UNIVERSIDADE DO EXTREMO SUL CATARINENSE
CIÊNCIA DA COMPUTAÇÂO

GIANCARLO BIANCHIN MACHADO

IMPLEMENTAÇÃO DE ASSINATURA DIGITAL NA EVOLUÇÃO MÉDICA DE PRONTUÁRIO ELETRÔNICO DO PACIENTE: UM ESTUDO DE CASO NO HOSPITAL REGIONAL DE ARARANGUÁ

CRICIÚMA, JULHO DE 2006

GIANCARLO BIANCHIN MACHADO

IMPLEMENTAÇÃO DE ASSINATURA DIGITAL NA EVOLUÇÃO MÉDICA DE PRONTUÁRIO ELETRÔNICO DO PACIENTE: UM ESTUDO DE CASO NO HOSPITAL REGIONAL DE ARARANGUÁ.

Trabalho de Conclusão de Curso apresentado para obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense.

Orientador: Profº M.Sc. Paulo João Martins.
Co-orientador: Profº M.Sc. Rafael Charnovscki

CRICIÚMA, JULHO DE 2006

RESUMO

Um prontuário eletrônico é um sistema que serve para auxiliar um médico no controle de informações de saúde de um paciente. No prontuário eletrônico são armazenadas várias informações, tais como o acompanhamento diário do paciente, por isso os aspectos de segurança destes dados e os riscos que envolvem essas informações são imprescindíveis sob os aspectos legais que regem o relacionamento entre paciente e agente de saúde. Uma das formas de obter segurança é utilizar a criptografia, que é um método muito importante para alcançar uma maior segurança de informações. A assinatura digital usa a criptografia para tentar garantir a integridade e o não-repúdio de uma mensagem. O certificado digital é um fator muito importante na assinatura digital, então este trabalho mostra o que é um certificado digital, a importância dele na assinatura digital, autoridades certificadoras, locais de armazenamentos e seus padrões. O padrão brasileiro é defendido pelo ICP-Brasil. Este trabalho envolve o estudo da assinatura digital e uma implementação no prontuário eletrônico do Hospital Regional de Araranguá em conjunto com Grupo de Pesquisa em Informática Médica da Unesc. Na implementação foi aplicada a assinatura digital no prontuário, mostrando como foi desenvolvida e descrevendo quais os passos que um médico tem que tomar para assinar uma evolução e verificar uma assinatura.

Palavras – Chave: ***Prontuário Eletrônico; Assinatura Digital; Segurança de informação.***

ABSTRACT

A electronic medical records is a system than serves to assist a doctor at the information control of the health of patient. In the electronic medical records are stored some information, such as daily accompaniment of the patient, therefore the security aspects of this data and the risks that involve this information are essential on the legal aspects that conduct the relationship between patient and doctor. One of the forms to get security it uses the cryptography that is a method very important to get a better information security. The digital signature uses the cryptography to try to guarantee the integrity and the nonrepudiation of message. The digital certificate it's a factor very important in the digital signature, then this work shows what is a digital certificate, your important in the digital signature, certificate authority, places of storage and yours standards. The Brazilian standard id defended by ICP-Brasil. This work involve the study of the digital signature and a implementation in the electronic medical records of the HRA in partner with Kiron Project of Unesc. In the implementation was applied at the electronic medical records, showing how was developed and describing with the steps that a doctor have to make to sign an evolution and verify a signature.

Keys works: **Electronic medical records, digital signature, information security.**

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

AC	Autoridade Certificadora
ACR	Autoridade Certificadora Raiz
AD	Assinatura Digital
AR	Autoridade de Registro
API	*Application Programming Interface*
CD	Certificado Digital
CFM	Conselho Federal de Medicina
CG	Comitê Gestor
CRC	Checagem de Redundância Cíclica
CRL	*Certification Revogation Lists*
DES	*Data Encryption Standard*
DLL	*Dynamic Link Library*
DSA	*Digital Signature Algorithm*
DSS	*Digital Standard Signature*
HRA	Hospital Regional de Araranguá
IDEA	*International Data Encryption Algorithm*
ITI	Instituto Nacional da Tecnologia da Informação
MAC	*Message Authentication Code*
MD	*Message Digest*
SHA	*Secure Hash Algorithm*
RSA	Algoritmo de criptografia assimétrica criado por Rivest, Shamir e Adelman
SBIS	Sociedade Brasileira de Informática em Saúde

PEP	Prontuário Eletrônico do Paciente
UFSC	Universidade Federal de Santa Catarina

SUMÁRIO

1 INTRODUÇÃO

Atualmente, a Unidade de Terapia Intensiva (UTI) do Hospital Regional de Araranguá (HRA) utiliza um Prontuário Eletrônico do Paciente (PEP) desenvolvido pelo projeto Kiron, do Departamento de Ciência da Computação da UNESC. Algumas informações desse prontuário precisam ser autenticadas pelos profissionais de saúde. Por isso, são impressos relatórios que precisam ser carimbados e assinados pelos médicos.

Um dos requisitos dos usuários do PEP da UTI tem sido a alteração do procedimento manual de autenticação para um procedimento eletrônico. Para isso, é preciso adicionar ao prontuário um sistema que permita aos médicos assinarem digitalmente algumas informações a respeito do paciente.

Este trabalho visa desenvolver um sistema de assinatura digital que será incorporado ao prontuário atual para que os médicos não tenham mais que imprimir e assinar manualmente os relatórios. O sistema deverá respeitar os requisitos definidos pela Sociedade Brasileira de Informática em Saúde (SBIS) no que diz respeito à assinatura digital de PEPs. Neste trabalho também serão abordadas questões sobre a própria segurança das assinaturas digitais.

Vale ressaltar que uma assinatura digital não é a digitalização de uma assinatura manuscrita. Ou seja, não será adicionada ao prontuário uma imagem da assinatura de um médico, mas sim um módulo capaz de associar um indivíduo com uma identidade eletrônica (certificado digital) a um documento eletrônico, utilizando métodos matemáticos complexos que garantem a autenticidade do indivíduo e a integridade do documento.

1.1 OBJETIVO GERAL

Desenvolver um módulo de software para inclusão de assinatura digital na evolução médica do prontuário eletrônico da UTI do HRA.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos desta pesquisa consistem em:

a) demonstrar a necessidade da segurança das informações médicas em prontuário eletrônico;
b) apresentar tecnologias computacionais que permitam a segurança da informação por meio do conceito de assinatura digital;
c) implementar um módulo de assinatura digital utilizando tecnologia Java;
d) desenvolver uma forma segura de armazenamento das assinaturas digitais;
e) analisar os aspectos técnicos e legais a respeito das Assinaturas Digitais no PEP.

1.3 JUSTIFICATIVA

De acordo com a SBIS, um dos requisitos para que um sistema de PEP seja certificado pela instituição é a utilização de assinatura digital (AD). A assinatura digital é um recurso eletrônico que identifica e responsabiliza o profissional de saúde sobre as informações por ele inseridas em um PEP.

Pode-se citar como exemplo as evoluções médicas dos pacientes inseridas no PEP da UTI do HRA. Essas evoluções precisam ser impressas, carimbadas e assinadas manualmente pelos médicos plantonistas. Assim, um sistema de AD poderia

substituir esse processo manual, já que ela funcionaria como uma assinatura eletrônica, criando um vínculo de responsabilidade entre o que foi escrito pelo médico plantonista e o paciente atendido.

Os métodos utilizados atualmente pela AD garantem a autenticidade da assinatura, ou seja, ela identifica a pessoa que produziu aquela assinatura. A AD também garante a integridade do texto, ou seja, é possível saber se tal texto foi modificado.

Um benefício adicional da utilização de assinatura digital é a diminuição de relatórios para serem assinados manualmente, o que também reduz custos com impressão e armazenamento de papéis.

Este trabalho dará continuidade ao TCC da acadêmica Regiane Pizzetti Borges (2004) e será realizado junto ao Projeto Kiron (Grupo de Informática Médica e Telemedicina), o qual desenvolve o PEP da UTI do HRA. Vale ressaltar que o TCC citado anteriormente não implementou um sistema de assinatura digital no prontuário em questão. O trabalho anterior produziu um protótipo de AD, mas este não foi implantado no PEP da UTI. O trabalho atual também investigará outras questões relativas ao armazenamento e segurança das assinaturas digitais.

2 SEGURANÇA DE DADOS

O bem mais valioso de uma organização não é a sua linha de produção ou serviços prestados, mas sim as informações relacionadas a eles.

O ser humano sempre procurou obter um controle sobre as informações que são importantes para ele. Desde a pré-história sabe-se que o homem guarda informações, sejam elas em pinturas em cavernas ou esculpidas em pedra. Mas foi nos últimos séculos que a informação começou a ter uma grande importância para vida humana (CARUSO; STEFFEN, 1999).

Antigamente, o meio mais seguro de controle de informações era restringir o acesso físico de uma pessoa ao local onde elas estavam armazenadas. Com a evolução da tecnologia, as informações começaram a ser mais portáteis, como placas de barro, pergaminho, papiro, ou mais recentemente, o papel. Cada vez mais as informações tornavam-se importantes para as pessoas ou organizações, necessitando, portanto, de um modo mais seguro de guardá-las.

Atualmente todas as organizações ou pessoas são dependentes de alguma forma da informação, umas mais que outras. Tal dependência aumentou com o crescimento do uso de tecnologia, que torna cada vez mais fácil armazenar uma informação e permite o armazenamento de grandes quantidades de informação em pequenos espaços (DIAS, 2000).

Essa tendência pode causar conseqüências graves a uma organização ou uma pessoa. Por exemplo, um banco quase não manipula dinheiro em espécie, mas informações que representam esses valores e os seus clientes. As maiorias dessas informações são altamente sigilosas e podem causar muitos danos caso sejam levadas a público.

Nas organizações, quase todos os setores econômicos de alguma forma guardam informações relacionadas com elas, como produção, estratégias de negócio e de *marketing* ou até mesmo atividades diárias da organização. Na maioria das vezes, essas informações são de valor inestimável, podendo comprometer a existência da organização ou até se tornar uma grande arma para um concorrente.

Até há pouco tempo, todas essas informações eram armazenadas em papéis que eram guardados em grandes arquivos, que podiam ocupar imensas salas ou até mesmo andares completos. A maior segurança que essas informações podiam ter estava relacionada a restrição ao acesso de pessoas não autorizadas em certos ambientes. Além do espaço e peso, havia o problema do envelhecimento dos materiais onde eram colocados os dados, por isso essas salas tinham que ser refrigeradas, dedetizadas e limpas.

Outro problema aparente era a dificuldade de se fazer cópias desses dados para aumentar a segurança, pois essa tarefa necessitava de muito tempo e um grande espaço de armazenamento. Com o avanço da tecnologia da informação, esses dados puderam ser armazenados de forma digital, ocupando menos espaço e facilitando as cópias de segurança. A digitalização trouxe benefícios na centralização dos dados, sendo alguns a maior facilidade na localização dos dados, segurança e administração dos mesmos. Um ponto negativo está na ocorrência de problemas no sistema que centraliza os dados em formato eletrônico, o que pode parar toda uma organização.

Agora se tem um novo problema: a segurança de todas essas informações. Segundo Caruso e Steffen (1999, p. 24) “É preciso, antes de tudo, cercar o ambiente de informação com medidas que garantam sua segurança efetiva a um custo aceitável, visto ser impossível obter-se segurança absoluta”.

Para que se faça segurança de uma forma mais organizada e efetiva, são adotadas políticas de segurança, as quais são medidas e regras que devem ser respeitadas para se conseguir a maior segurança possível das informações.

2.1 SEGURANÇA LÓGICA

Até há pouco tempo, o único modo de proteger o acesso a uma informação era impedir o acesso físico de uma pessoa, mas, com a informatização, surgiu um novo meio de ataque: o ataque lógico, normalmente por meios eletrônicos. A segurança lógica protege este tipo de ataque.

Esta segurança permite que uma pessoa tenha o acesso físico a um local onde esteja a informação. Essas informações ficam ocultas aos olhos de uma pessoa, sendo que precisa de um computador para acessar esses dados. Será preciso um controle de acesso que será visto mais adiante.

O acesso a essas informações também pode ser feito através de uma rede de computadores. Como o acesso pela rede não precisa do acesso físico ao local dos dados, a segurança lógica passa a ser muito importante. De modo geral, esse acesso é um acesso “invisível”, portanto pode ser mais difícil der ser controlado. Este acesso procura conhecer o conteúdo das informações e não onde elas estão armazenadas (DIAS, 2000).

2.1.1 Controle de acesso

A principal função do controle de acesso é garantir que o acesso aos dados seja somente feito por pessoas autorizadas.

À bem pouco tempo o controle lógico de uma informação era por meio de senhas, mas com o tempo necessitou-se de algo mais seguro, pois a senha já não era mais suficiente devido a sua fragilidade. Se uma outra pessoa descobrisse essa senha de acesso então nada impediria o acesso as informações. Para garantir mais segurança a esses dados, surgiram novos mecanismos de segurança. As principais ferramentas de controle lógico são (CARUSO; STEFFEN, 1999):

a) **senhas:** o sistema mais antigo de controle lógico depois que surgiram novos mecanismos. Começou a assumir o papel de autenticação de um usuário;
b) **chave de acesso:** identifica cada usuário. Portanto cada um tem uma chave de acesso e normalmente está em conjunto com uma senha. Este mecanismo permite que uma pessoa tenha o direito de acesso aos dados, e possa se responsabilizar por eles;
c) **lista de acesso:** usado para permitir quais usuários podem acessar quais dados. As listas de acesso trabalham em função das chaves de acesso, dando os privilégios necessários;
d) **operações:** determina as permissões que um usuário pode ter com um certo arquivo. Alguns tipos de permissões são:
    - leitura: o usuário só pode ler os dados;
    - gravação: o usuário pode incluir dados;
    - alteração: o usuário pode alterar dados existentes;
    - exclusão: o usuário pode excluir dados;
    - execução: o usuário pode executar os dados, ou programas que os manipule;

e) **privilégios:** controla as funções que um usuário tem dentro do controle de acesso, Exemplo: dar permissões a usuários. Está geralmente relacionado com uma hierarquia; quanto maior a hierarquia mais funções são permitidas ao usuário;

f) **ferramentas de segurança:** garante o controle de acesso as informações. Normalmente essas ferramentas são programas configurados com as operações e privilégios de cada usuário, mas podem ser outros tipos de ferramentas, como *smart card*, cartões magnético, biometria (reconhecimento da íris, impressão digital e reconhecimento facial), entre outros.

2.2 SEGURANÇA FÍSICA

Mesmo com toda a segurança lógica, ela será inútil se não houver uma aceitável segurança física das informações. Antes de tudo, deve-se projetar uma segurança física que esteja a altura dos dados armazenados.

A segurança física normalmente é implantada no local onde são armazenados os dados; é um controle mais "visível", mas não o mais fácil. A segurança não só protege contra ataques as informações, mas também preservação, recuperação e armazenamento. Em dados digitais a segurança acontece por completa, usando a segurança lógica e a física. Em casos em que as informações estão em meios físicos, como papel, não é possível fazer uma segurança lógica dos dados, então só ocorre a segurança física.

Os recursos a serem protegidos pela segurança física são equipamentos (servidores, estações de trabalho, CPUs, mouses, teclados, impressoras, roteadores,

entre outros), documentos, dispositivos de armazenamento (disquetes, fitas, CDs, formulários, entre outros) e o ambiente onde estão esses recursos (DIAS, 2000).

2.2.1 Acesso Físico

O acesso físico está relacionado com o local onde estão armazenados as informações protegendo contra ataques humanos e fenômenos da natureza.

Apesar de ser um acesso mais perceptivo que o lógico, o acesso físico pode se tornar muito mais complicado, pois este depende muito da intervenção humana. O controle de acesso físico é prejudicado quando várias pessoas circulam o local.

2.2.2 Plano de Contingência

O plano de contingência tem como principal intuito a recuperação caso ocorra algum desastre. Este plano é muito importante, mas muitas organizações não tem um plano pré-estabelecido, o que pode comprometer seu funcionamento no caso de perdas de dados. Caso ocorra um desastre, o papel do plano de contingência é a minimização dos danos causados pelo mesmo.

2.2.3 Preservação e Recuperação de Informações

Está ligado ao plano de contingência, por meio do conceito de recuperação dos dados. A preservação consiste em garantir que os dados estão realmente em lugares seguros, contra desastres naturais e do tempo. Em geral, exemplos de preservação são,

salas refrigeradas, limpas, seguras contra incêndio, e outros. A preservação das informações é algo indispensável, pois muitas informações podem ser irreparáveis.

2.3 RISCOS ENVOLVENDO INFORMAÇÕES

A evolução dos computadores e a centralização das informações tornou os riscos na segurança de informações muito maiores. Estes riscos se agravaram ainda mais com a rede de computadores e a disseminação da Internet (CARUSO; STEFFEN, 1999).

As pessoas ou organizações estão cada vez mais dependentes das informações armazenadas em computadores, ou em outros meios digitais, pela facilidade, praticidade e versatilidade. Mesmo com a evolução da tecnologia da segurança de informação, ainda têm-se muitos *softwares* e sistemas inseguros. É difícil depender somente de um sistema para garantir a proteção correta das informações e tende-se a procurar algumas medidas extras para aumentar esta segurança.

2.3.1 Centralização de Informações

A necessidade de uma rápida disponibilidade dos dados ajudou a centralização das informações. Com a centralização surgiram problemas variados e em larga escala. Um exemplo típico é o caso de uma pessoa não autorizada entrar no local onde estão armazenadas as informações, e com um disquete, CD gravável ou outro meio digital, copiar dados sigilosos de uma organização. Este problema se agrava ainda mais com redes de computadores, pois uma pessoa pode invadir a central de informações sem mesmo ter o acesso físico a ela.

Em um problema mais claro, no caso de destruição de dados, por exemplo, no caso de acontecer um incêndio na central, todos os dados podem ser perdidos se não tiverem alguma proteção contra esse risco. (CARUSO, STEFFEN, 1999).

2.3.2 Acesso Indiscriminado

O problema de acesso indiscriminado está sendo minimizado, mas, ainda é bastante encontrado. Nas organizações ainda é possível encontrar centrais de informações sem nenhum controle ou restrição ao acesso físico ou lógico as mesmas.

2.3.3 Obscuridade das Informações

As informações deixaram de ser colocadas em papéis para serem armazenadas em meios digitais, onde elas ficaram mais “invisíveis“. Portanto, elas ficaram mais vulneráveis a mudanças sem serem notadas. Este cuidado pode ser feito com um sistema de proteção aos documentos como a criptografia, que será vista mais adiante.

2.3.4 Acesso Não Autorizado

O problema do acesso não autorizado vem desde o surgimento dos computadores. Com a Internet, o problema tornou-se crítico. São acessos feitos por pessoas ou por programas que abrem brechas na segurança das informações. Alguns tipos de acesso não autorizados são:

a) ***cracker*[1]:** pessoa que normalmente usa a Internet com a finalidade de descobrir falhar no sistema de segurança e copiar informações que lhe podem ser úteis. *Crackers* podem causar muitos danos a organizações ou pessoas, resultando em prejuízos financeiros e morais;

b) **vírus:** criado a princípio por empresas de software para dar uma proteção maior a seus programas, e em seguida foi utilizado para outro fim. *Crackers* usam esses vírus para quebrar o funcionamento correto de alguns softwares;

c) **cavalo de tróia:** uma variante de vírus que é enviado ao computador hospedeiro para abrir caminhos na segurança por onde um *cracker* pode obter informações.

2.3.5 Quebra de Integridade

Em conseqüência de um aceso não autorizado, informações podem ser alteradas, sem que se perceba a modificação. Portanto, essas informações perdem sua integridade.

2.3.6 Técnicas de Defesa

Os riscos apresentados anteriormente, se não prevenidos, poderão gerar perdas de dados causando grandes prejuízos.

---

[1] O termo *hacker* se difere de *cracker* no caso que o *hacker* apenas burla a segurança para estudo, enquanto o *cracker quebra a segurança* para copiar, destruir ou alterar informações (CARUSO; STEFFEN, 1999).

Vírus são um dos maiores problemas no caso de microcomputadores. Algumas técnicas de defesa são adotadas para tentar prevenir este risco e maximizar a segurança. São citadas algumas soluções segundo Caruso e Steffen:

a) software de administração de rede;

b) software de segurança;

c) software de controle de oficialização de novos programas;

d) pacotes de administração de espaço em disco;

e) controle de fitoteca;

f) análise do sistema operacional.

g) anti-Vírus

2.4 SEGURANÇA DE INFORMAÇÕES MÉDICAS

Em hospitais as informações sobre um paciente são essenciais para um bom tratamento do mesmo. Para garantir um bom armazenamento e um acesso rápido às informações de saúde são usados prontuários eletrônicos.

2.4.1 Prontuário Eletrônico

Prontuários eletrônicos podem armazenar uma variedade de dados necessários para o tratamento de um paciente, como informações pessoais, exames, histórico, laudos e imagens, entre outros.

> O prontuário do paciente foi desenvolvido por médicos e enfermeiros para garantir que se lembrassem de forma sistemática dos fatos eventos clínicos sobre cada indivíduo de forma que todos os demais profissionais envolvidos

> no processo de atenção de saúde poderiam também ter as mesmas informações. (MARIN, MASSAD, AZEVEDO, 2003, p.1).

Desses dados pode-se extrair outros tipos de informações como relatórios, gráficos, tabelas e cálculos, com uma facilidade não encontrada nos prontuários em papéis.

Além de diminuir o espaço de armazenamento dos documentos em papéis nos hospitais, um prontuário tem como auxiliar um profissional da saúde em alguns pontos:

a) **acessibilidade:** um prontuário eletrônico tem como pré-requisito permitir acesso fácil às informações;
b) **disponibilidade:** as informações agora estão disponíveis em tempo mínimo, muito mais rápido do que a procura nos velhos arquivos de documentos em papéis;
c) **legibilidade:** prontuários em papel contêm informações manuscritas, que muitas vezes são de difícil leitura. Em um prontuário eletrônico os dados são digitalizados no computador, o que facilita a leitura e diminui as chances de má interpretação;
d) **segurança:** em um prontuário eletrônico as informações têm uma segurança lógica não encontrada nos prontuários em papel. Essa segurança pode vir por meio de controle de acesso lógico;
e) **autenticidade:** em informações com um maior grau de importância, deve-se ter uma identificação das pessoas que criaram ou modificaram certos documentos, e que eles sejam responsabilizados por seus atos. Essa autenticidade pode ser adquirida através de assinatura digital, que é apresentada neste trabalho;

f) **compartilhamento:** esses dados devem ser passíveis de compartilhamento com outros profissionais da saúde, seja ele através de um mesmo terminal ou através de uma rede de computadores.

2.4.2 Por que os Prontuários Precisam ser Seguros?

Durante o acompanhamento médico de um paciente é muito importante ter disponível o maior número de informações possíveis sobre ele. Portanto, há uma grande necessidade de armazenamento de dados médicos e manutenção desses dados de forma integra. Informações erradas, perda ou má interpretação muitas vezes põem em risco o tratamento de um paciente.

3 CRIPTOGRAFIA

A criptografia tem como um de seus objetivos transformar uma mensagem em outra cifrada por meios matemáticos permitindo que somente pessoas autorizadas possam decifrá-la.

A palavra criptografia tem a origem grega, *kryptos* (oculto, escondido, secreto); *graphos* (escrever, grafar). É uma técnica antiga, mas começou a se consolidar em âmbito militar na transmissão de informações diplomáticas (VOLPI, 2004). A criptografia está em quase todos períodos da história humana, pois é comum que as pessoas tenham algo a esconder, como fórmulas, informações confidenciais e outros, e que poderiam causar algum estrago em mãos inimigas. Dizem que ela é tão antiga quanto à escrita e já estava presente nos hierógrafos egípcios.

A técnica mais antiga que se tem conhecimento é a do código de César. Ela foi criada por volta de 50 a.C. por Júlio César para enviar informações a seus generais. Ela se baseava na substituição monolítica, que por César era a substituição de uma letra por outra com um avanço de três casas. Exemplo: a letra A era trocada pela letra D. Hoje em dia chamamos de código de César qualquer técnica que seja de substituição de uma letra por outra com uma relação fixa. (CARVALHO, 2001). Sendo assim, já que o alfabeto romano tinha 26 letras, então eram somente possíveis 26 chaves diferentes, tornando o sistema fácil de ser quebrado (mesmo sendo avançado para a época).

Na Renascença a criptografia começou a dar seus primeiros passos e ficar mais popular. Até chegar na última técnica antes do computador, o sistema de rotores usado pelos nazistas na Segunda Guerra Mundial. O sistema de rotores teve esse nome devido ao fato de ter sido implementado em máquinas com discos que eram chamados

de rotores. A partir da Segunda Guerra Mundial, com a utilização de computadores, a criptografia começou a ficar mais robusta e passou a ser mais utilizada.

Ela vem sendo aprimorada e é usada em uma variedade de aplicações, como, autenticações, transações bancárias, dinheiro eletrônico, troca de informações sigilosas e assinatura digital. É cada vez mais usada nas áreas de computação, segurança de rede e telecomunicações.

3.1 TERMINOLOGIA

Mensagem ou texto é a informação que se deseja proteger. No envio de uma mensagem, temos três elementos: o remetente que vai enviar a mensagem; o inimigo, que é o elemento não autorizado que poder ter acesso a essa mensagem e o receptor, para quem está endereçada a mensagem. Essa evento é melhor representado na figura 1.

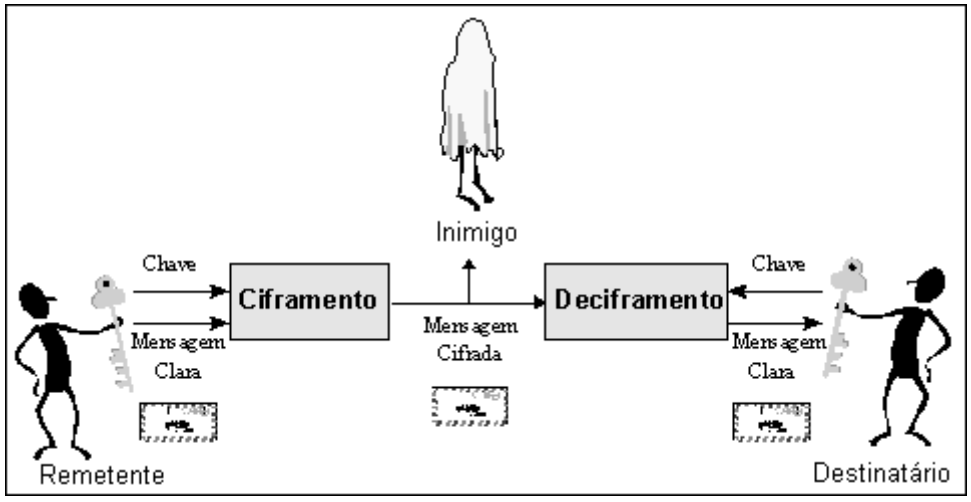

Figura 1. Exemplo de criptografia
Fonte: MAIA, PAGLIUSI. (2000)

Quando é enviada uma informação, a mensagem passa por um processo de criptografia (ou encriptação), no objetivo de tornar ilegível ou ocultar uma mensagem pura. No recebimento dessa mensagem cifrada, ela será descriptografada (ou desencriptada) tornando-se novamente um texto puro.

As ações de criptografar e descriptografar são controladas por uma chave secreta (as chaves podem ser iguais ou diferentes) e por um protocolo de criptografia, que são regras para criptografar e descriptografar.

3.3 PRINCÍPIOS MATEMÁTICOS

Quando se cifra uma mensagem, deve-se fazer com que ela fique o mais segura possível. Um meio de se conseguir essa segurança é com regras matemáticas.

Segundo Carvalho (2001), uma função que se pode definir como criptografia é a seguinte:

$$tc = E_{ch}\ (tp)$$

Nesta função, *tp* é o texto puro, *ch* é a chave, tc é o texto criptografado e *E*() é a função que se refere ao método de encriptação. A chave especifica o valor gerado.

No lado oposto existe a função de desencriptação:

$$tp = D_{ch}\ (tc)$$

Onde a desencriptação é definida por *D*( ), controlada pela mesma ou outra chave (*ch*), e o resultado é o texto puro (*tp*).

A figura 2 ilustra o processo de encriptação e desencriptação.

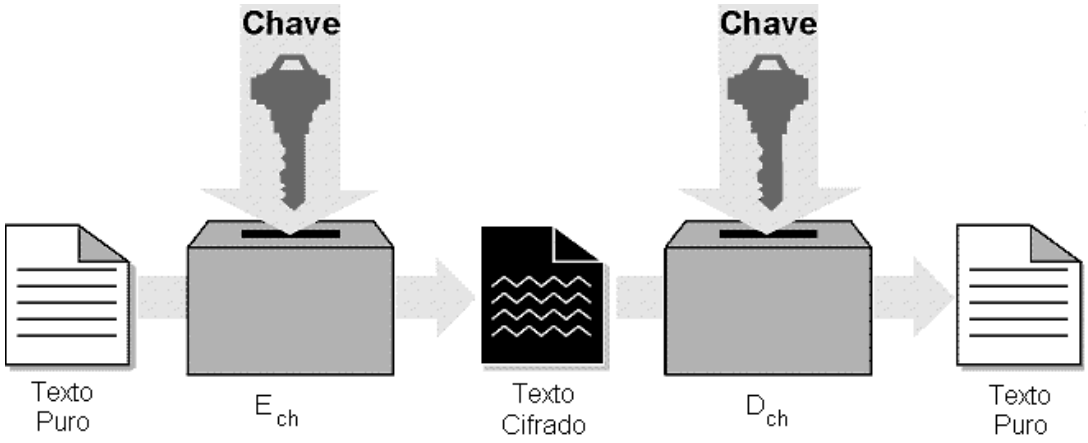

Figura 2. Aplicação de funções criptográficas
Fonte: TRINTA, MACÊDO. (1998)

3.4 TIPOS DE ATAQUE

Existem alguns tipos de ataques, sendo que a maioria tem como objetivo descobrir o conteúdo de uma mensagem cifrada. Em geral essas informações saem de um arquivo ou memória principal para um usuário ou outro arquivo. Os ataques a essas mensagens se apresentam de duas formas principais: o ataque passivo e o ativo. No ataque passivo o inimigo captura a mensagem cifrada e tenta descobrir seu conteúdo sem interferir na comunicação entre o remetente e o destinatário. Esse tipo de ataque pode ser classificado em duas categorias (CARVALHO, 2001):

a) análise de conteúdo: quando o inimigo tenta descobrir a mensagem ou uma parte dela. Em sistemas mais fracos é possível descobrir toda a mensagem apenas descobrindo uma pequena parte da mesma. É um ataque contra a confiabilidade da mensagem.

b) análise de tráfego: analisa-se o fluxo das mensagens; o inimigo tenta descobrir a freqüência, remetente ou destinatário dessas mensagens. Em geral esse não é um ataque muito perigoso.

O ataque ativo caracteriza-se pelo inimigo interferir na comunicação entre o remetente e o destinatário. Este ataque tem 3 categorias citadas abaixo (CARVALHO, 2001):

a) interrupção: quando o inimigo altera o fluxo normal das mensagens. Ele se torna o destinatário da mensagem e o destinatário original não recebe nada. Mexe com a disponibilidade da mensagem;
b) modificação: o inimigo intercepta uma mensagem, modifica e envia para o destinatário original, sem que ele perceba a modificação. Ataca a integridade de uma mensagem;
c) fabricação: gera-se mensagens falsas e envia-se para um destinatário.

Este tipo de ataque tem os seguintes objetivos:

a) disfarce: quando o inimigo faz se passar por outra entidade do processo;
b) repetição: intercepta-se uma mensagem e tenta retransmiti-la procurando obter informações;
c) modificação da mensagem: pega-se uma parte da mensagem legitima e altera sem a percepção do receptor;
d) negação de serviço: quando o inimigo atrapalha o processo normal das mensagens.

Os ataques passivos e ativos têm uma grande diferença. Enquanto os passivos são difíceis de serem detectados, os ataques ativos são muito mais perigosos.

Um sistema criptográfico deve proteger-se de todos esses tipos de ataques. Esta resistência é adquirida por algoritmos e protocolos.

3.5 SERVIÇOS DE UM SISTEMA CRIPTOGRÁFICO

Para que um sistema seja considerado seguro, ele tem que dar suporte a alguns serviços que serão descritos abaixo (STALLINGS, 1999):

a) **confiabilidade:** faz a proteção de um ataque passivo. Para que uma mensagem seja enviada ela tem que estar com um alto nível de proteção. Este serviço protege quando há transmissão entre duas entidades por um período de tempo, para que nenhuma entidade externa veja a mensagem. Outro aspecto da confiabilidade é a proteção contra a análise de tráfego, em não permitir que nenhum inimigo tenha informações sobre a emissão e o recebimento;

b) **autenticidade:** este serviço garante que os dois lados da comunicação sejam autênticos. Quando se recebe uma mensagem deve-se saber realmente qual foi o seu remetente. Ele tem dois aspectos principais. Primeiro, quando se inicia uma conexão é preciso que as duas entidades sejam autênticas. Segundo, a conexão não pode ser interferida por nenhum inimigo e garantir que ela não esteja disfarçada;

c) **integridade:** tem como principal objetivo garantir que a mensagem enviada seja a mesma recebida, sem que haja inserção, duplicação, modificação ou repetição;

d) **não-repúdio:** previne que alguém negue o envio ou o recebimento de uma mensagem;

e) **controle de acesso:** faz o controle de acesso ao meio por onde irá trafegar a informação. As entidades que terão acesso a esse meio terão que ser identificadas e autenticadas;

f) **disponibilidade:** garante que os documentos ou as informações sempre estejam disponíveis.

3.6 TIPOS DE CRIPTOGRAFIA EM RELAÇÃO AO USO DE CHAVES

A cifragem de uma mensagem baseia-se em algoritmo e chave. O algoritmo utiliza regras matemáticas para cifrar uma mensagem e a chave é uma cadeia de bits que é utilizada em alguns algoritmos. Cada chave faz com que o algoritmo obtenha resultados diferentes.

Antigamente a criptografia tinha como princípio somente o algoritmo para cifrar uma mensagem. Assim, se um inimigo descobrisse o algoritmo utilizado não teria mais problemas em decifrar uma mensagem.

A utilização de chaves em um sistema criptográfico oferece duas grandes vantagens. Primeiro, a utilização do mesmo algoritmo para diferentes destinatários. Segundo, a facilidade de trocar a chave caso ela seja quebrada, e mantendo o mesmo algoritmo.

Em algoritmos baseados em chaves existem dois tipos de criptografia. A primeira delas é a criptografia por chave simétrica, que ocorre na situação onde as chaves para cifrar e decifrar são idênticas. A segunda é a criptografia por chave assimétrica, onde a chave para cifrar é diferente da chave para decifrar.

Neste trabalho foi dado um maior enfoque à criptografia assimétrica, por ser base para implementação do processo de assinatura digital.

3.7 CRIPTOGRAFIA SIMÉTRICA

Em sistemas simétricos, o remetente e destinatários terão que possuir a mesma chave. Ela se caracteriza por criptografia por chave secreta, pois somente o remetente e o destinatário poderão ter conhecimento sobre essa chave.

Nesse tipo de criptografia, o remetente e o destinatário precisam intercambiar a chave secreta antes de iniciar a comunicação. Esse intercâmbio precisa ser feito em um canal seguro, pois qualquer inimigo que adquira o conhecimento sobre essa chave pode decifrar a mensagem. Um canal seguro é um meio por onde pode se passar informações sem o risco de uma terceira pessoa interceptar essa informação.

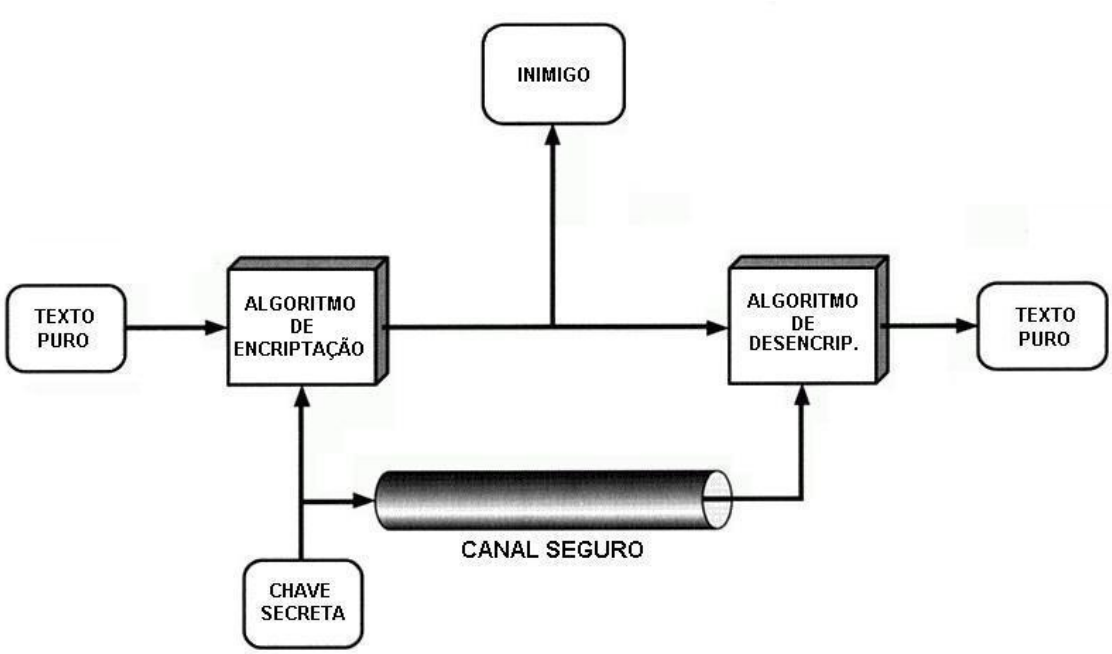

Figura 3. Esquema de criptografia simétrica
Adaptado de STALLINGS. (1999)

A figura 3 mostra como funciona uma criptografia simétrica, onde o canal seguro é por onde passa a chave secreta. Nenhum inimigo pode ter acesso a esse canal.

Segundo Carvalho (2000), os principais algoritmos de chave simétrica são:

a) DES (*Data Encryption Standard*): foi desenvolvido em 1977, e ainda continua sendo um dos algoritmos mais usados. Ele cria blocos de 64 bits usando uma chave de 54 bits;
b) AES (*Advanced Encryption Standard*): criado em 2000, aceita chaves de 128, 192 e 256 bits e trabalha com blocos de 128 bits. Ele foi adotado como padrão de criptografia substituindo o DES.
c) IDEA (*International Data Encryption Algorithm*): um algoritmo de blocos de 64 bits e uma chave de 128. É um algoritmo considerado muito bom. Foi desenvolvido em 1990;
d) RC5: desenvolvido em 1995 e diferente dos outros algoritmos parametrizado. Isto é, pode-se escolher o tamanho da chave e o tamanho do bloco.

3.8 CRIPTOGRAFIA ASSIMÉTRICA

A utilização da chave simétrica poderia trazer alguns problemas quando usada para um grande número de usuários. Assim, por volta de 1976 começou a surgir o conceito de criptografia de chave assimétrica, ou chave pública, a fim de tratar alguns problemas gerados pela criptografia de chave simétrica. O principal deles é da distribuição da chave secreta, que precisava ser passada em um canal seguro para as entidades autenticadas.

Em uma comunicação por chave privada (simétrica), um problema seria quando uma entidade quisesse enviar uma mensagem à outra sem que essa outra tivesse uma cópia dessa chave. Este problema seria ainda maior se não houvesse um canal

seguro disponível no momento causando um atraso maior na comunicação. Por exemplo, em uma empresa com 50 funcionários, onde cada um quer que cada mensagem seja somente lida pela pessoa a qual foi destinada a mensagem, haveria 1225 chaves diferentes em sistemas simétricos, um para cada par de pessoas, inviabilizando o processo.

Com um sistema assimétrico, há uma chave pública, que qualquer entidade pode ter uma cópia. Há também uma chave privada para cada entidade, podendo ela ser um remetente ou um destinatário.

Segundo Carvalho (2001), os principais algoritmos assimétricos são:

a) RSA: é o algoritmo mais utilizado e é considerado como algoritmo padrão para criptografia assimétrica. Será visto com mais detalhes mais adiante.
b) DAS : Algoritmo criado para implementar assinaturas digitais, como será visto mais diante.
c) Al Gamal: sua segurança consiste na dificuldade de cálculos de logaritmos discretos.

3.8.1 Segurança do Sistema de Chave Públicas

Em geral, os sistemas de chave públicas são mais seguros que os sistemas de chave simétricas, pois não precisam do canal seguro e somente a entidade receptora precisa saber a chave secreta (privada), tendo as outras entidades somente a chave pública. Sendo assim cria-se um novo problema com qual o sistema tem que se preocupar: agora o inimigo também pode ter uma cópia da chave pública e com isso ele pode tentar interceptar uma mensagem e tentar decifrá-la a partir dessa chave pública.

Outro problema que pode ocorrer é na situação onde o inimigo tenta enganar o remetente com outra chave pública criada por ele, então o sistema necessita de uma autenticação também das chaves públicas.

4 ASSINATURA DIGITAL

Desde a antiguidade sempre houve a necessidade de garantir a autenticidade de um documento, comprovando a verdadeira intenção de um indivíduo em relação ao mesmo. Esses documentos poderiam ser desde cartas de amor até documentos oficiais. O modo clássico de autenticação de um documento é por meio da assinatura manuscrita.

Com o avanço computacional e a chegada da Internet, surgiram à transferência eletrônica de documentos, o *e-commerce* e outros, que muitas vezes são feitos por pessoas que estão a milhares de quilômetros umas da outras. Portanto, surgiram algumas questões: o autor de um documento pode autenticá-lo eletronicamente? E como o destinatário pode ter certeza de que o texto recebido é o mesmo que foi enviado?

Uma forma de legitimar a intenção de uma pessoa em relação a um documento eletrônico é usar a assinatura digital.

4.1 CONCEITOS

A príncipio, a assinatura digital tem o mesmo objetivo da assinatura manual, mas utiliza formas computacionais e matemáticas para alcançar a autenticação desejada.

Segundo o dicionário Aurélio (1997), a assinatura digital tem como significado, “assinar: firmar com seu nome ou sinal (carta, documento, etc.); digital: que é representado exclusivamente por números (segundo um código convencional) e, portanto, passível de processamento por computador digital”.

A assinatura digital não só busca garantir a autenticidade de um documento como a integridade e o não-repúdio do mesmo.

> Assinatura digital é um método que garante que determinada mensagem não seja alterada durante seu trajeto. Esse processo envolve criar a mensagem, cifrá-la e enviá-la conjuntamente tanto da mensagem original como da cifrada. Uma vez recebidas, o destinatário compara o conteúdo da mensagem original com o da cifrada, para se certificar de que não houve alteração. (FORD, BAUM, 1997 apud VOLPI, 2001, p. 4).

Segundo Carvalho (2001), espera-se de uma assinatura digital alguns requisitos:

a) Seja fácil de produzir para quem assina;
b) Seja fácil de verificar por qualquer um;
c) Seja muito difícil de ser falsificada;
d) Tenha uma vida útil apropriada (de modo que quem assina não possa negar a autoria).

Normalmente, utilizam-se senhas e chaves para assinar um documento, mas, existem outras formas de segurança no lugar de uma simples senha. Biometria, entre outros, são formas de garantir autenticidade de uma pessoa para que possa assinar um documento, usando a sua chave.

A filosofia de uma aplicação de assinatura digital se baseia em um autor que possa cifrar um documento juntamente com sua chave e identificação para que uma outra pessoa possa, descriptografar a mensagem, e verificar a autenticidade e integridade do documento. A Figura 4 ilustra uma aplicação.

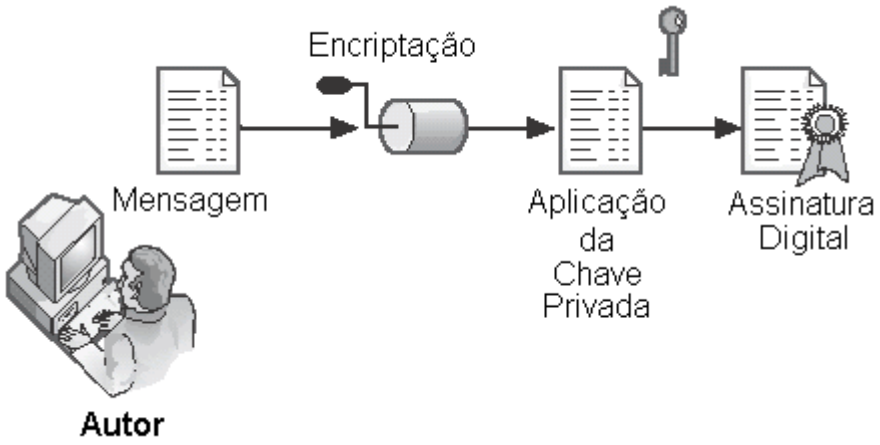

Figura 4. Assinatura digital
Fonte: MAIA, PAGLIUSI. (2000)

4.2 CRIPTOGRAFIA EM ASSINATURA DIGITAL

Para manter um documento seguro contra alterações são usados métodos de criptografia, a qual é o recurso principal de uma assinatura digital.

Quando se codifica um documento em um sistema de assinatura digital, é normalmente usada criptografia de chave pública (assimétrica). A criptografia por chave pública permite que um emissor ou autor e um receptor ou leitor tenham chaves diferentes. Esse tipo de criptografia está mais bem detalhado no capítulo 3.

Geralmente, a assinatura digital faz uma relação direta com algoritmos de autenticação. Sempre partindo de um conceito de assinatura digital como integridade e autenticidade de um determinado documento sobre o remetente do mesmo.(VOLPI, 2001).

A assinatura digital é baseada em uma chave privada do remetente ou autor em conjunto com o conteúdo do documento. Uma chave pública, essa aberta a todos, é usada para que um leitor possa ter certeza da autenticidade e integridade de um mesmo documento. Esse procedimento é ilustrado na figura 5.

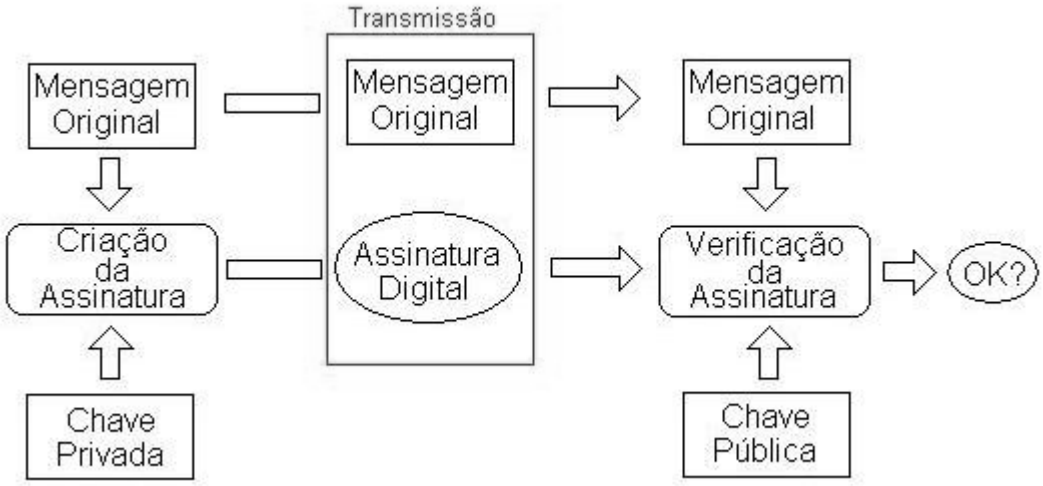

Figura 5. Verificação de uma mensagem assinado digitalmente
Adaptado de VOLPI. (2001)

4.3 TÉCNICAS E ALGORITMOS

Um sistema de assinatura digital (AD) deve demonstrar ser o mais seguro possível. Várias técnicas e algoritmos foram criados para dar uma maior fidelidade. Em muitos casos juntam-se técnicas e algoritmos para aumentar a segurança.

4.3.1 Checksum

Utiliza uma chave secreta que trabalha em conjunto de um algoritmo que aplicados a uma mensagem resulta em um bloco de dados de dimensão fixa. Este bloco pode ser chamado de *checksum* criptográfico ou *Message Authentication Code* (MAC). (VOLPI, 2001).

MAC = checksum (Mensagem, Chave secreta)

Esta técnica utiliza algoritmos de chave privada. Assim, quando uma pessoa for conferir a integridade de um documento, ela necessita do MAC e da chave privada da mesma.

A princípio o *Checksum* era o resultante da soma do código ASCII de todos os caracteres da mensagem. Como o *checksum* poderia ter valores muito grandes, era necessário deixar o checksum com um valor fixo, surgiu, então, a seguinte solução: pegar o resto da divisão entre a soma dos caracteres e o valor máximo alcançado pelo bloco de bit mais 1. Assim, uma função para se alcançar o checksum seria:

Checksum = Total_caracteres % (Valor_máximo + 1)

Na criptografia de uma mensagem poderia surgiu a seguinte seqüência de caracteres: “S%7B+”.

Passando para o código ASCII obteríamos:

S	%	7	B	+
83	37	55	66	43

Então a soma dos caracteres ficaria 284, e o valor máximo em um bloco de 8 bits é 255, logo a soma seria 284, pegando o restante da divisão por 255 mais 1. O checksum desta mensagem seria 28.

O *Checksum* é um modo simples de conseguir uma certa integridade, mas fica longe de ser um método seguro, pois é muito fácil de ser quebrado. Um dos motivos dessa fragilidade é que se pode resultar em muitos *checksum* iguais em diferentes cadeias de caracteres. Enganando um leitor e quebrando a integridade.

4.3.2 Checagem de Redundância Cíclica

O CRC é uma outra técnica de integridade com algoritmos que, como o Checksum, geram um bloco de dados.

Essa técnica foi usada por muito tempo em adaptadores de cadeia e controladores de disco, mas, recentemente é somente usada em programas de verificação de pacotes. (PROSISSE, 2000).

Como o checksum, o CRC é uma técnica muito simples. Ela é baseada na divisão poligonal de cada bit da mensagem. Exemplo: podem-se ter uma seqüência 01001011 em uma mensagem. Para o cálculo do CRC teríamos:

$$F(x) = 0x7 + 1x6 + 0x5 + 0x4 + 1x3 + 1x2 + 0x1 + 1 = 12$$

O CRC é mais flexível que o checksum e um pouco mais seguro, mas nada que impeça uma pessoa com más intenções de modificar a mensagem deixando a mesma soma de CRC.

4.3.3 Funções Hash

As técnicas Hash são algoritmos de sentidos únicos (*one-way function*). Elas são diferentes das funções normais de criptografia, por não possuírem uma chave e serem irreversíveis.

Criptografar uma mensagem inteira pode ser demorado e ter um resultado muito grande. Então pode se utilizar uma função Hash para obter um resultado de tamanho fixo que corresponde à mensagem original. Esse resultado é chamado de *Message Digest*. Assim não importando o tamanho da mensagem, ele sempre vai retornar um resultado de tamanho único (CARVALHO, 2001).

Funções Hash têm algumas características importantes:

a) Os valores Hash são tão únicos que é quase impossível reproduzir valores iguais;
b) É impossível chegar a um texto original partindo de uma *message digest.* Por isso o nome de *one-way* function.

Algoritmos Hash são de difícil desenvolvimento, os dois tipos de algoritmos Hash mais conhecidos são:

a) *Message Digest* (MD2, MD4, MD5): aceitam todos tamanhos de mensagem e produzem blocos de tamanho de 128 bits.
b) *Secure Hash Algorithm* (SHA): criado em 1994 pelo governo dos EUA para fazer parte do seu DSS (*Digital Standard Signature*). Ele foi desenvolvido baseado no MD4, mas por ter um digest de 160 bits ele se torna mais seguro e mais lento que o MD5.

4.3.4 Algoritmo RSA

O algoritmo de chave assimétrica mais usado foi desenvolvido em 1977 por Ron Rivest, Adi Shamir e Len Adleman, e teve sua publicação em 1978. (STALLINGS, 1998).

Um algoritmo de chave assimétrica é normalmente lento. Então, o que se faz é usar uma criptografia simétrica com uma chave escolhida aleatoriamente. Toma-se essa chave e utiliza-se o RSA para criptografá-la e enviar junto com a mensagem criptografada com o algoritmo de chave simétrica. Assim, o lento RSA só criptografa a

chave utilizada. Este é um método vantajoso, pois não perde em nada na segurança e ganha trabalhando em uma maior velocidade. (CARVALHO, 2004).

Segundo Carvalho, 2001, para escolha das chaves deve-se escolher dois números primos aleatórios p e q.

$$n = p.q$$

$$O = (p\text{-}1)(q\text{-}1)$$

Escolhe-se um número aleatório e>1 tal que mdc(e,O)=1, i.e., e e O devem ser primos.

$$(e.d) \bmod O = 1$$

A chave pública constitui [n,e], e a chave privada será d. Para certificar segurança no algoritmo, os números p e q devem ser aleatórios e com mais de cem algarismos decimais.

Para criptograr uma mensagem w usa-se:

$$c = w^e \bmod n$$

E descriptografar:

$$w = c^d \bmod n$$

Assinatura digital pode apresentar alguns problemas, principalmente com tempo de envio e processamento. Para resolver esse problema, usa-se o algoritmo RSA em conjunto com funções Hash. Assim, criptografa-se somente a *Message Digest*.

4.3.5 Digital Signature Algorithm

Foi criado em 1991 pelo governo dos Estados Unidos para ser considerado como base para o *Digital Signature Standard* (DSS).

A princípio esse algoritmo gerou algumas controvérsias, segundo Carvalho, 2001:

a) O RSA é mais rápido, por esse motivo tornou padrão adotado pelo DSS;

b) O DSA foi projetado pelo governo, e não se pode saber se foi feito com segundas intenções;

O DSA necessita de dois primos aleatórios *p* e *q*. Dado um valor *l* (0<=*l*<=8), os números primos tem que seguir as seguintes regras:

a) *q* tem o tamanho de 160 bits;

b) *p* tem l bits;

c) *q* é divisor de *p*-1.

Agora se deve selecionar um número aleatório x, tal que x<q, e um outro numero aleatório h, tal que h<(p-1). Assim:

$$i=h^{(p-1)/q} \bmod I$$

$$y = g^x \bmod p$$

Isso resulta em uma chave pública [p,*q*,*g*,*y*] e uma chave privada x.

Para um usuário final, os métodos RSA e DSA podem parecer muito semelhantes. Esses dois métodos são os mais usados em assinaturas digitais.

4.4 APLICAÇÕES DA ASSINATURA DIGITAL

Inicialmente, quando se falava em assinatura digital, pensava-se em simplesmente a autenticação de uma mensagem, carta ou documento. Mas em outros

casos também são aplicadas assinaturas digitais, segundo o Instituto Nacional da Tecnologia da Informação (ITI) (VOLPI, 2001):

a) Comércio eletrônico;
b) Processos judiciais e administrativos em meio eletrônico;
c) Assinatura da declaração de renda e outros serviços prestados pela Secretaria da Receita Federal;
d) Obtenção e envio de documentos cartorários;
e) Transações seguras entre instituições financeiras;
f) Diário Oficial Eletrônico;
g) Identificação de sítios na rede mundial de computadores, para que se tenha certeza de que se está acessando o endereço realmente desejado;
h) Certificação digital.

4.5 CERTIFICAÇÃO DIGITAL E ASSINATURA DIGITAL

Numa primeira visão sobre Certificação Digital, pode-se pensar que eles são sinônimos, mas, apesar de estarem relacionadas, são coisas distintas. Segundo Ford e Baum (2000), "No mundo eletrônico, uma certificação é uma coleção de informações com as quais uma assinatura digital é anexada por alguma autoridade que é reconhecida por alguma comunidade de usuários de Certificados".

Certificação digital é a técnica de identificar se uma pessoa assinou mesmo um documento eletrônico. Ela utiliza assinatura digital e seus algoritmos criptográficos para dar integridade e não repúdio de um documento. Normalmente uma mensagem passa pelo processo de assinatura digital para garantir a integridade da mensagem e depois é anexada com um certificado digital.

Para uma pessoa poder assinar um documento com assinatura digital, ela tem que adquirir um certificado digital, o qual é emitido por autoridades certificadoras.

4.5.1 Autoridade Certificadora

Uma autoridade certificadora é uma organização comercial ou não responsável por emitir certificados digitais. (VOLPI, 2001).

Para adquirir um certificado digital usa-se uma autoridade certificadora. Com a certificação digital uma pessoa tem o direito de assinar um documento eletronicamente e comprovar sua autoria.

Além de emitir certificados digitais, a autoridade certificadora também tem o mesmo papel de um tabelião em assinaturas manuais. Ela pode identificar a autoria de uma assinatura.

Normalmente, um certificado digital tem as seguintes informações (VOLPI, 2001):

a) Chave pública do titular;

b) Nome e endereço de e-mail do autor;

c) Período de validade do certificado;

d) Nome da autoridade certificadora que emitiu o certificado;

e) Número de série do certificado digital;

f) Assinatura digital da autoridade certificadora.

Existem vários padrões referentes aos certificados digitais, sendo o mais usado o X.509. Conforme a figura 6, existe uma chave pública dentro do Certificado Digital, e através dessa chave é possível verificar a validade da assinatura digital.

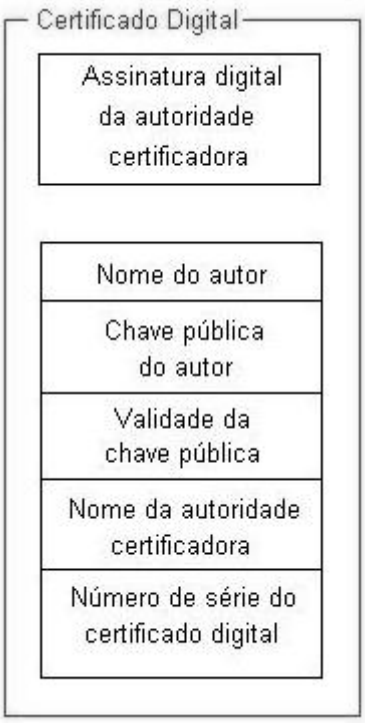

Figura 6. Certificado Digital
Fonte: VOLPI. (2001)

O certificado digital tem uma data de validade, sendo necessário renovar o certificado em uma autoridade certificadora. Se não houver a renovação, cabe a autoridade certificadora a revogação do certificado.

Há outras situações em que pode ocorrer revogação, como por exemplo, a própria requisição do portador. Quando se revoga um certificado digital, a autoridade torna essa revogação pública, de modo a evitar prejuízos aos usuários. Para publicar essas revogações foram criadas as listas de revogação, também conhecidas por *Certification Revogation Lists* (CRLs). (VOLPI, 2004). Uma forma mais segura de verificar os certificados válidos é acessar as listas de revogação.

4.6 ARMAZENAMENTO

Os certificados digitais geralmente são guardados em *smart cards* ou *tokens*, por serem portáteis e de fácil manuseio. O *smart card* se assemelha a um cartão magnético, precisando de um leitor específico ligado ao computador para seu funcionamento. O *token* é um pequeno dispositivo USB que contém memória própria.

Tanto o *smart* card quanto o *token*, contém um *chip* onde é armazenada a chave privada do usuário. O acesso às informações se dá por meio de senha criada pelo titular da certificação.

Apesar de não ter a mesma segurança do *token* e do *smart card*, também é possível guardar os certificados digitais no disco rígido do computador. Esse tipo de armazenamento é o usado deste trabalho.

Todas esses tipos de armazenamento seguem o padrão da infra-estrutura do ICP-Brasil.

4.7 ICP – BRASIL

Com a necessidade de regulamentar a questão de certificação digital, o governo brasileiro implantou uma Infra-Estrutura de Chaves Públicas, o ICP-Brasil.

Uma das principais características do ICP-Brasil é a sua estrutura hierárquica, que é dividida em 3 (três) níveis básicos: o nível de Gestão, onde cuida da normalização; nível de Credenciamento, que escolhe os métodos e processos a serem utilizados pelo nível de Operação, onde este que executa as atividades de registro, certificação e guarda de documentos do usuário para emissão da certificação digital. A figura 7 mostra essa hierarquia.

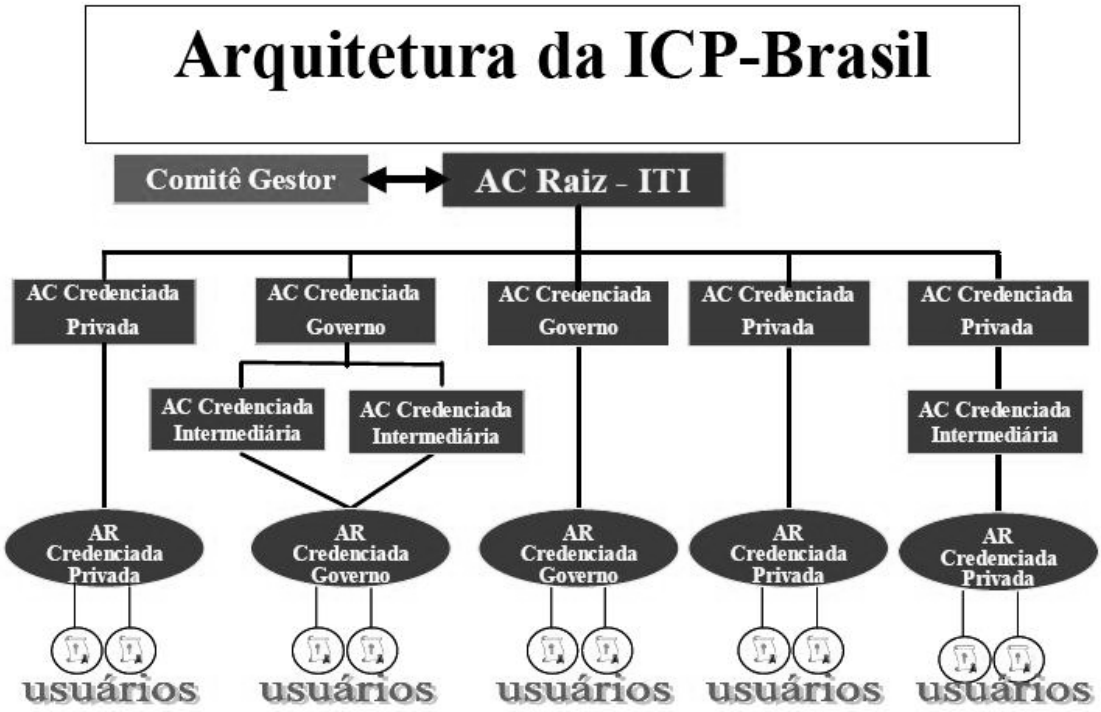

Figura 7. Arquitetura ICP-Brasil

Fonte: SERASA. (2004)

Definições de cada entidade segundo SERASA (2004):

a) Comitê Gestor (CG): estabelece, avalia e aprova políticas, critérios e normas da ICP-Brasil;

b) Autoridade Certificadora Raiz (ACR): emite, revoga, distribui e gerencia certificados digitais, de entidades de nível inferior ao seu. Alem de fiscalizar as Autoridades Certificadoras;

c) Autoridades Certificadoras (AC): emite, revoga e gerencia certificados digitais e também divulga as listas de certificados revogados;

d) Autoridade de Registro (AR): identifica e cadastra usuários diretamente com o mesmo. Encaminha as solicitações às respectivas Autoridades Certificadoras.

Os certificados são divididos em níveis, sendo eles

a) Certificados de Assinatura Digital: A1, A2, A3 e A4;

b) Certificados de Sigilo: S1, S2, S3 e S4.

A tabela 1 abaixo mostra a comparação entre os níveis para um Certificado Digital.

Tipo de Certificado	Chave Criptográfica			Validade Máxima do Certificado Digital (anos)	Freqüência de emissão da LCR (horas)	Tempo Limite de Revogação (horas)
	Tam. (bits)	Processo de Geração	Mídia Armazenadora			
A1 e S1	1024	Software	Repositório protegido por senha	1	48	72
A2 e S2	1024	Hardware	Cartão Inteligente ou *token*, ambos sem capacidade de geração de chave e protegidos por senha	2	36	54
A3 e S3	1024	Hardware	Cartão Inteligente ou *token*, ambos com capacidade de geração de chave e protegidos por senha, ou hardware criptográfico aprovado pelo CG da ICP-Brasil	3	24	36
A4 e S4	2048	hardware	Cartão inteligente ou *token*, ambos com capacidade de geração de chave e protegidos por senha, ou hardware criptográfico aprovado pelo CG da ICP-Brasil	3	12	18

Tabela 1. Níveis de Certificação.

FONTE: SERASA. (2004)

4.7.1 Passos para obter um Certificado Digital

Uma pessoa para conseguir retirar um Certificado Digital precisa seguir os passos (BORGES, 2004):

a) enviar o requerimento do certificado digital a uma AR ou AC, dependendo da estrutura da ICP;
b) o usuário deverá comprovar sua identidade junto a AR;
c) a AR envia o pedido do Certificado a AC;
d) AC assina e divulga o Certificado Digital;
e) usuário instala seu certificado e passa a utilizá-lo.

4.8 ASPECTOS LEGAIS

No Brasil existe algumas regulamentações sobre assinatura digital, que já pode ser usada legalmente e possui validade jurídica.

4.8.1 Legislação Brasileira

Alguns dos principais projetos e decretos usados no Brasil são:

a) Lei Modelo das Nações Unidas sobre o Comércio Eletrônico: as Nações Unidas criou em 1996 um modelo para o comércio eletrônico internacional (UNCITRAL). Este modelo buscou uma maior uniformização possível em um plano internacional;
b) Projeto de Lei nº 672, de 1999, do Senado Federal: incorpora no Brasil a lei modelo da UNCITRAL;
c) Projeto de Lei nº 1.483, de 1999, da Câmera dos Deputados: contendo apenas dois artigos, ela institui a fatura eletrônica e a assinatura digital (certificada por órgão público);

d) Projeto de Lei nº 1.589, de 1999, da Câmera dos Deputados: impõe uma validade jurídica sobre os documentos eletrônicos e a assinatura digital. Adota o sistema de criptografia assimétrico como padrão para assinatura digital;
e) Lei nº 9.983, de 2000: Altera o Decreto-Lei nº 2.848 de 1948 – Código Penal e dá outras providências;
f) Medida Provisória nº 2.200-2, de 2001: Institui a Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil), e dá outras providências;
g) Decreto nº 3.505, de 2000: Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP – Brasil, e dá outras providências;
h) Decreto nº 3.872, de 2001: Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira – CGICP – Brasil, sua Secretária-Executiva, sua Comissão Técnica Executiva e dá outras providências;
i) Decreto nº 3.996, de 2001: Dispõe sobre a prestação de serviços de certificado digital no âmbito da Administração Pública Federal.

4.8.2 Uso de AD em Sistemas de Informação em Saúde

Com o intuito de legalizar a utilização de sistemas informatizados o Conselho Federal de Medicina (CFM) por meio da Câmara Técnica de Informática em Saúde e Telemedicina estabeleceu um convênio de cooperação técnica com a Sociedade Brasileira de Informática em Saúde. Desse modo procurou-se desenvolver um processo de certificação de sistemas informatizados em saúde.

Duas resoluções resultantes da parceria entre CFM e SBIS estabelecem normas para uso de sistemas informatizados em saúde.

a) 1638/2002: “define prontuário eletrônico médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde”.
b) 1639/2002: “dispõe sobre o tempo do tempo de guarda dos prontuários, estabelece critérios para certificação dos sistemas de informação e dão outras providências”.

4.9 TRABALHOS CORRELATOS

Trabalho de Conclusão de Curso, apresentado por Regiane Borges em 2004 na UNESC, é o principal trabalho correlato deste, pois este faz seqüência ao trabalho dela. Neste trabalho desenvolvido não foi anexado a implementação da ao prontuário eletrônico.

No mercado há vários softwares que realizam o processo de assinatura digital. A maioria deles utiliza o padrão x509 e algoritmos RSA.

4.9.1 BRy Signer 2.1

Uma empresa brasileira, atuando na área de desenvolvimento de softwares de segurança. Com sede em Florianópolis, Santa Catarina, a BRy trabalha em cooperação da Universidade Federal de Santa Catarina (UFSC) através do Laboratório de Segurança em Computação do Departamento de Informática e Estatística (LabSEC);

BRy Signer 2.1	
Características	**Descrição**
Custo do software	R$ 240,00
Plataforma	Windows 9x,NT,2000,ME e XP
Algoritmo utilizado	RSA
Padrão	X509
Idioma	Português, espanhol e inglês

Tabela 2. Características do BRy Signer 2.1

4.9.2 Sign Corporate

Criado pela empresa Xsign, o software dá suporte a assinatura biométrica. Uma empresa brasileira que trabalha com prestação de serviços, consultoria e treinamento em desenvolvimento de softwares.

Sign Corporate	
Características	**Descrição**
Custo do software	R$ 500,00
Tempo de licença	1 Ano
Plataforma	Windows 98, 2000, XP e 2003
Algoritmo utilizado	sha1RSA (1024 bits)
Idioma	Português

Tabela 3. Características do Sign Corporate

4.9.3 Sistema Criptográfico Omega

Desenvolvida pela Omega.net, também especializada em criação de sites, portais e *home-pages*, desenvolvimento de sistemas para empresas utilizando criptografia comercial e comunicação em rede.

Sistema Criptográfico Omega 1.2	
Características	**Descrição**
Custo do software	**R$ 150,00**
Tempo de licença	Ilimitado
Plataforma	Windows 2000, XP, 2003
Algoritmo utilizado	Não disponível
Padrão	PKCS e X.509
Idioma	Português

Tabela 4. Características do Omega

4.2 APIS

Em algumas linguagem de programação já existem APIs específicas para criptografia ou até mesmo assinatura digital. Isso poupa trabalho de um desenvolvedor que quer criar *software* que usem assinaturas digitais.

Este trabalho terá um maior foco nas APIs Java, pois é a linguagem de programação escolhida para implementar a assinatura digital.

5 IMPLEMENTAÇÃO DA ASSINATURA DIGITAL NA EVOLUÇÃO DO PACIENTE DO PEP DO HRA

Como já foi falado anteriormente a segurança em um prontuário médico é muito importante e está relacionada a aspectos legais. A segurança quanto à integridade dos dados é feita por Assinatura Digital. A Assinatura Digital foi desenvolvida nas evoluções do paciente, onde somente um médico pode escrever e assinar digitalmente.

A evolução médica é um acompanhamento diário do paciente. É necessária para que um médico possa ver o acompanhamento detalhado e tomar melhores medidas para tratamento do paciente.

No sistema desenvolvido um médico pode ver todas as evoluções e verificar a legitimidade delas, mas ele só pode assinar caso ele tenha uma Certificação Digital adicionada na base de Certificações Digitais do prontuário eletrônico.

O trabalho de conclusão de curso apresentado per Regiane Borges apenas desenvolveu um módulo de assinatura digital e não o implementou no prontuário.

5.1 RECURSOS USADOS

O sistema foi desenvolvido em Java, pois a Sun já possui APIs nativos com suporte a criptografia e assinatura digital, bem como a documentação necessária para implementação. Foi utilizada a versão JDK 1.5 do Java, por ser a versão mais recente disponível para desenvolvimento, assim podendo utilizar alguns recursos novos presentes nessa versão.

Para o ambiente de desenvolvimento foi utilizado o Netbeans 5.0, por se tratar de um ambiente de desenvolvimento de fácil usabilidade e por ser um *software* gratuito.

O banco de dados das informações é o PostgreSQL 8.1, por ser um banco de dados relacional, *freeware* e o mesmo banco de dados já utilizado no prontuário eletrônico desenvolvido pelo Projeto Kiron.

5.2 SISTEMA DESENVOLVIDO

No sistema desenvolvido, um médico somente pode escrever uma evolução se ele tiver um certificado registrado no banco de certificados. No entanto, ele pode ver e verificar evoluções escritas por outros médicos. A figura 8 mostra um diagrama de Caso de Uso da utilização do sistema por um médico.

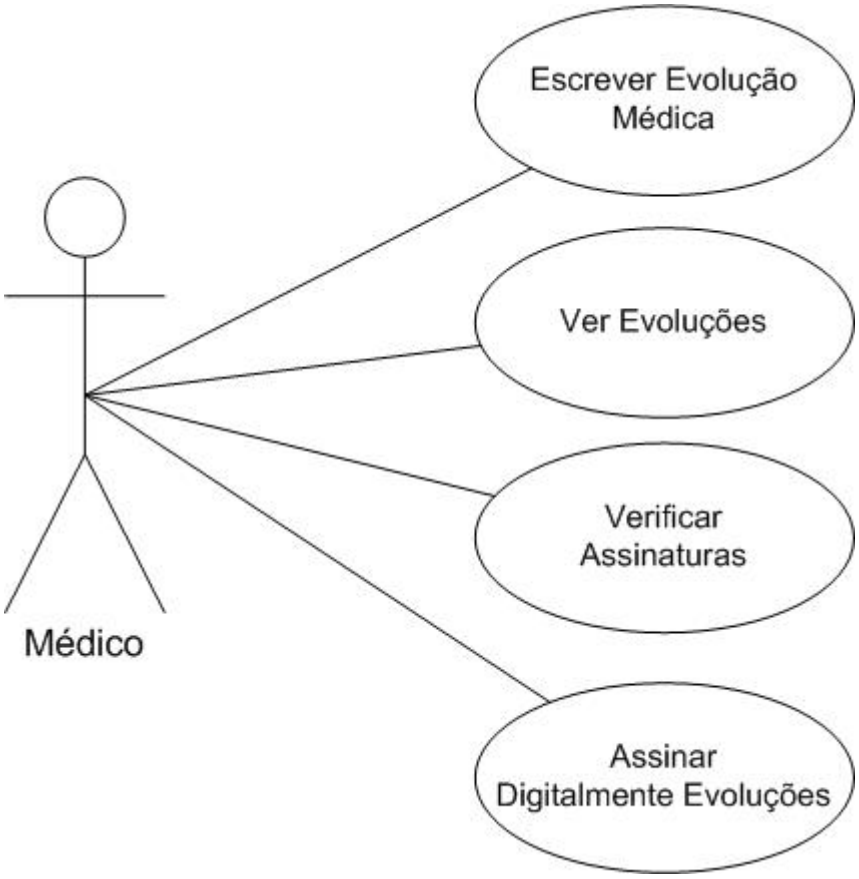

Figura 8. Diagrama Caso de Uso na utilização do sistema por um médico

A Assinatura Digital foi implementada na evolução médica que fica na aba "evolução do dia" no prontuário eletrônico, conforme figura 9. Nesta interface o médico pode adicionar e verificar as evoluções.

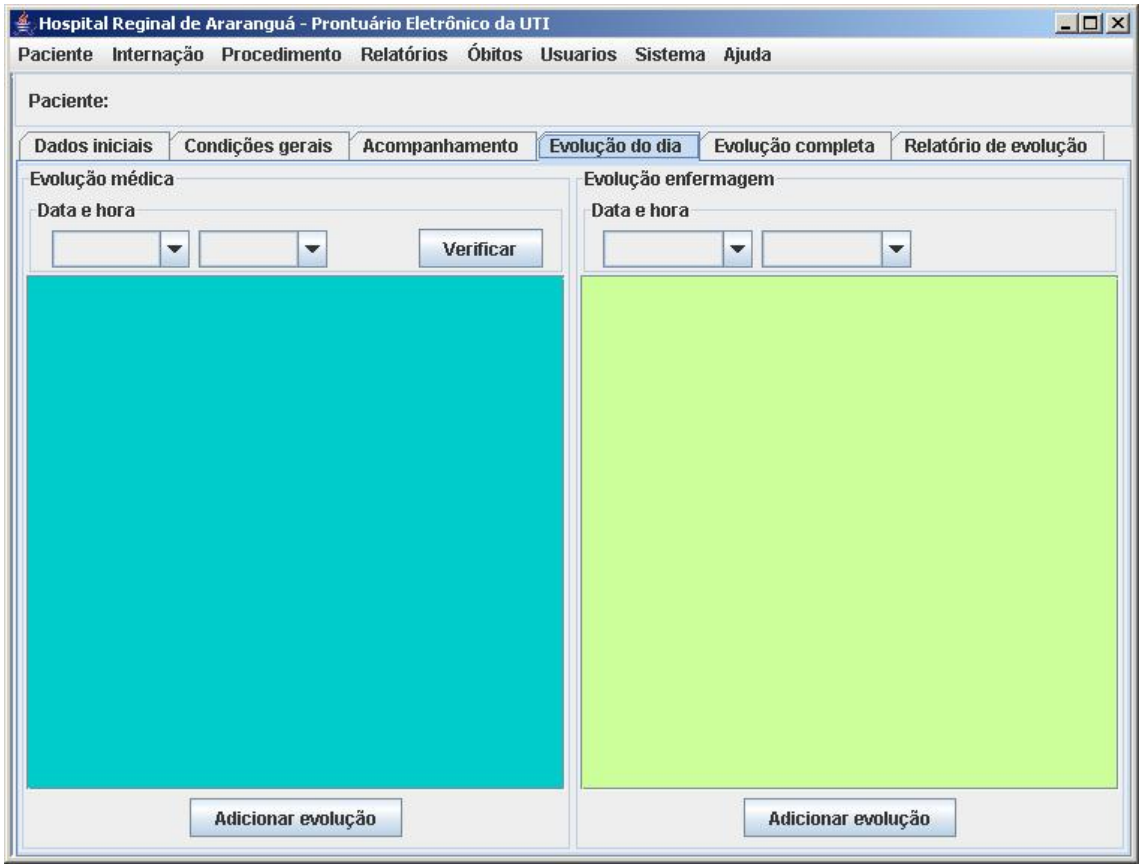

Figura 9. Tela de evolução médica

A figura 10 mostra o diagrama com o fluxo do sistema quando um médico assinar uma evolução.

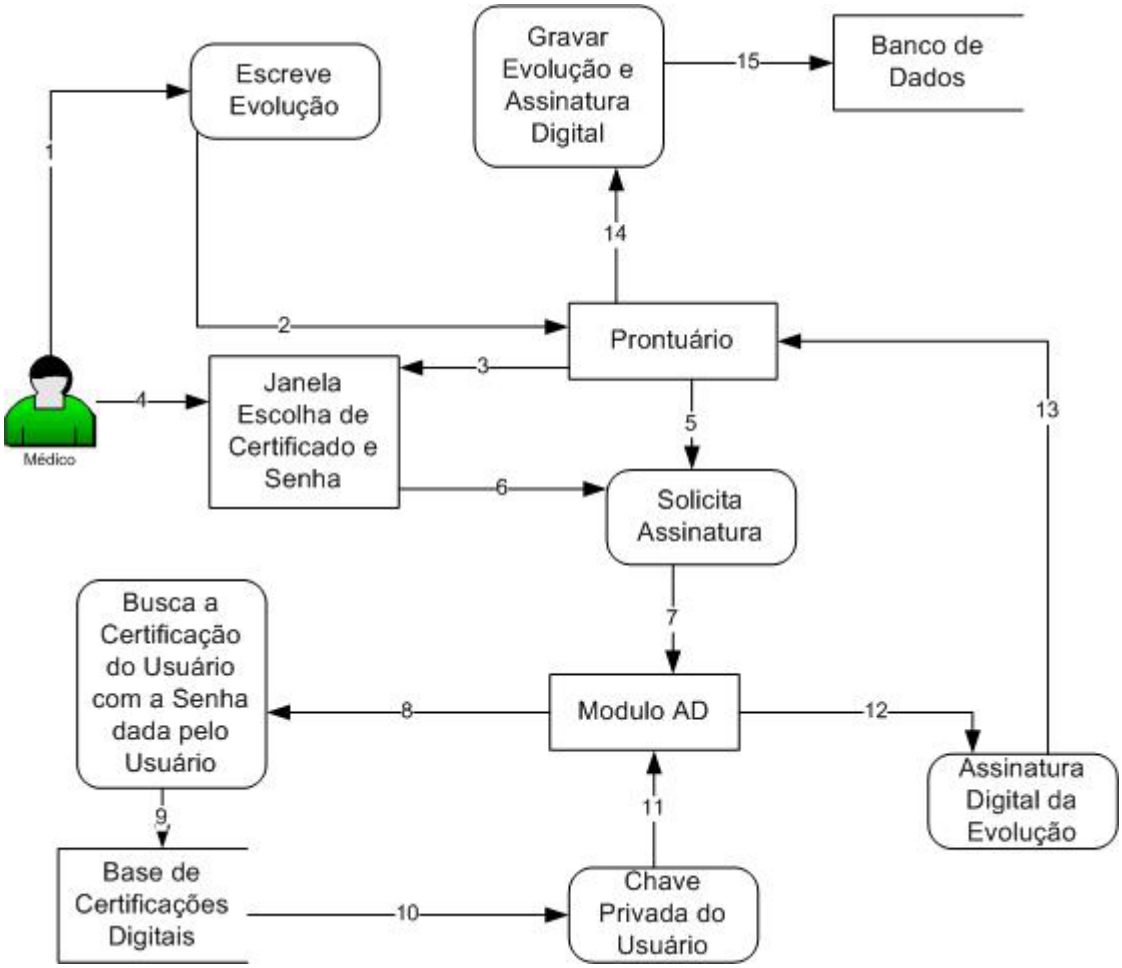

Figura 10. Diagrama da assinatura de uma evolução

Para que um médico possa assinar uma evolução, ele tem que ter seu Certificado Digital no banco de certificados. Para adicionar uma evolução ele vai à opção Adicionar evolução (figura 9) onde irá abrir uma janela para escrever a evolução (figura 11). Ao gravar a evolução o sistema pedirá que o médico escolha um certificado e que digite a senha de acesso.

Caso o médico não possua um certificado digital, ele terá que procurar uma autoridade certificadora e seguir os passos necessários para obter um Certificado Digital, esses passos foram descritos anteriormente. Após obter o Certificado Digital administrador do sistema poderá adicioná-lo na Base de Certificações Digitais.

A Base de Certificações Digitais é um arquivo gerado pela ferramenta keytool desenvolvido pela Sun. Essa ferramenta acompanha a instalação do Java JDK 1.5 e serve para administrar Certificações Digitais na base.

Neste trabalho foram usados Certificados que não tem validade jurídica, gerados pela ferramenta keytool. Para o uso no Hospital serão usados somente Certificados Digitais legais.

Um médico só tem permissão para registrar novas evoluções, sendo proibido a ele e a qualquer outro usuário alterar ou remover as evoluções e assinaturas já gravadas no banco de dados. Somente o administrador do banco de dados terá essas permissões.

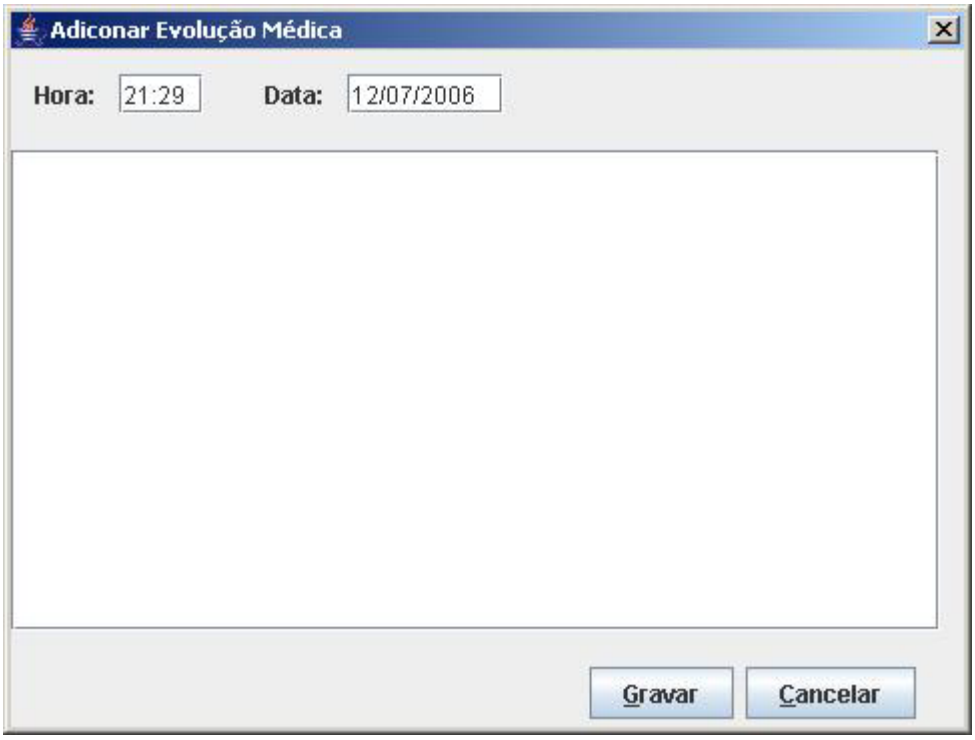

Figura 11. Tela adicionar evolução

Para criar a message digest da evolução é utilizado a API Java Security. Isso é feita através dos métodos:

```
//cria uma instancia de MessageDigest usando algoritmo SHA
MessageDigest messageDigest = MessageDigest.getInstance("SHA");
//passa o texto da evolução para o objeto de MessageDigest
messageDigest.update(evolução);
```

Uma assinatura digital é criada através de um objeto Signature que também é da API Java Security. O algoritmo para criar um assinatura digital é o DAS.

```
//Cria uma instancia de Signature para utilizar o algoritmo DSA
Signature signature = Signature.getInstance("DSA");
//passa a MessageDigest como parâmetro para criar a mensagem
de //assinatura digital
signature.update(messageDigest);
```

Com a evolução e a assinatura digital, então grava-se no banco de dados. A evolução é gravada na tabela “evolucao_med” e a assinatura na tabela “assinatura” a qual tem uma chave estrangeira em “evolucao_med”. Somente um administrador do banco de dados pode remover ou alterar estes registros. Os campos com dados estão das tabelas estão descritos nas figuras 12 e 13.

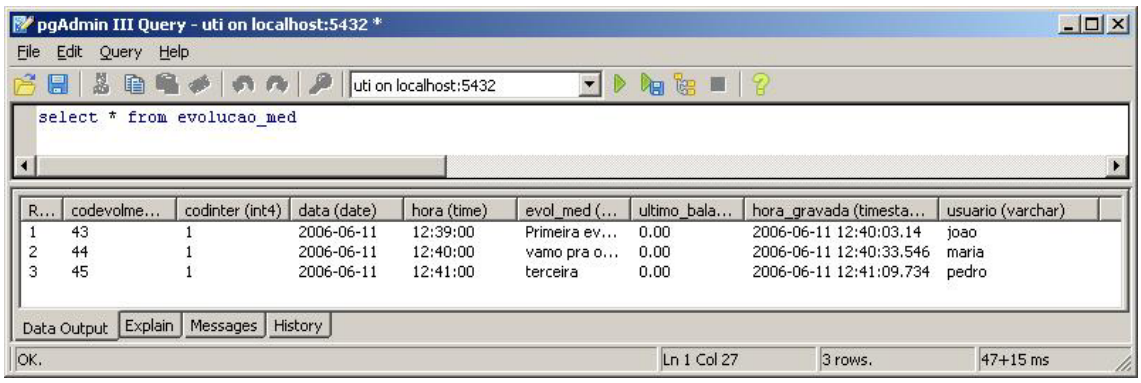

Figura 12. Registros da tabela “evolução_med”

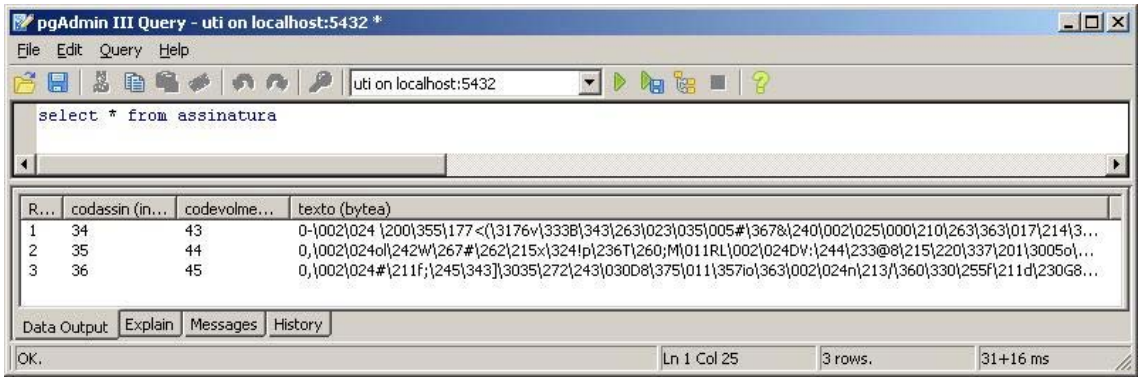

Figura 13. Registros da tabela “assinatura”

Qualquer usuário pode verificar a assinatura de uma evolução, as etapas dentro do sistema para uma verificação estão descritas na figura 14.

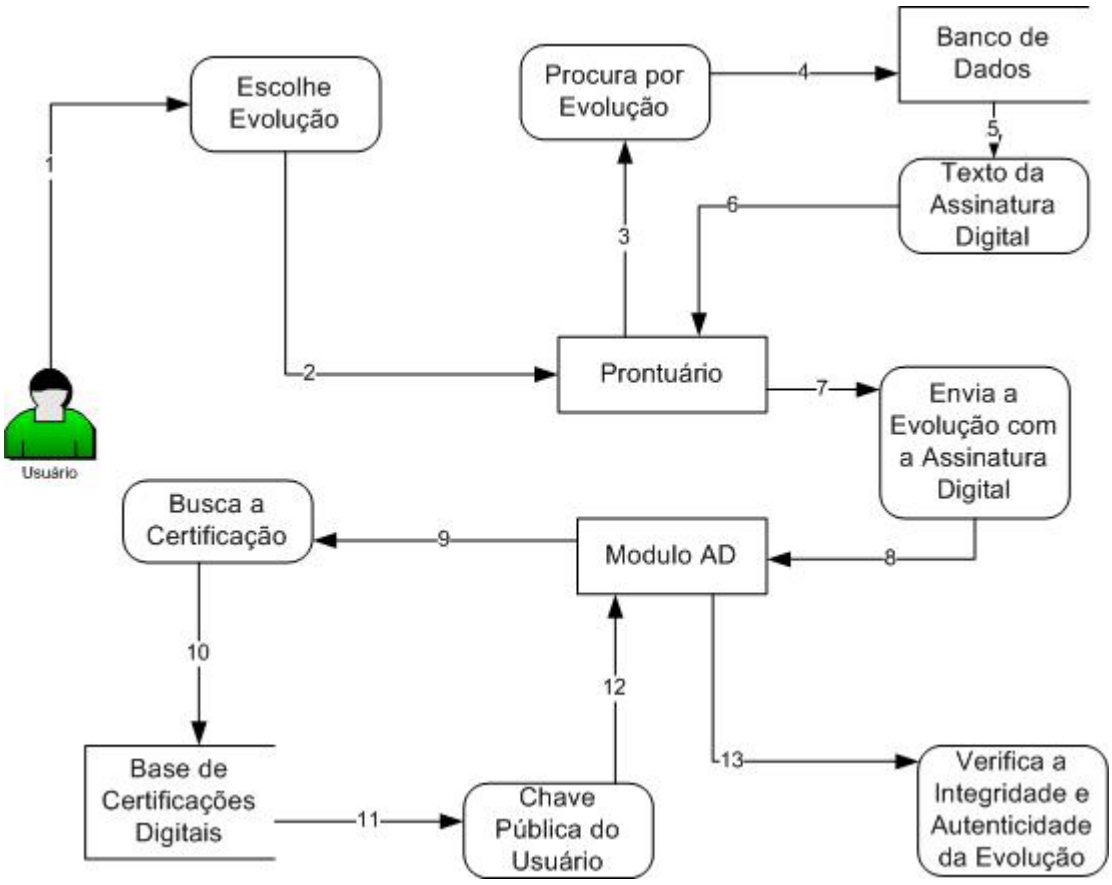

Figura 14. Diagrama da verificação de uma evolução

Um usuário escolhe a evolução através dos *Combo Boxes* de data e hora (Figura 9). Com o botão "Verificar" o sistema começará os procedimentos para verificação da evolução escolhida.

O primeiro procedimento feito pelo sistema é a busca da evolução escolhida e da assinatura digital no banco de dados. O sistema acusará um erro caso não encontre ambos. Para a verificação de uma mensagem também é usada a API Java Security, onde é verificada pela classe *Signature*. Uma parte do código de verificação está descrito abaixo.

```
//passa a chave pública
signature.initVerify(certificado.getPublicKey());
//carrega  o texto de evolução
signature.update(evolucao);
//verifica com o texto da assinatura digital
signature.verify(assinatura);
```

O sistema mostrará os dados da certificação em uma nova tela caso a evolução esteja com a assinatura correta. Esta tela está ilustrada na figura 15. Caso a assinatura não esteja correta o sistema irá mostrar uma mensagem alertando o usuário conforme figura 16.

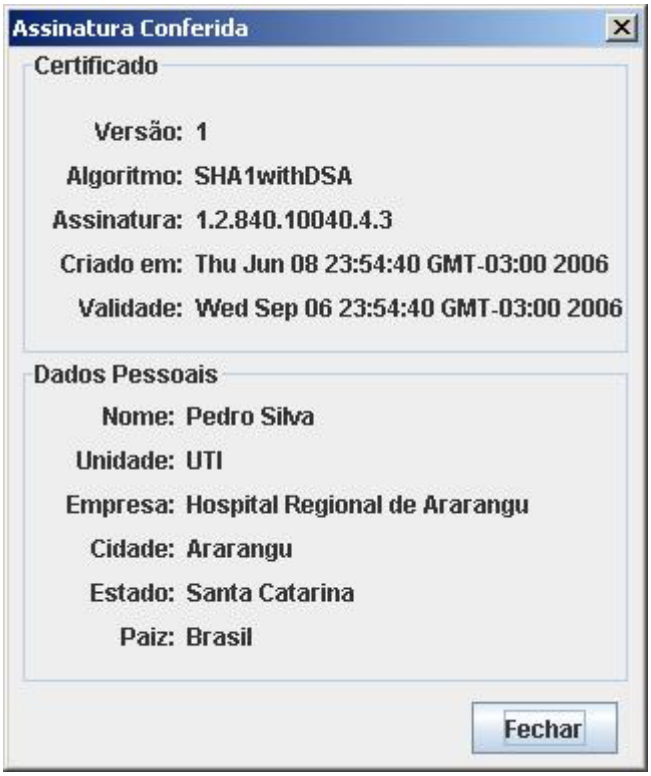

Figura 15. Tela com dados do certificado

Figura 16. Mensagem de assinatura inválida.

5.3 RESULTADOS OBTIDOS

O uso da linguagem Java facilitou a implementação por terem algumas bibliotecas da auxilio a criptografia e a assinatura digital onde principalmente foi usada a API Java Security.

O sistema mostrou uma grande facilidade para um médico assinar uma evolução. Sendo que o sistema tentou manter o máximo possível da interface do antigo prontuário apenas acrescentado uma tela de senha para um médico assinar uma evolução e um botão de verificação, com isso facilitando sua adaptação.

O sistema está em base de testes no Projeto Kiron na Unesc para depois ser instalado no Hospital Regional de Araranguá. Os resultados obtidos pela assinatura digital no Prontuário Eletrônico foram satisfatórios apesar de ainda não usar certificados com validade legal.

CONCLUSÃO

Com o crescente avanço da tecnologia do armazenamento de informações em meios digitais, sentiu-se a necessidade de não-repúdio. Uma forma de responsabilizar uma pessoa do que ela escreveu em um documento é através da assinatura digital. Na área de saúde já existem regulamentações que legalizam o uso de assinatura digital para autenticar um documento digital. Assim, este trabalho apresentou uma forma de um médico escrever uma evolução do paciente assinando digitalmente.

Na implementação desse projeto foram alcançados os objetivos requeridos para uma assinatura digital, apesar do sistema estar ainda em testes e usar somente certificados digitais sem validade no ICP-Brasil.

O uso da assinatura digital se mostrou uma grande vantagem pela praticidade e facilidade para um médico assine uma evolução, mas ainda à uma desvantagem por usar somente uma senha para assinar um documento, necessitando formas mais seguras.

Sugestões de trabalhos futuros: abranger um maior número dados a serem assinados digitalmente no PEP; implementar o uso de cartões magnéticos e *tokens* para assinar um documento; permitir que os enfermeiros também possam assinar documentos; armazenar os Certificados Digitais em um banco de dados.

REFERÊNCIAS

BORGES, Regiane Pizzeti. **Segurança de informações médicas em prontuário eletrônico utilizando assinatura digital.** 2004. 101 f. Trabalho (Trabalho de conclusão de curso) – Ciência da Computação, Universidade do Extremo Sul Catarinense, 2004.

BUCHMANN, Johannes. **Introdução à criptografia**. 1ª ed. São Paulo: Ed Berkeley, 2002.

BURNETT, Steve, STEPHEN Paine. **Criptografia e segurança:** O guia oficial RSA. 3ª ed. Rio de Janeiro: Ed. Campus, 2002.

CARUSO, Carlos, STEFFEN; Flávio Deny. **Segurança em informática e de informações**. 2ª ed. São Paulo: Ed SENAC, 1999.

CARVALHO, Daniel Balparda de. **Criptografia:** Métodos e Algoritmos. 2ª ed. Rio de Janeiro: Ed. Book Express, 2001.

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação.** 1ª ed. Rio de Janeiro: Ed. Axcel Books, 2000.

Conselho Federal de Medicina. Resolução CFM nº 1.639/2002. Disponível em http://www.portalmedico.org.br/resolucoes/cfm/2002/1639_2002.htm. Acesso em: 01 de dezembro 2005.

COSTA, Claudio Giulliano Alves da. **Desenvolvimento e Avaliação Tecnológica de um Sistema de Prontuário Eletrônico do Paciente, Baseado nos Paradigmas da World Wide Web e da Engenharia de Software**. Dissertação (Mestrado em Computação) – UNICAMP, Campinas.

Cryptography. Disponível em <http://en.wikipedia.org/wiki/Cryptography>. Acesso em: 28 novembro 2005.

GIL, Antonio de Lourenço. **Segurança em informática.** 2. ed. São Paulo: Atlas, 1998.

HORSTMANN, Cay, CORNELL, Gary. **Core Java:** Recursos Avançados. 1ª ed. São Paulo: Ed. Pearson Education do Brasil, 2003.

MAIA, Luiz Paulo, PAGLIUSI, Paulo Sergio. **Criptografia e Certificação Digital**. Disponível em http://www.training.com.br/lpmaia/pub_seg_cripto.htm. Acesso em 06/07/2006.

PROSISE, Jeff. Digital signatures: how they work. Disponível em http://www.zdnet.com/pcmag/issues/1507pcmg.htm. Acesso em: 25 novembro 2005;

STALLINGS, William. **Cryptography and Networks Security:** Principles and Pratice. 2ª ed. New Jersey: Ed Pratice Hall, 1999.

TRINTA, Fernando Antonio Mota, MACEDO, Rodrigo Cavalcanti. **Um Estudo Sobre Criptografia e Assinatura Digital**. Setembro de 1998.Disponível em http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm. Acesso em 15/10/2005.

VOLPI, Marlon Marcelo. **Assinatura Digital:** Aspectos Técnicos, Práticos e Legais . 1ª ed. Rio de Janeiro: Ed Excel, 2001.