard Adleman*.

Capítulo 1

Introdução

Com a popularização da internet, cada vez mais pessoas utilizam esse recurso para disponibilizar informações, enviar documentos, efetuar transações bancárias, efetivar negócios etc. Sua funcionalidade e praticidade tornam alguns processos cotidianos mais ágeis. Com isso, várias possibilidades estão surgindo e fronteiras sendo atravessadas. Uma delas é a capacidade de garantir o reconhecimento de firma de documentos eletrônicos. Porém, garantir a privacidade e segurança desses procedimentos em um ambiente público, como a internet, é uma tarefa complexa.

A evolução tecnológica possibilitou a transformação de vários processos. Novos recursos foram criados e a tecnologia da informação passou a ser um elemento estratégico nas empresas. A informática possibilitou a criação de novas formas de negócio, como o *e-commerce*. No entanto, diversas organizações foram obrigadas a se adaptarem às mudanças impostas pela sociedade no sentido de agilizar o trâmite de informações de forma segura. Um exemplo dessa obrigatoriedade é a assinatura eletrônica em alguns documentos fiscais eletrônicos.

A assinatura digital surgiu, portanto, como um aparato tecnológico capaz de representar uma assinatura tradicional em um documento eletrônico. Ela possibilita, ainda, a racionalização do uso do papel, além de garantir uma identidade segura entre as partes no trâmite de arquivos e documentos pela grande rede de computadores.

Atualmente, observa-se que várias empresas buscam a redução de custos. Isso se deve não só às questões de sobrevivência, mas também às questões de competitividade. Dado esse contexto e, também, incentivos governamentais, o uso da assinatura digital passou a fazer parte do cotidiano de muitas empresas e indivíduos. Essa tecnologia possibilitou, por exemplo, a desmaterialização de processos e rotinas, como assinaturas em contratos, envio de informações sensíveis, dentre outros, e iniciou o processo de transformação de procedimentos em *bytes*, gerando redução de custos e eficiência econômica, além de propiciar conforto ao cidadão [da Silveira Martini 2009].

Mas, somente o uso da assinatura digital em documentos eletrônicos não consegue suprir todas as necessidades dos processos de informação existentes atualmente. Os cartórios brasileiros, por exemplo, já utilizam a assinatura digital há algum tempo. Entretanto, eles não

disponibilizam o análogo digital de vários procedimentos, como é o caso do reconhecimento de firma com autenticidade, em um documento eletrônico.

1.1 Contexto e Definição do Problema

A maioria dos cartórios brasileiros realiza dois serviços importantes que são: o reconhecimento de firma e a autenticação de documentos. Ambos os serviços têm características próprias e se complementam. O reconhecimento de firma pode ser definido como o ato de um cartório atestar que uma assinatura, em papel, é realmente de quem diz ser [Cunha 2006]. Para que o cartório possa reconhecer a firma, é necessário que, previamente, a pessoa tenha firma aberta. E abrir uma firma significa ter uma ficha de assinaturas no cartório. Essa, por sua vez, é utilizada para atestar a autenticidade da assinatura em documentos.

Existem dois tipos de reconhecimento de firma: por semelhança e por autenticidade. O processo de reconhecimento por semelhança é feito por comparação grafotécnica entre a assinatura no documento físico efetuada pela pessoa e a outra que ela efetuou em sua ficha de firma armazenada no cartório. Se as assinaturas forem semelhantes, o cartório reconhece que a assinatura do documento apresentado é semelhante à assinatura padrão da ficha. Então, é colocado, no documento físico, um selo de autenticidade assinado pelo tabelião do cartório. O processo de reconhecimento por autenticidade é feito quando é necessário maior segurança no reconhecimento da assinatura. Ele é semelhante ao reconhecimento de firma por semelhança. Contudo, no caso da autenticação de firma por autencidade, é exigida a presença física do dono da assinatura. Nesse caso, o tabelião atesta a autenticidade da assinatura e confere os documentos de identificação do dono da assinatura [Arpen-SP 2011].

Em alguns documentos o reconhecimento da firma somente pode ser feito através do processo de reconhecimento por autenticidade, como é o caso da escritura pública de compra e venda de imóvel, ou na venda de veículos automotores.

Além disso, o processo de reconhecimento de firma em um documento não garante necessariamente, a veracidade do documento em si, apenas da assinatura. Para isso, existe o serviço de autenticação de documentos, o qual atesta que a fotocópia de um documento original é verdadeira.

Os processos descritos acima dependem da apresentação de um documento físico no cartório, ou da presença do signatário, como é o caso do processo de reconhecimento de firma por autenticidade. Nesse contexto, o uso da criptografia possibilita a reprodução de análogos desses processos em meio digital. A certificação digital, por exemplo, considera algoritmos de reconhecimento de firma e a autenticidade dos documentos. Tal certificação digital possui meios de garantir a autoria de uma assinatura digital e a integridade do documento, sendo um processo reconhecido judicialmente [MP2.200/2 2001].

Além disso, alguns processos, quando considerados em meio digital, podem até se apresentar mais seguros que seus análogos usuais. Por exemplo, em relação ao processo de reco-

nhecimento de firma por semelhança, a assinatura digital é mais segura do que o processo de comparação de assinaturas por similaridade. Isso ocorre porque a prova da autoria e irretratabilidade da assinatura digital, além da integridade da mensagem, é feita por meio de fundamentos matemáticos. No caso usual, o reconhecimento de firma por semelhança, por exemplo, depende apenas da comparação entre a assinatura do documento físico com a da ficha de assinatura. E, usualmente, tal comparação pode ser feita por funcionários despreparados ou sem a devida atenção, o que coloca em risco a confiabilidade de todo o processo.

No caso do processo de reconhecimento de firma com autenticidade, implementar o seu análogo digital é uma tarefa bem mais complexa. Isso porque esse tipo de reconhecimento de firma exige a presença física do signatário como requisito para elevar o nível de segurança e certeza do reconhecimento da firma. Apesar de a certificação digital garantir a autoria da assinatura digital, ela não garante necessariamente, que um documento assinado digitalmente foi assinado pelo dono da assinatura. Isso se deve à necessidade da assinatura digital ser armazenada em algum dispositivo, como *pendrive*, cartão de memória, *chip* eletrônico ou mesmo em algum computador. Caso um desses dispositivos seja roubado, ou corrompido[1] , não se pode, então, afirmar que há autenticidade da assinatura digital do documento. Nesse caso, alguém pode ter se passado pelo signatário e usado sua assinatura válida no documento.

Diante desse contexto, e visando resolver o problema do processo de reconhecimento de firma por autenticidade em meio digital e aumentar a segurança do armazenamento da chave privada do usuário, essa dissertação propõe um protocolo para emissão da assinatura digital por autenticidade.

1.2 Justificativa

O uso da assinatura digital certificada ou certificação digital, tem impulsionado o oferecimento de alguns serviços na internet. Como exemplo, há o Sistema Público de Escrituração Digital, SPED, que permite o envio de Escrituração Fiscal Digital, EDF e informações fiscais à Receita Federal utilizando também um e-CPF ou e-CNPJ. Outro serviço que pode ser citado é o Centro Virtual de Acesso ao Contribuinte¸ e-CAC, que disponibiliza a maioria dos serviços oferecidos pela Receita Federal do Brasil para proprietários do e-CPF ou e-CNPJ, dentre outros.

No contexto dessa dissertação, alguns serviços notariais também já são oferecidos como notificação digital, emissão de sinal público, etc. Esses serviços dispensam a presença física do cidadão no cartório, evitando filas, trazendo mais segurança e praticidade ao processo.

Porém, como no ambiente virtual não há a possibilidade de presença física, então são necessários dispositivos tecnológicos capazes de garantir a autenticidade, irretratabilidade e integridade das informações trafegadas. Além do mais, deve-se criar um mecanismo para impedir que fraudes aconteçam, evitando o uso não autorizado de uma assinatura digital autêntica ou mesmo a criação de assinaturas falsas.

[1] Ter seu conteúdo copiado para outro dispositivo.

Em relação à proposta desta dissertação, que é um protocolo de reconhecimento de firma por autenticidade; pelo que se sabe, não foi encontrado serviço dessa natureza oferecido por cartórios no meio digital.

1.3 Hipóteses

Os levantamentos iniciais apontaram que o principal problema no contexto estudado consiste em criar um mecanismo para autenticar e reconhecer firma de uma assinatura eletrônica em um documento, em um processo análogo ao de uma escritura de compra e venda de imóvel, na qual , tradicionalmente, assinam o vendedor, comprador, tabelião e duas testemunhas.

Evidentemente, a escolha do problema de assinatura em uma escritura de compra e venda de um imóvel serve apenas como elemento didático. E, nesse sentido, a emissão de assinatura compartilhada poderia ser considerada, também, em outros contextos.

Além disso, existe um problema secundário e não menos importante, que é aumentar a segurança de armazenamento da assinatura eletrônica de uma pessoa, a qual é utilizada em documentos análogos ao citado acima.

Diante disso, levantou-se a hipótese de que a criação de protocolos criptográficos utilizando algoritmos de chave assimétrica e manipulação matemática pode resolver esses problemas. Para garantir a segurança da assinatura digital do usuário, ela deve ser dividida e suas partes armazenadas em locais distintos. Este protocolo se baseia na ideia de que a chave privada não deve ser armazenada em um único dispositivo do usuário. Para aumentar sua segurança, somente uma parte da chave privada é armazenada no dispositivo do usuário. A parte da chave privada de posse do usuário deve ser essencial para formação da totalidade da chave privada. Mas, não deve ser capaz de formar uma assinatura válida sozinha. Além do mais, como os cartórios são órgãos públicos que reconhecem firmas e autenticam documentos, eles devem também ter sua parcela de responsabilidade na emissão de uma assinatura digital, por autenticidade, e no armazenamento da chave privada.

1.4 Organização do Texto

Esta dissertação, além deste capítulo introdutório, organiza-se em outros cinco capítulos descritos resumidamente a seguir:

O capítulo 2 descreve a metodologia utilizada nesta dissertação, analisa alguns trabalhos correlatos em relação ao protocolo proposto, e mostra ainda uma breve descrição desse protocolo como forma de confirmação da hipótese levantada.

No capítulo 3 apresentam-se os conceitos sobre assinatura digital e certificação digital. Descreve-se o modelo de infraestrutura de chaves públicas do Brasil, mostrando as autoridades certificadoras e de registros bem como os serviços já prestados por cartórios na internet.

No capítulo 4 apresentam-se conceitos sobre segurança e criptografia, o esquema de assinatura RSA e o esquema de compartilhamento de segredos de limiar proposto por Adi Shamir.

O capítulo 5 apresenta um protocolo para emissão de assinatura digital com reconhecimento de firma por autenticidade. Além disso, o protocolo considera a emissão de uma assinatura conjunta com testemunhas além de aumentar a segurança do armazenamento da chave privada do usuário, tornando impraticável seu roubo ou cópia e evitando que um intruso se passe pelo signatário.

O capítulo 6 encerra o trabalho, apresenta sugestões de melhoria, arrola os pontos positivos e negativos, tece as considerações finais, incluindo o levantamento da contribuição desta dissertação e propostas para trabalhos futuros.

Capítulo 2

Estrutura da Solução Proposta

Este capítulo apresenta a metodologia e uma descrição da fundamentação teórica utilizadas no desenvolvimento desta dissertação. Também são analisados trabalhos similares que serviram de base para a construção do protocolo proposto. São destacadas ainda, as necessidades da solução proposta em relação a esses trabalhos correlatos e quais foram os artifícios utilizados para saná-las.

Por fim, como comprovação das hipóteses levantadas, é feita uma breve descrição do protocolo.

2.1 Material e Metodologia

A metodologia utilizada no desenvolvimento deste trabalho consiste em pesquisa bibliográfica e exploratória, utilizando o método indutivo. Conforme [de Oliveira Bertucci 2008], a pesquisa bibliográfica consiste:

> [...] na realização do trabalho monográfico tendo como referência a leitura, a análise e interpretação de documentos existentes acerca de um determinado fenômeno. Esses materiais tanto podem ser livros e artigos científicos, como também outros relatórios de pesquisa, documentos internos disponibilizados por órgãos públicos, organizações e famílias, documentos de época, fotos, gravações, informações extraídas de jornais, revistas e boletins [...]

Foi feita, então, uma pesquisa bibliográfica sobre os serviços notariais ofertados ao cidadão brasileiro pela internet. Percebeu-se, a partir daí, que determinados serviços necessitam de maior garantia de segurança por parte do tabelionato. Isso porque tais serviços exigem a presença física de pessoas. Portanto, seus análogos digitais não são ainda oferecidos via internet. Mais precisamente, serviços que necessariamente precisam de uma forma de identificação pessoal mais eficaz e segura, como o caso de uma escritura pública de compra e venda de imóveis. Além disso, nesse caso, para comprovar sua validade, tais documentos requerem, ainda, as assinaturas das partes: *Vendedor* , *Comprador* , *Tabelião* e *Testemunhas*.

Nesse tipo de documento, reconhecido judicialmente pela fé pública[1], é expressa a vontade de comprar e vender um imóvel por meio de um tabelião e suas testemunhas. Como a autenticidade desse documento está baseada em seu conteúdo e nas assinaturas ali postas, foi pesquisado um artifício computacional que representasse tais requisitos.

Diante dessa necessidade, foi pesquisado o uso da assinatura e certificação digital para emissão de assinatura em documentos eletrônicos. Também é mostrado seu embasamento legal e o modelo de infraestrutura de chaves públicas adotado no Brasil, citando as autoridades certificadoras e registradoras.

Como o foco do trabalho é propor uma solução, via internet, foram mostradas as principais ameaças presentes nesse meio para transmissão de arquivos e informações, bem como alguns requisitos de segurança para evitar tais vulnerabilidades. Também foi observado que o uso de modelos criptográficos pode garantir a segurança das informações trafegadas em um ambiente como a internet. Optou-se, então, por utilizar o criptosistema de assinatura digital RSA proposto por [Rivest et al. 1978]. Isso porque ele é, geralmente, utilizado na emissão de certificados digitais, além de ser um algoritmo assimétrico do qual somente o signatário possui sua chave privada. Além do mais, é um dos criptositemas mais utilizados para essa finalidade [Stallings 2007].

A utilização do criptosistema de assinatura RSA garante a segurança da emissão da assinatura digital e não o seu armazenamento. Ela pode ser armazenada em um dispositivo móvel como *pen-drive*, *chip* e outros, que podem estar sujeitos à perda e roubos. Sendo assim, uma das formas de aumentar a segurança do armazenamento da assinatura digital do usuário é dividindo-a e armazenando-a em vários locais.

Para efetuar a divisão da assinatura digital do usuário, foi utilizado o criptosistema de compartilhamento de segredos proposto por Adi Shamir em [Shamir 1979]. Esse critptosistema considera a divisão de um segredo em partes, denominadas sombras. Essas sombras são armazenadas em dispositivos distintos e permanecem secretas. Para reconstruir um segredo compartilhado, é necessário reunir uma quantidade mínima de sombras, definidas no momento da divisão da assinatura. Utilizando esse conceito, foi possível dividir o expoente secreto do criptosistema de assinatura RSA, utilizado na operação matemática para emissão da assinatura digital e sua posterior reconstrução a partir de um limiar definido.

Apesar da divisão da chave secreta ser possível, deve-se garantir que o usuário, dono da assinatura digital, sempre participe de sua reconstrução. Nesse sentido, uma das sombras reunidas para a reconstrução da assinatura deve, necessariamente, pertencer ao usuário. Sendo assim, foi proposto nesse trabalho estender o esquema de compartilhamento proposto por Adi Shamir, considerando o veto do usuário, ou seja, a assinatura do usuário não poderá ser reconstruída caso ele não seja integrante do conjunto de limiar determinado.

A pesquisa se estendeu a artigos correlatos que visavam resolver problemas similares os quais são descritos na seção 2.2 dessa dissertação

[1]Crédito dado aos documentos lavrados em cartórios. O documento é verdadeiro até que se prove o contrário.

Também foi feita uma pesquisa exploratória, cuja finalidade é levantar questionamentos advindos do problema da pesquisa. Nesse caso, é utilizado o método de abordagem indutiva, partindo de premissas menores para se chegar às generalidades [Lira 2008]. Desse modo, o estudo sobre o processo de criar um protocolo criptográfico para uma escritura pública de compra e venda de imóveis pode prover conhecimento, o qual contribua para solução de problemas mais abrangentes.

2.2 Estado da Arte

Alguns trabalhos descrevem como a internet vem agregando valor aos serviços dos cartórios no Brasil, como em [de Oliveira Fairbanks 2010]. Nele, o autor descreve a mudança dos cartórios paulistas face à informatização dos serviços. Mostra que alguns serviços já são oferecidos pelos cartórios paulistas e aponta ainda os benefícios e desafios oriundos da informatização. Já em [Lira 2008], um estudo de caso sobre o uso da certificação digital nos cartórios extrajudiciais de Salvador é exposto, destacando-se questionamentos levantados a respeito de autenticidade de documentos e segurança no trâmite entre computadores. Ambos os trabalhos indicam mudanças e requisitos da informatização de processos nos cartórios e consideram alguns aspectos computacionais específicos de segurança. Porém, não detalham como implementar, de forma segura, um determinado processo notarial para que seja disponibilizado na internet.

Existem diversos trabalhos que tratam da melhoria dos protocolos de assinatura digital. Um trabalho pioneiro nessa área foi desenvolvido por Adi Shamir em [Shamir 1979]. Nele, é introduzido o conceito de compartilhamento de segredos, no qual um segredo é dividido em partes e distribuído a um conjunto de participantes. Posteriormente, um determinado número mínimo de participantes, pertencentes ao conjunto, reconstrói o segredo utilizando técnicas de interpolação de polinômios. Em [Salomaa 1990] o autor descreve como compartilhar um segredo, utilizando aritmética modular e o Teorema Chinês do Resto.

Os protocolos de Shamir e Salomaa compartilham o segredo entre w participantes e o reconstitui com a participação de no mínimo t participantes. Entretanto, os protocolos propostos não consideram o direito de veto para algum participante. O direito de vetar uma assinatura digital compartilhada, em um esquema de limiar, é relevante em várias aplicações. Neste trabalho, por exemplo, para garantir que um dos participantes sempre participará na reconstrução da assinatura digital é proposto um protocolo que considera a possibilidade de veto. O participante com direito a veto é o usuário, dono da assinatura digital.

Outro protocolo que também considera o compartilhamento de segredo é proposto por [Damgård e Mikkelsen 2009]. Nesse trabalho, os autores propõem um protocolo de assinatura com base no esquema de assinatura RSA. Ele compartilha uma chave secreta com dois participantes e usa propriedades matemáticas de exponenciação em uma mesma base para a reconstrução da chave. Nesse protocolo, o direito do veto é considerado por meio de uma mensagem de confirmação da assinatura que é enviada para o usuário. Então, o usuário deve

responder positivamente caso deseje reconstruir a chave ou negativamente para vetar a assinatura e impedir a reconstrução da chave.

Já em [Vanderlei e de Queiroz 2004] é mostrado um esquema de assinatura digital tolerante à falha utilizando criptografia de limiar. Nele, os autores propõem o uso do criptosistema de compartilhamento de segredos de Shamir como forma de aumentar a segurança do armazenamento dos certificados digitais nas autoridades certificadoras de assinaturas digitais RSA, porém, não consideram o direito ao veto.

Outros exemplos de protocolos que consideram esquemas de compartilhamento de segredos com a capacidade de veto, podem ser encontrados em [Obana e Kurosawa 1996] e [Blundo et al. 1994]. Vale ressaltar que a capacidade de veto nesses artigos citados, não se refere a participantes específicos.

O protocolo proposto neste trabalho se fundamenta no esquema recomendado por [Damgård e Mikkelsen 2009], adaptando-o para dividir a responsabilidade de emitir uma assinatura digital. Ele também se fundamenta no protocolo de compartilhamento de segredos de Adi Shamir [Shamir 1979]. Porém, o compartilhamento e a reconstrução da chave secreta não utilizam propriedades matemáticas de exponenciação em uma mesma base, como é feito em [Damgård e Mikkelsen 2009], e sim na interpolação de polinômios como em [Shamir 1979]. Além disso, o protocolo proposto em [Damgård e Mikkelsen 2009] utiliza 5(cinco) participantes, sendo um deles o usuário. Também deve ser considerado que no trabalho de [Damgård e Mikkelsen 2009] não é possível que vários usuários emitam uma assinatura em conjunto. Neste trabalho, é considerado um protocolo no qual o usuário tem a capacidade de veto e o número de participantes pode ser maior que 5(cinco), acarretando, assim, maior segurança na emissão da assinatura digital.

O protocolo também utiliza um esquema de assinatura RSA, como em [Stinson 2005], [Damgård e Mikkelsen 2009], [Stallings 1999], [Stallings 2007]. A chave secreta é compartilhada através do esquema de limiar, similar ao protocolo proposto por Adi Shamir em [Stinson 2005], mas o modelo é estendido, implementando o direito ao veto para três dos participantes.

2.3 Descrição do Protocolo Proposto

O protocolo proposto nessa dissertação utiliza o criptosistema de criptografia e assinatura RSA para garantir a confidencialidade e autoria da informação. Também utiliza criptosistema de compartilhamento de segredos de limiar proposto por Adi Shamir para dividir um segredo aumentando, assim, sua segurança. Para exemplificar seu uso, é considerado o problema da emissão de uma assinatura digital em uma escritura de compra e venda de um imóvel com reconhecimento de firma e autenticação.

O protocolo se inicia quando um *Vendedor* e *Comprador* desejam formalizar seu negócio em um *Cartório* digital, por meio de uma escritura de compra e venda de imóveis. O protocolo parte do princípio de que é possível emitir uma única assinatura digital que contemple os requisitos

necessários para uma escritura dessa natureza, que são:

- O reconhecimento de firma, por autenticação, das partes envolvidas, *Vendedor* e *Comprador* pelo *Cartório* ;
- Garantia da integridade da informação contida na escritura e assinada digitalmente;
- Assinatura de testemunhas atestando a existência do negócio efetuado e representado pela escritura;

Considerando esses requisitos, a assinatura digital emitida no protocolo proposto é formada a partir da composição das assinaturas de cada participante, que são: *Comprador* , *Vendedor* e *Cartório* .

Depois de formada a assinatura digital, específica para determinada transação, ela é dividida por uma *Entidade Certificadora* confiável que estabelece o compartilhamento dessa assinatura digital entre os participantes e as *Testemunhas*.

Para assinar um documento eletrônico, como por exemplo, uma escritura de compra e venda de imóveis, todos devem apresentar suas partes, para que a assinatura seja recriada e emitida. Caso algum dos participantes não apresente a sua parte, a assinatura não pode ser emitida e, consequentemente, não é possível assinar o documento.

Alguns cuidados devem ser considerados no sentido de garantir a identificação correta de cada integrante. Assim, o protocolo garante que cada participante seja autenticado, além de não poder negar sua própria assinatura no documento.

Também é possível verificar se o documento é válido e se a assinatura ali posta pertence aos participantes.

2.4 Considerações

Para solucionar a necessidade de sigilo e confidencialidade das informações, é utilizado o esquema de criptografia e assinatura do RSA. Para aumentar a segurança do armazenamento da assinatura do usuário, ela é dividida, utilizando o esquema de compartilhamento de segredos de limiar de Adi Shamir.

A utilização desses esquemas possibilita a criação de um protocolo o qual permite o oferecimento de serviços que atualmente não são encontrados no meio digital, como no caso de uma escritura de compra e venda de um imóvel.

Sendo assim, essa dissertação propõe esse tipo de protocolo, mostrando os fundamentos necessários ao seu entendimento e construção.

Capítulo 3

Assinatura e Certificado Digital

Esse capítulo apresenta as principais diferenças entre a assinatura manuscrita, ou convencional e a digital. É mostrado que a assinatura digital é mais segura do que a convencional por utilizar algoritmos públicos de verificação baseados em fundamentos matemáticos, o que dificulta as fraudes. Também é feita uma breve introdução à certificação digital e ao modelo adotado no Brasil. São descrito ainda alguns serviços já prestados por cartórios brasileiros na internet.

O capítulo está estruturado da seguinte forma:

Na seção 3.1 é feita uma comparação entre a assinatura convencional e a digital mostrando suas vantagens e desvantagens, bem como as características e os requisitos de uma assinatura digital.

A seção 3.2 mostra a lei que regulamenta o uso do certificado digital no Brasil e o modelo de Infraestrutura de Chaves Públicas adotado. Também são conceituadas Autoridades Certificadores e de Registro, relatados os tipos de certificados digitais utilizados no Brasil e suas funcionalidades.

Já na seção 3.3 é exposto de que maneira os cartórios brasileiros estão utilizando a internet como meio de modernização em busca de um melhor atendimento aos cidadãos, oferecendo-lhes serviços através da grande rede de computadores. São elencados os principais serviços utilizados como o e-CPF e o e-CNPJ.

A seção 3.4 descreve os requisitos de uma escritura pública de compra e venda de imóveis.

Por fim, na seção 3.5 são feitas algumas considerações finais sobre o capítulo.

3.1 Assinatura Digital

O uso da assinatura digital no Brasil é, atualmente, uma realidade. Com a informatização dos processos organizacionais crescendo em ordem exponencial e o apoio governamental, o uso dessa tecnologia procura atender à necessidade de acelerar trâmites de documentos legais em todos os ramos de negócios. Sua utilização foi impulsionada, principalmente, devido às

mudanças de serviços implantadas por bancos, governos, cartórios e poderes públicos, buscando maior segurança, controle e qualidade na arrecadação de tributos [Trevisan 2009].

Alguns serviços informatizados se mostram eficientes e estão amplamente difundidos na sociedade em geral, como por exemplo, o e-mail. Outros serviços ainda são objetos de estudos como é o caso da autenticidade de documentos eletrônicos. Comprovar a autoria e a integridade de um documento não é, necessariamente, uma tarefa fácil, nem mesmo no meio convencional, como documentos físicos escritos em papel.

No geral, a informatização trouxe inúmeras vantagens como a possibilidade de copiar arquivos, modificá-los e transformá-los em outros arquivos preservando muito de suas características. Porém, essas vantagens trouxeram certas desconfianças em relação a sua autenticidade, pois também facilitou o ato de forjar e copiar documentos e suas assinaturas utilizando programas de computador. Com isso, tornou-se intuitivo não aceitar uma assinatura impressa por um computador como prova de sua autoria [de Oliveira Fairbanks 2010].

Quando um documento é assinado de forma manuscrita, essa assinatura é usada para especificar quem é o responsável por esse documento. A maioria das pessoas está acostumada com esse tipo de documento. E se o reconhecimento de firma é feito em cartório, aumenta-se a certeza de que a assinatura ali posta é realmente do signatário.

A assinatura digital é análoga à manuscrita com a vantagem de que o documento assinado digitalmente pode ser guardado em um meio eletrônico sem a necessidade de impressão, e ainda pode ser transmitido de um computador para outro, via internet , por exemplo. No entanto, algumas questões devem ser consideradas a respeito do uso de uma assinatura digital em relação à manuscrita.

Primeiro, a assinatura convencional é uma parte física do documento. Quando uma assinatura é feita em papel, passa a fazer parte desse documento. Não é possível removê-la sem causar danos ao documento. Já a assinatura digital não é anexada fisicamente ao documento, existe um algoritmo criptográfico que de alguma forma vincula a assinatura digital ao documento.

Segundo, a verificação de uma assinatura convencional em um documento é feita por comparação a outras assinaturas autênticas. Esse método não é muito seguro, pois nem todos são peritos grafotécnicos e dispõem de recursos para garantir a semelhança entre as assinaturas. Também, deve-se considerar a possibilidade de alguém forjar uma assinatura e se passar por outra pessoa. A assinatura digital pode ser verificada utilizando algoritmos públicos de verificação baseados em conceitos matemáticos conhecidos, o que impossibilita a fraude.

Terceiro, a cópia de uma assinatura convencional pode apresentar imperfeições, enquanto a assinatura digital é idêntica à original.

Na verdade, uma assinatura digital é um protocolo criptográfico de autenticação de um documento. Ela permite ao criador da mensagem anexar um código que atue como uma assinatura. Além do mais, são desejáveis as seguintes características segundo [Stallings 1999]:

- Deve-se verificar o remetente , a data e a hora da assinatura;

- Deve-se autenticar o conteúdo no momento da assinatura;
- Deve ser verificável por terceiros.

Com base nessas propriedades, [Stallings 1999] define os seguintes requisitos para uma assinatura digital:

- Ela precisa ser um padrão de bits que dependa da mensagem que será assinada;
- Precisa usar alguma informação exclusiva do emissor, para impedir tanto a falsificação quanto a retratação;
- Deve ser relativamente fácil produzi-la;
- Deve ser computacionalmente inviável falsificá-la, seja construindo uma nova mensagem para uma assinatura digital existente, seja construindo uma assinatura digital fraudulenta para determinada mensagem;
- Deve ser prático armazenar uma cópia da assinatura digital.

Dados tais requisitos, tem-se a necessidade da certificação digital, na qual uma entidade confiável e organizada garante a identificação do proprietário de uma assinatura digital [Stinson 2005].

3.2 Certificado Digital

A Medida Provisória 2.200/2 de 24 de agosto de 2001 instituiu a Infraestrutura de Chaves Públicas Brasileiras[1] nomeada ICP-Brasil que garante a integridade e validade jurídica, no território brasileiro, de documentos em forma eletrônica que utilizam certificados digitais [MP2.200/2 2001]. Ela garante ainda condições seguras quanto à autoria dos documentos eletrônicos assinados digitalmente.

A ICP-Brasil é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para a identificação de um usuário no meio eletrônico como a internet . O modelo dessa cadeia hierárquica adotado no Brasil foi o de certificação com raiz única, sendo o Instituto Nacional de Tecnologia da Informação - ITI a Autoridade Certificadora raiz. Ela é responsável também por credenciar ou descredenciar os demais participantes dessa cadeia [ICP-Brasil 2011]. Uma visão geral da cadeia de hierarquia definida pela ICP-Brasil pode ser visualizada na figura 3.1 a seguir.

A figura 3.1 mostra, de forma simplificada, a hierarquia do modelo de infraestrutura de chaves públicas adotado no Brasil. Compete também à Autoridade Certificadora Raiz - ITI emitir, expedir, distribuir, revogar e gerenciar os certificados digitais emitidos pelas Autoridades Certificadoras de nível imediatamente subsequente ao seu como o SERPRO, Caixa Econômica Federal, Serasa Experian, Receita Federal, CERTISIGN, Imprensa Oficial, AC-Jus, ACPR, Casa

[1] Do inglês PKI - Public Key Infraestructure.

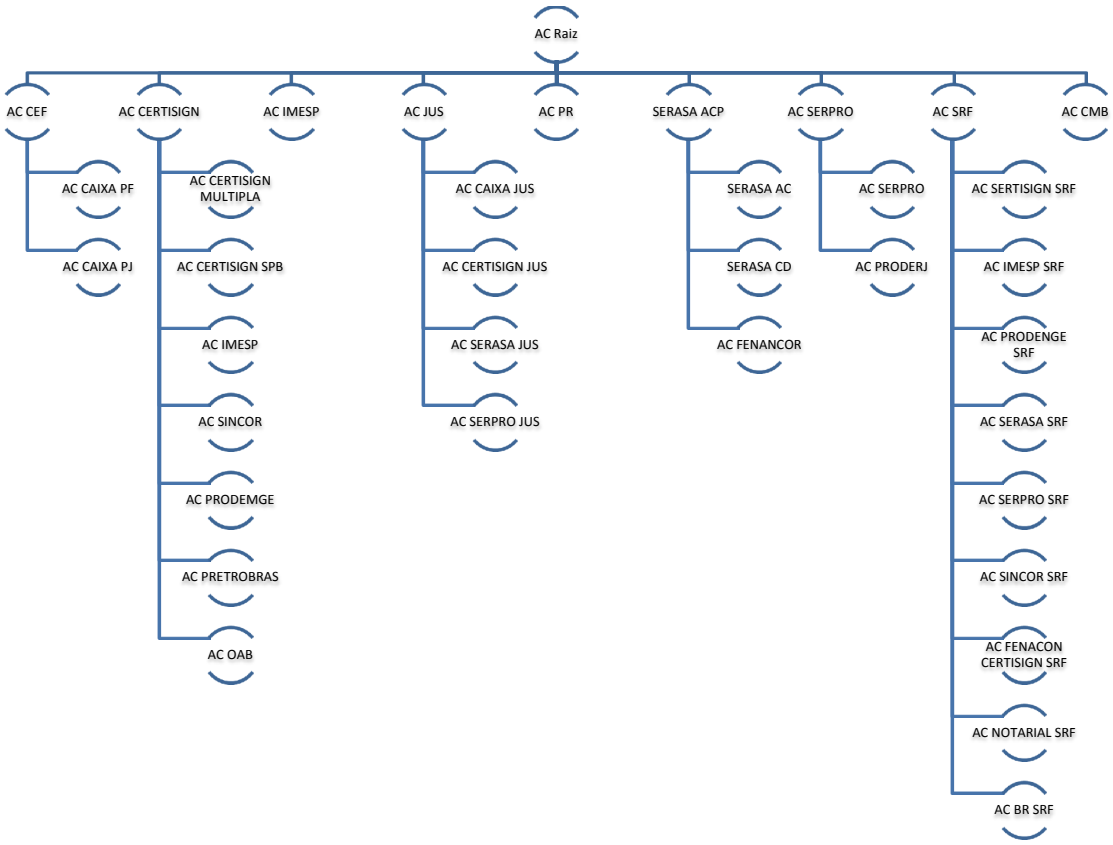


Figura 3.1: Hierarquia simplificada da ICP-Brasil [ICP-Brasil 2011].

da Moeda do Brasil, etc. [ICP-Brasil 2011]. A estrutura detalhada da ICP-Brasil pode ser encontrada em [ICP-Brasil 2011].

Já às Autoridades de Certificadoras - ACs subordinadas à ICP-Brasil, compete emitir, gerenciar e revogar certificados para uma comunidade de usuários finais. A AC assume as tarefas de autenticação desses usuários finais. Esses serviços também podem ser executados por terceiros, devidamente habilitados pela ICP-Brasil, denominados Autoridades Registradoras - ARs. Essas entidades são subordinadas às suas respectivas ACs. Uma AR pode servir como uma entidade intermediária entre uma AC e seus usuários finais, ajudando a AC em suas funções rotineiras para o processamento do certificado [Burnett e Paine 2002].

O uso do certificado digital em documentos eletrônicos identifica a assinatura digital de uma pessoa e garante validade jurídica aos atos praticados com seu uso. É um artifício computacional que permite que transações virtuais as quais demandam identificação inequívoca de um indivíduo ocorram com segurança.

Um documento eletrônico assinado digitalmente tem sua validade conferida automaticamente pelo computador através de programas de assinatura digital. Esses contêm a capacidade de verificar a validade do certificado digital por meio da lista de certificados disponibilizados pela ICP-Brasil. Os certificados podem ser revogados por diversos motivos, por exemplo, se um usuário reportar um roubo de sua assinatura digital, ou destruição de seu dispositivo de armazenamento ou mesmo se tiverem seu prazo de validade vencido.

Também podem verificar a integridade do documento eletrônico garantindo assim, que ele não foi alterado após a sua assinatura. Pode-se afirmar que um documento eletrônico, após assinado digitalmente, não pode mais ser alterado, pois isso acarretaria a alteração da composição dos elementos do documento e sua integridade estaria comprometida. Vale ressaltar ainda que um documento devidamente assinado digitalmente pode receber novas assinaturas.

Outra característica do certificado digital é o carimbo de tempo. Com ele, é possível determinar exatamente o período de validade da assinatura digital. Novamente, fazendo uma analogia com a assinatura manuscrita, essa é uma característica fundamental, pois é mais difícil determinar a data da assinatura de um documento em papel, ou mesmo descobrir se o documento foi datado após a sua assinatura. Segundo [de Oliveira Fairbanks 2010] é comum a solicitação de reconhecimento de firma em documentos com o intuito de obter prova de que o documento já existia em determinada data. Nesse caso, apesar de o processo de reconhecimento de firma valer apenas para a comprovação da autoria do documento, é utilizado para resguardar também a data. Essa prova é obtida, em certa medida, pela fé pública .

Em sua forma mais básica, um certificado contém uma chave pública, a identidade da pessoa a qual ele pertence e o nome da parte que está atestando a validade dos fatos. A figura 3.2 ilustra a estrutura básica dos campos de um certificado padrão X.509 versão 3. Esse é o formato de certificado mais amplamente aceito [Burnett e Paine 2002] e foi publicado segundo a rfc2459 pela *Internet Engineering Task Force* - IETF [Housley et al. 1999] para todas as suas versões. Esse padrão, em sua versão 3(três), é o modelo adotado no Brasil [Prodemge 2011].

A estrutura do certificado padrão X.509 mostrado na figura 3.2 aponta quais informações compõem o certificado. Os significados de seus campos são descritos conforme [Burnett e Paine 2002]:

- **Versão**: diferencia as sucessivas versões do certificado;
- **Número serial de certificado**: contém um número inteiro único em cada certificado gerado pela AC;
- **Identificador do algoritmo de assinatura**: indica o identificador do algoritmo utilizado para assinar o certificado juntamente com quaisquer parâmetros associados;
- **Nome do emissor**: identifica o nome distinto com o qual a AC cria e assina o certificado;
- **Validade - não antes/não depois**: contém valores de data/hora. Define o período de tempo em que o certificado é considerado válido, a menos que seja revogado;
- **Nome do sujeito**: identifica a entidade final a que o certificado se refere, ou seja, é o sujeito que mantém a chave privada correspondente;
- **Informações sobre a chave pública do sujeito**: contém o valor da chave pública do sujeito, bem como o identificador de algoritmo e quaisquer parâmetros associados ao algoritmo pelos quais a chave deve ser utilizada;

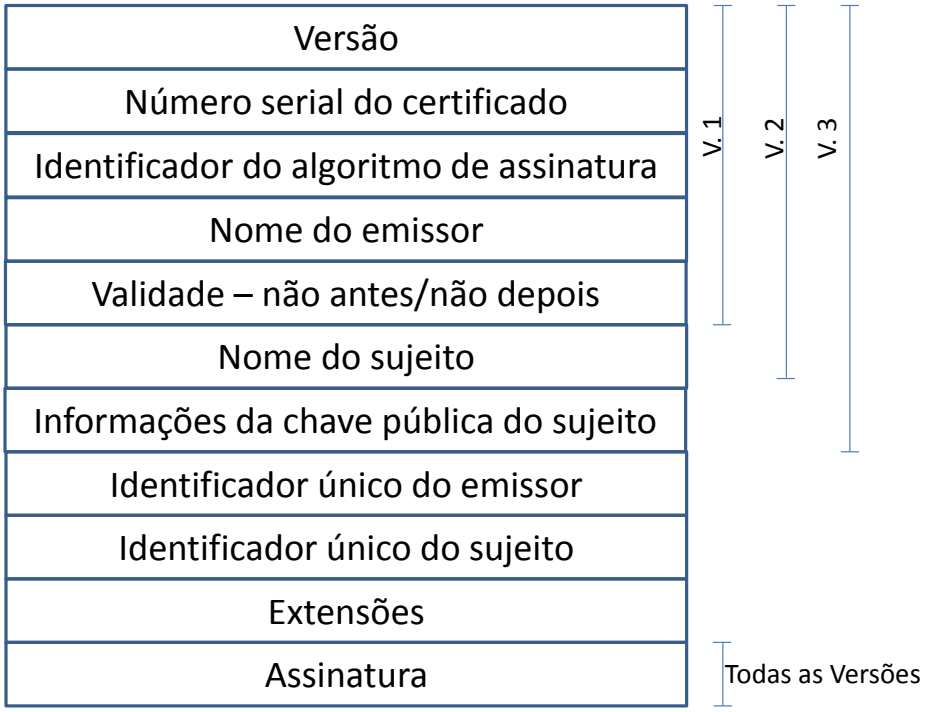


Figura 3.2: Estrutura do Certificado X.509 [Burnett e Paine 2002]

- **Identificador único do emissor**: contém um identificador único que é utilizado para exibir de maneira não-ambígua o nome X.500 da AC. A utilização desse campo não é recomendada conforme a rfc 2459 [Housley et al. 1999];
- **Identificador único do sujeito**: contém um identificador único que é utilizado para exibir de maneira não ambígua o nome X.500 do proprietário do certificado. A utilização desse campo não é recomendada conforme a rfc 2459 [Housley et al. 1999];
- **Extensões**: abrangem informações sobre a política, a chave, os atributos de sujeito e de emissor e as restrições do caminho de certificação;
- **Assinatura**: Assinatura da Autoridade Certificadora.

Os certificados digitais são classificados em tipos de acordo com seu dispositivo de armazenamento e prazo de validade.

A ICP-Brasil dispõe de duas categorias de certificados digitais, **A** e **S** sendo cada uma dividida em quatro tipos, respectivamente: **A1**,**A2**,**A3** e **A4**; **S1**,**S2**,**S3** e **S4**. A categoria A tem como finalidade a identificação e autenticação, já a categoria S, atividades sigilosas, que são definidas, conforme [Alecrim 2009], a seguir:

- **A1** e **S1**: tipo de certificado em que o par de chaves gerado pelo titular por meio de um *software* pode ser armazenado em discos rígidos ou em mídias. O prazo de validade é de um ano. O tamanho mínimo da chave é de 1024 *bits*;

- **A2** e **S2**: tipo de certificado em que o par de chaves gerado pelo titular por meio de um *software* pode ser armazenado em cartão inteligente (*chip*) ou *token* (*pendrive* ou cartões de memória). O prazo de validade é de um ano. O tamanho mínimo da chave é de 1024 *bits*;
- **A3** e **S3**: tipo de certificado em que o par de chaves gerado por *hardware* pode ser armazenado em cartão inteligente (*chip*) ou *token* (*pendrive* ou cartões de memória). O prazo de validade é de três anos. O tamanho mínimo da chave é de 1024 *bits*;
- **A4** e **S4**: tipo de certificado em que o par de chaves gerado por *hardware* pode ser armazenado em cartão inteligente (*chip*) ou *token* (*pendrive* ou cartões de memória). O prazo de validade é de três anos. O tamanho mínimo da chave é de 2048 *bits*.

Os tipos de certificados **A1** e **A3** são os mais comercializados [Lira 2008], sendo o primeiro armazenado no computador do usuário e o segundo em **smartcards** ou **tokens** protegidos por senha. Vale ressaltar que os certificados podem ser adquiridos por pessoas físicas e jurídicas.

De posse dos certificados digitais, usuários, empresas e órgãos governamentais podem usufruir de uma série de serviços disponibilizados na internet , garantindo assim, sua identificação ao registrar sua assinatura em algum documento. Também com intuito de agilizar seus serviços e manter a segurança, os cartórios já utilizam a certificação digital em suas atividades notariais.

3.3 Cartório Digital

A evolução do comércio eletrônico alavancou a economia digital. Esse fato se deve à garantia de segurança oferecida nas transações eletrônicas e na eficácia jurídica dos documentos digitais. Porém, o uso da internet como meio de transmissão de informações contábeis e fiscais à Receita Federal, alavancou o uso do certificado digital.

O titular de um certificado digital pode usufrui, atualmente, de vários serviços oferecidos, por órgãos governamentais ou privados como:

- **e-CAC**: Centro Virtual de Acesso ao Contribuinte que disponibiliza a maioria dos serviços oferecidos pela Receita Federal do Brasil para proprietários do e-CPF ou e-CNPJ;
- **SPED**: Sistema Público de Escrituração Digital que permite o envio de Escrituração Fiscal Digital - EDF e informações fiscais à Receita Federal utilizando também um e-CPF ou e-CNPJ;

Além desses, vários outros serviços estão disponíveis como o Sistema de Pagamento Brasileiro - SPB, o Serviço de Documentos Oficiais - SIDOF, etc.

Nesse contexto, a utilização dos certificados digitais por órgãos públicos como os cartórios brasileiros, não só facilita suas próprias atividades tornando-as mais ágeis e seguras como também transmite à população brasileira o sentimento de confiança nessa nova tecnologia.

A Associação dos Notários e Registradores - Anoreg, por meio de de convênio com o Serpro, Autoridade Certificadora, criou quatro Autoridades de Registro em seu nome a fim de dispor de soluções para melhoria dos serviços dos cartórios brasileiros [Lira 2008]. Afirma ainda que a certificação digital tem sido bastante útil não somente nas autenticações digitais oferecidas, mas também como auxílio no melhor tráfego de informações.

Alguns serviços como a Consulta Eletrônica são acessíveis ao cidadão que possui um certificado do tipo A3. A Consulta Eletrônica permite localizar imóveis e outros direitos reais registrados nos cartórios integrantes do sistema de Registradores Imobiliários do Estado de São Paulo [de Oliveira Fairbanks 2010]. A busca apenas informa os números de matrículas e informações sobre os imóveis . Também é possível acompanhar o trâmite do título de registro de um imóvel, ou mesmo consultar as firmas abertas em determinados cartórios.

Em outros cartórios, são oferecidos serviços pela internet como notificação digital, registros de documentos eletrônicos, assinatura digital de e-mail, emissão do sinal público, emissão do selo digital, certidão digital, dentre outros serviços, inclusive o de emissão de um certificado digital para uma empresa ou cidadão.

Em relação à proposta desta dissertação, que é um protocolo de reconhecimento de firma por autenticidade, como no caso de escritura pública de compra e venda de imóveis, não foi encontrado serviço dessa natureza oferecido por cartórios no meio digital.

No entanto, existe um projeto para modernização dos cartórios de registros de imóveis da Amazônia Legal sendo desenvolvido pela Escola Politécnica da Universidade de São Paulo - USP em parceria com o Conselho Nacional de Justiça, Ministério de Desenvolvimento Agrário, a Advocacia Geral da União e o Tribunal do Estado do Paraná e a Fundação Biblioteca Nacional. Esse projeto prevê a especificação de um modelo de sistema digital para modernizar o serviço de registro de imóveis por meio de Sistema de Registro Eletrônico para Cartórios de Registro de Imóveis [CNJ 2011]. Contudo, não provê o reconhecimento de firma por autenticação, muito menos a informatização de uma escritura pública de compra e venda.

3.4 Escritura Pública de Compra e Venda de Imóvel

A escritura pública pode ser definida como um documento elaborado em um cartório, representando a declaração de vontades das partes envolvidas [Araújo 2010]. Para que uma escritura pública seja lavrada em cartório, é necessária a presença física das partes envolvidas perante o tabelião responsável, que atesta a livre vontade das partes por intermédio desse documento.

Particularmente, no caso de uma escritura pública de compra e venda de imóveis devem constar os dados pessoais das partes que firmam o negócio de compra e venda, como nome, nacionalidade, estado civil, RG, CPF de tal forma que as partes possam ser plenamente identificadas. Também é preciso a matrícula do imóvel devidamente registrada no livro do cartório de registro de imóveis e a descrição do imóvel [Duckworth 2011]. Além dos documentos de identificação das partes, e do imóvel, após a lavratura da escritura, assinam as partes envolvi-

das: o vendedor, o comprador e o tabelião, atestando o registro da escritura e a fé pública na veracidade das informações contidas na escritura. Além disso, também assinam a escritura pelo menos duas testemunhas.

Nesse contexto, para reproduzir em meio digital, o serviço de escrituração pública, mais precisamente o de compra e venda de imóvel, são necessários aparatos tecnológicos que fundamentem e representem fielmente todos os requisitos de identificação das partes envolvidas. Por se tratar de um documento que exige diversas assinaturas perante o tabelião, é preciso que todas as autorias sejam atestadas e confirmadas por autenticidade.

Nesta dissertação é proposto um protocolo que efetua de forma digital todo o processo de assinatura de uma escritura de compra e venda de imóvel. Dessa forma, são necessários, em um meio digital:

1. O reconhecimento digital de firma por autenticidade, por um cartório, da assinatura do vendedor e do comprador.
2. A escritura deve, também, conter a assinatura digital de testemunhas.

Neste trabalho é proposto um protocolo que representa o análogo digital do processo de assinatura de uma escritura de compra e venda de imóveis. As identificações das partes envolvidas, inclusive o tabelião, são atestadas e garantidas com o uso de assinaturas digitais devidamente certificadas por órgãos subordinados, por exemplo, a ICP-Brasil. A responsabilidade da emissão da assinatura digital é compartilhada por todos os envolvidos, conforme detalha o capítulo 5 dessa dissertação.

3.5 Considerações

A utilização de certificados digitais pelos cartórios impulsiona a utilização dessa tecnologia, promovendo uma verdadeira evolução cultural. As pessoas se sentem mais confiantes para adquirir e utilizar seus dados pessoais como, por exemplo, o e-CPF.

Além do mais, alguns serviços tornam-se mais ágeis e a presença física do cidadão no cartório acaba sendo evitada, diminuindo assim as filas. No entanto, ainda existem muitos serviços prestados pelos cartórios que não possuem seu análogo digital, como é o caso da escritura pública para compra e venda de imóveis.

Capítulo 4

Fundamentos Criptográficos

Neste capítulo são apresentados os fundamentos matemáticos da criptografia utilizados em assinatura digital. É, também, analisada a segurança de tais sistemas de assinatura às ameaças advindas de um ambiente inseguro. Tais fundamentos formam a base conceitual e de notação necessários para o desenvolvimento do protocolo proposto no capítulo 5.

O capítulo está estruturado da seguinte forma: Na seção 4.1 são mostrados os tipos de ameaças existentes em um ambiente digital. Já na seção 4.2 é definida a notação utilizada nessa dissertação. Na seção 4.3 é explicado o funcionamento do criptosistema RSA. Na seção 4.4 são expostos conceitos e fundamentos criptográficos sobre assinatura digital. A seção 4.5 fundamenta um protocolo criptográfico para compartilhar segredos. Finalmente, na seção 4.6, o capítulo é concluído.

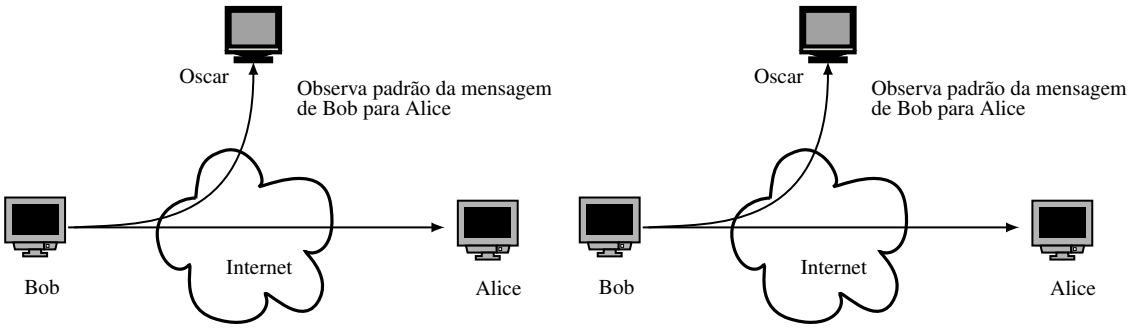
4.1 Segurança da Informação

Em um ambiente de rede podem ser transmitidos documentos sigilosos, oriundos de empresas, organizações, governos, etc. Enfim, arquivos digitais que só devem ser acessados pelos seus reais destinatários. O meio de transmissão desses arquivos, na maioria das vezes, é a internet, caracterizada por ser um ambiente público e sem restrições. Sendo assim, essas transmissões estão sujeitas a ameaças do meio digital cujos ataques se classificam em ataques passivos e ativos [Stallings 2007].

Nos ataques passivos, não há modificação do conteúdo nas mensagens ou documentos. Eles são geralmente de espionagem, ou monitoramento de uma transmissão. As figuras 4.1a e 4.1b ilustram o cenário de ataques passivos.

Na figura 4.1a *Oscar* lê o conteúdo da mensagem que *Bob* enviou para *Alice*. Já na figura 4.1b *Oscar* não consegue visualizar o conteúdo da mensagem que *Bob* enviou para *Alice*, pois ela foi disfarçada. Então ele observa e analisa os padrões das mensagens enviadas para tentar descobrir seu significado.

Nos ataques ativos, têm-se modificações no fluxo das mensagens ou criação de mensagens



(a) Liberação de Conteúdo (b) Análise de tráfego

Figura 4.1: Os Dois Grupos de Ataques Passivos [Ashidani 2009]

falsas. Esses se classificam em disfarce, repetição, modificação de mensagens e negação de serviço, como ilustra a figura 4.2.

Um ataque de disfarce ocorre quando um indivíduo finge se passar por outro, e envia mensagens como mostra a figura 4.2a.

A repetição envolve a captura passiva de mensagens e posteriormente sua retransmissão, como mostra a 4.2b.

Na modificação de mensagens, o intruso captura e modifica as mensagens a serem enviadas a seu destinatário, como mostra a figura 4.2c.

A negação de serviços impede ou dificulta o uso dos serviços de rede. Esse ataque pode ter como alvo a interrupção inteira de uma rede, seja desativando-a ou sobrecarregando-a com mensagens, conforme a figura 4.2d.

Para prover a segurança em relação aos ataques expostos na figura 4.2d, existem alguns serviços de segurança existentes: confidencialidade, autenticação, integridade e irretratabilidade [Stallings 1999], [Stallings 2007].

A confidencialidade é uma proteção em relação à transmissão de dados em um ataque passivo. Deve ser utilizada quando há a necessidade de proteger o segredo das informações em uma mensagem. É a garantia de que a mensagem será acessada somente pelo seu destinatário.

A autenticação é a garantia de que a comunicação entre as partes seja corretamente identificada e que haja certeza sobre a identidade dos participantes. É um tipo de proteção contra ataque de disfarce.

A integridade garante que a mensagem não seja alterada ao ser transmitida para o destinatário, ou seja, fornece proteção contra modificações não autorizadas. A mensagem enviada pelo remetente deve ser exatamente a mesma acessada pelo destinatário. A integridade protege contra ataques do tipo modificação.

A irretratabilidade é a garantia de que o remetente não pode negar a criação de uma informação transmitida. Esse serviço protege contra ataques do tipo negação.

Os ataques passivos e ativos têm características opostas. Os passivos são difíceis de detectar, mas existem medidas para impedir que eles aconteçam. Por outro lado, é muito difícil impedir que os ativos aconteçam, pois isso exigiria proteção física de todos os meios de comunicação

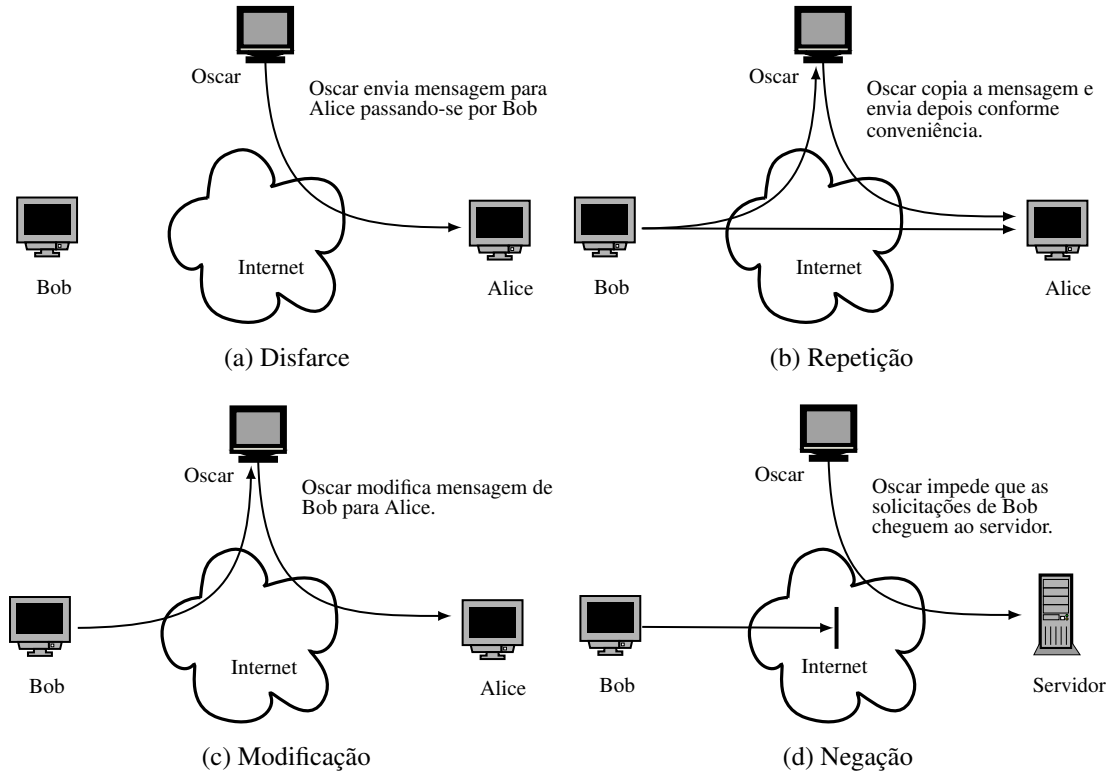


Figura 4.2: Os Quatro Grupos de Ataques Ativos [Ashidani 2009]

a todo instante. Em vez disso, pode-se detectar e corrigir interrupções ou atrasos causados por eles. [Stallings 1999]

A criptografia é um método para se prevenir de determinadas ameaças passivas e ativas. Através de seus fundamentos matemáticos, criam-se protocolos que garantem sigilo, autenticidade, autenticação e a irretratabilidade. O objetivo fundamental da criptografia é permitir que duas pessoas se comuniquem com segurança através de um meio de transmissão inseguro. Por exemplo, permitir que *Alice* e *Bob* possam se comunicar utilizando a internet onde *Oscar*, o intruso, não pode compreender as mensagens trocadas entre eles. Dentre os muitos algoritmos criptográficos existentes, optou-se por utilizar nessa dissertação, o algoritmo de criptografia RSA, por se mostrar um dos mais difundidos nesse meio. Porém, não há como defini-lo sem antes estabelecer a notação para protocolos criptográficos utilizada nessa dissertação, haja vista que não existe um padrão.

4.2 Notação

Nessa dissertação é considerada a seguinte notação:

$ID \rightarrow$ Identificador único

$(\phi) \rightarrow$ Função de Euler. Dado n, (ϕ) é igual ao número de inteiros positivos menores que n

e relativamente primos a n [Stallings 2007].

$mdc(a,b) \rightarrow$ *Máximo divisor comum* entre a e b [Shoup 2008]. Nesse trabalho, é utilizada a versão estendida do algoritmo de Euclides para calcular mdc(a,b), [Stinson 2005]. Tal algoritmo também pode calcular o inverso multiplicativo de um número.

$\kappa \rightarrow$ Denota um conjunto finito de chaves.

$K \rightarrow$ Denota uma chave.

$KR \rightarrow$ Denota uma chave privada ou secreta.

$KU \rightarrow$ Denota uma chave pública.

$m \rightarrow$ Denota uma mensagem ou texto claro.

$M \rightarrow$ Denota um conjunto finito de mensagens ou textos claros m.

$c \rightarrow$ Denota uma mensagem ou texto cifrado.

$P \rightarrow$ Denota um conjunto de participantes.

$A \rightarrow$ Denota um conjunto finito de assinaturas.

$y \rightarrow$ Denota a assinatura de um documento m.

$T \rightarrow$ Denota um conjunto de *Testemunhas*.

$E(K,m) \rightarrow$ Denota uma função que criptografa um texto claro ou mensagem m utilizando a chave K, produzindo um texto cifrado c.

$D(K,c) \rightarrow$ Denota uma função que descriptografa um texto cifrado c, utilizando a chave K e produzindo um texto decifrado ou mensagem m.

$sig(K,m) \rightarrow$ Função responsável por criar a assinatura y no documento m, utilizando a chave K.

$ver(K,y) \rightarrow$ Função responsável por verificar a validade da assinatura y no documento m, utilizando a chave K.

4.3 O Criptosistema RSA

Um dos algoritmos de chave pública mais utilizados é o algoritmo RSA. Em 1977, Ron Rivest, Adi Shamir e Leonard Adleman inventaram este Criptositema [Rivest et al. 1978] O esquema do RSA é uma cifra de bloco em que o texto claro e o texto cifrado são inteiros entre 0 e $n - 1$, para algum n [Stallings 2007]. Na prática, portanto, o primeiro passo é transformar o texto a ser cifrado em números. Isso pode ser feito utilizando algum código padrão como o ASCII.

Segundo [Rivest et al. 1978], [Ashidani 2009], [Stinson 2005] o algoritmo RSA é dado por:

1. Escolher dois números primos aleatórios p e q;
2. Calcular $n = p \times q$;
3. Calcular a função tociente de Euler $\phi(n)$;
4. Escolher um número aleatório $b < \phi(n)$ tal que o $mdc(b, \phi(n)) = 1$ e calcular um inteiro a de tal maneira que:
   $a \times b \equiv 1 \bmod \phi(n)$
5. Chave pública = $KU = (n, b)$
6. Chave privada = $KR = (n, a)$
7. Cifrar
   Dado $m \in Z_n$
   $c \equiv m^b \bmod n$
8. Decifrar
   $m \equiv c^a \bmod n$

Figura 4.3: Algoritmo RSA [Rivest et al. 1978]

Para cifrar um texto claro m usando o método descrito no algoritmo RSA, primeiramente deve-se escolher dois números primos p e q suficientemente grandes. Posteriormente, deve-se calcular o número de inteiros positivos menores que n e relativamente primos de n, usando a função de Euler:

$$\phi(n) = (p - 1)(q - 1).$$

É necessário escolher aleatoriamente um número b, tal que $b < \phi(n)$ e relativamente primo com $\phi(n)$. Então, b é a chave pública KU utilizada para cifrar o texto claro m. A partir de b, calcula-se o número a tal que $ab \equiv 1 \bmod \phi(n)$. Esse cálculo pode ser feito com o algoritmo de Euclides estendido, usando como parâmetros de entrada b e $\phi(n)$. O número a é, então, utilizado para decifrar um texto criptografado, e é denominado chave privada.

Um texto claro m é cifrado em c, tal que, $c = m^b \bmod n$. Portanto, c representa o texto claro, m, cifrado. Para decifrar c e obter, novamente, m, utiliza-se a expressão: $m = c^a \bmod n$.

O fato de a e b serem inversos multiplicativos módulo n é o que possibilita a cifragem usando o número b e a decifragem usando o número a. A correção desse processo ocorre porque:

$$\begin{aligned} m = c^a \bmod n &\Leftrightarrow (m^b)^a (\bmod n) \\ &\Leftrightarrow m^{ba} \bmod n \\ &\Leftrightarrow m^{ab} \bmod n \end{aligned}$$

Mas como b é o inverso multiplicativo de a módulo (n), então

$$ab = 1 + k\phi(n) = 1 + k(p-1)(q-1)$$

Logo,

$$\begin{aligned} m^{ab} \bmod n &= m^{1+k(p-1)(k-1)} \bmod n \\ &= m^1 m^{k(p-1)(q-1)} (\bmod n) \end{aligned}$$

mas pelo teorema de Fermat [Stallings 2007]

$$m^{k(p-1)(q-1)} \equiv m^{(p-1)(q-1)} \equiv 1 \bmod n$$

Portanto

$$c^a \equiv m \bmod n$$

é a prova da correção do algoritmo RSA. Um exemplo de utilização do RSA é apresentado a seguir.

4.3.1 Exemplo de uso do Algoritmo RSA

Este exemplo considera a cifragem e decifragem de um texto utilizando o algoritmo RSA.

Suponha que *Alice* deseja cifrar o texto claro (caractere) "X" e enviá-lo para *Bob* de forma que somente *Bob* consiga decifrá-lo. O primeiro passo é transformar o texto a ser cifrado em uma sequência de dígitos numéricos. O correspondente ao texto "X" em um número decimal, segundo a tabela ASCII é 88.

Para que *Alice* possa cifrar um texto claro e enviá-lo para *Bob*, ela necessita da chave pública KU de *Bob*, que deve ser calculada e publicada antecipadamente, da seguinte forma:

Suponha que o algoritmo RSA utilizado por *Alice* e *Bob* tenha os parâmetros:

$$p = 4.027 \text{ e } q = 3.373$$

Então, *Bob* calcula n e $\phi(n)$.

$$n = p \times q = (4.027) \times (3.373) = 13.583.071$$

e

$$\phi(n) = (p-1) \times (q-1) = (4.027-1) \times (3.373-1) = 13.575.672$$

Bob escolhe, de forma aleatória, um número b, tal que, $b < \phi(n)$ e, além disso, b é relativamente primo com $\phi(n)$. Considere;

$$b = 5.$$

Além disso, *Bob* calcula o número inteiro a, tal que $ab \equiv 1 \bmod \phi(n)$. Nesse caso,

$$a = 5.430.269$$

Ou seja, a é o inverso multiplicativo de b. Isto é, $a = b^{-1} \bmod \phi(n)$.
Bob, então, publica para *Alice* os valores de sua chave pública KU.

$$\begin{aligned} KU &= (n, b) \\ &= (13.583.071, 5) \end{aligned}$$

Bob armazena secretamente os valores de sua chave privada KR.

$$\begin{aligned} KR &= (n, a) \\ &= (13.583.071, 5.430.269) \end{aligned}$$

De posse da chave pública de *Bob*, *Alice* envia para *Bob*, o texto claro 88 na forma cifrada, garantindo a confidencialidade da informação.
Alice, então, calcula c, como indicado a seguir, e o envia para *Bob*.

$$\begin{aligned} c &= m^b \bmod n \\ &= 88^5 \bmod 13.583.071 = 7.087.620 \end{aligned}$$

Bob recebe o texto cifrado c de *Alice* e o decifra utilizando sua KR, da seguinte forma:

$$c^a \bmod n = 7.087.620^{5.430.269} \bmod 13.583.071 = 88$$

O protocolo mostrado na figura 4.4 indica o processo de definição do par de chaves pública e privada de *Bob*.

Definição de KU e KR de *Bob*
Entrada: $p = 4.027$, $q = 3.373$, $b = 5$

1. Calcula n:
$$n = p \times q = 4.027 \times 3.373 = 13.583.071$$
2. Calcula $\phi(n)$:
$$\phi(n) = (p-1) \times (q-1) = (4.027-1) \times (3.373-1) = 13.575.672$$
3. Calcula a
$$a = b^{-1} \bmod \phi(n) = 5^{-1} \bmod \ = 13.575.672 = 5.430.269$$
4. Calcula KU_{Bob}:
$$KU_{Bob} = (n, b) = (13.583.071, 5)$$
5. Calcula KR_{Bob}:
$$KR_{Bob} = (n, a) = (13.583.071, 5.430.269)$$

Figura 4.4: Definição do par de chaves de *Bob*: *Bob* define seu par de chaves KU e KR

O protocolo da figura 4.5 mostra o processo de cifragem e decifragem entre *Alice* e *Bob*:

Alice (cifragem)	*Bob* (decifragem)
Entrada: $m = 88, b = 5, n = 13.583.071$	
1. Calcula c $c = 88^5 \bmod 13.583.071 = 7.087.620$ 2. Envia c para *Bob*	3. Recebe c e calcula m $m = 7.087.620^{54.30.269} \bmod 13.583.071 = 88$

Figura 4.5: *Alice* envia texto cifrado e *Bob* decifra-o.

4.3.2 Características do RSA

Uma característica do uso do algoritmo do RSA diz respeito ao processo de geração do par de chaves, respectivamente a chave pública KU e a chave privada KR. Esse processo depende diretamente da escolha dos números aleatórios a e b, conforme mostrado na linha 4 da figura 4.3, que descreve o algoritmo RSA. Nessa linha é definida a escolha de um número aleatório b, tal que, $b < \phi(n)$ e $mdc(b, \phi(n)) = 1$. Além disso, deve-se calcular um inteiro a de tal maneira que: $ab = 1 \bmod \phi(n)$;

O número b escolhido faz parte da chave pública e é definido, a princípio, como qualquer número menor que $\phi(n)$ e relativamente primo a $\phi(n)$. Já o cálculo de a, depende do número b escolhido, pois ele é o inverso multiplicativo de a módulo $\phi(n)$. Por questões de segurança, a escolha de a, não é inteiramente aleatória e deve satisfazer um conjunto de quesitos como é analisado em [Bellare e Rogaway 2005].

Para determinar o inverso multiplicativo de um número, pode-se utilizar o Algoritmo de Euclides estendido. Em sua forma básica, esse algoritmo calcula o *máximo divisor comum* de dois números inteiros positivos.

Sejam $a, b \in \mathbb{Z}$. Um inteiro d é um máximo divisor comum de a e b se [Scheinerman 2011]:

- d é um divisor comum de a e b e;
- se e é um divisor comum de a e b então $e \leq d$.

O *máximo divisor comum* de a e b, denotado por $mdc(a, b)$, é o maior inteiro que divide, sem resto, a e b. O algoritmo de Euclides pode ser encontrado em [Shoup 2008]. Contudo, existe uma extensão do algoritmo apresentada em [Stinson 2005] que calcula também o inverso multiplicativo de um número e é descrito na figura 4.6:

Um exemplo de utilização desse algoritmo é mostrado na tabela 4.1 que considera a operação de geração de uma chave secreta a partir de uma chave pública, escolhida conforme exemplo do uso do algoritmo RSA mostrado anteriormente.
Considere, então,

$$a = \phi(n) = 13.575.672$$

e

$$b = 5$$

Nesse caso, o objetivo é determinar o inverso multiplicativo de b módulo $\phi(n)$. Na Tabela 4.1, as colunas representam, respectivamente,

$Seq.$ = nº da iteração do algoritmo;

a= valor de $\phi(n)$ calculado anteriormente e definido como módulo;

b = número escolhido aleatoriamente definido como chave pública no algoritmo RSA;

Algoritmo Estendido de Euclides.
Entrada: (a, b)

$a_0 \leftarrow a$
$b_0 \leftarrow b$
$t_0 \leftarrow 0$
$t \leftarrow 1$
$q \leftarrow \lfloor \frac{a_0}{b_0} \rfloor$
$r \leftarrow a_0 - q \times b_0$
Enquanto $r > 0$

faça
$temp \leftarrow (t_0 - q * t) \bmod a$
$t_0 \leftarrow t$
$t \leftarrow temp$
$a_0 \leftarrow b_0$
$b_0 \leftarrow r$
$q \leftarrow \lfloor \frac{a_0}{b_0} \rfloor$
$r \leftarrow a_0 - q \times b_0$

Se $b_0 \neq 1$
então não existe inverso multiplicativo de b módulo a
senão retorne (t, r)

Saída: t, r

Figura 4.6: Algoritmo de Euclides Estendido [Stinson 2005]

t_0 = variável utilizada para cálculos no algoritmos;

t = inverso multiplicativo de b;

q = quociente inteiro da divisão de $\frac{a}{b}$;

r = resto da divisão de $\frac{a}{b}$;

A iteração do algoritmo para quando o resto da divisão for 0 é:

Entrada (a, b)

Seq.	a	b	t_0	t	q	r
0	13.575.672	5	0	1	27.15.134	2
1	5	2	1	108.60.538	2	1
2	2		108.60.538	5.430.269	2	0

Saída (t)

Tabela 4.1: Cálculo do inverso multiplicativo de 5 mod 13.575.672

A tabela 4.1 mostra o cálculo do algoritmo e o valor de cada variável durante as 3 iterações necessárias para o cálculo do inverso multiplicativo de 5 mod 13.575.672. O resultado é igual a 5.430.269. Diz-se então que 5.430.269 é o inverso multiplicativo de 5 módulo 13.575.672. E, conforme o algoritmo do RSA, a é a chave privada e b a chave pública.

Outras características do uso do algoritmo do RSA dizem respeito à complexidade da computação exigida. Como sua segurança está baseada na dificuldade de se fatorar o número n

em p e q, [Campello e Leal 2007], deve-se utilizar números inteiros grandes para tornar essa fatoração impraticável.[1]

Além disso, no RSA, tanto a criptografia quanto descriptografia envolvem elevar um inteiro a uma potência inteira mod n. Caso o resultado dessa exponenciação fosse feita sobre os inteiros e depois reduzida a mod n, números gigantescos seriam gerados. Para tornar os cálculos mais eficientes é utilizado o método de elevação ao quadrado repetida [Cormen 2002]. Esse método calcula de forma eficiente uma operação do tipo a^b mod n, utilizando a representação binária de b.

Considere, então,

$$\{b_k, b_{k-1}, \cdots, b_1, b_0\}$$

a representação binária de b. Nesse caso, a representação binária tem $k + 1$ *bits* de comprimento, na qual b_k é o *bit* mais significativo e b_0 o menos significativo. O algoritmo a seguir calcula a^b mod n. No algoritmo, o expoente é incrementado por duplicações desde 0 até b [Cormen 2002].

Entrada: (a, b, n)

$c \leftarrow 0$
$d \leftarrow 1$
Seja $\{b_k, b_{k-1}, \cdots, b_1, b_0\}$ a representação binária de b
Para $i \leftarrow k$ *downto* 0
faça
- $temp \leftarrow (t_0 - q \times t) \bmod a$
- $c \leftarrow 2c$
- $d \leftarrow (d \times d) \bmod n$
- se $b_i = 1$
- faça
  - Então $c \leftarrow c + 1$
  - $d \leftarrow (d \times a) \bmod n$

Saída d

Figura 4.7: Algoritmo *Modular-Exponentiation* (a, b, n) [Cormen 2002]

Um exemplo de utilização desse algoritmo é mostrado na tabela 4.2 a seguir, que considera a operação de descriptografia mostrada anteriormente, na qual,

$$7.087.620^{5.430.269} \bmod 13.583.071 = 88$$

Considere, portanto, que:

$a = 7.087.260$

$b = 5.430.269_{10} = 10100101101101111111101_2$

$n = 13.583.071$

Na qual as colunas da tabela representam respectivamente:

[1] A segurança do RSA é discutida no tópico 4.3.3 dessa dissertação.

$Seq.$ = nº da iteração do algoritmo;

i= comprimento da representação binária de b;

b_i = a representação binária de b;

c e d são variáveis de cálculo utilizadas no algoritmo.

Entrada (a, b, n)

$Seq.$	i	b_i	c	d
1	22	1		7.087.620
2	21	0	2	4.286.674
3	20	1	5	8.525.733
4	19	0	10	3.031.593
5	18	0	20	5.783.771
6	17	1	41	9.772.488
7	16	0	82	8.988.682
8	15	1	165	8.339.164
9	14	1	331	8.006.416
10	13	0	662	1.530.188
11	12	1	1.325	176.105
12	11	1	2.651	364.955
13	10	0	5.302	10.140.870
14	9	1	10.605	1.926.571
15	8	1	21.211	6.600.046
16	7	1	42.423	7.796.444
17	6	1	84.847	13.521.221
18	5	1	169.695	13.078.219
19	4	1	339.391	7.343.477
20	3	1	678.783	7.821.639
21	2	1	1.357.567	3.858.827
22	1	0	2.715.134	9.150.682
23	0	1	5.430.269	88

Tabela 4.2: Exemplo de execução do algoritmo *Modular-Exponentiation*

4.3.3 A Segurança do RSA

A segurança do algoritmo RSA está na dificuldade de se fatorar o número n em p e q, que são números primos grandes. Caso exista um algoritmo que consiga determinar p e q, de forma eficiente, então é possível o cálculo de $\phi(n)$, pois $\phi(n) = (p-1)(q-1)$. Isso permite determinar $a = b^{-1} (\text{mod } \phi(n))$, e a segurança do algoritmo estaria comprometida. Entretanto, até hoje não há um algoritmo de fatoração tão eficiente de modo a determinar p e q em um tempo razoável [Campello e Leal 2007].

Existe uma ameaça constante à segurança do RSA, são os ataques matemáticos produzidos por pesquisadores. Esses ataques se resumem em refinamentos dos algoritmos de fatoração

aliados ao crescente poder de processamento dos computadores atuais. A tabela 4.3 mostra a evolução dos ataques matemáticos alcançados pelos pesquisadores.

Tabela 4.3: Evolução da Fatoração

Dígitos Decimais	Número de bits	Ano	Algoritmo
110	332	1991	Crivo quadrático
110	365	1992	Crivo quadrático
120	398	1993	Crivo quadrático
129	428	1994	Crivo quadrático
130	431	1996	Crivo de corpo numérico generalizado
140	465	1999	Crivo de corpo numérico generalizado
155	512	1999	Crivo de corpo numérico generalizado
160	530	2003	Crivo de malha(*Lattice sieve*)
174	576	2003	Crivo de malha(*Lattice sieve*)
200	663	2005	Crivo de malha(*Lattice sieve*)

Fonte: [Stallings 2007]

Diante dos fatos expostos na tabela 4.3, nota-se que a segurança do algoritmo RSA depende do tamanho em *bits* da chave secreta. Porém, vale ressaltar que quanto maior a chave secreta, maior o *overhead* causado para se efetuar os cálculos para a cifragem e decifragem.

Além dos ataques matemáticos, existem ainda os ataques por força bruta, de temporização e de texto cifrado escolhido [Stallings 1999].

O ataque por força bruta consiste na tentativa de tentar todas as chaves privadas possíveis.

O ataque de temporização (*timing attack*) se baseia na análise de tempo que um computador leva para decifrar as mensagens [Kocher et al. 1999]. Na prática, a exponenciação modular não tem variações de tempo tão extremas, mas existe uma variação de tempo suficiente para tornar o ataque prático [Stallings 2007]. Apesar de esse ataque ser uma ameaça séria, algumas medidas podem ser usadas para evitá-lo, como manter o tempo de exponenciação constante ou introduzir atrasos aleatórios.

Já no ataque de texto escolhido (CCA - *chosen ciphertext attack*) um intruso escolhe diversos textos cifrados e então recebe os textos claros correspondentes. Dessa forma, o intruso pode selecionar um texto claro, criptografá-lo com a chave pública do destinatário e depois ser capaz de obter o texto claro de volta. Nesse caso, nenhuma informação nova é conseguida pelo intruso, porém permite que ele explore propriedades do RSA como:

$$E(KU, m_1) \times E(KU, m_2) = E(KU, [m_1 \times m_2])$$

Suponha que dado c, o intruso queira determinar o texto claro m, onde $c = m^b \bmod n$. Isso pode ser feito da seguinte forma:

1. Calcula-se $X = (c \times 2^b) \bmod n$
2. Envia-se X como um texto cifrado escolhido e recebe-se $Y = X^a$

Porém:

$$\begin{aligned} X &= (c \bmod n) \times (2^b \bmod n) \\ &= (m^b \bmod n) \times (2^b \bmod n) \\ &= (2m^b \bmod n) \end{aligned}$$

Portanto $Y = (2m) \bmod n$ a partir disso, o intruso pode deduzir m.

Para contornar esse ataque a RSA *Security Inc.* recomenda modificar o texto claro usando um preenchimento ideal de criptografia assimétrica (OAEP - *optimal asymmetric encryption padding*) [Pointcheval 2002].

4.4 Protocolo Criptográfico para Assinatura Digital

Para efetuar a assinatura digital, são propostos protocolos criptográficos que, em geral, utilizam a seguinte notação:

"Um participante P_i assina uma mensagem m, usando sua chave secreta KR_i, e envia m e sua assinatura $y = sig(KR_i, m)$ para o participante P_j".

Além das propriedades de uma assinatura digital, expostas no capítulo 3 dessa dissertação, um sistema de assinatura digital utiliza as definições e notações a seguir [Stinson 2005]:

Esquema de Assinatura Digital

Um esquema de assinatura é um conjunto de 5 elementos (M, A, K, S, V), no qual:

1. M é um conjunto finito de mensagens;
2. A é um conjunto finito de assinaturas;
3. κ é um conjunto finito de chaves;
4. Para cada $KR_i \in \kappa$, existe um algoritmo de assinatura $sig_k \in S$, e um algoritmo de verificação correspondente $ver_k \in V$. Os algoritmos de assinatura e verificação são funções do tipo:

$$sig_k : M \to A \text{ e } ver_k : M \times A \to verdade, falso.$$

Além disso, essas funções satisfazem as seguintes condições: para toda mensagem $m \in M$ e para toda assinatura $y \in A$

$$ver_K = \begin{cases} \text{verdade se } y = sig_K(m) \\ \text{falso se } y \neq sig_k(m) \end{cases}$$

Finalmente, um par (m, y), tal que $m \in M$ e $y \in A$ é chamada de mensagem assinada.

Figura 4.8: Protocolo de Assinatura Digital [Stinson 2005]

Em geral, um algoritmo de assinatura digital tem dois componentes: uma função para a

assinatura e outra para a verificação dessa assinatura. Essas funções são esquemas de protocolos de assinaturas, frequentemente padronizados, por exemplo, o esquema de assinatura RSA ou ElGamal [Stinson 2005].

Na prática, um usuário cria uma mensagem e a criptografa utilizando sua chave privada. A partir daí, a mensagem é transmitida ao seu destinatário. Após receber a mensagem, o destinatário, que tem acesso à chave pública do remetente, utiliza tal chave para decifrar a mensagem.

A figura 4.9 mostra *Bob* produzindo uma mensagem e assinando-a com sua chave secreta. Como todos possuem acesso à chave pública de *Bob*, todos podem decifrar a mensagem que foi criada por ele. Além do mais, todos têm a certeza de que a mensagem foi criada por ele, pois ele é o único que possui a chave secreta utilizada para cifrar a mensagem.

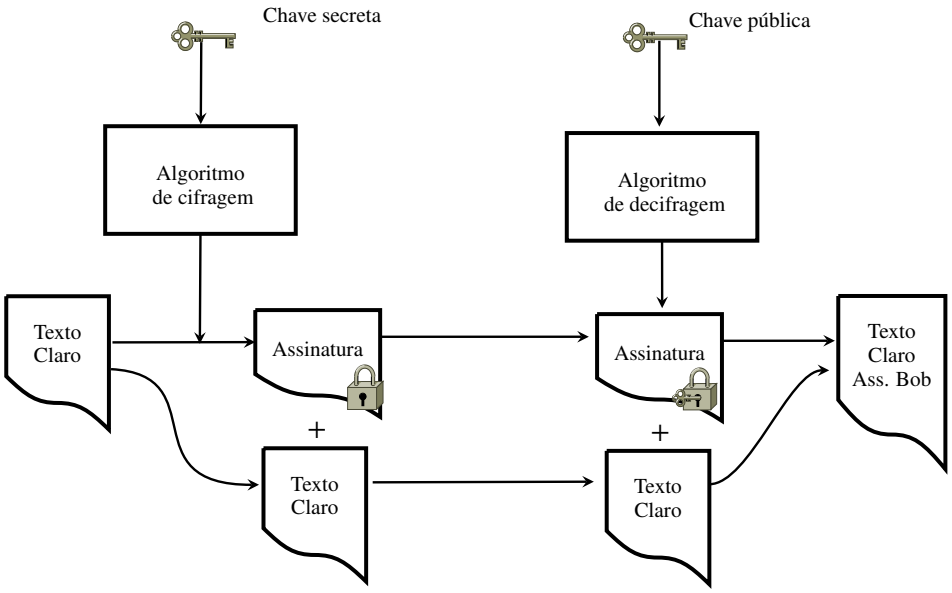


Figura 4.9: Esquema de Assinatura Digital [Ashidani 2009]

O esquema de assinatura utilizado para o protocolo proposto nessa dissertação é o RSA. Como o algoritmo de criptografia RSA demanda um alto custo computacional, dependendo do tamanho da chave utilizada, não é recomendável cifrar toda a mensagem e sim um resumo [Burnett e Paine 2002].

O resumo de uma mensagem pode ser calculado por meio de uma função *hash* segura. Em geral, funções do tipo *hash* são responsáveis por garantir a integridade de mensagens, calculando um código único e identificador para cada mensagem. Esse código é calculado com base no conteúdo da mensagem e qualquer alteração nesse conteúdo modifica o resultado da função. Tal fato resulta, então, em um novo código identificador para a mensagem modificada. Além disso, os códigos *hash* calculados possuem tamanho único. Algumas funções *hash* podem ser encontradas em [Stinson 2005], [Stallings 2007], [Stallings 1999].

Em um esquema de assinatura digital, a confidencialidade da mensagem nem sempre é requerida e sim a autenticidade. Sendo assim, a função de assinatura pode ser implementada

calculando-se o código *hash* da mensagem, assinando-o com a chave privada do remetente e anexando este código *hash* assinado à mensagem criada. Isto reduz o *overhead* computacional, garantindo a integridade e a autenticidade da mensagem usando-se o código *hash*.

Ao receber a mensagem e o código *hash* assinado, o destinatário, que tem acesso à chave pública do remente, usa-a para decifrar o código *hash*. De posse do código *hash* decifrado e calculado pelo remetente, ele calcula novamente o código *hash* da mensagem e o compara ao código *hash*, que foi decifrado por ele. Se forem rigorosamente iguais, o destinatário tem a certeza de que a mensagem não foi alterada, ou seja, está íntegra e foi realmente o remetente que a enviou. Isso porque somente o remetente possui a chave privada que cifrou o código *hash* anexado à mensagem. Esse esquema de assinatura pode ser visualizado na figura 4.10 em que *Bob*, calcula o código *hash* da mensagem, cifra-o com sua chave secreta, anexa-o à mensagem em texto claro e envia ambos para *Alice*. Por outro lado, *Alice* recebe a mensagem de *Bob* em texto claro e calcula seu código *hash*. Depois decifra a assinatura da mensagem utilizando a chave pública de *Bob*. De posse dos dois códigos *hash*, um calculado por ela e o outro enviado juntamente com a mensagem, ela os compara. Caso sejam iguais, *Alice* tem a certeza de que foi realmente *Bob* quem enviou a mensagem e que ela não foi alterada durante a transmissão.

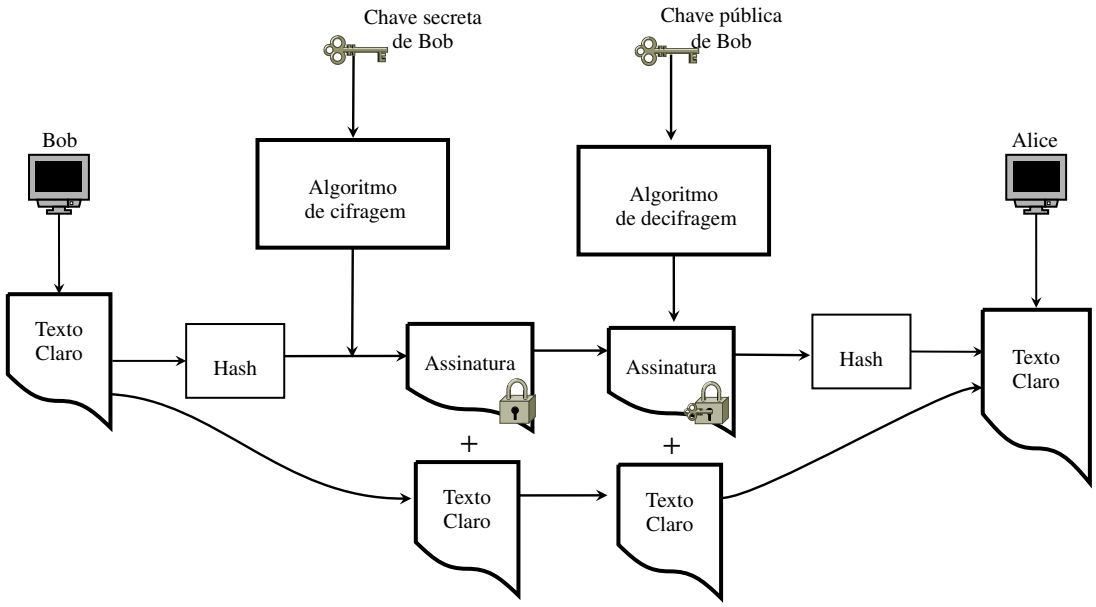


Figura 4.10: Esquema de Assinatura Digital utilizando código *hash* [Ashidani 2009]

Dessa forma, as propriedades de autenticidade e integridade estão garantidas com um *overhead* computacional menor do que se tivesse cifrado a mensagem completa. Vale ressaltar que a propriedade de confidencialidade é perdida utilizando esse método.

O esquema de assinatura apresentado na figura 4.10 é utilizado no protocolo proposto nessa dissertação com pequenas alterações que são apresentadas no capítulo 5.

A assinatura digital pode ainda ser compartilhada por muitos usuários. Existem situações

em que para uma assinatura ser válida, é necessário que mais de um usuário assine, como é o caso de algumas assinaturas de cheques empresariais. Nesse caso, pode ser necessário que duas ou até mesmo três pessoas assinem, para que a assinatura tenha validade. Nesse cenário, há protocolos criptográficos que atendem tal necessidade. Tais protocolos se fundamentam em esquemas de compartilhamento de segredos.

4.5 Compartilhamento de Segredos

No protocolo proposto neste trabalho, o compartilhamento de segredos é utilizado para se dividir responsabilidade da garantia de autenticidade do documento e da assinatura dos usuários. O desejável é que, por exemplo, o cartório reconheça a firma do comprador e do vendedor em um documento, sendo, portanto, uma testemunha de que as assinaturas no documento são válidas. Assim, se vários elementos, cartório, vendedor e comprador, participarem da emissão da assinatura em um documento, eles reconhecerão a firma e o documento como autênticos, pois eles ajudaram a emitir a assinatura se tornando testemunhas.

Motivado por um problema de análise combinatória proposto em [Liu 1968], Adi Shamir em 1979 propôs uma solução prática e eficaz para compartilhar segredos, utilizando interpolação de polinômios, chamado esquema de limiar(t, w) [Shamir 1979].

A ideia básica é dividir um segredo S em partes $S_1, S_2, \cdots, S_n$ de tal forma que as seguintes condições sejam satisfeitas:

- O conhecimento de t partes, ou mais, entre as partes $S_1, S_2, \cdots, S_n$ partes fazem com que S seja calculável facilmente;
- Dado o conhecimento de $t-1$ partes, ou menos, não é possível determinar S.

O compartilhamento de um segredo é aplicável em muitas áreas nas quais a responsabilidade não pode ficar nas mãos de uma só pessoa, como o lançamento de mísseis, abertura de cofres bancários, contratos diversos, etc.

No geral, esse esquema é um caso especial em que um subconjunto, com pelo menos um número determinado de participantes, é um subconjunto qualificado a determinar o segredo. Esse número determinado de participantes é chamado de limiar. Cada parte do segredo entregue aos participantes é chamado sombra [Vanderlei e de Queiroz 2004].

Tal esquema utiliza a notação (t, w), onde t é o número mínimo de sombras necessárias para reconstruir o segredo e w é o número total de participantes que recebem as sombras. Esse esquema pode ser entendido como:

Sejam t, w inteiros positivos; $t \leq w$. Um esquema de limiar (t, w), no contexto deste trabalho, é um método de compartilhamento da chave privada KR entre um conjunto com w participantes. Nesse caso, qualquer subconjunto com, pelo menos, t participantes consegue calcular o valor de KR, mas nenhum subconjunto com $t-1$, ou menos, participantes pode fazê-lo [Stinson 2005].

O esquema de criptografia de limiar é descrito em [Stinson 2005] conforme a figura 4.11:

Esquema de Limiar (t, w)

Considere:

- D é uma entidade confiável, que não é um participante do esquema de compartilhamento de segredo.
- κ é um conjunto finito de chaves
- S é o conjunto finito de segredos
- Seja $P = P_i : 1 \leq i \leq w$ o conjunto de w participantes. Portanto, D não pertence a P.
- Para cada i, tal que $1 \leq i \geq w$, P_i é um dos participantes do esquema de compartilhamento de segredo.

O protocolo Esquema de Limiar é dividido em duas fases:

Fase de Inicialização

- D escolhe w elementos distintos e diferentes de 0, denotados por: x_i; $1 \leq i \leq w$. Cada elemento x_i pertencem a $\mathbb{Z}_q$, sendo $q \leq w + 1$. Para $1 \leq i \leq w$, D entrega cada valor x_i para cada participante P_i. Os valores de x_i são públicos.

Fase de distribuição das partes

- Supondo que D deseja compartilhar uma chave privada $KR \in \mathbb{Z}_q$, em um esquema (t, w), então D, secretamente, escolhe (randomicamente) $t - 1$ elementos de $\mathbb{Z}_q$, os quais são denotados por $a_i, \cdots, a_{t-1}$.
- Para $1 \leq i \leq w$. D calcula $y_i = a(x_i)$ tal que:

$$a(x) = K + \sum_{j=1}^{t-1} a_j x^j \bmod q$$

- Na expressão acima K é uma constante definida por D

Para $1 \leq i \leq w$, D entrega cada parte y_i para P_i

Figura 4.11: Protocolo de Criptografia de Limiar [Shamir 1979] [Stinson 2005]

O valor da constante K é escolhido pela entidade confiável denotada por D (*dealer*, ou entidade confiável) tal que $D \notin P$. K é a constante e chave secreta a ser compartilhada, ou seja,

$$K = KR$$

Quando D deseja compartilhar a chave KR entre os participantes P, ele entrega a cada participante uma parte da informação denominada sombra. A sombra é então distribuída secretamente de forma que nenhum participante conheça a sombra dada a outro participante.

Posteriormente, um subconjunto de participantes B, tal que $B \subseteq P$, expõem suas sombras a uma entidade confiável que realizará determinados cálculos para reconstruir a chave KR. Se

$| B | \geq t$ eles são capazes de calcular o valor KR. Se $| B | < t$ eles não são capazes de calcular o valor de KR.

Seja $K \in \mathbb{Z}_q$, e $q \geq w + 1$ é primo. Seja ainda $S \in \mathbb{Z}_q$. Assim, a chave e cada segredo são elementos de $\mathbb{Z}_q$. D define um polinômio $a(x)$ de grau no máximo $t - 1$ em que a constante KR é a chave secreta a ser compartilhada. Todos os participantes recebem pontos (x_i, y_i) deste polinômio.

Supondo que os participantes $(P_{i_1}, ..., P_{i_t})$ desejam reconstruir K. Eles sabem que:

$$y_{i_j} = a(x_{i_j})$$

e que $1 \leq i \leq w$, considerando que $a(x)$ é um polinômio secreto definido por D e para cada x, $a(x) \in \mathbb{Z}_q$ Como $a(x)$ tem grau máximo igual a $t - 1$, $a(x)$ pode ser definido como:

$$a(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}$$

Nesse caso, os coeficientes $a_0, \cdots, a_{t-1}$ são elementos desconhecidos, pelas partes, em $\mathbb{Z}_q$, e $a_0 = KR$ é a chave. Uma vez que $y_{i_j} = a x_{i_j}$, $1 \leq j \leq t$, o subconjunto B pode obter t equações lineares desconhecidas em $a_0, \ldots, a_{t-1}$, em que toda a aritmética é feita em $\mathbb{Z}_q$. Se as equações são linearmente independentes há uma única solução, e a_0 é revelado como a chave.

Um exemplo de utilização do protocolo de compartilhamento de segredos é analisado a seguir.

4.5.1 Exemplo de Compartilhameno de Segredos

O exemplo a seguir considera a divisão de um segredo em partes e sua reconstrução, utilizando o protocolo de compartilhamento de segredos de limiar proposto por Adi Shamir e definido na figura 4.11.

Suponha um esquema de limiar $(3, 5)$. Nesse esquema, o segredo é dividido em cinco partes. Além disso, são necessárias para sua reconstrução, três partes quaisquer dessas cinco partes. Portanto, o limiar do esquema é três.

Uma vez definido o limiar para o esquema, ou seja, a quantidade mínima de partes necessárias para a reconstrução do segredo, a entidade confiável D (*Dealer*), determina um polinômio arbitrário de grau limiar igual ao limiar menos uma unidade. Considerando, nesse caso, que o limiar é igual a 3, então o polinômio tem grau igual a 2 e possui o seguinte formato:

$$a(x) = rx^2 + sx + k$$

Como os cálculos são feitos segundo os princípios da aritmética modular, D escolhe aleatoriamente um número inteiro primo q que é usado como módulo para os cálculos. Evidentemente, por questões de segurança, esse número deve ser grande para dificultar um possível ataque.

Logo, o polinômio para compartilhamento de segredos tem o seguinte formato:

$$a(x) = rx^2 + sx + k \pmod{q}$$

No qual

r e s são coeficientes gerados aleatoriamente e menores que q;

k é a constante do polinômio e recebe o segredo a ser compartilhado;

q é o módulo.

Suponha que o segredo a ser compartilhado é a chave secreta, KR, do algoritmo RSA, considerado no item 4.3.1. Considere, ainda, que os valores dos coeficientes r e s do polinômio e o módulo q são definidos de forma aleatória e possui os valores:

$$r = 17.890$$

$$s = 568.903$$

$$KR = k = 5.430.269$$

$$q = 13.994.087$$

Como está sendo considerado apenas um exemplo didático, tais números são pequenos e não há, nesse caso, preocupação com a segurança do compartilhamento de segredo.

Logo, o polinômio é dado por:

$$a(x) = 17.890x^2 + 568.903x + 5.430.269 \pmod{13.994.087}$$

Conforme definido, anteriormente, um esquema $(3, 5)$ de compartilhamento de segredos divide o segredo em cinco partes. Calculam-se, então, as sombras y_i, $1 \leq i \leq 5$, que são entregues aos cinco participantes do protocolo. Nesse caso, cada participante é denotado por $a_i, 1 \leq i \leq 5$. O cálculo das sombras é dado por:

$$a(1) = 17.890 \times 1^2 + 568.903 \times 1 + 5.430.269 \pmod{13.994.087} = 6.017.062$$
$$a(2) = 17.890 \times 2^2 + 568.903 \times 2 + 5.430.269 \pmod{13.994.087} = 6.639.635$$
$$a(3) = 17.890 \times 3^2 + 568.903 \times 3 + 5.430.269 \pmod{13.994.087} = 7.297.988$$
$$a(4) = 17.890 \times 4^2 + 568.903 \times 4 + 5.430.269 \pmod{13.994.087} = 7.992.121$$
$$a(5) = 17.890 \times 5^2 + 568.903 \times 5 + 5.430.269 \pmod{13.994.087} = 8.722.034$$

Cada participante do protocolo a_i recebe seu valor sombra y_i, que é utilizado para reconstrução do segredo. E, conforme os cálculos anteriores,

$$a(1) = y_1 = 6.017.062$$
$$a(2) = y_2 = 6.639.635$$
$$a(3) = y_3 = 7.297.988$$
$$a(4) = y_4 = 7.992.121$$
$$a(5) = y_5 = 8.722.034$$

Caso seja necessário reconstruir o segredo KR, pode-se utilizar a forma de interpolação de Lagrange[2] , da seguinte maneira:

Suponha que os participantes a_1, a_3 e a_4 desejam reconstruir o segredo a partir de suas partes. Têm-se, portanto, três participantes para construir o segredo, tal que:

$$x_1 = a_1 = y_1 = 6.017.062$$
$$x_3 = a_3 = y_3 = 7.297.988$$
$$x_4 = a_4 = y_4 = 7.992.121$$

Segundo a forma de interpolação de Lagrange, cálcula-se $P(x)$, tal que,

$$P(x) = \frac{(x - x_3(x - x_4)}{(x_1 - x_3)(x_1 - x_4)}y_1 + \frac{(x - x_1)(x - x_4)}{(x_3 - x_1)(x_3 - x_4)}y_3 + \frac{(x - x_1)(x - x_3)}{(x_4 - x_1)(x_4 - x_3)}y_4 \pmod q$$

Substituindo os valores, tem-se:

$$P(x) = \frac{(x - 3)(x - 4)}{(1 - 3)(1 - 4)}y_1 + \frac{(x - 1)(x - 4)}{(3 - 1)(3 - 4)}y_3 + \frac{(x - 1)(x - 3)}{(4 - 1)(4 - 3)}y_4 \pmod q$$

$$P(x) = \frac{x^2 - 3x - 4x + 12}{(-2)(-3)}y_1 + \frac{x^2 - 1x - 4x + 4}{(2)(-1)}y_3 + \frac{x^2 - 1x - 3x + 3}{(3)(1)}y_4 \pmod q$$

$$P(x) = \frac{x^2 - 7x + 12}{6}y_1 + \frac{x^2 - 5x + 4}{-2}y_3 + \frac{x^2 - 4x + 3}{3}y_4 \pmod q$$

$$P(x) = \frac{x^2 - 7x + 12}{6}6.017.062 + \frac{x^2 - 5x + 4}{-2}7.297.988 + \frac{x^2 - 4x + 3}{3}7.992.121 \pmod{13.994.087}$$

[2] A forma de interpolação de Lagrange é explicada em detalhes em [Ruggiero e da Rocha Lopes 1996]

$$P(x) = (\frac{x^2 - 7x + 12}{6} 6.017.062 \pmod{13.994.087}) +$$
$$(\frac{x^2 - 5x + 4}{-2} 7.297.988 \pmod{13.994.087}) +$$
$$(\frac{x^2 - 4x + 3}{3} 7.992.121 \pmod{13.994.087})$$
$$(\pmod{13.994.087})$$

Mas;

$$\frac{1}{6} \equiv 2.332.348 \pmod{13.994.087}$$

$$\frac{1}{(-2)} \equiv 6.997.043 \pmod{13.994.087}$$

$$\frac{1}{3} \equiv 4.664.696 \pmod{13.994.087}$$

Portanto;

$$P(x) = (6.017.062 \times 2.332.348 \times (x^2 - 7x + 12) \pmod{13.994.087}) +$$
$$(7.297.988 \times 6.997.043 \times (x^2 - 5x + 4) \pmod{13.994.087}) +$$
$$(7.992.121 \times 4.664.696 \times (x^2 - 4x + 3) \pmod{13.994.087})$$
$$(\pmod{13.994.087})$$

$$P(x) = (10.332.235 \times (x^2 - 7x + 12) \pmod{13.994.087}) +$$
$$(10.345.093 \times (x^2 - 5x + 4) \pmod{13.994.087}) +$$
$$(7.328.736 \times (x^2 - 4x + 3) \pmod{13.994.087})$$
$$(\pmod{13.994.087})$$

$$P(x) = (10.332.235x^2 + 11.638.877x + 12.034.124) +$$
$$(10.345.093x^2 + 4.250.883x + 13.392.198) +$$
$$(7.328.736x^2 + 12.667.317x + 7.992.121)$$
$$(\pmod{13.994.087})$$

$$P(x) = 17.890x^2 + 568.903x + 5.430.269 \text{ (mod } 13.994.08)$$

Dessa forma, tem-se o cálculo de $P(x)$. A partir desse polinômio, o valor da constante KR, que é o valor do segredo, é recuperado. Isso porque a forma de Interpolação de Lagrange é dada por:

$$P(x) = \sum_{j=1}^{t} \left(y_{i_j} \prod_{1 \leq k \leq t, k \neq j} \frac{x - x_{i_k}}{x_{i_j} - x_{i_k}} \right) \bmod q$$

Considerando a definição do Polinômio de Lagrange,

$$P(x) = b_j = \prod_{1 \leq k \leq t, k \neq j} \frac{x_{i_k}}{x_{i_k} - x_{i_j}} \bmod q$$

e

$$c = \sum_{j=1}^{t} b_{i_j} y_{i_j} \bmod q$$

Utilizando tais igualdades, a constante do Polinômio de Lagrange é determinada. No caso do exemplo,

$$b_1 = \frac{x_3 x_4}{(x_3 - x_1)(x_4 - x_1)} \bmod q = \frac{3 - 4}{(3 - 1)(4 - 1)} \bmod 13.994.087 = 2$$

$$b_2 = \frac{x_1 x_4}{(x_1 - x_3)(x_4 - x_3)} \bmod q = \frac{1 - 4}{(1 - 3)(4 - 3)} \bmod 13.994.087 = 13.994.085$$

$$b_3 = \frac{x_1 x_3}{(x_1 - x_4)(x_3 - x_4)} \bmod q = \frac{1 - 3}{(1 - 4)(3 - 4)} \bmod 13.994.087 = 1$$

Tem-se, portanto:

$k = b_1 \times y_1 + b_2 \times y_2 + b_3 \times y_3 \bmod q$

$k = 2 \times 6.017.062 + 13.994.085 \times 7.297.988 + 1 \times 7.992.121 \bmod 5.430.269$

$k = 5.430.269$

que é igual ao valor definido, inicialmente, para k, no início do exemplo.

4.5.2 Características do Compartilhamento de Segredos

Uma das características para a reconstrução do segredo do protocolo de compartilhamento de segredos de limiar é a interpolação de polinômios. Adi Shamir utiliza um polinômio de grau igual ao limiar, menos uma unidade. Dessa forma, o grau do polinômio não é secreto. Entretanto, o polinômio é definido aleatória e secretamente por uma **Autoridade Confiável** (*Dealer*). Tal polinômio possibilita a divisão do segredo e a geração de suas sombras.

Particularmente, o segredo deve ser definido como o valor da constante do polinômio. Além disso, as sombras são entregues aos participantes do protocolo. Caso esses participantes desejem reconstruir novamente o segredo, basta que um número determinado de participantes, o limiar definido, apresente suas sombras para recalcular a constante do polinômio, revelando, assim, o segredo.

Apesar de o polinômio ser secreto e conhecido apenas pela Autoridade Confiável, ele pode ser reconstruído utilizando interpolação polinomial.

Considere a existência de um número primo p e os elementos distintos $x_1, x_2, \cdots, x_{n+1}$ pertencentes a $\mathbb{Z}_q$. Considere, ainda, que $y_1, y_2 \cdots, y_{n+1}$ também são elementos de $\mathbb{Z}_q$, porém, não necessariamente distintos. Então existe um único polinômio $A(x)$ em $\mathbb{Z}_q$ de grau no máximo n, tal que $A(x) = y_i, 1 \leq i \leq n + 1$ [Stinson 2005]. Nesse sentido, o polinômio pode ser definido conforme seção 4.5.1 desta dissertação.

Conforme exemplo anterior, é compartilhado o segredo 5.430.269, que é igual ao expoente secreto utilizado no algoritmo RSA. Também, no exemplo, é definido um esquema de compartilhamento $(3, 5)$, no qual o segredo é dividido em 5(cinco) partes sendo 3(três) delas o limiar necessário para a reconstrução do segredo. Após a definição do limiar, igual a 3 (três), o grau do polinômio é definido como sendo igual a $(3 - 1)$, que é igual a grau 2 (dois).

$$a(x) = rx^2 + sx + k(\text{mod } q)$$

Como os coeficientes r e s do polinômio são definidos aleatoriamente, pelo *Dealer*, pode-se calcular as sombras a partir dele. Para cada valor de x, tal que $1 \leq x \leq 5$, obtém-se um valor de y_i para cada um dos 5 (cinco) participantes. Sendo assim, cada participante possui um par (x_i, y_i) tal que $1 \leq i \leq 5$, sendo que x_i representa sua ordem dentro do conjunto de participantes e y_i seu valor de sombra. A partir daí, todos os participantes possuem um par ordenado (x_i, y_i), no qual x_i corresponde à ordenada e y_i às abcissas.

A interpolação de polinômios é um método que permite construir um novo conjunto de dados a partir de um conjunto discreto de dados pontuais conhecidos, por exemplo, as abcissas e ordenadas [Haetinger e de Souza Martinez 2006]. Pela interpolação, é possível determinar uma função $f(x)$ que assuma valores conhecidos nos nós de interpolação.

No exemplo apresentado, a função $f(x)$ possui o gráfico da figura 4.12 :

A função $f(x)$ é o polinômio interpolador. Existem algumas formas de se obter o polinômio interpolador como Interpolação Linear, Forma de Newton ou Forma de Lagrange, que é a forma utilizada nesta dissertação. A escolha da utilização da Forma de Lagrange para descobrir o polinômio interpolador, se deu pelo fato dos trabalhos correlatos estudados, utilizarem essa forma, como por exemplo em [Vanderlei e de Queiroz 2004] e [Stinson 2005]. Mas, vale ressaltar que as outras formas também poderiam ser utilizadas.

Mais informações sobre como determinar um polinômio interpolador podem ser obtidas em [Ruggiero e da Rocha Lopes 1996].

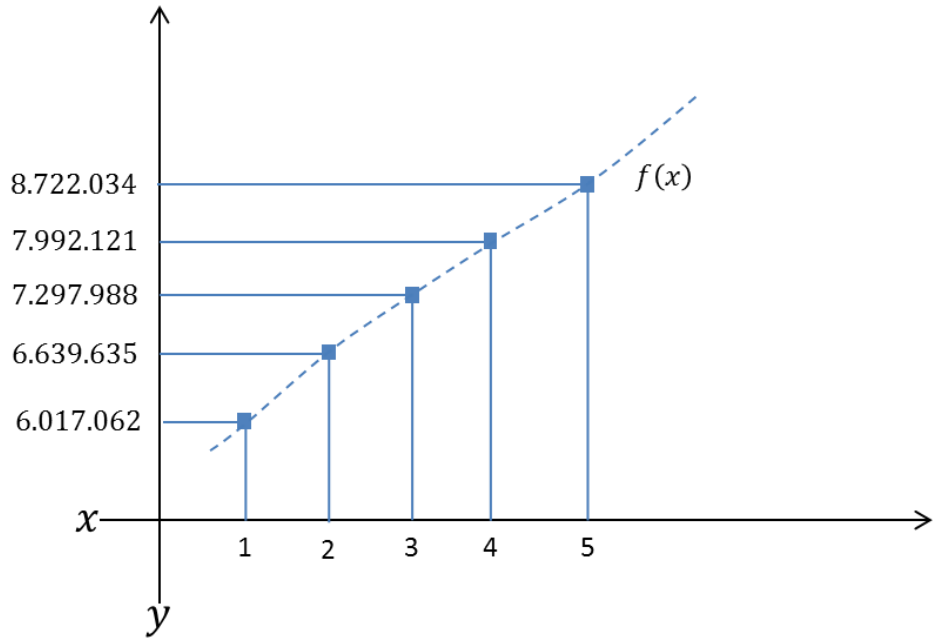


Figura 4.12: Interpolação de Polinômios.

4.6 Considerações

Dados os conceitos e fundamentos apresentados nesse capítulo, será proposto a seguir um protocolo de assinatura digital para um documento que empregue a característica de compartilhamento de segredos.

O compartilhamento é necessário para que a responsabilidade de emissão da assinatura seja distribuída entre as partes, por exemplo, o *Comprador* e o *Vendedor* e o *Cartório* e consequentemente, o reconhecimento das firmas por autenticidade dessas partes.

Capítulo 5

Protocolo Proposto

Neste capítulo, é proposto um protocolo para emissão de assinatura digital, com reconhecimento de firma e testemunhas. Como analisado anteriormente, esse protocolo corresponde ao análogo digital da seguinte situação: 1) O reconhecimento, por um *Cartório* da assinatura de um *Vendedor*, de um *Comprador* e de duas *Testemunhas* em uma escritura de compra e venda. 2) O *Cartório* reconhece as firmas das partes por autenticidade. Isto é, a presença das partes é exigida. Observe que nesse caso, as *Testemunhas* assinam o documento sem que, necessariamente, tenham conhecimento de seu conteúdo.

Portanto, o protocolo corresponde ao análogo digital do reconhecimento de firma presencial, em *Cartório*, da assinatura em uma escritura pública de compra e venda de um imóvel. Mas, além disso, com algumas modificações, o protocolo também possibilita a assinatura conjunta das partes envolvidas em qualquer documento.

O protocolo também aumenta a segurança do armazenamento da chave privada do usuário, dificultando seu roubo por algum intruso, que pretende se fazer passar pelo signatário.

O capítulo está estruturado da seguinte forma: Na seção 5.1, é descrita uma extensão do protocolo de criptografia de limiar de Shamir (t, w) utilizado para dividir a chave privada do usuário e reconstruí-la posteriormente. Ja na seção 5.2, é descrito o protocolo de assinatura em duas fases: distribuição das chaves e emissão da assinatura. Na seção 5.3, é mostrado um exemplo do uso do protocolo proposto nesta dissertação. Por último, na seção 5.4, são feitas algumas considerações finais sobre o capítulo.

5.1 Esquema de Criptografia de Limiar (t, w) Estendido

Esta seção considera uma extensão do esquema de criptografia de limiar de Shamir, tendo como objetivo sua utilização no protocolo proposto nesta dissertação.

Inicialmente, observa-se que no protocolo proposto é necessário garantir o uso da assinatura digital em um ambiente compartilhado como a internet. Considerando o esquema de assinatura RSA, isso corresponde a dividir o expoente secreto do esquema entre as diferentes partes ou

usuários do sistema. Além disso, como ocorre no protocolo de criptografia de limiar estendido, deve ocorrer no sistema a capacidade de veto de, pelo menos, três das partes.

No esquema de criptografia de limiar de Shamir, não é previsto o veto a nenhum dos participantes. Com isso, não importa quais são os participantes necessários para a reconstrução do segredo. Considera-se apenas que o número de participantes seja igual ou maior do que o limiar do sistema de compartilhamento do segredo. Diante desse fato, não há como garantir que o usuário, proprietário da assinatura, sempre participe do processo de reconstrução do segredo. Isso poderia implicar, por exemplo, que nem sempre a assinatura seria emitida por seu proprietário. Em uma escritura pública de compra e venda, por exemplo, para garantir que o *Vendedor* o *Comprador* e o *Cartório* sempre participem no processo de reconstrução do segredo e emissão de suas próprias assinaturas, é necessário adicionar a capacidade de veto ao esquema de criptografia de limiar de Shamir.

O protocolo proposto por Damgård e Mikkelsem [Damgård e Mikkelsen 2009] implementa a capacidade de veto e o compartilhamento de segredo, porém, de forma limitada. Nele, o segredo é armazenado em no máximo dois dispositivos (participantes). Além do mais, as duas partes da chave podem ser descobertas, caso esses dois dispositivos específicos sejam corrompidos. Com isso, basta aplicar as propriedades matemáticas de exponenciação em uma mesma base para revelar a chave secreta. Então, nesse esquema, toda a segurança está relacionada à confirmação ou não do usuário em emitir sua assinatura digital. Já o protocolo proposto em [Blundo et al. 1994], que também implementa a capacidade de veto e compartilhamento de segredo, é definido um conjunto minoritário de participantes que podem evitar a reconstrução do segredo. Porém, não especifica que um único participante em particular deve fazer parte desse conjunto. Logo, desde que seja satisfeito esse conjunto mínimo, qualquer participante pode vetar a reconstrução do segredo. Para aumentar a segurança no protocolo proposto nesta dissertação, a chave secreta é dividida entre mais participantes. Além disso, alguns participantes devem, necessariamente, participar da reconstrução do seu segredo para emitir suas próprias assinaturas. Assim, mesmo que o número estabelecido como limiar seja satisfeito, o segredo não é descoberto se aqueles com poder de veto não compuserem o grupo total de participantes.

Para satisfazer todas essas condições, o protocolo proposto nesta dissertação requer uma capacidade computacional maior que o protocolo proposto por Damgård e Mikkelsem em [Damgård e Mikkelsen 2009], pois utiliza o esquema de criptografia de limiar para dividir um segredo e a interpolação de polinômios para sua reconstrução, enquanto que em [Damgård e Mikkelsen 2009], são utilizadas propriedades matemáticas de exponenciação em uma mesma base. E tal fato, do ponto de vista de eficiência computacional, é uma desvantagem. Isso significa que há uma troca de eficiência computacional pela satisfação das condições de autenticação de firma por autenticidade. Em relação ao protocolo de [Blundo et al. 1994], tem-se a garantia de que alguns participantes, em particular, podem vetar suas próprias assinaturas, assegurando, assim, sua participação no processo.

O algoritmo é definido conforme a notação apresentada em [Stinson 2005] e apresentado na

figura 5.1 a seguir.

Esquema de Limiar com Veto (t, w)

Notação

- Seja $P = P_i : 1 \leq i \leq w$ o conjunto de w participantes. Portanto, P_i, tal que $1 \leq i \leq w$, é um participante do esquema de compartilhamento de segredo;
- D é uma entidade confiável que não pertence a P;
- κ é um conjunto finito de chaves;
- S é o conjunto finito de segredos.

Fase de Inicialização:

1. D escolhe w números distintos e diferentes de 0. Tais números devem pertencer a $\mathbb{Z}_q$. Os w números são denotados como x_i; $1 \leq i \leq w$.

   Além disso, considere $q \geq w + 1$. Para cada i, tal que $1 \leq i \leq w$, D entrega o número x_i para o participante P_i. Os números x_i são públicos.

Fase de distribuição das partes:

1. Supondo que D deseja compartilhar uma chave privada $KR_i; \in \mathbb{Z}_q$, em um esquema (t, w). Então D, secretamente, escolhe (randomicamente) $t - 1$ elementos de $\mathbb{Z}_q$, os quais são denotados por $a_i \cdots, a_{t-1}$.
2. Para i, tal que $1 \leq i \leq 2$, D calcula $Y_i = a(x_i)$ no qual,

$$a(x) = K + \sum_{j=1}^{t-1} a_j x^j \bmod q$$

3. Para $1 \leq i \leq 2$, D entrega a parte Y_i para P_i
4. Para i, tal que $2 < i \leq w$, D calcula $Y_i = a(x_{i-1})$ em que,

$$a(x) = K + \sum_{j=1}^{t-1} a_j x^j \bmod q$$

5. Para i, tal que $3 \leq i \leq w$, D entrega a parte Y_i para P_i

Figura 5.1: Protocolo de Criptografia de Limiar de Shamir Estendido

Para reconstruir o segredo, os participantes devem apresentar suas partes. Dado que um sistema com t equações lineares possui somente uma solução, a reconstrução do segredo pode ser feita usando a fórmula de interpolação polinomial de Lagrange, conforme mostrado a seguir [Stinson 2005]:

$$P(x) = \sum_{j=1}^{t} \left(y_{i_j} \prod_{1 \leq k \leq t, k \neq j} \frac{x - x_{i_k}}{x_{i_j} - x_{i_k}} \right) \bmod q$$

Na fase de distribuição das partes aos participantes, inicialmente, a chave é dividida em duas partes, conforme o esquema de limiar de $(2, 2)$. Uma das partes da chave é entregue ao

participante com o poder de veto, ou seja, o usuário proprietário da assinatura. A segunda parte é dividida novamente utilizando o mesmo esquema de limiar entre w partes.

Suponha, por exemplo, que o segredo (chave secreta do usuário) é dividido segundo um esquema de criptografia de limiar $(3, 5)$. Isso quer dizer que são necessários pelo menos 3 (três) dos 5 (cinco) participantes para a reconstrução do segredo. E que, além disso, há um participante com poder de veto.

Como exemplo, considere que os participantes sejam, respectivamente, x_1, x_2, x_3, x_4, x_5 e que o primeiro participante x_1 tenha poder de veto.

Primeiramente, o segredo é compartilhado em um esquema $(2, 2)$ gerando as subchaves Y_1 e Y_2 respectivamente. Portanto, é necessário 2 de 2 participantes para a reconstrução do segredo. Y_1 é entregue ao participante x_1. A outra subchave, Y_2 é dividida em mais 4 partes utilizando um esquema de limiar $(2, 4)$. Nesse esquema, são necessários 2 de 4 participantes para reconstruir o segredo. Sejam Y_{2_1}, Y_{2_2}, Y_{2_3}, Y_{2_4} as subchaves geradas a partir de Y_2. Essas subchaves são entregues, respectivamente, aos participantes x_2, x_3, x_4, x_5.

Para a reconstrução da chave, pelo menos 2 (dois), dentre os participantes x_2, x_3, x_4, x_5, devem apresentar suas subchaves para reconstruir Y_2. Após esse processo, x_1 apresenta sua subchave Y_1, que, juntamente, com a subchave Y_2 reconstitui o segredo.

No esquema proposto, conforme o exemplo, a chave não pode ser gerada sem a participação do participante com poder de veto. Ou seja, sem a participação de x_1. Nesse sentido, diz-se que x_1 tem o poder de vetar a assinatura pela reconstrução final de sua chave secreta. E que os outros participantes, sem o auxílio de x_1, não conseguem obter a chave, que é o segredo compartilhado.

5.2 Protocolo para Emissão da Assinatura Compartilhada

Esse protocolo considera a emissão da assinatura digital em, por exemplo, uma escritura de compra e venda de um imóvel.

É importante observar que a escolha do problema de assinatura em uma escritura de compra e venda de um imóvel serve apenas como elemento didático.

A emissão de assinatura digital compartilhada, como apresentada no protocolo proposto nesse trabalho, pode ser considerada, também, em outros contextos.

O protocolo emite uma única assinatura digital em nome dos participantes do processo que são: *Vendedor*, *Comprador*, *Cartório* e *Testemunhas*. Essa assinatura é formada pelos pares de chaves, KU_{Trans} e KR_{Trans}, que são respectivamente, a chave pública e privada. A chave privada é utilizada para assinar a escritura de compra e venda enquanto a chave pública, para a verificação dessa assinatura. Considera-se que o *Cartório* é uma entidade confiável e seu papel é reconhecer a firma da assinatura do *Vendedor*, do *Comprador* e das *Testemunhas*, garantindo e atestando o desejo dos signatários em vender e comprar o imóvel.

Atualmente, cada imóvel é registrado em um Cartório de Registro de Imóveis e recebe um número único de identificação em determinada localidade ou município.

Sendo assim, a identificação do imóvel negociado pelo *Vendedor* e *Comprador*, em uma escritura de compra e venda de imóvel é referenciado por um número, que neste trabalho é denotado por: ID_{Imovel}.

Considere, também, que cada participante do protocolo possua um par de chaves; pública e privada, que são usadas para garantir o sigilo durante o tráfego de informações. Nesse caso, tais chaves não são usadas para assinar documentos.

Além disso, a chave pública é certificada, de forma segura, por uma *Autoridade Certificadora*. Portanto, a *Autoridade Certificadora* possui um repositório de todas as chaves públicas certificadas de seus usuários. Os pares de chaves dos participantes são denotados por:

$Vendedor_{Vend} \rightarrow$ possui a chave privada KR_{Vend} correspondente à chave pública KU_{Vend}; e uma identificação única ID_{Vend};

$Comprador_{Comp} \rightarrow$ possui a chave privada KR_{Comp} correspondente à chave pública KU_{Comp}; e uma identificação única ID_{Comp};

$Cartório_{Cart} \rightarrow$ possui a chave privada KR_{Cart} correspondente à chave pública KU_{Cart}; e uma identificação única ID_{Cart}

$Testemunha_i \rightarrow$ possui a chave privada KR_{Ti} correspondente à chave pública KU_{Ti}; e uma identificação única ID_{Ti}.

O protocolo para emissão de assinatura para os usuários é dividido em duas fases, definidas a seguir:

- Fase 1 - geração e distribuição das chaves e
- Fase 2 - emissão das assinaturas,

Fase 1: Geração e Distribuição de chaves

Antes do início do processo de distribuição de chaves, considera-se que as partes: *Vendedor*, *Comprador*, *Cartório* e *Testemunhas*, envolvidas no processo possuem chaves públicas e privadas autenticadas pela *Autoridade Certificadora* e que podem ser utilizadas em sessões de comunicação.

O *Vendedor*, por exemplo, possui um certificado digital, emitido pela *Autoridade Certificadora*, que diz que KU_{Vend} é sua chave pública.

Suponha, então que o *Vendedor* solicite a um *Cartório* o início do processo para criação de uma assinatura digital e o seu reconhecimento de firma com autenticidade.

Nesse contexto, a assinatura pode ser utilizada em algum documento importante, por exemplo, a escritura de compra e venda de um imóvel, que é o exemplo considerado neste trabalho.

Nesse caso, também deve ser informada a identificação do *Comprador* e do imóvel a ser vendido.

Em seguida, o *Cartório*, por sua vez, requer à *Autoridade Certificadora* a criação de tal assinatura para o *Vendedor*. Esse protocolo é representado, esquematicamente, na figura 5.2:

Vendedor	*Cartório*	*Autoridade Certificadora*
1. *Vendedor*, ou *Comprador*, solicita um reconhecimento de firma, com autenticidade, para a assinatura digital de uma escritura. O *Vendedor* informa a identificação do imóvel e a identificação do *Comprador*.	2. O *Cartório* recebe a solicitação e a encaminha à *Autoridade Certificadora* os nomes das partes: *Comprador*, *Vendedor*.	3. A *Autoridade Certificadora* fornece ao cartório as chaves públicas, certificadas, do *Comprador* e do *Vendedor*.

Figura 5.2: Solicitação da assinatura digital

O fornecimento ao *Cartório*, pela *Autoridade Certificadora*, das chaves públicas garante que as partes possam a ser identificadas de forma inegável [ICP-Brasil 2011].

Como o objetivo do protocolo proposto é o compartilhamento de segredo, o certificado de cada uma das partes, criado e fornecido pela *Autoridade Certificadora*, segue o seguinte esquema:

Inicialmente, a *Autoridade Certificadora* cria um par de chaves, pública e privada, e uma identificação única, para a presente transação de compra e venda. Assim, para cada transação, a *Autoridade Certificadora* define um único par de chaves e sua identificação.

Considere KU_{Trans} a chave pública, KR_{Trans} a chave secreta e ID_{Trans} a identificação da presente transação.

O processo de criação de KU_{Trans} e KR_{Trans}, pela *Autoridade Certificadora*, é descrito a seguir:

Após a *Autoridade Certificadora* criar ID_{Trans}, ela envia esse identificador da transação a cada uma das partes envolvidas. Esse processo é mostrado nas figuras 5.3, 5.4 e 5.5:

Autoridade Certificadora	*Cartório*
4. A *Autoridade Certificadora* cria uma identificação única ID_{Trans} para a transação de compra e venda e a envia para o *Cartório*. $E(KU_{Cart}, ID_{Trans})$	5. *Cartório* decifra a informação recebida e obtém a ID_{Trans}. $D(KR_{Cart}, E(KU_{Cart}, ID_{Trans}))$

Figura 5.3: *Autoridade Certificadora* envia ID_{Trans} para o *Cartório*.

Autoridade Certificadora	*Vendedor*
6. A *Autoridade Certificadora* cria uma identificação únic a ID_{Trans} para a transação de compra e venda e a envia para o *Cartório*. $E(KU_{Vend}, ID_{Trans})$	7. *Vendedor* decifra a informação recebida e obtém a ID_{Trans}. $D(KR_{Vend}, E(KU_{Vend}, ID_{Trans}))$

Figura 5.4: *Autoridade Certificadora* envia ID_{Trans} para o *Vendedor*.

Autoridade Certificadora	*Comprador*
8. A *Autoridade Certificadora* cria uma identificação únic a ID_{Trans} para a transação de compra e venda e a envia para o *Comprador*. $E(KU_{Comp}, ID_{Trans})$	9. *Comprador* decifra a informação recebida e obtém a ID_{Trans}. $D(KR_{Comp}, E(KU_{Comp}, ID_{Trans}))$

Figura 5.5: *Autoridade Certificadora* envia ID_{Trans} para o *Comprador*.

Como a *Autoridade Certificadora* possui um repositório de todas as chaves públicas certificadas, ela cifra essa identificação com as respectivas chaves públicas de cada participante. Isso garante que ID_{Trans} será conhecida apenas pelos envolvidos.

Também garante que cada participante reconheça ID_{Trans} como a identificação da transação. Essa informação, portanto, é comum ao *Cartório*, *Vendedor* e *Comprador*. Esses, por sua vez, cifram essa informação com suas respectivas chaves privadas, definindo as chaves K_1, K_2 e K_3:

Vendedor define $K_1 = E(KR_{Vend}, ID_{Trans})$

Comprador define $K_2 = E(KR_{Comp}, ID_{Trans})$

Cartório define $K_3 = E(KR_{Cart}, ID_{Trans})$

Em seguida, cada um desses participantes envia a sua parte correspondente para a *Autoridade Certificadora*, conforme mostra a figura 5.6.

Vendedor	*Comprador*	*Cartório*	*Autoridade Certificadora*
10. *Vendedor* envia K_1 *para Autoridade Certificadora*: $E(KU_{AutCert}, K_1)$			
	11. *Comprador* envia K_2 *para Autoridade Certificadora*: $E(KU_{AutCert}, K_2)$		
		12. *Cartório* envia K_3 *para Autoridade Certificadora*: $E(KU_{AutCert}, K_3)$	
			13. *Autoridade Certificadora* decifra cada parte recebida e obtêm K_1, K_2, K_3

Figura 5.6: Participantes enviam suas chaves para a *Autoridade Certificadora*

Vendedor, *Comprador* e *Cartório* enviam suas respectivas chaves K_1, K_2 e K_3 de forma cifrada, para a *Autoridade Certificadora*. A cifragem é feita com a chave pública $KU_{AutCert}$ da *Autoridade Certificadora*. Dessa forma, somente a *Autoridade Certificadora* conhece as três chaves.

A *Autoridade Certificadora* então define KU_{Trans} como sendo uma combinação das chaves K_1, K_2 e K_3. Considere, por exemplo, que

$$KU_{Trans} = K_1 \times K_2 + K_3$$

A partir de

$$KU_{Trans}$$

a *Autoridade Certificadora*, determina

$$KR_{Trans}$$

utilizando os procedimentos para geração de chaves do protocolo criptográfico RSA.

A definição de KU_{Trans} é feita pela multiplicação das chaves K_1 e K_2 adicionando-se ao resultado dessa multiplicação o valor de K_3 e seguem ainda algumas especificidades em função dos procedimentos de geração de chaves do esquema RSA. Essas especificidades são detalhadas a seguir.

A linha 4 da figura 4.3, que descreve o algoritmo RSA, mostra que se deve escolher um certo número b, tal que, $b < \phi(n)$ e $mdc(b, \phi(n)) = 1$. Ou seja, b, que é a chave pública do algoritmo, deve ser relativamente primo a $\phi(n)$.

Nesse protocolo, considera-se que

$$KU_{Trans} = b$$

Além disso, $\phi(n)$ é definido pela *Autoridade Certificadora*. Sendo assim:

$$KU_{Trans} = (K_1 \times K_2 + K_3) \bmod(\phi(n))$$

para que se tenha:

$$KU_{Trans} < \phi(n)$$

Logo,

$$KU_{Trans} = (ID_{Trans}^{KR_{Comp}} \times ID_{Trans}^{KR_{Vend}} + ID_{Trans}^{KR_{Cart}}) \bmod (\phi(n))$$

Portanto,

$$KU_{Trans} = (ID_{Trans}^{KR_{Comp}+KR_{Vend}} + ID_{Trans}^{KR_{Cart}}) \bmod (\phi(n))$$

Conforme a igualdade acima, a chave pública da transação é formada, necessariamente, pelos três participantes envolvidos, que são *Comprador*, *Vendedor* e *Cartório*.

Porém, observe que nem sempre a operação

$$(K_1 \times K_2 + K_3) \bmod(\phi(n))$$

resulta em um número relativamente primo a $\phi(n)$. Se isso ocorre, tal fato impede a criação do par de chaves, pública e privada, assimétricas, utilizadas no esquema de assinatura RSA.

Para solucionar essa situação, caso isso aconteça, a *Autoridade Certificadora* recalcula KU_{Trans} , substituindo a chave K_3 por K_4, obtendo-se:

$$KU_{Trans} = (K_1 \times K_2 + K_4) \bmod(\phi(n))$$

tal que

$$mdc(K_1 \times K_2 + K_4 \bmod(\phi(n)), \phi(n)) = 1$$

Dessa forma, a relação de primariedade entre os números é respeitada, garantindo, assim, a geração das chaves assimétricas, no protocolo proposto.

A definição de K_4 é mostrada a seguir:

No momento em que a *Autoridade Certificadora* certifica-se de que

$$mdc(K_1 \times K_2 + K_4 \bmod(\phi(n)), \phi(n)) \neq 1$$

ela solicita ao *Cartório* que envie uma nova chave, K_4, que substitui K_3.

K_4 é gerada, pelo *Cartório*, a partir de $K_3 + 1$ e enviada a *Autoridade Certificadora*. Essa por sua vez, verifica a igualdade:

$$mdc(K_1 \times K_2 + K_4 \bmod(\phi(n)), \phi(n)) = 1$$

Caso essa condição ainda não esteja satisfeita, a *Autoridade Certificadora* solicita novamente um novo valor de K_4. O *Cartório*, por sua vez, recalcula K_4, incrementando uma unidade ao valor anterior de K_4.

$$K_4 = K_4 + 1$$

Essa operação se repete até que a condição

$$mdc(K_1 \times K_2 + K_4 \bmod(\phi(n)), \phi(n)) = 1$$

seja satisfeita.

O processo de definição do valor de K_4 é mostrado na figura 5.7.

Observe que são os participantes que determinam os pedaços da chave pública da transação

Autoridade Certificadora	*Cartório*
14. Autoridade Certificadora verifica a condição: $mdc(K_1 \times K_2 + K_3 \bmod(\phi(n))) = 1$ Caso verdadeiro, define $KU_{Trans} = (K_1 \times K_2 + K_3) \bmod(\phi(n))$ Caso contrário, solicita a chave K_4 para o *Cartório*. $request_{Cart}(K_4)$	
	14.1. Cartório recebe solicitação da *Autoridade Certificadora* e calcula valor de K_4, como: $K_4 = E(KR_{Cart}, K_3 + 1)$ *Cartório* envia K_4 para *Autoridade Certificadora* $E(KU_{AutCert}, K_4)$
14.2 *Autoridade Certificadora* recebe valor de K_4 e verifica a condição: $KU_{Trans} = (K_1 \times K_2 + K_4) \bmod(\phi(n))$ Caso verdadeiro, define $KU_{Trans} = (K_1 \times K_2 + K_4) \bmod(\phi(n))$ Caso contrário, solicita novo valor para a chave K_4 para o *Cartório*. $request_{Cart}(K_4)$	
	14.3. *Cartório* recebe solicitação da *Autoridade Certificadora* e recalcula valor de K_4, como:: $K_4 = E(KR_{Cart}, K_4 + 1)$ Cartório envia K_4 para Autoridade Certificadora: $E(KU_{AutCert}, K_4)$

Figura 5.7: Definição do valor da chave K_4

e não a *Autoridade Certificadora*. A partir da chave pública, a *Autoridade Certificadora* determina, então, com base no esquema de geração de chaves do RSA, a chave privada que é utilizada para emissão da assinatura digital. Isso é importante para que a *Autoridade Certificadora* não assine pelas partes.

Nesse ponto do protocolo, tem-se, portanto, definidos: KU_{Trans} e KR_{Trans}

Em seguida, a chave pública, KU_{Trans}, e a identificação das partes: *Vendedor*, *Comprador* e

Cartório: ID_{Vend}, ID_{Comp} e ID_{Cart} são publicadas pela *Autoridade Certificadora*, em uma forma certificada.

Dessa maneira, a *Autoridade Certificadora* garante que a chave pública da transação corresponda, de forma segura, à referida transação de compra e venda.

Em seguida, a *Autoridade Certificadora* promove a divisão da chave privada KR_{Trans} em quatro partes: para o *Comprador*, para o *Vendedor*, para o *Cartório* e para as *Testemunhas*. Nesse contexto, a divisão é feita, utilizado o esquema de criptografia de limiar proposto por Adi Shamir em [Shamir 1979]. O protocolo é apresentado no esquema das figuras 5.8 e 5.9.

Autoridade Certificadora

15. A *Autoridade Certificadora* cria um par de chaves para a transação, com base nas chaves K_1, K_2 e K_3 ou K_1, K_2 e K_4 enviadas pelos participantes anteriormente.

    Considere KR_{Trans} a chave privada e KU_{Trans} a chave pública da transação e ID_{Trans} a identificação da transação.

16. A *Autoridade Certificadora* divide a chave privada KR_{Trans} em quatro partes, utilizando o esquema de criptografia de limiar de Shamir (4,4), criando, assim, as subchaves: KR_1, KR_2, KR_3 e KR_4

17. A *Autoridade Certificadora* cifra a subchave KR_1, utilizando a chave pública do *Vendedor* KU_{Vend}, definida anteriormente, obtendo:

    $$E(KU_{Vend}, KR_1 || ID_{Trans})$$

    Depois de cifrados, esses dados são enviados ao *Vendedor*, juntamente com a identificação da transação: ID_{Trans}.

    O *Vendedor* utiliza esses dados, posteriormente, para assinar eletronicamente o documento da transação.

18. A *Autoridade Certificadora* cifra a subchave KR_2, utilizando a chave pública do *Comprador* KU_{Comp}, definida anteriormente, obtendo:

    $$E(KU_{Comp}, KR_2 || ID_{Trans})$$

    Depois de cifrados, esses dados são enviados ao *Comprador*, juntamente com a identificação da transação: ID_{Trans}.

    O *Comprador* utiliza esses dados, posteriormente, para assinar eletronicamente, o documento da transação.

Figura 5.8: Esquema de distribuição das chaves para *Vendedor*, *Comprador* e *Cartório*.

Autoridade Certificadora

19. A *Autoridade Certificadora* cifra a subchave KR_3, utilizando a chave pública do *Cartório* KU_{Cart} definida anteriormente, obtendo:

$$E(KU_{Cart}, KR_3||ID_{Trans})$$

Depois de cifrados, esses dados são enviados ao *Cartório*, juntamente com a identificação da transação: ID_{Trans}.

O *Cartório* utiliza esses dados, posteriormente, para assinar o documento da transação e reconhecer as firmas do *Vendedor* e *Comprador*, por autenticidade.

20. A *Autoridade Certificadora* divide a subchave KR_4, em w partes. É utilizado um esquema $(w, 2)$. Nesse caso, são necessárias duas partes, pelo menos, para a reconstrução de KR_4. Portando são geradas subchaves KR_{4_i} tal que $1 \leq i \leq w$.

Considere w o número de testemunhas disponíveis na jurisdição do *Cartório*. A seguir, a *Autoridade Certificadora* cifra cada subchave de KR_{4_i} e a distribui a cada testemunha, obtendo:

$$E(KU_{testemunha_i}, KR_{4_i}||ID_{Trans})$$

Depois de cifrados, esses dados são enviados às respectivas *Testemunhas*, juntamente com a identificação da transação: ID_{Trans}.

As *Testemunhas* utilizam esses dados, posteriormente para atestarem a existência da escritura.

Figura 5.9: Esquema de distribuição das chaves para as *Testemunhas*.

No protocolo proposto, o esquema de criptografia de limiar de Shamir é utilizado duas vezes. Inicialmente, na forma $(4, 4)$ e, em seguida na forma $(w, 2)$, na qual w é o número total de testemunhas da jurisdição do cartório que estão aptas a participarem da transação. Nesse caso, necessariamente, o cartório deve escolher, pelo menos, duas testemunhas para assinar a escritura de compra e venda.

Dada a divisão de chaves descrita, é impraticável para um intruso tentar corromper todas as partes que possuem as subchaves para formar KR_{Trans}, e se passar por alguma das partes.

Observe que no protocolo proposto, a escolha inicial do conjunto das *Testemunhas* pode ser feita pela *Autoridade Certificadora* ou por indicação de uma das partes.

Entretanto, dada a escolha do conjunto das partes, somente a *Autoridade Certificadora* deve emitir suas chaves para assinatura.

Além disso, a *Autoridade Certificadora* determina qual o número mínimo de testemunhas é necessário para a assinatura da escritura. Em outras palavras, qual é o limiar no conjunto das testemunhas.

Nesse protocolo proposto, as partes: *Vendedor*, *Comprador* e *Cartório* tem poder de veto.

E no conjunto das *Testemunhas*, as duas que assinam a escritura também possuem tal poder de veto. Dessa forma, ninguém, além dessas partes, consegue emitir sua assinatura sem o seu consentimento.

Portanto, ninguém além do *Vendedor* e *Comprador* pode expressar e atestar seu desejo de realizar a transação de compra e venda de um determinado imóvel.

Além disso, ninguém a não ser o *Cartório* consegue reconhecer a firma, por autenticidade, sem o seu consentimento.

Nesse sentido, o reconhecimento de firma, efetuado pelo *Cartório* é efetuado no ato de sua assinatura.

Observe que tal fato ocorre no reconhecimento de firma usual, no qual, além de colocar um selo no documento, há a assinatura do tabelião do *Cartório*.

Observações

Após a divisão da chave KR_{Trans}, a *Autoridade Certificadora* envia ao *Vendedor* sua subchave KR_1 e a identificação da transação ID_{Trans}.

Essas informações são cifradas com a chave pública KU_{Vend} do *Vendedor* garantindo o sigilo da informação trafegada.

Como só o *Vendedor* possui a chave privada KR_{Vend}, ele é o único que pode decifrar a informação enviada pela *Autoridade Certificadora*.

Essa subchave garante ao *Vendedor* a sua participação na emissão de sua própria assinatura.

Garante ainda que sua assinatura não seja emitida sem a sua subchave, ou seja, o *Vendedor* tem o direito de vetar a criação de sua assinatura.

Ao decifrar a mensagem, o *Vendedor* armazena em algum dispositivo, como um computador ou mesmo *pendrive*, a informação:

$$ID_{Trans} || KR_1$$

Mesmo que esse dispositivo seja corrompido de alguma forma, um intruso não consegue assinar um documento, pois as informações estão incompletas uma vez que a assinatura é emitida com KR_{Trans}.

Portanto, um intruso não consegue, como *Vendedor*, assinar sozinho a escritura de compra e venda.

É importante ressaltar que para a formação de KR_{Trans} são necessários KR_1, KR_2, KR_3 e KR_4.

No contexto desse trabalho, ninguém pode assinar a transação sozinho.

De forma análoga, a *Autoridade Certificadora* envia ao *Comprador* a subchave KR_2 e a identificação da transação ID_{Trans}.

Essas informações também são cifradas com a chave pública KU_{Comp} do *Comprador*, ga-

rantindo o sigilo da informação trafegada.

Como só o *Comprador* possui a chave privada KR_{Comp} ele é o único que pode decifrar a informação enviada pela *Autoridade Certificadora*.

Além disso, ele é o único que pode emitir sua própria assinatura ou vetá-la.

Ao decifrar a mensagem, o *Comprador* armazena em algum dispositivo a informação:

$$ID_{Trans}||KR_2$$

Mesmo que esse dispositivo seja corrompido de alguma forma, um intruso não consegue assinar um documento, pois as informações estão incompletas, uma vez que a assinatura é emitida com KR_{Trans}.

Portanto, um intruso não consegue assinar a escritura, sozinho, como se fosse um *Comprador*.

A *Autoridade Certificadora*, também, envia ao *Cartório* a subchave KR_3 e a identificação da transação ID_{Trans}.

Essas informações são cifradas com a chave pública KU_{Cart} do *Cartório*, garantindo o sigilo da informação veiculada.

Como só o cartório possui a chave privada KR_{Cart}, ele é o único que pode decifrar a informação enviada pela *Autoridade Certificadora*.

A subchave KR_3 garante ao *Cartório* a sua participação na emissão da assinatura. Ao emitir sua assinatura no documento, o *Cartório* reconhece que as assinaturas do *Vendedor* e *Comprador* são autênticas.

O mesmo procedimento é feito em relação às *Testemunhas*.

Fase 2 - Emissão da Assinatura

Uma vez que a chave privada da *Transação* está dividida em partes e armazenada em locais diferentes, algumas dessas partes devem ser reunidas para a emissão da assinatura digital no documento. Nesse caso, na escritura de compra e venda do imóvel.

Observe que em uma escritura de compra e venda de imóvel, os seguintes requisitos são necessários:

- As assinaturas do *Vendedor* e *Comprador* devem ter sua firma reconhecida pelo *Cartório*;
- O *Cartório* também deve assinar o documento, garantido sua autenticidade e o reconhecimento de firma das assinaturas;
- É necessário que pelo menos duas *Testemunhas* assinem a escritura atestando a existência da transação.

O protocolo que reconhece a firma do *Vendedor* e *Comprador* são apresentados nas figuras 5.10 e 5.11:

Vendedor

Vendedor envia ao *Cartório* a sua subchave e a identificação da transação que corresponde ao imóvel vendido. Essas informações são cifradas, utilizando a chave pública da *Autoridade Certificadora*. Além disso, também envia a identificação do imóvel. Todas as informações são cifradas utilizando a chave privada do *Vendedor*, da seguinte forma:

$$E(KR_{Vend}, ID_{Imovel} || E(KU_{AutCert}, KR_1 || ID_{Trans}))$$

Figura 5.10: *Vendedor* envia sua subchave ao *Cartório*

Quando o *Cartório* recebe a informação cifrada do *Vendedor*, ele a decifra utilizando a chave pública do mesmo KU_{Vend}, obtendo:

$$ID_{Imovel} \text{ e } E(KU_{AutCert}, KR_1 || ID_{Trans})$$

Observe que como a chave pública KU_{Vend}, do *Vendedor*, é certificada, ela é a única que consegue decifrar uma mensagem cifrada com KR_{Vend}.

Ao decifrar a mensagem oriunda do *Vendedor* e obter ID_{Imovel}, o *Cartório* tem a certeza de que foi realmente o *Vendedor* que enviou a mensagem, pois somente ele possui sua chave privada KR_{Vend}. Isso possibilita ao *Cartório* reconhecer a firma da assinatura do *Vendedor*.

Além disso, ele obtém outra informação:

$$E(KU_{AutCert}, KR_1 || ID_{Trans})$$

Essa informação está cifrada com a chave pública da *Autoridade Certificadora* e somente ela consegue decifrá-la.

Isso garante ao *Vendedor* que o *Cartório* não tem conhecimento de sua subchave KR_1.

O processo de reconhecimento de firma do *Comprador* é similar ao do *Vendedor*.

Comprador

Comprador envia ao *Cartório* a sua subchave e a identificação da transação que corresponde ao imóvel vendido. Essas informações são cifradas utilizando a chave pública da *Autoridade Certificadora*. Além disso, também envia a identificação do imóvel. Todas as informações são cifradas utilizando a chave privada do *Comprador*, da seguinte forma:

$$E(KR_{Comp}, ID_{Imovel} || E(KU_{AutCert}, KR_2 || ID_{Trans}))$$

Figura 5.11: *Comprador* envia sua subchave ao *Cartório*.

Quando o *Cartório* recebe a informação cifrada do *Comprador*, ele a decifra utilizando a chave pública do mesmo KU_{Comp}, obtendo:

$$ID_{Imovel} \text{ e } E(KU_{AutCert}, KR_2 || ID_{Trans})$$

Como KU_{Comp} é certificada, ela é a única capaz de decifrar uma mensagem cifrada com KR_{Comp}. Ao decifrar a mensagem utilizando KU_{Comp}, o *Cartório* tem a certeza de que foi realmente o *Comprador* que enviou a mensagem, pois somente ele possui sua chave privada KR_{Comp}. Isso possibilita ao *Cartório* reconhecer a firma da assinatura do *Comprador*.

Além disso, ele obtém também:

$$E(KU_{AutCert}, KR_2||ID_{Trans})$$

Essa está cifrada com a chave pública da *Autoridade Certificadora* e somente ela consegue decifrá-la. Isso garante ao *Comprador* que o *Cartório* não tem conhecimento de sua subchave KR_2.

Observe que o *Cartório* recebe a identificação do imóvel negociado do *Vendedor* e *Comprador*. Como são entidades distintas fornecendo a mesma informação, caso sejam iguais, é garantido ao *Cartório* que a identificação do imóvel negociado está correta.

Após a identificação das partes e do imóvel, o *Cartório* preenche a escritura de compra e venda com os dados do *Vendedor*, *Comprador* e Imóvel.

Considere que o texto da escritura seja denotado por: $m_{Escritura}$.

Para garantir a integridade da escritura preenchida, o *Cartório* emite um selo de identificação único σ, utilizando uma função *hash* H, segura, da seguinte forma:

$$\sigma = H(m_{Escritura})$$

A partir daí, o *Cartório* solicita à *Autoridade Certificadora* a emissão de uma assinatura com reconhecimento de firma e autenticidade para o selo de identificação único da escritura de compra e venda σ, como mostra a figura 5.12:

Ao decifrar *request*, oriundo do *Cartório*, com sua chave privada $KR_{AutCert}$, a *Autoridade Certificadora* obtêm:

$$m_{Escritura}$$

$$E(KR_{Cart}, ||KR_3||ID_{Trans})$$

$$E(KU_{AutCert}, KR_1||ID_{Trans})$$

$$E(KU_{AutCert}, KR_2||ID_{Trans})$$

A *Autoridade Certificadora* então calcula outro selo de identificação único da escritura de compra e venda, obtendo:

Cartório

O *Cartório* envia uma solicitação para emissão de uma assinatura digital com reconhecimento de firma e autenticidade em σ, tal que

$$\sigma = H(m_{Escritura})$$

Essa solicitação contém:

- A escritura de compra e venda do imóvel preenchida $m_{Escritura}$
- O selo de identificação único da escritura σ
- A subchave do *Vendedor* $E(KU_{AutCert}, KR_1||ID_{Trans})$
- A subchave do *Comprador* $E(KU_{AutCert}, KR_2||ID_{Trans})$
- A subchave do *Cartório* e identificação da transação $E(KU_{Cart}, KR_3||ID_{Trans})$

Da seguinte forma:

$$\begin{aligned} request = E(KU_{AutCert}, m_{Escritura} \quad &|| \quad E(KR_{Cart}, \sigma||KR_3||ID_{Trans}) \\ &|| \quad E(KU_{AutCert}, KR_1||ID_{Trans}) \\ &|| \quad E(KU_{AutCert}, KR_2||ID_{Trans})) \end{aligned}$$

Figura 5.12: *Cartório* envia solicitação da Assinatura Digital para *Autoridade Certificadora*

$$\sigma^{'} = H(m_{Escritura})$$

Para certificar-se de que a solicitação *request* realmente veio do *Cartório*, a *Autoridade Certificadora* decifra $E(KR_{Cart}, \sigma||KR_3||ID_{Trans})$ utilizando a chave pública do Cartório KU_{Cart} e obtêm:

$$\sigma$$

$$KR_3$$

$$ID_{Trans}$$

Após isso, a *Autoridade Certificadora* verifica a igualdade:

$$\sigma = \sigma^{'}$$

Caso a igualdade seja confirmada, tem-se a certeza de que a solicitação partiu do *Cartório*.

Além disso, é garantida a integridade da escritura de compra e venda $m_{Escritura}$. Com o processo de verificação completo, a *Autoridade Certificadora* inicia a emissão da assinatura no selo de identificação único da escritura de compra e venda σ. Ela decifra ainda $E(KU_{AutCert}, KR_1||ID_{Trans})$

e $E(KU_{AutCert}, KR_2 \| ID_{Trans})$, utilizando sua chave privada $KR_{AutCert}$ obtendo:

$$KR_1$$

$$KR_2$$

$$ID_{Trans}$$

Nesse instante, a *Autoridade Certificadora* possui as subchaves KR_1, KR_2 e KR_3 pertencentes respectivamente ao *Vendedor*, *Comprador* e *Cartório*.

Porém, para a emissão da assinatura é necessária a participação de pelo menos duas testemunhas, as quais atestarão a existência do negócio.

A *Autoridade Certificadora* então escolhe aleatoriamente duas testemunhas em um conjunto de w pertencentes à jurisdição do *Cartório* e solicita suas subchaves.

Essas, por sua vez, enviam suas subchaves para a *Autoridade Certificadora* conforme mostra a figura 5.13:

Testemunhas
Duas *Testemunhas* escolhidas aleatoriamente e pertencentes à jurisdição do *Cartório* enviam suas subchaves a *Autoridade Certificadora*: $$E(KU_{AutCert}, E(KR_{Ti}, KR_{4_i} \| ID_{Trans}))$$

Figura 5.13: *Testemunhas* enviam suas subchaves para a *Autoridade Certificadora*

Após receber as subchaves das *Testemunhas*, a *Autoridade Certificadora* decifra as mensagens utilizando sua chave privada $KR_{AutCert}$ e obtêm:

$$E(KR_{Ti}, KR_{4_i} \| ID_{Trans})$$

A *Autoridade Certificadora* então decifra cada mensagem utilizando as respectivas chaves públicas de cada *Testemunhas* KU_{Ti}.

Como somente as *Testemunhas* possuem as chaves privadas KR_{Ti}, a *Autoridade Certificadora* tem certeza de que as subchaves vieram realmente das *Testemunhas*.

Observe que as *Testemunhas* não reconhecem nenhuma firma. Elas apenas atestam a existência da escritura.

De posse das duas subchaves das *Testemunhas* KR_{4_i}, a *Autoridade Certificadora* recalcula KR_4, utilizando o esquema de compartilhamento de segredos $(w, 2)$.

A garantia de que todas as subchaves, KR_1, KR_2, KR_3 e KR_4 pertencem à mesma transação é dada pela identificação da transação ID_{Trans} enviada anteriormente por cada parte envolvida.

Nesse momento, a *Autoridade Certificadora* utiliza, novamente, o esquema de compartilhamento de segredos $(4, 4)$ e reconstrói KR_{Trans}.

Ela utiliza essa chave para assinar o selo de identificação único da escritura de compra e venda do imóvel, conforme figura 5.14:

Autoridade Certificadora

A *Autoridade Certificadora* de posse das quatro subchaves, reconstrói KR_{Trans}, assina o selo de identificação único para a escritura de compra de venda do imóvel, utilizando uma função de assinatura baseada no esquema de assinatura do RSA explicado em 4.4.

$$y = sig(KR_{Trans}, \sigma)$$

Após a criação da assinatura, a *Autoridade Certificadora* responde ao *request* enviando para o *Cartório*:

$$E(KU_{Cart}, y)$$

Figura 5.14: Reconstrução de KR_{Trans}

O *Cartório*, por sua vez, decifra a resposta da *Autoridade Certificadora* utilizando sua chave privada KR_{Cart},obtendo:

$$y$$

Se é o desejo de qualquer pessoa verificar se y realmente corresponde à respectiva assinatura da escritura de compra e venda do imóvel, utiliza-se a função de verificação de assinatura baseada no esquema de assinatura do RSA, obtendo-se:

$$\sigma'' = ver(KU_{Trans}, y)$$

Se a igualdade de σ'' e σ é verificada, então, tem-se a certeza de que y corresponde à assinatura no documento solicitado em *request*.

Nesse caso, a assinatura y garante:

- O reconhecimento de firma do *Vendedor*, *Comprador*, *Cartório* e *Testemunhas*;
- A vontade do *Comprador* e *Vendedor* em realizar o negócio;
- A integridade da escritura de compra e venda do imóvel;
- A autenticidade das assinaturas na escritura de compra e venda do imóvel.

Portanto, o protocolo garante a segurança na emissão de uma assinatura em uma escritura de compra e venda de imóvel.

5.3 Exemplo de uso do protocolo proposto

Este exemplo considera a emissão de uma assinatura digital com reconhecimento de firma e autenticação por uma *Autoridade Certificadora* em uma escritura de compra e venda de imóvel.

Como se trata de um exemplo didático, não se teve a preocupação de trabalhar com números grandes, visando a segurança do protocolo. Portanto, são considerados números pequenos, o que não ocorre na realidade.

Suponha, então, que *Alice* deseja vender um imóvel para *Bob*.

Para formalizar o negócio, ambos procuram um cartório que ofereça esse tipo de serviço pela internet. Essa formalização é feita através da emissão de uma escritura de compra e venda atestando que o imóvel foi vendido de *Alice* para *Bob*. Nesse documento, todas as assinaturas devem ter sua firma reconhecida, além de autenticadas pelo *Cartório*. É necessário ainda garantir a integridade do conteúdo do documento após assinado. Também assinam duas testemunhas que atestam a existência do documento e a formalização do negócio.

Alice, a *Vendedora* do imóvel, encontra um *Cartório*, em Araxá, que oferece esse tipo de serviço pela internet. Esse *Cartório* possui cinco entidades próximas pertencentes a sua jurisdição, e que estão habilitadas a testemunhar a existência de negócios como o citado acima.

Considere que *Alice*, a *Vendedora*, *Bob*, o *Comprador*, o *Cartório* de Araxá e *Testemunhas* possuem cada um, uma identificação única e um par de chaves, privada e pública, que são utilizados para transmitir informações seguras. Todas as chaves públicas são certificadas por uma *Autoridade Certificadora* que garante a propriedade de cada chave. Além do mais, são chaves geradas segundo as propriedades do algoritmo RSA.

Supondo, então, as seguintes definições de cada participante do protocolo:

Alice→ possui a chave privada KR_{Alice} correspondente à chave pública KU_{Alice}; e uma identificação única ID_{Alice}.

Bob→ possui a chave privada KR_{Bob} correspondente à chave pública KU_{Bob}; e uma identificação única ID_{Bob}.

Cart-Araxá→ possui a chave privada KR_{Cart} correspondente à chave pública KU_{Cart}; e uma identificação única KR_{Cart}.

Testemunhas$_i$ → possuem a chave privada KR_{Ti} correspondente à chave pública KU_{Ti}; e uma identificação única KR_{Ti}; tal que $i \leq 1 \leq 5$.

Autoridade Certificadora→ possui a chave privada $KR_{AutCert}$ correspondente à chave pública $KU_{AutCert}$; e uma identificação única $KR_{AutCert}$.

Considere que o valor de cada chave é definido a seguir na tabela 5.1:

Tabela 5.1: Participantes com suas respectivas chaves, pública e privada, e identificação.

Participante	*Chave Pública*	*Chave Privada*	*ID*
Alice	13	2.088.565	1
Bob	17	798.569	2
Cart-Araxá	29	3.745.013	3
Marques	211	5.790.571	4
Gabriel	337	4.149.241	5
Humberto	37	660.4381	6
Daniele	311	1.222.247	7
Cíntia	119	2.053.463	8
Autoridade Certificadora	103	5.140.303	9

Todas as chaves definidas na tabela 5.1 são geradas com base no esquema de assinatura do RSA. São considerados para geração de tais valores de chaves, os valores.

$$p = 4.027 \text{ e } q = 3.373$$

Então

$$n = 13.583.071 \text{ e } \phi(n) = 13.675.672$$

Alice então procura o *Cartório* de Araxá e informa seus dados e os de *Bob*. O *Cartório* de Araxá, por sua vez, solicita a uma *Autoridade Certificadora* a emissão de uma assinatura única para uma escritura de compra e venda.

A *Autoridade Certificadora*, por sua vez, cria uma identificação única para a transação.

Considere que a identificação da transação seja denotada por ID_{Trans}

Suponha que $ID_{Trans} = 88$

A *Autoridade Certificadora*, por sua vez, envia para o *Vendedor*, *Comprador* e *Cartório* essa identificação, de forma sigilosa. Ela cifra ID_{Trans} com a chave pública de cada um, e em seguida, envia o resultado para os participantes, da seguinte forma:

Considere que a *Autoridade Certificadora* envia para:

Alice: $E(KU_{Alice}, ID_{Trans}) = 88^{13} \bmod 13.583.071 = 5.139.513$

Comprador: $E(KU_{Bob}, ID_{Trans}) = 88^{17} \bmod 13.583.071 = 12.329.134$

Cartório: $E(KU_{Cart}, ID_{Trans}) = 88^{29} \bmod 13.583.071 = 5.383.653$

Cada participante recebe a informação da *Autoridade Certificadora* e a decifra utilizando suas respectivas chaves privadas, obtendo:

Alice: $D(KR_{Alice}, 5.139.513) = 5.139.513^{2.088.565} \bmod 13.583.071 = 88$

Comprador: $D(KR_{Comp}, 12.329.134) = 12.329.134^{798.569} \bmod 13.583.071 = 88$

Cartório: $D(KR_{Cart}, 5.383.653) = 5.383.653^{3.745.013} \bmod 13.583.071 = 88$

Visto que, somente os participantes possuem as chaves secretas, as informações só podem ser decifradas por eles próprios, garantindo assim, o sigilo da informação.

Nesse instante, cada participante conhece o valor de ID_{Trans} fornecido pela *Autoridade Certificadora*. Eles, por sua vez, cifram o valor de ID_{Trans} com suas respectivas chaves privadas e geram novas chaves K_1, K_2 e K_3 que são utilizadas para formar a assinatura digital da escritura. As chaves K_1, K_2 e K_3 são definidas como:

Alice: $K_1 = E(KR_{Alice}, ID_{Trans}) = 88^{2.088.565} \bmod 13.583.071 = 2.956.102$

Bob: $K_2 = E(KR_{Bob}, ID_{Trans}) = 88^{978.569} \bmod 13.583.071 = 7.752.869$

Cartório: $K_3 = E(KR_{Cart}, ID_{Trans}) = 88^{3.745.013} \bmod 13.583.071 = 7.988.787$

Depois de geradas as chaves K_1, K_2 e K_3, elas são cifradas com a chave pública da *Autoridade Certificadora* e enviadas para a mesma.

Alice envia:$K_1 = E(KU_{CertAut}, K_1) = 2.956.102^{103} \bmod 13.583.071 = 4.865.957$

Bob envia: $K_2 = E(KU_{CertAut}, K_2) = 7.752.869^{103} \bmod 13.583.071 = 6.324.859$

Cartório envia:$K_3 = E(KU_{CertAut}, K_3) = 7.988.787^{103} \bmod 13.583.071 = 8.364.250$

Isso garante que somente a *Autoridade Certificadora* conhece os valores de K_1, K_2 e K_3, pois é a única que consegue decifrar essas informações, obtendo:

$K_1 = D(KR_{CertAut}, 4.865.957) = 4.865.957^{5.140.303} \bmod 13.583.071 = 2.956.102$

$K_2 = D(KR_{CertAut}, 6.324.859) = 6.324.859^{5.140.303} \bmod 13.583.071 = 7.752.869$

$K_3 = D(KR_{CertAut}, 8.364.250) = 8.364.250^{5.140.303} \bmod 13.583.071 = 7.988.787$

Nesse ponto do protocolo, a *Autoridade Certificadora* calcula a chave pública KU_{Trans} a partir das chaves K_1, K_2 e K_3 entregues respectivamente por *Alice*, *Bob*, e *Cartório*.

Sendo assim, a *Autoridade Certificadora* calcula:

$$KU_{Trans} = (K_1 \times K_2 + K_3) \bmod (\phi(n))$$

Obtendo:

$$KU_{Trans} = (2.956.102 \times 7.752.869 + 7.988.787)(\text{mod } 13.575.672) = 6.558.761$$

Depois de calculado esse valor, a *Autoridade Certificadora* verifica a primariedade entre KU_{Trans} e $\phi(n)$. Isso pode ser feito através do Algoritmo de Euclides detalhado na seção 4.6 desse trabalho. Esse passo é essencial para que a geração das chaves, pública e privada, seja assimétrica. Portanto é calculado:

$$mdc(KU_{Trans}, \phi(n))$$

Tal que:

$$mdc(6.558.761, 13.575.672) = 11$$

Esse resultado mostra que os números não são primos entre si, pois o

$$mdc(KU_{Trans}, \phi(n)) \neq 1$$

A *Autoridade Certificadora* então faz a requisição de um novo valor de chave K_4 para o *Cartório*. A chave K_4 substitui a chave K_3 e KU_{Trans} será formada da seguinte forma:

$$KU_{Trans} = K_1 \times K_2 + K_4 \bmod (\phi(n))$$

A *Autoridade Certificadora* requisita então ao *Cartório* o valor para a chave K_4. O *Cartório*, por sua vez, calcula o valor de K_4 e o envia para a *Autoridade Certificadora* da seguinte forma:

$$K_4 = K_3 + 1$$

Tal que:

$$K_4 = 7.988.787 + 1 = 7.988.788$$

O *Cartório*, então, cifra K_4 com a chave pública da *Autoridade Certificadora* e a envia para a *Autoridade Certificadora* tal que:

$$E(KU_{AutCert}, K_4) = 7.988.788^{103} \bmod 13.583.071 = 13.368.744$$

A *Autoridade Certificadora* recebe o valor de K_4 cifrado, decifra-o obtendo:

$$D(KR_{AutCert}, 13.368.744) = 13.368.744^{5.140.303} \bmod 13.583.071 = 7.988.788$$

A *Autoridade Certificadora* calcula então o valor de KU_{Trans}

$$KU_{Trans} = K_1 \times K_2 + K_4 \bmod (\phi(n))$$

Obtendo:

$$KU_{Trans} = (2.956.102 \times 7.752.869 + 7.988.788)((mod)13.575.672) = 6.558.762$$

Porém, a primariedade entre KU_{Trans} e $\phi(n)$, também não é atendida, pois:

$$mdc(6.558.762, 13.575.672) = 6$$

A *Autoridade Certificadora* então, solicita um novo valor de K_4 para o *Cartório*. Esse, por sua vez, incrementa em uma unidade o valor anterior de K_4 e obtendo 7.988.789. O *Cartório* cifra o valor de K_4 e o envia para a *Autoridade Certificadora*.

Após decifrar o novo valor de K_4, a *Autoridade Certificadora* recalcula KU_{Trans} e testa novamente sua primariedade em relação à $\phi(n)$. Dessa vez, a propriedade de primariedade é atendida obtendo, portanto, o valor da chave pública da transação KU_{Trans}da seguinte forma:

$$KU_{Trans}(2.956.102 \times 7.752.869 + 7.988.789)(\text{ mod } 13.575.672) = 6.558.763$$

E, portanto

$$mdc(6.558.763, 13.575.672) = 1$$

A *Autoridade Certificadora* então define KU_{Trans} como se segue:

$$KU_{Trans} = K_1 \times K_2 + K_4 = 6.558.763$$

A partir de

$$KU_{Trans}$$

a *Autoridade Certificadora*, utilizando o algoritmo de Euclides estendido mostrado na figura 4.6, determina

$$KR_{Trans} = 3.649.003$$

Uma vez determinado os pares de chaves, pública e privada, a *Autoridade Certificadora* promove a divisão da chave privada KR_{Trans} utilizando o algoritmo de compartilhamento de segredos de limiar, em um esquema (4,4) criando assim as subchaves: KR_1, KR_2, KR_3 e KR_4

Considere, portanto, que o limiar definido é quatro, a *Autoridade Certificadora* define um polinômio de grau três aleatoriamente.

Suponha o polinômio definido como:

$$rx^3 + sx^2 + ux + k \text{ (mod } q)$$

No qual

- r, s e u são coeficientes gerados aleatoriamente e menores que q;
- k é a constante do polinômio e recebe o segredo a ser compartilhado;
- q é o módulo;

Considere que os valores dos coeficientes r, s e u do polinômio e o módulo q são definidos de forma aleatória e possuem os valores:

$$r = 17.890$$

$$s = 568.903$$

$$u = 59.951$$

$$KR_{Trans} = k = 3.649.003$$

$$q = 13.994.087$$

Logo, o polinômio é dado por:

$$17.890x^3 + 568.903x^2 + 59.951x + 3.649.003 (\text{mod } 13.994.087)$$

Conforme definido, anteriormente, um esquema $(4, 4)$ de compartilhamento de segredos divide o segredo em quatro partes. Calculam-se, então, as sombras Y_i, $1 \leq i \leq 4$, que são entregues aos quatro participantes do protocolo *Alice*, *Bob*, *Cartório* de Araxá e *Testemunhas*. Nesse caso, cada participante é denotado por a_i; $1 \leq i \leq 4$. Cada participante do protocolo a_i recebe seu valor sombra Y_i, que é utilizado para reconstrução do segredo, tal que:

$$a(1) = 17.890 \times 1^3 + 568.903 \times 1^2 + 59.951 \times 1 + 3.649.003 (\text{mod } 13.994.087) = 4.295.747$$
$$a(2) = 17.890 \times 2^3 + 568.903 \times 2^2 + 59.951 \times 2 + 3.649.003 (\text{mod } 13.994.087) = 6.187.637$$
$$a(3) = 17.890 \times 3^3 + 568.903 \times 3^2 + 59.951 \times 3 + 3.649.003 (\text{mod } 13.994.087) = 9.432.013$$
$$a(4) = 17.890 \times 4^3 + 568.903 \times 4^2 + 59.951 \times 4 + 3.649.003 (\text{mod } 13.994.087) = 142.128$$

E, conforme os cálculos anteriores,

$$a(1) = Y_1 = 4.295.747$$
$$a(2) = Y_2 = 6.187.637$$
$$a(3) = Y_3 = 9.432.013$$

$a(4) = Y_4 = 142.128$

De tal forma que:

Alice recebe o par $(1, 4.295.747)$

Bob recebe o par $(2, 6.187.637)$

O *Cartório* recebe o par $(3, 9.432.013)$

O par $(4, 142.128)$ é dividido e entregue ao conjunto de Testemunhas T

Em uma escritura de compra e venda de imóveis são necessárias duas testemunhas para atestarem a existência do negócio.

Conforme definições anteriores, existem cinco entidades autorizadas a testemunhar um documento reconhecido pelo *Cartório*. Então a *Autoridade Certificadora* utiliza novamente o esquema de compartilhamento de segredos de limiar, para dividir Y_4 de acordo com o número de entidades autorizadas, ou seja, cinco.

Portanto, a *Autoridade Certificadora* divide Y_4 utilizando agora o esquema $(2, 5)$ no qual 2(dois) é o limiar necessário para reconstruir o segredo, representando duas em um conjunto de cinco *Testemunhas* que receberão as sombras.

Considere outro polinômio gerado aleatoriamente pela *Autoridade Certificadora* que é utilizado para dividir y_4 de grau um definido como:

$$ex + f \pmod{g}$$

Considere ainda, que o valor do coeficiente e do polinômio e o módulo g são definidos de forma aleatória e possui os valores:

$$e = 43.411$$

$$g = 13.994.087$$

Logo, o polinômio é dado por:

$$43.411x + 142.128 \text{ (mod } 13.994.087)$$

Conforme definido anteriormente, um esquema $(2, 5)$ de compartilhamento de segredos divide o segredo em cinco partes. Calculam-se, então, as sombras Y_{4_i}; $1 \leq i \leq 5$, que são entregues aos cinco participantes do protocolo, as $Testemunhas_i$, tal que $1 \leq i \leq 5$. Nesse caso, cada participante é denotado por a_{4_i}, $1 \leq i \leq 5$. Cada participante do protocolo a_{4_i} recebe seu valor sombra Y_{4_i}, que é utilizado para reconstrução do segredo. E, conforme os cálculos:

$a_{4_1} = Y_{4_1} = 185.539$

$a_{4_2} = Y_{4_2} = 228.950$

$a_{4_3} = Y_{4_3} = 272.361$

$a_{4_4} = Y_{4_4} = 315.772$

$a_{4_5} = Y_{4_5} = 359.183$

De tal forma que:

A $Testemunha_1$, *Marques*, recebe o par (1, 185.539)

A $Testemunha_2$, *Gabriel*, recebe o par (2,228.950)

A $Testemunha_3$, *Humberto*, recebe o par (3, 272.361)

A $Testemunha_4$, *Daniele*, recebe o par (4, 315.772)

A $Testemunha_5$, *Cíntia*, recebe o par (5, 359.183)

Nesse instante, cada participante possui seu valor de sombra ou subchave, oriundo da divisão de KR_{Trans}. Tem-se portanto, como participantes do protocolo, *Alice*, *Bob*, *Cartório* de Araxá além de cinco Testemunhas. Esses com suas respectivas sombras são mostradas a seguir na tabela 5.2:

Tabela 5.2: Participantes com suas respectivas identificações e sombras

Participante	*Chave* K_i	*Sombra*	*Ordem*
Alice	KR_1	4.295.747	1
Bob	KR_2	6.187.637	2
Cart-Araxá	KR_3	9.432.013	3
Marques	KR_{4_1}	185.539	4_1
Gabriel	KR_{4_2}	228.9501	4_2
Humberto	KR_{4_3}	272.361	4_3
Daniele	KR_{4_4}	315.772	4_4
Cíntia	KR_{4_5}	359.183	4_5

A emissão da assinatura digital na escritura de compra e venda do imóvel com reconhecimento de firma e autenticação é iniciada quando *Alice* envia sua subchave, a identificação da transação e a identificação do imóvel para o *Cartório*. Essas informações são cifradas utilizando a chave pública da *Autoridade Certificadora* e posteriormente a chave privada de *Alice*, como a seguir:

$$E(KR_{Alice}, ID_{Imovel} || E(KU_{AutCert}, KR_1 || ID_{Trans}))$$

Supondo que o imóvel possua a identificação de número 34, em que:

$$ID_{Imovel} = 34$$

Alice então envia para o*Cartório*:

$$E(2.088.565, 34||E(103, 4.277.857||88))$$

que utiliza a chave pública da *Autoridade Certificadora* $KU_{AutCert}$ calculando:

$$4.295.747^{103} \bmod 13.583.071 = 8.373.218$$

$$88^{103} \bmod 13.583.071 = 10.363.487$$

Depois cifra a identificação do imóvel e o resultado calculado acima com sua chave privada KR_{Alice}, obtendo

$$34^{2.088.565} \bmod 13.583.071 = 6.159.416$$

$$8.373.218^{2.088.565} \bmod 13.583.071 = 9.039.772$$

$$10.363.487^{2.088.565} \bmod 13.583.071 = 4.865.957$$

Tal que;

$$6.159.416||(9.039.772||4.865.957)$$

É o resultado de

$$E(2.088.565, 34||E(103, 4.277.857||88))$$

que é enviado para o *Cartório*.

O *Cartório* recebe as informações acima e utilizando a chave pública de *Alice* decifra parte da informação, da seguinte forma:

$$D(KU_{Alice}, E(KR_{Alice}, ID_{Imovel}||E(KU_{AutCert}, KR_1||ID_{Trans})))$$

Que substituindo os valores tem-se:

$$D(13, 6.159.416||(9.039.772||4.865.957))$$

em que

$$6.159.416^{13} \bmod 13.583.071 = 34$$

$$9.039.772^{13} \bmod 13.583.071 = 8.373.218$$

$$4.865.957^{13} \bmod 13.583.071 = 10.363.487$$

Obtendo

$$ID_{Imovel} = 34$$

E o valor cifrado com a chave pública da *Autoridade Certificadora*

$$(8.373.218||10.363.487)$$

Que representam respectivamente

$$ID_{Imovel} \text{ e } E(KU_{AutCert}, KR_1||ID_{Trans})$$

O *Cartório*, então, armazena esses valores até que o comprador, *Bob*, envie seus dados.

Bob, por sua vez, também envia suas informações para o *Cartório*. Ele envia sua subchave, a identificação da transação e a identificação do imóvel. Essas informações são cifradas utilizando a chave pública da *Autoridade Certificadora* e a sua chave privada, como a seguir:

$$E(KR_{Bob}, ID_{Imovel}||E(KU_{AutCert}, KR_2||ID_{Trans}))$$

Bob então envia para o *Cartório*:

$$E(798.569, 34||E(103, 6.187.637||88))$$

em que utiliza a chave pública da *Autoridade Certificadora* a $KU_{AutCert}$ calculando:

$$6.187.637^{103} \bmod 13.583.071 = 6.279.863$$

$$88^{103} \bmod 13.583.071 = 10.363.487$$

Depois, cifra a identificação do imóvel e o resultado calculado acima com sua chave privada KR_{Bob}, obtendo:

$$34^{798.569} \bmod 13.583.071 = 10.788.298$$

$$6.279.863^{798.569} \bmod 13.583.071 = 4.672.726$$

$$10.363.487^{798.569} \bmod 13.583.071 = 6.324.859$$

Tal que;

$$10.788.298||(4.672.726||6.324.859)$$

É o resultado de

$$E(798.569, 34||E(103, 6.187.637||88))$$

O *Cartório* recebe as informações acima e utilizando a chave pública de *Bob* decifra parte da informação, da seguinte forma:

$$D(KU_{Bob}, E(KR_{Bob}, ID_{Imovel}||E(KU_{AutCert}, KR_2||ID_{Trans})))$$

Que substituindo os valores tem-se:

$$D(17, 10.788.298||(4.672.726||6.324.859)$$

no qual

$$10.788.298^{17} \bmod 13.583.071 = 34$$

$$4.672.726^{17} \bmod 13.583.071 = 6.279.863$$

$$6.324.859^{17} \bmod 13.583.071 = 10.363.487$$

Obtendo

$$ID_{Imovel} = 34$$

E o valor cifrado com a chave pública da *Autoridade Certificadora*

$$(6.279.863||10.363.487)$$

Que representam respectivamente

$$ID_{Imovel} \text{ e } E(KU_{AutCert}, KR_2||ID_{Trans})$$

Observe que o *Cartório* recebe a identificação do imóvel negociado de *Alice* e *Bob*. Como são entidades distintas fornecendo a mesma informação, o *Cartório* tem certeza de que a identificação do imóvel negociado está correta, ou seja:

$$ID_{Imovel} = 34$$

Após a identificação das partes e do imóvel, o *Cartório* preenche a escritura de compra e venda com os dados de *Alice*, *Bob* e do Imóvel.

Considere que a escritura de compra e venda do imóvel é denotado por:

$$m_{Escritura}$$

Para garantir a integridade da escritura devidamente preenchida, o *Cartório*, emite um selo de identificação único σ para $m_{Escritura}$, utilizando uma função hash, H, segura, da seguinte forma:

$$\sigma = H(m_{Escritura})$$

Supondo que;

$$m_{Escritura} = 100$$

Então, considere que seu selo de identificação é calculado como;

$$\sigma = 101$$

A partir daí, o *Cartório* solicita a *Autoridade Certificadora* a emissão de uma assinatura com reconhecimento de firma e autenticidade para o selo de identificação único da escritura de compra e venda σ.

O *Cartório* cifra algumas informações com sua chave privada e posteriormente com a chave pública da *Autoridade Certificadora*.

Considere que a requisição é denotada por *request*.

Tal que;

$$\begin{aligned} request = E(KU_{AutCert}, m_{Escritura} \quad &|| \quad E(KR_{Cart}, \sigma||KR_3||ID_{Trans}) \\ &|| \quad E(KU_{AutCert}, KR_1||ID_{Trans}) \\ &|| \quad E(KU_{AutCert}, KR_2||ID_{Trans})) \end{aligned}$$

Que substituindo os valores tem-se:

$$\begin{aligned} request = E(103, 100 \quad &|| \quad E(3.745.013, 101||9.432.013||88) \\ &|| \quad E(103, 4.295.747||88) \\ &|| \quad E(103, 6.187.637||88)) \end{aligned}$$

O *Cartório*, então, utiliza sua chave privada KR_{Cart} e cifra:

$$E(3.745.013, 101||9.432.013||88)$$

Tal que;

$$1013.745.013 \bmod 13.583.071 = 10.868.551$$

$$9.432.013^{3.745.013} \bmod 13.583.071 = 12.312.555$$

$$88^{3.745.013} \bmod 13.583.071 = 7.988.787$$

Depois cifra toda a informação de *request* utilizando a chave pública da *Autoridade Certificadora* obtendo:

$$100^{103} \bmod 13.583.071 = 1.447.930$$

$$||$$

$$10.868.551^{103} \bmod 13.583.071 = 1.680.061$$

$$12.312.555^{103} \bmod 13.583.071 = 8.191.912$$

$$7.988.787^{103} \bmod 13.583.071 = 8.364.250$$

$$||$$

$$8.373.218^{103} \bmod 13.583.071 = 4.835.157$$

$$10.363.487^{103} \bmod 13.583.071 = 1.515.146$$

$$||$$

$$6.279.863^{103} \bmod 13.583.071 = 7.036.886$$

$$10.363.487^{103} \bmod 13.583.071 = 1.515.146$$

Tal que;

$$\begin{aligned} request = (1.447.930 \quad &|| \quad (1.680.061||8.191.912||8.364.250) \\ &|| \quad (4.835.157||1.515.146) \\ &|| \quad (7.036.886||1.515.146)) \end{aligned}$$

É o resultado de

$$\begin{aligned} request = E(103, 100 \quad &|| \quad E(3.745.013, 101||9.432.013||88) \\ &|| \quad E(103, 4.295.747||88) \\ &|| \quad E(103, 6.187.637||88)) \end{aligned}$$

Depois de calculado o conteúdo da requisição da assinatura digital, o *Cartório* envia *request* para a *Autoridade Certificadora*.

Ao receber a requisição do *Cartório* a *Autoridade Certificadora* decifra *request*, com sua chave privada $KR_{AutCert}$, da seguinte forma:

$$\begin{aligned} D(KR_{AutCert}, E(KU_{AutCert}, m_{Escritura} \quad &|| \quad E(KR_{Cart}, \sigma||KR_3||ID_{Trans}) \\ &|| \quad E(KU_{AutCert}, KR_1||ID_{Trans}) \\ &|| \quad E(KU_{AutCert}, KR_2||ID_{Trans}))) \end{aligned}$$

Que substituindo os valores tem-se:

$$\begin{aligned} D(5.140.303, (1.447.930 \quad &|| \quad (1.680.061||8.191.912||8.364.250) \\ &|| \quad (4.835.157||1.515.146) \\ &|| \quad (7.036.886||1.515.146))) \end{aligned}$$

E calculando, obtém:

$$1.447.930^{5.140.303} \bmod 13.583.071 = 100$$

Ou seja;

$$m_{Escritura} = 100$$

E os valores cifrados;

$$1.680.061^{5.140.303} \bmod 13.583.071 = 10.868.551$$

$$8.191.912^{5.140.303} \bmod 13.583.071 = 12.312.555$$

$$8.364.250^{5.140.303} \bmod 13.583.071 = 7.988.787$$

$$\|$$

$$4.835.157^{5.140.303} \bmod 13.583.071 = 8.373.218$$

$$1.515.146^{5.140.303} \bmod 13.583.071 = 10.363.487$$

$$\|$$

$$7.036.886^{5.140.303} \bmod 13.583.071 = 6.279.863$$

$$1.515.146^{5.140.303} \bmod 13.583.071 = 10.363.487$$

A *Autoridade Certificadora*, então, calcula um novo selo de identificação único da escritura de compra e venda, da seguinte forma:

$$\sigma' = H(m_{Escritura})$$

$$\sigma' = H(100)$$

Obtendo;

$$\sigma' = 101$$

Para certificar-se de que a solicitação *request* realmente veio do *Cartório*, a *Autoridade Certificadora* decifra $E(KR_{Cart}, \sigma \| KR_3 \| ID_{Trans})$ utilizando a chave pública do *Cartório* KU_{Cart}, em que:

$$E(KR_{Cart}, \sigma || KR_3 || ID_{Trans})$$

que representa;

$$(1.680.061 || 8.191.912 || 8.364.250)$$

É decifrado da seguinte forma:

$$10.868.551^{29} \bmod 13.583.071 = 101$$

$$12.312.555^{29} \bmod 13.583.071 = 9.432.013$$

$$10.516.058^{29} \bmod 13.583.071 = 88$$

no qual

$$\sigma = 101$$

$$KR_3 = 9.432.013$$

$$ID_{Trans} = 88$$

Após isso, a *Autoridade Certificadora* verifica a igualdade:

$$\sigma = \sigma^{'}$$

Essa verificação garante a integridade da escritura de compra e venda $m_{Escritura}$. Após essa verificação, a *Autoridade Certificadora* usa novamente sua chave privada e decifra o restante da informação, em que:

$$E(KU_{AutCert}, KR_1 || ID_{Trans})$$

Que representa:

$$E(5.140.303, 8.373.218 || 10.363.487)$$

É decifrado da seguinte forma;

$$8.373.218^{5.140.303} \bmod 13.583.071 = 4.295.747$$

$$10.363.487^{5.140.303} \bmod 13.583.071 = 1.515.146$$

que são respectivamente;

$$KR_1 = 4.295.747$$

e

$$ID_{Trans} = 4.295.747$$

A *Autoridade Certificadora* usa novamente sua chave privada e decifra o restante da informação, onde:

$$E(KU_{AutCert}, KR_2||ID_{Trans})$$

Que representa:

$$E(5.140.303, 6.279.863||10.363.487)$$

É decifrado da seguinte forma;

$$6.279.863^{5.140.303} \bmod 13.583.071 = 6.187.637$$

que são respectivamente;

$$KR_2 = 6.187.637$$

e

$$ID_{Trans} = 88$$

Nesse instante, a *Autoridade Certificadora* possui as subchaves KR_1, KR_2 e KR_3 pertencentes respectivamente a *Alice*, *Bob* e *Cartório*. A *Autoridade Certificadora*, então, escolhe aleatoriamente duas *Testemunhas* no conjunto de T pertencentes à jurisdição do *Cartório* e solicita suas subchaves.

Suponha que foram escolhidas as testemunhas 3 e 5.

Essas, por sua vez, enviam suas subchaves para a *Autoridade Certificadora* da seguinte forma:

A $Testemunha_3$, *Humberto*, envia para a *Autoridade Certificadora*, sua subchave K_{4_3} cifrada com sua chave privada e posteriormente com a chave pública da *Autoridade Certificadora* da

seguinte forma:

$$E(KU_{AutCert}, E(KR_{Humberto}, KR_{4_3}||ID_{Trans}))$$

Que representa;

$$E(103, E(6.604.381, 272.361||88))$$

Humberto cifra sua subchave e a identificação da transação com sua chave privada, calculando:

$$272.361^{6.604.381} \bmod 13.583.071 = 4.600.499$$

$$||$$

$$88^{6.604.381} \bmod 13.583.071 = 10.021.136$$

Depois disso, cifra o resultado acima com a chave pública da *Autoridade Certificadora*, calculando:

$$4.600.499^{103} \bmod 13.583.071 = 8.256.560$$

$$10.021.136^{103} \bmod 13.583.071 = 13.570.567$$

A exemplo de *Humberto*, a $Testemunha_5$, *Cíntia*, também envia para a *Autoridade Certificadora* sua subchave K_{4_5} cifrada com sua chave privada. Depois cifra, com a chave pública da *Autoridade Certificadora*, da seguinte forma:

$$E(KU_{AutCert}, E(KR_{Cíntia}, KR_{4_5}||ID_{Trans}))$$

Que representa;

$$E(103, E(2.053.463, 359.183||88))$$

Cíntia, então, cifra sua subchave e a identificação da transação com sua chave privada, calculando:

$$359.183^{2.053.463} \bmod 13.583.071 = 6.473.165$$

$$||$$

$$88^{2.053.463} \bmod 13.583.071 = 12.460.022$$

Depois disso, cifra o resultado acima com a chave pública da *Autoridade Certificadora*, calculando:

$$6.473.165^{103} \bmod 13.583.071 = 2.228.509$$

$$\|$$

$$12.460.022^{103} mod 13.583.071 = 6.020.166$$

A *Autoridade Certificadora* após receber as informações das *Testemunhas*, *Humberto* e *Cíntia*, decifra cada mensagem utilizando as respectivas chaves públicas de cada testemunha.

A *Autoridade Certificadora* recebe, então, a mensagem;

$$(8.256.560\|10.021.136)$$

da testemunha *Humberto* e decifra da seguinte forma:

$$8.256.560^{5.140.303} \bmod 13.583.071 = 4.600.499$$

$$\|$$

$$13.570.567^{5.140.303} \bmod 13.583.071 = 10.021.136$$

Depois disso, utiliza a chave pública da testemunha para decifrar o cálculo acima, obtendo:

$$4.600.499^{37} \bmod 13.583.071 = 272.361$$

$$\|$$

$$10.021.136^{37} \bmod 13.583.071 = 88$$

Tal que

$$KR_{4_3} = 272.361$$

e

$$ID_{Trans} = 88$$

O mesmo procedimento é feito para decifrar a mensagem da testemunha *Cíntia*.

A *Autoridade Certificadora* recebe então a mensagem;

$$(2.228.509 \| 6.020.166)$$

e a decifra da seguinte forma:

$$2.228.509^{5.140.303} \bmod 13.583.071 = 6.473.165$$

$$\|$$

$$6.020.166^{5.140.303} \bmod 13.583.071 = 12.460.022$$

Depois disso, utiliza a chave pública da testemunha para decifrar o cálculo acima, obtendo:

$$6.473.165^{37} \bmod 13.583.071 = 359.183$$

$$\|$$

$$12.460.022^{119} \bmod 13.583.071 = 88$$

Tal que

$$KR_{4_5} = 359.183$$

e

$$ID_{Trans} = 88$$

De posse das duas subchaves KR_{4_3} e KR_{4_5} das *Testemunhas*, a *Autoridade Certificadora* recalcula KR_4, utilizando o esquema de compartilhamento de segredos $(w, 2)$, utilizando a forma de Interpolação de Lagrange:

O segredo KR_4, é então, reconstruído a partir de duas sombras, x_3 e x_5, tal que:

$x_3 = a_3 = Y_3 = 272.361$

$x_5 = a_5 = Y_5 = 359.183$

Segundo a forma de interpolação de Lagrange, calcula-se um polinômio $P(x)$, tal que:

$$P(X) = \frac{(x - x_5)}{(x_3 - x_5)} \times y_3 + \frac{(x - x_3)}{(x_5 - x_3)} \times y_5 \pmod{g}$$

Substituindo os valores, tem-se:

$$P(X) = \frac{(x-5)}{(3-5)} \times 272.361 + \frac{x-3}{5-3} \times 359.183 \text{ (mod } 13.994.087)$$
$$= \frac{x-5}{-2} \times + \frac{x-3}{2} \times 359.183 \text{ (mod } 13.994.087)$$

mas

$$\frac{1}{-2} \equiv 6.997.043 (\text{mod } 13.994.087)$$

$$\frac{1}{2} \equiv 6.997.044 (\text{mod } 13.994.087)$$

Portanto

$$\begin{aligned} P(x) &= (6.997.043 \times 272.361(x-5) \text{ (mod } 13.994.087)) \\ &+ (6.997.044 \times 359.183(x-3) \text{ (mod } 13.994.087)) \text{ (mod } (13.994.087)) \\ &= (6.860.863x + 7.677.946) + (7.176.635x + 6.458.269) \text{ (mod } (13.994.087)) \\ &= 43.411x + 142.128 \text{ (mod } (13.994.087)) \end{aligned}$$

Dessa forma, tem-se a definição do polinômio $P(x)$. A partir desse polinômio, o valor da constante, que é o valor do segredo, é recuperado, ou seja, KR_4.

Nesse momento, a *Autoridade Certificadora* possui o valor das quatro subchaves KR_1, KR_2, KR_3 e KR_4. De posse desses valores, ela reconstrói KR_{Trans} da seguinte forma:

Utilizando a definição do Polinômio de Lagrange apresentado na seção 4.5.1 e considerando:

$$b_j = \prod_{1 \leq k \leq t, k \neq j} \frac{x_{i_k}}{x_{i_k} - x_{i_j}} \bmod q$$

e

$$k = \sum_{j=1}^{t} b_{i_j} y_{i_j} \bmod q$$

Utilizando tais igualdades, a constante do Polinômio de Lagrange é determinada. No caso do exemplo, por:

$$b_1 = \frac{x_2 x_3 x_4}{(x_2 - x_1)(x_3 - x_1)(x_4 - x_1)} \bmod p = \frac{2 \times 3 \times 4}{(2-1)(3-1)(4-1)} \bmod 13.994.087 = 4$$

$$b_2 = \frac{x_1 x_3 x_4}{(x_1 - x_2)(x_3 - x_2)(x_4 - x_2)} \bmod p = \frac{1 \times 3 \times 4}{(1-2)(3-2)(4-2)} \bmod 13.994.087 = 13.994.081$$

$$b_3 = \frac{x_1 x_2 x_4}{(x_1 - x_3)(x_2 - x_3)(x_4 - x_3)} \bmod p = \frac{1 \times 2 \times 4}{(1-3)(2-3)(4-3)} \bmod 13.994.087 = 4$$

$$b_4 = \frac{x_1 x_2 x_3}{(x_1 - x_4)(x_2 - x_4)(x_3 - x_4)} \bmod p = \frac{1 \times 2 \times 4}{(1-4)(2-4)(3-4)} \bmod 13.994.087 = 13.994.086$$

Tem-se, portanto:

$$\begin{aligned} k &= b_1 \times y_1 + b_2 \times y_2 + b_3 \times y_3 + b_4 \times y_4 \bmod q \\ &= 4 \times 4.295.747 \\ &+ 13.994.081 \times 6.187.637 \\ &+ 4 \times 9.432.013 \\ &+ 13.994.086 \times 142.128 (\bmod 13.994.087) \\ &= 3.649.003 \end{aligned}$$

Tal que

$$KR_{Trans} = 3.649.003$$

Nesse momento, a *Autoridade Certificadora* reconstruiu a chave secreta que é utilizada para emitir a assinatura digital para documento solicitado. A assinatura digital é emitida, portanto, cifrando o código de autenticação único da escritura de compra e venda com a chave secreta calculada acima, da seguinte forma:

$$y = sig(KU_{Trans}, \sigma) = E(KR_{Trans}, \sigma)$$

Substituindo os valores, tem-se;

$$y = E(3.649.003, 101)$$

E calcula-se:

$$y = 101^{3.649.003} \bmod 13.583.071 = 308.468$$

Esse código é, por sua vez, anexado à mensagem como sendo a assinatura digital do documento.

A *Autoridade Certificadora* envia ao *Cartório* em resposta à sua requisição *request*, a mensagem $m_{Escritura}$ e seu código de identificação único assinado digitalmente.

Após assinado o documento, qualquer pessoa pode verificar se a assinatura y realmente corresponde à assinatura da escritura de compra e venda do imóvel, utiliza-se a função de verificação de assinatura baseada no esquema de assinatura do RSA, obtendo-se:

$$\sigma'' = ver(KU_{Trans}, y)$$

Utilizando exemplo acima, y pode ser verificado da seguinte forma:
Calcula-se código *hash* da escritura de compra e venda, tal que;

$$\sigma'' = H(m_{Escritura})$$

Substituindo-se os valores tem-se:

$$\sigma'' = H(100) = 101$$

Utiliza-se a função de verificação da assinatura, tal que;

$$\sigma'' = ver(KU_{Trans}, y)$$

Substituindo-se os valores;

$$101 = ver(6.558.763, 308.468)$$

Tem-se como resultado

$$101 = 101$$

Como a igualdade de σ'' e $ver(KU_{Trans}, y)$ é verificada, então, tem-se a certeza de que y corresponde à assinatura na escritura de compra e venda do imóvel.

5.4 Considerações

O esquema de criptografia de limiar de Shamir é escolhido para efetuar a divisão da chave secreta, KR_{Trans}, pois nele não são necessárias todas as w partes para a reconstrução da chave KR_{Trans}.

Portanto, das w *Testemunhas* que possuem subchaves, são necessárias, no mínimo, 2 (duas) para a reconstrução de KR_4.

Para garantir a participação do *Vendedor*, *Comprador*, *Cartório* e *Testemunhas* na emissão de suas próprias assinaturas foi necessário estender o esquema de Shamir ao fazer primeira-

mente uma divisão $(4, 4)$ gerando obrigatoriamente KR_1, KR_2, KR_3 e KR_4.

Nesse caso, KR_1 é entregue ao *Vendedor* de forma que, sem sua parte da chave, não é possível emitir a assinatura. Analogamente, KR_2 é entregue ao *Comprador* e KR_3 ao *Cartório*. Já KR_4 é dividida e entregue ao conjunto de *Testemunhas*. Isso dá a todos os participantes o direito de vetar a sua própria assinatura.

Dada a divisão de chaves descrita, é impraticável para um intruso tentar corromper todas as partes que possuem as subchaves para formar KR_{Trans}, e se passar por algum dos participantes.

A partir da chave pública, formada através de KR_1, KR_2, KR_3 e KR_4 a *Autoridade Certificadora* determina, então, com base no esquema de geração de chaves do RSA, a chave privada que é utilizada para emissão da assinatura digital.

É importante ressaltar que a assinatura digital da escritura de compra e venda é única por transação. Portanto, é impossível emitir uma assinatura para uma determinada escritura sem o consentimento desses participantes. Isso impede, por exemplo, que a *Autoridade Certificadora* que faz apenas os cálculos, assine a escritura como se fosse as partes.

Capítulo 6

Considerações, Conclusão e Trabalhos Futuros

Este capítulo apresenta algumas considerações finais sobre o trabalho, ressaltando o motivo da escolha dos esquemas criptográficos utilizados.

Também é apresentada uma análise da solução, mostrando algumas desvantagens observadas. Por fim, é apresentada a conclusão do trabalho bem como algumas melhorias que podem servir de base para trabalhos futuros.

6.1 Considerações Finais

Na maioria das vezes, a chave privada, que é utilizada para emitir a assinatura digital, é armazenada em um dispositivo, como *pendrive*, cartão magnético ou mesmo em um computador. Essa chave é, na verdade, um arquivo de computador como outro qualquer. Porém, com suas especificidades e funcionalidades bem definidas.

Sendo um arquivo, e armazenada em um único dispositivo, está sujeita a alguns imprevistos como roubo, invasão seguida de roubo de arquivos, dentre outros. Caso essa chave seja roubada, não se pode mais garantir que seu uso em algum documento tenha o consentimento de seu signatário.

Vale ressaltar que se o roubo ou invasão acontecer, comprometendo a segurança da assinatura, ela não deixa de ser uma assinatura válida, e sim usada indevidamente. Fazendo uma analogia com a assinatura convencional, é como se um indivíduo forjasse a assinatura de outro e se passasse por ele.

Para exemplificar essa situação, foi pesquisado sobre os serviços notariais oferecidos por cartórios brasileiros na internet. A razão dessa pesquisa foi o fato de os cartórios serem munidos de fé pública e órgãos que têm como competência o reconhecimento da autenticidade de assinaturas convencionais. Foi constatado que o serviço de reconhecimento de firma com autenticação não é oferecido no meio digital por requerer um nível de segurança mais elevado

na a identificação dos signatários. Nele, os interessados devem estar presentes fisicamente nos cartórios e se identificarem devidamente. Também devem possuir suas fichas de firma aberta no cartório, para que seja feito o processo de reconhecimento de firma. Além do mais, o cartório verifica a integridade e autenticidade do documento assinado e ainda solicita que testemunhas atestem a existência do documento.

Um dos documentos que necessitam dos requisitos citados acima é a escritura de compra e venda de um imóvel. Nesse tipo de documento, assinam o vendedor, comprador, cartório e no mínimo duas testemunhas. Todas as assinaturas devem ter suas firmas reconhecidas. O cartório também atesta a integridade e autenticidade do documento após assinado por todos.

Diante desse cenário, esta dissertação mostra um mecanismo para autenticar e reconhecer firma de uma assinatura eletrônica em um documento. Mais precisamente confirmou a hipótese levantada de que a criação de protocolos criptográficos utilizando algoritmos de chave assimétrica e manipulação matemática resolveria esses problemas.

Também foi confirmada a hipótese da utilização de protocolos criptográficos para aumentar a segurança da assinatura digital de um usuário, dividindo-a em partes e armazenando-a em locais distintos. Foi garantida, ainda, a participação do dono da assinatura na emissão de sua própria assinatura, evitando assim que ela seja forjada.

O protocolo proposto resolve o problema do processo de reconhecimento de firma por autenticidade em um meio digital. Além disso, pelo fato da chave secreta estar separada em partes e armazenada em locais distintos, o nível de segurança contra roubo ou invasão diminui. Foi utilizado, como exemplo, a emissão de assinaturas em uma escritura de compra e venda de imóveis.

Para garantir o sigilo das informações transmitidas, empregou-se o esquema de criptografia do RSA, por ser um dos mais usados atualmente. Apesar de muitos estudiosos afirmarem que é possível quebrar sua segurança, tal fato ainda não foi confirmado, uma vez que o tamanho da chave secreta pode ser aumentado exponencialmente. Isso torna impraticável determinados ataques, garantindo assim, sua segurança.

Para emissão das assinaturas, foi usado também o esquema de assinatura do RSA, por ser utilizada pelo Instituto Nacional de Tecnologia da Informação responsável pela infraestrutura de chaves públicas no Brasil. O Instituto é a Autoridade Certificadora Raiz brasileira.

A divisão da assinatura foi possível aproveitando o algoritmo de compartilhamento de segredos proposto por Adi Shamir, adicionado à capacidade de veto. Isso possibilitou a divisão da responsabilidade em emitir uma única assinatura na escritura de compra e venda. A capacidade de veto garantiu que a assinatura ali posta é de seu signatário.

Porém, mesmo atingindo o objetivo de resolver o problema proposto nesta dissertação, algum pontos devem ser analisados criticamente, conforme mostra o item 6.2 dessa dissertação.

6.2 Conclusão

Para garantir a segurança da informação transmitida, foi utilizado o esquema do algoritmo de criptografia RSA. A segurança do algoritmo está condicionada ao tamanho da chave secreta empregada. Isso torna impraticável a fatoração do número n em p e q, que são números primos grandes. Caso exista um algoritmo que consiga determinar p e q de forma eficiente a segurança do algoritmo estaria comprometida, como mostra a seção 4.3.3 desta dissertação.

O fato de se utilizar números primos grandes para p e q, faz com que seja consumido alto recurso computacional para efetuar os cálculos matemáticos. Pode-se ainda afirmar que o tamanho da chave privada também influencia no custo computacional, pois atualmente são utilizadas chaves na ordem de 1.024 a 2.048 *bits*.

A figura 6.1 mostra um exemplo de um número com 1.024 *bits*.

```
104359678280899728972689130282574970044678317647033799883043195113247889335502574
792705684943227907419842131029559699275503456743337475500785887035879558938442018
417992467595625969221699995520859230769512143361488366340704723060107334120296061
202399248137525511987573111568302681270492253889182407474399504721
```

Figura 6.1: Exemplo de um número primo de 1.024 bits

Com isso, os cálculos feitos lançando mão da aritmética modular requerem alto desempenho computacional.

Outro ponto a ser analisado é a utilização do esquema de compartilhamento de segredos como forma de dividir a assinatura digital. Na verdade, como a assinatura segue o esquema RSA, dividir a assinatura significa dividir a chave secreta ou ainda dividir o expoente secreto do esquema de assinatura RSA.

Essa divisão faz uso o conceito de polinômios. O grau do polinômio é definido conforme o limiar menos uma unidade. Os coeficientes são definidos aleatoriamente. A constante é o segredo a ser dividido, ou seja, a chave secreta.

Sua segurança depende do armazenamento secreto das sombras entregues às partes. Caso um número de sombras definidas como o limiar sejam corrompidas ou descobertas, o segredo pode ser reconstruído e a assinatura digital ficaria exposta.

Para dificultar essa operação, foi adicionada a capacidade de veto. Isso aumenta a dificuldade de um intruso reconstruir o segredo. Pois além de ser necessário adquirir o valor das sombras dos participantes de acordo com um limiar mínimo, ele deve saber quais exatamente são os participantes que têm o poder de vetar a assinatura. Sem a sombra desses participantes, o segredo não pode ser reconstruído e a assinatura não pode ser utilizada.

Pode-se ainda aumentar a segurança desse método escolhendo números grandes para os coeficientes do polinômio e também para o módulo. Apesar de requerer um maior custo computacional na solução das operações modulares, é preservada a segurança do segredo

Conclui-se, portanto, que os objetivos desta dissertação foram alcançados. Constatou-se que as hipóteses propostas foram suficientes para a solução do problema levantado.

Foi criado, portanto, um protocolo com artefatos computacionais de criptografia que possibilitaram o análogo digital do processo de reconhecimento de firma com autenticidade. Mais especificamente foi criado um protocolo para emissão de assinatura digital em uma escritura de compra e venda de imóveis.

Foi utilizado o esquema de criptografia RSA para sigilo das informações transmitidas e para a emissão da assinatura digital. Apesar de ser um processo que requer alto custo computacional, sua segurança é comprovada, sendo um dos protocolos de criptografia mais utilizados atualmente. Também foi utilizado o esquema de compartilhamento de segredos para dividir a chave secreta em partes distintas e armazenadas em locais diferentes. Isso aumentou a segurança do esquema uma vez que para a emissão da assinatura digital é necessário corromper um limiar mínimo definido. Além disso, com a capacidade de veto, é necessário ainda saber quais são as sombras que vetam a emissão da assinatura

A escritura de compra e venda de imóvel pode ser implantada no meio digital através do protocolo proposto nessa dissertação com a vantagem de que não é necessária a presença física dos participantes. Isso foi possível devido ao fato de a legislação brasileira reconhecer como válida a assinatura digital que utiliza o certificado digital. Esse, por sua vez, certifica a assinatura digital e garante a propriedade da assinatura.

Também se pode citar como vantagem a emissão de uma única assinatura no documento eletrônico que garante os seguintes requisitos:

- Reconhecimento de firma das assinaturas dos participantes pelo cartório;
- Autenticidade e integridade do documento assinado;
- Assinatura de testemunhas atestando a existência do negócio;
- Irretratabilidade de todas as assinaturas.

Apesar de o protocolo atingir os objetivos propostos algumas modificações podem ser feitas no sentido de melhorar o desempenho computacional e aplicabilidade em outros contextos.

6.3 Trabalhos Futuros

Algumas melhorias são visualizadas no protocolo proposto e são apresentadas como sugestões para trabalhos futuros, são elas:

- Para diminuir o consumo computacional, os cálculos de cifragem, decifragem, divisão e reconstrução da chave feitos pela autoridade certificadora poderiam ser implementados por *hardware*; O trabalho de [Machado 2008], mostra que esse tipo de implementação acelera o processo de criptografia.
- Foi utilizada a forma de interpolação de Lagrange para reconstrução do segredo. Propõe-se um estudo comparativo dessa reconstrução através da interpolação Linear e também

pela forma de Newton. Pode-se com isso verificar se a forma de recuperação de segredo utilizada nessa dissertação é a melhor em termos de desempenho ou não.

- Utilizar protocolo de compartilhamento de segredos com veto em outro contexto para proporcionar que mais serviços sejam oferecidos na internet, como assinatura de cheques empresariais, assinaturas de outros contratos, etc.
- Fazer um estudo sobre o número de sombras mínimas necessárias para garantir a segurança do protocolo de compartilhamento de segredo e também determinar o número de sombras máximas para que os cálculos não se tornem ineficientes computacionalmente.
- Fazer um estudo sobre o impacto do tamanho das chaves utilizadas nas transações para determinar chaves seguras com menor *overhead* computacional.

Referências Bibliográficas

[Alecrim 2009] Alecrim, E. (2009). Entendendo a certificação digital. Acessado em 19/04/2011 Disponível em: http://www.infowester.com/assincertdigital.php.

[Araújo 2010] Araújo, E. T. S. O. (2010). A Importânciada escritura pública. Acessado em 10/03/2011 Disponível em: http://www.arpensp.org.br/principal/index.cfm?pagina_id=200.

[Arpen-SP 2011] Arpen-SP (2011). Reconhecimento de Firmas. Acessado em 10/03/2011 Disponível em: http://www.arpensp.org.br/principal/index.cfm?pagina_id=200.

[Ashidani 2009] Ashidani, P. J. (2009). Autenticação de remetente em servidor de email com assinatura baseada em identidade. Master's thesis, Universidade Federal de Uberlândia: Faculdade de Ciências da Computação.

[Bellare e Rogaway 2005] Bellare, M. e Rogaway, P. (2005). Introduction to Modern Cryptography. In *UCSD CSE 207 Course Notes*, p. 207.

[Blundo et al. 1994] Blundo, C., Santis, A. D., Gargano, L., De, A., Gargano, S. L., e Vaccaro, U. (1994). Secret Sharing Schemes with Veto Capabilities. In *in: Proceedings of French-Israeli Workshop in Algebraic Coding*, pp. 82–89. Springer-Verlag.

[Brown 2009] Brown, D. (2009). *O Símbolo Perdido*. Sextante, Rio de Janeiro, RJ.

[Burnett e Paine 2002] Burnett, S. e Paine, S. (2002). *Criptografia e segurança: o guia oficial do RSA*. Elsevier, São Paulo, SP.

[Campello e Leal 2007] Campello, A. C. e Leal, I. (2007). Teoria Aritmética dos Números e Criptografia RSA. Acessado em 28/01/2011 Disponível em: http://www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/antonio_RSA.pdf.

[CNJ 2011] CNJ (2011). Modelo para informatização dos cartórios deve ser definido até junho. Conselho Nacional de Justiça - Acessado em 19/04/2011 Disponível em: http://www.tiinside.com.br/08/02/2011/modelo-para-informatizacao-dos-cartorios-deve-ser-definido-ate-junho/gf/213247/news.aspx.

[Cormen 2002] Cormen, T. H. (2002). *Algoritmos : teoria e prática*. Campus, Rio de Janeiro, RJ.

[Cunha 2006] Cunha, M. V. (2006). Reconhecimento de firma. Jusnavigandi. Acessado em 10/03/2011 Disponível em: http://jus.uol.com.br/revista/texto/9256/reconhecimento-de-firma.

[da Silveira Martini 2009] da Silveira Martini, R. (2009). Tecnologia na vida da população. In de Tecnologia da Informação, I. N. (editor), *Revista Digital: a assintura do futuro*, número 1.

[Damgård e Mikkelsen 2009] Damgård, I. e Mikkelsen, G. L. (2009). On the Theory and Practice of Personal Digital Signatures. In *Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography: PKC '09*, Irvine, pp. 277–296, CA, Berlin, Heidelberg. Springer-Verlag.

[de Oliveira Bertucci 2008] de Oliveira Bertucci, J. L. (2008). *Metodologia básica para elaboração de trabalhos de conclusão de cursos (TCC): ênfase na elaboração de TCC de Pós graduação Latu Sensu*. Atlas, São Paulo, SP.

[de Oliveira Fairbanks 2010] de Oliveira Fairbanks, O. J. (2010). Cartório Digital:a informatização mudando a face dos cartórios paulistas. Master's thesis, Faculdade Arthur Tomas, Londrina.

[Duckworth 2011] Duckworth, L. S. M. (2011). A escritura pública de Compra e Venda de imóveis. Acessado em 19/04/2011 Disponível em: `http://jetroimoveis.com.br/a_escritura_publica_de_compra_e_venda_de_imoveis_/t=6_1`.

[Haetinger e de Souza Martinez 2006] Haetinger, C. e de Souza Martinez, C. (2006). Interpolação. Acessado em 14/06/2011 Disponível em: `http://ensino.univates.br/~chaet/Materiais/Apresentacao_Interpolacao_Celene.pdf`.

[Housley et al. 1999] Housley, R., Ford, W., Polk, W., e Solo, D. (1999). Internet X.509 Public Key Infrastructure Certificate and CRL Profile. RFC 2459 (Proposed Standard). Obsoleted by RFC 3280.

[ICP-Brasil 2011] ICP-Brasil (2011). Estrutura da ICP-Brasil. Acessado em 19/04/2011 Disponível em: `http://www.iti.gov.br/twiki/bin/view/Certificacao/EstruturaIcp`.

[Kocher et al. 1999] Kocher, P., Jaffe, J., e Jun, B. (1999). Differential Power Analysis. *Lecture Notes in Computer Science*, pp. 388–397.

[Lira 2008] Lira, I. S. (2008). Certificação digital para os cartórios extrajudiciais de Salvador. Master's thesis, Universidade Federal da Bahia, Instituto de Ciências da Informação, Salvador.

[Liu 1968] Liu, C. L. (1968). *Introduction to Combinatorial Mathematics*. McGraw-Hill, New York. Department of Eletrical Engineering Massashusetts Institute Tecnology.

[Machado 2008] Machado, D. J. M. (2008). Acelerador Criptográfico em Hardware Reconfigurável. Master's thesis, Instituto Superior Técnico da Universidade de Lisboa.

[MP2.200/2 2001] MP2.200/2 (2001). Medida Provisória 2.200/2: Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Acessado em 22/04/2011 Disponível em: `http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm`.

[Obana e Kurosawa 1996] Obana, S. e Kurosawa, K. (1996). Veto Is Impossible in Secret Sharing Schemes. *II, Network*, 2:27–5.

[Pointcheval 2002] Pointcheval, D. (2002). How to Encrypt Properly with RSA. *RSA Laboratories' CryptoBytes. Winter/Spring*, 5(1):9–19.

[Prodemge 2011] Prodemge (2011). Como adquirir - Certificado de servidor web. Acessado em 19/04/2011 Disponível em: https://wwws.prodemge.gov.br/index.php?option=com_content&task=view&id=27&Itemid=91.

[Rivest et al. 1978] Rivest, R., Shamir, A., e Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21:120–126.

[Ruggiero e da Rocha Lopes 1996] Ruggiero, M. A. G. e da Rocha Lopes, V. L. (1996). *Cálculo Numérico: aspec tos teóricos e computacionais*. Pearson Education do Brasil, São Paulo, SP, 2ª edition.

[Salomaa 1990] Salomaa, A. (1990). *Public-key cryptography*. Springer-Verlag New York, Inc., New York, NY, USA.

[Scheinerman 2011] Scheinerman, E. R. (2011). *Matemática discreta: uma introdução*. Cengage Learning, São Paulo, SP.

[Shamir 1979] Shamir, A. (1979). How to share a secret. *Commun. ACM*, 22(11):612–613.

[Shoup 2008] Shoup, V. (2008). *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press.

[Stallings 1999] Stallings, W. (1999). *Cryptography and Network Security: Principles and Practice*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 2nd edition.

[Stallings 2007] Stallings, W. (2007). *Criptografia e Segurança de Redes*. Pearson, São Paulo, SP, 4ª edição edition.

[Stinson 2005] Stinson, D. R. (2005). *Cryptography: Theory and Practice, Third Edition (Discrete Mathematics and Its Applications)*. Chapman & Hall/CRC.

[Trevisan 2009] Trevisan, A. M. (2009). O profissional da era digital e o governo eletrônico. Acessado em 19/04/2011 Disponível em: http://www.sinfor.org.br/index.php?option=com_content&view=article&id=157:o-profissional-da-era-digital-e-o-governo-eletronico&catid=1:artigos&Itemid=163.

[Vanderlei e de Queiroz 2004] Vanderlei, I. M. e de Queiroz, R. J. G. B. (2004). Esquema de Assinaturas Digitais Tolerante a Falhas Utilizando Criptografia de Limiar.