CENTRO EDUCACIONAL DA FUNDAÇÃO SALVADOR ARENA

FACULDADE DE TECNOLOGIA TERMOMECANICA

PROTOCOLOS CRIPTOGRÁFICOS

SÃO BERNARDO DO CAMPO, 2008

CENTRO EDUCACIONAL DA FUNDAÇÃO SALVADOR ARENA
FACULDADE DE TECNOLOGIA TERMOMECANICA

PROTOCOLOS CRIPTOGRÁFICOS

Trabalho de Conclusão de Curso apresentado pelos alunos Dinarde Almeida Bezerra e Gustavo Magno de Sousa, sob orientação da Profª Ms. Samáris Ramiro Pereira, como parte das exigências para obtenção do grau de Tecnólogo em Análise e Desenvolvimento de Sistemas.

SÃO BERNARDO DO CAMPO, 2008

Catalogação elaborada na fonte pela Biblioteca da Faculdade de Tecnologia Termomecanica

Bibliotecária: Miriam da Silva Nascimento CRB 8/5347

Bezerra, Dinarde Almeida
Protocolos criptográficos. Dinarde Almeida Bezerra; Gustavo Magno de Sousa. São Paulo: FTT, 2008.
74 p. : il. ; 30 cm.

Orientador: Samáris Ramiro Pereira
Trabalho de Conclusão de Curso – Faculdade de Tecnologia Termomecanica, FTT, Tecnologia em Análise e Desenvolvimento de Sistemas, 2008

1. Protocolo criptográfico. 2. Criptografia. 3. Certificação digital. I. Pereira, Samáris Ramiro. II. Faculdade de Tecnologia Termomecanica, FTT, Curso de Tecnologia em Análise e Desenvolvimento de Sistemas. III. Título

Tecnólogo em Análise e Desenvolvimento de Sistemas

Banca Examinadora:

Prof. Francisco José Martins (presidente, FTT)

Prof. Ms. Fábio Henrique Cabrini (mestre, FTT)

Aprovado em 21/06/2008

Dinarde Almeida Bezerra

e-mail: dinarde@gmail.com

Gustavo Magno de Sousa

e-mail: gusmags@hotmail.com

DEDICATÓRIA

Dedicamos esse trabalho à nossa orientadora Samáris Ramiro Pereira que contribuiu intelectualmente e emocionalmente para que concretizássemos esse TCC.

AGRADECIMENTOS

Agradecemos primeiramente a Deus que nos permitiu chegar até aqui.

Também aos nossos pais, familiares, amigos, educadores, colegas de sala, a nossa orientadora e a todos que contribuíram diretamente ou indiretamente.

Agradecemos a toda a estrutura da Fundação Salvador Arena que colaborou para que alcançássemos o diploma de nível superior.

Agradecemos, sinceramente, a todos.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE SIGLAS

AC - Autoridade Certificadora

AC-JUS - Autoridade Certificadora do Judiciário

AES - *Advanced Encryption Algorithm*

AR - Autoridade Registradora

CN - *Common Name*

DES - *Data Encryption Standard*

DLP - *Discrete Logarithm Problem*

DoS - *Denial of Service*

ECDLP - *Elliptic Curve Discrete Logarithm Problem*

e-NF - Nota Fiscal Eletrônica

HMAC - *Keyed-Hashing for Message Authentication Code*

HTTP - *Hypertext Transfer Protocol*

HTTPS- *Hypertext Transfer Protocol Secure*

ICP - Infra-estrutura de chaves públicas

IDEA - *International Data Encryption Algorithm*

IETF - *Internet Engineering Task Force*

IFP - *Integer Factorization Problem*

IKE - *Internet Key Exchange*

INSS - Instituto Nacional de Seguridade Social

IP - *Internet Protocol*

IPSec - *Internet Protocol Security*

ITI - Instituto Nacional de Tecnologia da Informação

MAC - *Message Authentication Code*

MD5 - *Message-Digest algorithm 5*

MIT - *Massachusetts Institute of Technology*

MP - Medida Provisória

NIST - *National Institute of Standards and Technology*

PGP - *Pretty Good Privacy*

PKI - *Public key infrastructure*

PKP - *Public Key Partners*

PRNG - *Pseudo-Random Number Generator*

ProUni - Programa Universidade para Todos

RC4 - *Rivest Chipher* 4

RC6 - *Rivest Chipher* 6

RFC - *Request For Comments*

RNG - *Random Number Generator*

RSA - Rivest, Shamir e Adleman

SA - *Security Association*

SET - *Secure Electronic Transaction*

SHA - *Secure Hash Algorithm*

SPB - Sistema de Pagamentos Brasileiros

SSL - *Secure Sockets Layer*

TCP - *Transmission Control Protocol*

TLS - *Transport Layer Security*

USC - *University of Southern California*

XOR - *EXclusive OR*

RESUMO

A *internet* revolucionou o mundo das comunicações. Hoje, virtualmente, de forma segura, podem-se compartilhar documentos, realizar compras, transações bancárias, entre uma infinidade de serviços. Mas para possibilitar a utilização correta destes serviços, o homem precisa manter informações em sigilo, e desta forma a criptografia ganhou e está continuamente ampliando seu espaço. Mas a criptografia isolada não proporciona um ambiente seguro em um meio inseguro como a *internet*, o que fez com que surgissem e se aprimorassem rapidamente os protocolos criptográficos. Essa produção acadêmica, após apresentar um breve panorama da segurança da informação, apresenta os protocolos criptográficos SSL, IPSec e SET, visto que estes são uma ferramenta fundamental de segurança, possibilitando a implementação de tecnologias como assinatura e certificação digital. Para possibilitar uma visão completa, são apresentados desde conceitos como o de criptografia, tipos de chave criptográfica, a infra-estrutura de chaves públicas e sua validade jurídica, até um tutorial de instalação e configuração de um servidor seguro em ambiente Windows através das ferramentas Apache e SSL.

Palavras-chave: Protocolo Criptográfico. Criptografia. Assinatura Digital. Certificação Digital. SSL. IPSec. SET. Apache.

ABSTRACT

The internet has revolutionized the world communications. Today, virtually, in a safe way, they can be shared documents, to accomplish purchases, bank transactions, among an infinity of services. But to make possible the correct use of these services, men need to maintain information in secrecy, and this way the cryptography won and it is continually enlarging his space. But the isolated cryptography doesn't provide a safe environment in an insecure way as the internet, what did with that they appeared and if they perfected the cryptographic protocols quickly. That academic production, after presenting an abbreviation panorama of the safety of the information, presents the cryptographic protocols SSL, IPSec and SET, because these are a fundamental tool of safety, making possible the implementation of technologies as signature and digital certification. To make possible a complete vision, they are presented from concepts as the one of cryptography, cryptographic key types, the infrastructure of public keys and her juridical validity, until an installation tutorial and configuration of a safe servant in environment windows through the APACHE tools and SSL.

Keywords: Cryptographic Protocol. Cryptography. Digital Signatures. Digital Certification. SSL. IPSec. SET. Apache.

CAPÍTULO 1

1 INTRODUÇÃO

Com a popularização dos serviços oferecidos na *internet*, cresceu também número de crimes digitais. A necessidade de aumentar a segurança dos serviços e documentos que estão na rede mundial de computadores, fez da infra-estrutura de segurança da informação e em particular da criptografia, uma obrigação nas transações realizadas virtualmente.

1.1 Objetivos

Prover material que possibilite o entendimento de protocolos criptográficos, partindo da estrutura de chave simétrica e assimétrica, algoritmo criptográfico, assinatura e certificado digital, autoridade certificadora e concluindo com funcionamento, características, vantagens, desvantagens e evoluções de alguns protocolos criptográficos que utilizam técnicas de segurança e garante integridade na comunicação *on-line*.

1.2 Motivação

O número de usuários da *internet* cresce a cada dia. No mesmo ritmo, cresce o número de serviços oferecido pela rede mundial de computadores, como transações bancárias e serviços de compra e venda. Mas como garantir a segurança nessas ações? Não existe uma forma precisa e única para se garantir a segurança na *internet*. Essa é assegurada por um conjunto de procedimentos e tecnologias adequadas a determinada situação. Desta forma, este trabalho foi desenvolvido visando apresentar meios para tornar o tráfego de dados na rede mundial de computadores mais seguros.

1.3 Plano de trabalho

O método utilizado para o desenvolvimento desta pesquisa foi o monográfico, tendo como objetivo descrever de forma detalhada o tema, partindo dos conceitos da criptografia, passando por outros conceitos envolvidos e chegando aos protocolos criptográficos atualmente em uso para prover uma conexão segura na *internet* e apresentando exemplos práticos.

Para tal, foram realizadas pesquisas em materiais teóricos relacionados ao tema assim como a participação em alguns cursos *on-line* oferecidos pela Next Generation Center com o apoio da Intel [15].

O plano de trabalho seguiu os tópicos abaixo:

- Levantamento e seleção bibliográfica, buscando livros, revistas técnicas, artigos e trabalhos acadêmicos sobre o tema.
- Desenvolvimento, com base nas pesquisas realizadas, partindo dos conceitos iniciais até os mais específicos.
- Apresentação de aplicações.
- Conclusões do tema, sintetizando a proposta conforme o objetivo.

1.4 Referencial teórico

As referências do trabalho ficaram baseadas em:

- Livros técnicos: Livros renomados da área como do Burnett e Painel “Criptografia e segurança - O guia oficial RSA”, Stephen Thomas “SSL and TLS essencials” entre outros;
- Produções acadêmicas: Diversos trabalhos acadêmicos de faculdades conceituadas como: UNB, UFSC, UFRJ, USP, etc., agregando valor ao trabalho;
- Material corporativo: Materiais de empresas do ramo de segurança da informação, unindo prática e teoria, voltada ao meio comercial;
- Órgãos governamentais: Material de sítios governamentais na *internet*, de órgãos que gerenciam a tecnologia da informação brasileira;

- Curso *on-line*: Foram realizados dois cursos de “Certificação digital” e “Segurança da Informação”, promovidos pela Intel, no seu programa de treinamentos “Next Generation”;
- Outros artigos publicados em sítios da *internet*.

CAPÍTULO 2

2 SEGURANÇA DA INFORMAÇÃO

2.1 Importância

Segurança da Informação é um assunto de interesse geral. Burnett e Paine [5] citam no livro “Criptografia e segurança – o guia oficial RSA” que se alguém diz: “Não preciso de segurança. Não tenho nenhum segredo, nada a ocultar”, uma boa resposta seria “OK, deixe-me ver seu prontuário médico. Que tal seu contracheque, saldo bancário, planilha de investimento e faturas de cartão de crédito? Deixe-me anotar seu número de CPF, números de cartão de crédito e números da conta bancária? Qual a senha do seu cartão bancário e do seu cartão de crédito? Qual é sua senha para conectar-se à rede no trabalho? Onde você mantém a chave sobressalente da sua casa?”.

O fato é que toda pessoa tem informações que quer manter em segredo. Às vezes, a razão é simplesmente o desejo de privacidade. Ninguém se sente confortável tornando público detalhes sobre o seu perfil médico ou financeiro. Outra boa razão é autoproteção - ladrões poderiam utilizar informações confidenciais de determinada vítima para assaltá-la. Em outras palavras, os motivos para uma pessoa manter um segredo não são necessariamente de má fé.

Empresas também têm segredos – informações estratégicas, previsões de vendas, detalhes técnicos sobre produtos, resultados de pesquisas, arquivos pessoais e assim por diante. Embora empresas desonestas talvez tentem ocultar do público as suas atividades ilícitas, a maioria das organizações quer proteger suas informações valiosas de pessoas que podem estar trabalhando para concorrentes, *hackers e crackers*[1] ou mesmo funcionários.

Os motivos para invasão de um computador doméstico são inúmeros [7]:

---

[1] Hackers: Pessoas que violam sistemas de forma ética. Visam à melhoria e a resolução de problemas dos mesmos.
Crackers: Pessoas que violam sistemas a fim de prejudicá-los e obter benefícios próprios. Roubam informações, como senha bancária.

- Utilizar o computador em alguma atividade ilícita, para esconder a real identidade e localização do invasor;
- Utilizar o computador para lançar ataques contra outros computadores;
- Utilizar o disco rígido como repositório de dados;
- Destruir informações (vandalismo);
- Disseminar mensagens alarmantes e falsas;
- Ler e enviar e-mails em nome de seu real proprietário;
- Propagar vírus de computador;
- Furtar números de cartões de crédito e senhas bancárias;
- Furtar a senha da conta de provedor do equipamento invadido, para acessar a *Internet* se fazendo passar pelo seu usuário;
- Furtar dados do computador, como por exemplo, informações de imposto de renda.

Os motivos para invasão em uma rede corporativa são inúmeros:

- Obter informações sigilosas da empresa;
- Acessar e-mails internos da empresa;
- Sobrecarregar a rede;
- Propagar vírus de computador;
- Deixar fora do ar serviços providos pela empresa;
- Modificar dados empresariais;
- Utilizar recursos da empresa para benefício de terceiros;
- Obter dados de funcionários.

2.2 Conceitos

Segundo FILHO, A. M. S., informação compreende qualquer conteúdo que possa ser armazenado ou transferido de algum modo, servindo a determinado propósito e sendo de utilidade ao ser humano. Trata-se de tudo aquilo que permite a aquisição de conhecimento. Nesse sentido, a informação digital é um dos principais, senão o mais importante, produto da era atual. Ela pode ser manipulada e visualizada de diversas maneiras. Assim, à medida que a informação digital circula pelos mais variados ambientes, percorrendo diversos fluxos de trabalho, ela pode

ser armazenada para os mais variados fins, possibilitando ela ser lida, modificada ou até mesmo apagada [10].

A segurança da informação é a proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão[2], e a modificação não-autorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento [19].

Considera-se ameaça, toda possibilidade de exploração de fragilidades de sistemas, de forma intencional ou não, podendo ser uma ameaça interna (um funcionário que pode explorar os sistemas internos da corporação) ou uma ameaça externa (alguém de fora tentando comprometer os dados da corporação).

Já um ataque, é a tentativa, bem ou mal sucedida, de acesso ou uso não autorizado a um programa ou computador. Também são considerados ataques as tentativas de negação de serviço [7].

Classificam-se em:

1. Ataque ativo: informações são modificadas. Podem ser de vários tipos, tais como:

   1.1 Interrupção: O atacante sobrecarrega o sistema, causando lentidão e indisponibilidade dele;

   1.2 Modificação: O atacante obtém dados e os modifica;

   1.3 Falsidade: O atacante faz se passar por outra pessoa.

2. Ataque passivo: informações não sofrem modificação, sendo somente copiadas. Caracteriza-se pela interceptação.

A figura 1 representa a classificação acima:

[2] Intrusão: Acesso não autorizado ao sistema, a fim de comprometê-lo ou simplesmente obter informações.

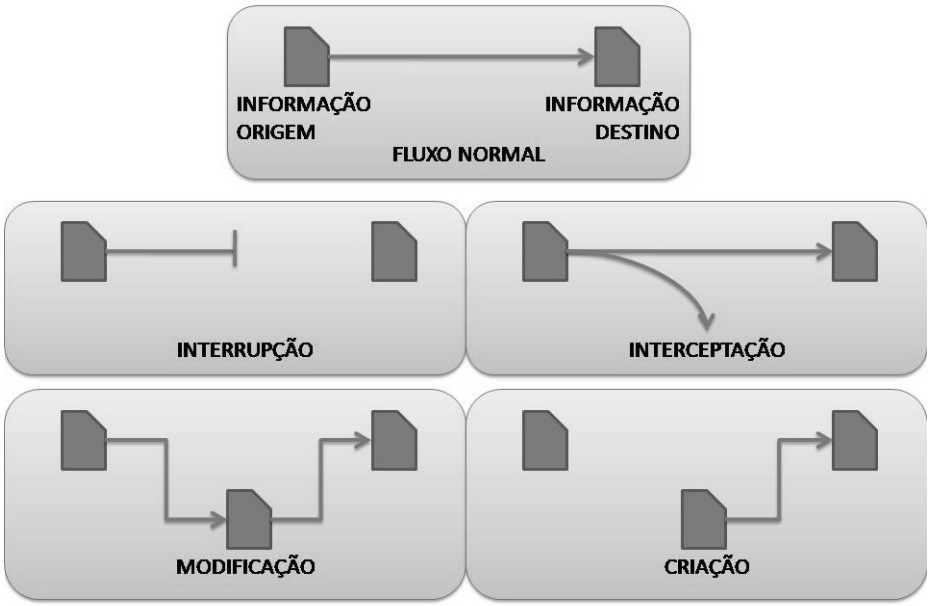

Figura 1 – Esquema de tipos de ataques. Fonte: O autor.

2.3 Objetivos

A segurança da informação tem por objetivo, assegurar uma ou mais, das seguintes propriedades [23]:

1. Confidencialidade: assegura o sigilo de determinada informação;

2. Integridade: garante que a informação não seja manipulada sem autorização. Por manipulação entendem-se inclusões, exclusões ou modificações de dados;

3. Disponibilidade: garante o acesso à informação quando esta for requerida por um usuário legítimo;

4. Autenticação: a idéia de autenticação está associada à identificação e inclui autenticação de entidade e de dados. A autenticação de entidade é o processo que associa o indivíduo a uma identificação única, ou seja, é a forma pela qual o usuário prova que é quem alega ser, estabelecendo a validação de sua identidade. A autenticação de dados é o processo que identifica como legítimas as informações sobre os dados tais como: origem, data de origem, hora de envio, conteúdo;

5. Não repúdio: garante que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica, não poderá posteriormente

negar sua autoria, visto que somente sua chave privada poderia ter gerado aquela assinatura digital. Deste modo, a menos que haja um uso indevido do certificado digital, fato que não exime de responsabilidade, o autor não pode negar a autoria da transação.

6. Legalidade: Outra propriedade que tem sido objetivo da segurança da informação é a legalidade envolvida na situação em questão. Têm-se como exemplos, que a criptografia é proibida em alguns países, a certificação digital não é reconhecida mundialmente, apresentando regras especificas conforme a localização, assim como determinada invasão pode ser crime em um país e em outro não.

CAPÍTULO 3

3 CRIPTOLOGIA

3.1 Conceitos

A palavra criptologia deriva da palavra grega *kryptos* (oculto) e *logos* (estudo). Este campo de estudo engloba criptografia e a criptoanálise.

Criptologia**:** É a ciência de estuda as cifras.

Uma cifra não é um código. Um código é um sistema pré-estabelecido de substituição de palavras ou de parágrafos. Um idioma estrangeiro, por exemplo, é como um código secreto onde cada palavra em português possui uma equivalente nele. Assim, "oi" em português equivale a "*hola*" em espanhol ou "*hi*" em inglês. A maioria dos códigos funciona com um "livro de códigos" onde as palavras estão relacionadas a equivalências, como se fosse um dicionário [36].

A palavra cifra vem do hebraico *saphar*, que significa "dar número". As maiorias dos ciframentos são intrinsecamente sistemáticos, freqüentemente baseados em técnicas de sistemas numéricos.

A cifra pode ser visualizada por qualquer pessoa. Porém, a mensagem a ser transmitida só poderá ser decifrada pela pessoa autorizada. Caso a mensagem ou cifra estivesse oculta, estaria sendo utilizada a técnica de esteganografia.

Esteganografia: É o estudo das técnicas de ocultação de mensagens dentro de outras, diferentemente da criptografia, que altera a mensagem de forma a tornar seu significado original ininteligível [18].

A esteganografia não é considerada parte da criptologia, é uma tecnologia de segurança de informação paralela, sendo usualmente estudada em contextos semelhantes aos da criptografia e pelos mesmos pesquisadores.

Criptografia: Formada a partir da concatenação do termo grego *kryptos* (escondido, oculto) e *grapho* (grafia, escrita), a criptografia apresenta-se como a ciência de escrever em cifras, ou seja, a ciência que provê meios através de técnicas matemáticas, para se transformar um texto em claro (inteligível) em um texto cifrado (ininteligível).

Criptoanálise: É o processo de examinar informações criptografadas para tentar determinar qual a mensagem cifrada ou qual a chave que criptografou a mensagem (que, evidentemente, leva à própria mensagem) [33].

Para muitos autores o grande compromisso da criptografia seria o provimento da privacidade das comunicações. De fato, a proteção de comunicações sensíveis tem sido a ênfase da criptografia ao longo de toda história.

Dentro da criptologia, a ciência da criptografia tem como seu objeto de estudos os processos de ciframento.

Ciframento: É a transformação dos dados em uma forma que torna impossível a sua leitura sem o apropriado conhecimento da chave. O seu principal propósito é assegurar privacidade da informação protegendo o entendimento da mensagem oculta de qualquer um a qual ela não seja destinada [36].

Deciframento: O deciframento é o processo inverso do ciframento; é a transformação de dados cifrados novamente em uma forma legível.

Texto simples: É qualquer informação que está escrita de maneira legível.

Texto cifrado: É resultado de um texto simples que passou pelo processo de ciframento.

Chave: A chave é um código secreto utilizado por algoritmos de ciframento para criar versões únicas do texto codificado; isto faz com que uma mensagem, ao ser cifrado com chaves diferentes, apresente textos codificados diferentes [27].

3.2 Ciframento e deciframento

O ciframento e o deciframento são realizados por programas de computador chamados de cifradores e decifradores. Um programa cifrador ou decifrador, além de receber a informação a ser cifrada ou decifrada, recebe um número chave que é utilizado para definir como o programa irá se comportar (figura 2). Os cifradores e decifradores se comportam de maneira diferente para cada valor da chave. Sem o conhecimento da chave correta não é possível decifrar um texto cifrado. Assim, para manter uma informação secreta, basta cifrar a informação através de um algoritmo criptográfico reconhecido pela comunidade técnica, mantendo todos os cuidados técnicos especificados e manter em sigilo a chave [16].

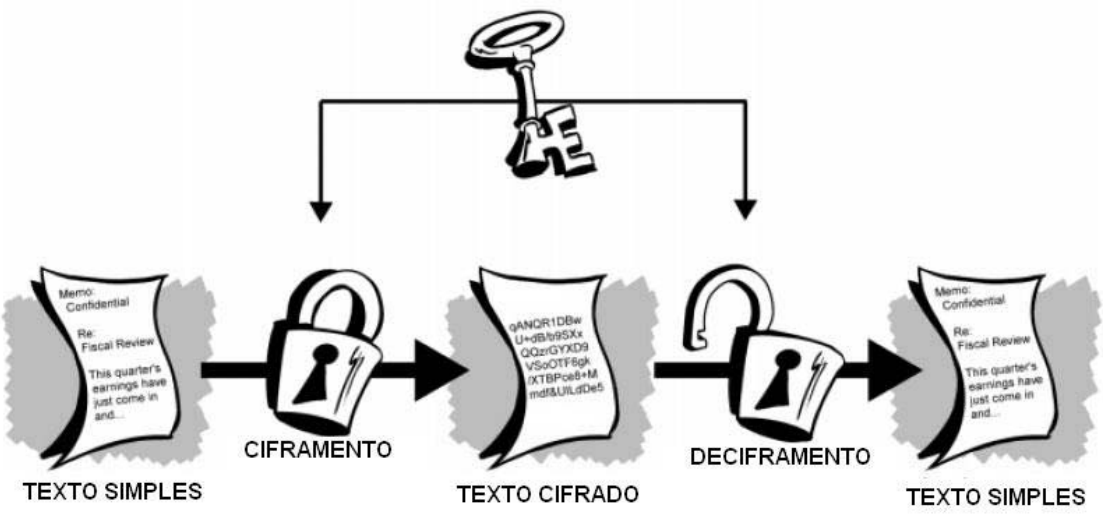

Figura 2 - Esquema de ciframento e deciframento. Fonte: [9].

3.3 Panorama Histórico

A criptografia é tão antiga quanto à própria escrita. Já estava presente no sistema de escrita hieroglífica dos egípcios. Os romanos utilizavam códigos secretos para comunicar planos de batalha. O mais interessante é que a tecnologia de criptografia não mudou muito até meados deste século [11].

A história da criptografia da era moderna foi marcada pelo seu uso militar. Em situações de guerra nenhum comandante deseja que seus inimigos conheçam suas estratégias caso viesse interceptar uma mensagem.

Em 17 de janeiro de 1917, por exemplo, o serviço de Inteligência Naval Britânica interceptou, decodificou e entregou aos Estados Unidos uma mensagem que havia sido enviada ao embaixador alemão na Cidade do México pelo governo germânico. Na mesma se autorizava ao diplomata a negociar um acordo com o México para entrar a favor da Alemanha na Primeira Guerra Mundial, com o propósito de deixar os Estados Unidos neutralizados durante a guerra e também ele propunha ao México convidar o Japão para participar do plano. Em troca, os mexicanos iriam receber um grande valor financeiro e os territórios de Novo México, Arizona e Texas caso resultassem vencedores. O texto conhecido como *Telegrama de Zimmermann* (figura 3), levou os norte-americanos trocarem sua política neutra pela guerra, o que prova o poder da criptoanálise. Se o telegrama não tivesse sido

interceptado e os planos contra os Estados Unidos tivessem dado certo a história atual poderia ter sido bem diferente [32] [36].

Na Segunda Guerra Mundial os códigos da máquina Enigma (máquina eletromecânica de criptografia com rotores), utilizada pelos alemães, foram quebrados pelos analistas norte-americanos, o mesmo se dando com os códigos utilizados pelos japoneses. Os alemães, na Primeira Guerra venceram os russos facilmente, por conta disso. Os Estados Unidos conseguiram não perder do Japão na Segunda Guerra por possuírem os códigos de transmissão deste. Os alemães, por sua vez, não conseguiram invadir a Inglaterra pelo mesmo motivo. Rommel deve sua fama de “raposa do deserto” em parte ao fato de que conseguiu capturar uma transmissão americana detalhando como era o modo de operação dos britânicos no deserto [36].

O advento dos computadores, e a capacidade de processamento de dados sempre crescente, fizeram com que a criptografia se fizesse agora de forma digital.

Em 1976, a IBM desenvolveu um sistema criptográfico denominado *Data Encryption Standard* (DES), que logo foi aprovado pelos órgãos de normatização do governo americano. O DES baseia-se em elaborados sistemas matemáticos de substituição e transposição os quais fazem com que seja particularmente difícil de ser rompido um ciframento [36].

O DES é um exemplo clássico de criptografia simétrica e o RSA é um padrão mundial de criptografia assimétrica ou pública.

O RSA é um sistema criptográfico de chave pública amplamente aceito e divulgado, desenvolvido em abril de 1977, pelos professores do *Massachusetts Institute of Technology* (MIT) Ronald Rivest e Adi Shamir e pelo professor da *University of Southern California* (USC) Leonard Adleman, batizado com as iniciais de seus nomes. Mais tarde a patente do RSA foi registrada pelo MIT que a cedem a um grupo denominado *Public Key Partners* (PKP) para uso doméstico. Esta patente foi expirada por completo em setembro de 2000 [23].

Em 1991, o programador Phil Zimmermann autorizou a publicação em boletins eletrônicos e grupos de notícias de um programa por ele desenvolvido e batizado como *Pretty Good Privacy* (PGP). O PGP tem como base entre outros o algoritmo do RSA. Quando Zimmermann publicou o PGP se viu em problemas com o departamento de estado norte-americano que abriu uma investigação para determinar se ele havia violado as restrições de exportação de criptografia ao

autorizar a divulgação do código fonte do PGP na *internet*. Apesar do mesmo ter se comprometido a deter seu desenvolvimento, diversos programadores em várias partes do mundo continuaram adiante, portando-o para distintas plataformas e assegurando sua expansão. Stale Schumacher, um programador norueguês, tem se encarregado das versões internacionais do PGP, que são totalmente compatíveis com sua contraparte norte americana apenas observando o objetivo da legalidade [36].

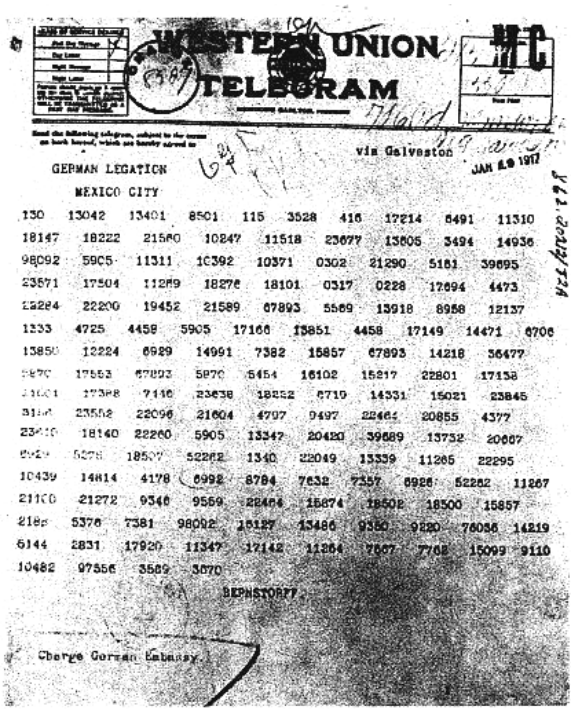
WESTERN UNION
TELEGRAM
via Galveston
JAN 19 1917
GERMAN LEGATION
MEXICO CITY
130 13042 13401 8501 115 3528 416 17214 8491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22224 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
17388 7110 23638 18252 6719 14331 15021 23845
23552 22096 21604 4797 9497 22464 20855 4377
18140 22260 5905 13347 20420 39689 13732 20667
5278 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 9926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
5376 7381 98092 16127 13486 9350 9220 76036 14219
6144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3070
BERNSTORFF
Charge German Embassy.

Figura 3 - Telegrama criptografado de Zimmermann. Fonte: [32].

Nos dias atuais, com o aumento do comércio e de transações eletrônicas que requerem algum tipo de segurança, a criptografia tornou-se uma ferramenta fundamental para a utilização da *internet*.

3.4 Criptografia Simétrica e Pública

Existem dois tipos de criptografia conforme a sua chave: Criptografia simétrica e a criptografia assimétrica ou de chave pública.

3.4.1 Criptografia simétrica

A criptografia de chave simétrica, representada na figura 4, utiliza a mesma chave para ciframento e deciframento. Dessa forma, a chave deve ser conhecida tanto pelo remetente quanto pelo destinatário da mensagem. Nesse fato, reside a maior dificuldade do método: a distribuição segura das chaves.

Segundo Burnett e Painel em um sistema criptográfico de chave simétrica, a chave é apenas um número qualquer que tenha um tamanho correto e que o selecione aleatoriamente. Serão detalhadas ainda neste capítulo as técnicas utilizadas para a geração de números aleatórios [5].

Se uma pessoa quer se comunicar com outra com segurança, ela deve passar primeiramente a chave utilizada para cifrar a mensagem. Este processo é chamado de “distribuição de chaves”, e como a chave é o principal elemento de segurança para o algoritmo, ela deve ser transmitida por um meio seguro.

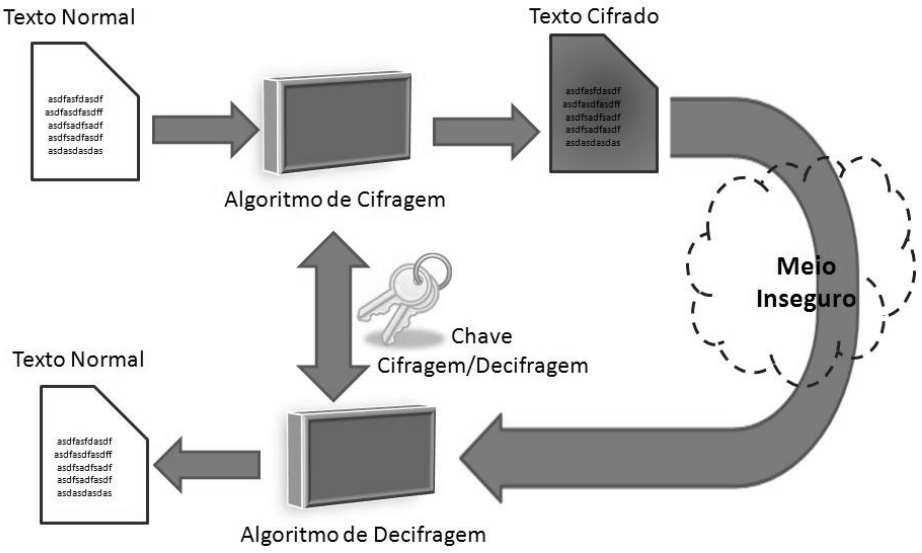

Figura 4 - E*squema de criptografia simétrica.* Fonte: O autor.

3.4.2 Tipos de algoritmos de chave simétrica

Há duas formas de se cifrar dados. Através de ciframento de bloco ou de fluxo.

Ciframento de bloco

Quando é definido para o algoritmo um tamanho de fragmento de dado para cifrar ou decifrar, ele divide o texto simples em blocos e opera de maneira independente [5].

Suponha que um texto tenha 227 bytes e é utilizado uma ciframento que opera com blocos de 16 bytes. O algoritmo irá utilizar os 16 primeiros bytes, cifrar, depois os próximos 16 bytes e assim por diante. Ele realizará esse procedimento 14 vezes sobrando apenas 3 bytes. Contudo, ele só opera com 16 bytes. Então para cifrar os últimos 3 bytes, será adicionado bytes extras no último bloco para torná-lo completo. O algoritmo de deciframento dos dados deve ser capaz de reconhecer e ignorar esse preenchimento.

O esquema mais popular de efetuar esse preenchimento é identificar o número de bytes que deve ser preenchido e repetir esse valor até o final dos dados. No caso acima, ele repetirá o byte “13” em cada um dos 13 bytes de preenchimento. A figura 5 apresenta o esquema de ciframento do exemplo.

Ciframento de fluxo

Na ciframento de fluxo, os dados vão sendo criptografados bit a bit, conforme as informações vão chegando. Estes algoritmos são úteis quando o transmissor precisa enviar para o receptor um fluxo contínuo de dados criptografados [38].

Uma operação matemática *L* é realizada com cada bit da mensagem separadamente de forma a alterar-lhe o valor, cifrando-a. Essa operação pode ser a função XOR ou OU Exclusivo [3].

A chave de ciframento deve ser constituída de bits que variam no tempo. Ela deve ser do mesmo tamanho da mensagem. Na deciframento o processo é semelhante ao de ciframento, bastando apenas aplicar a operação inversa $L_{inv.}$ Na figura 6 pode ser visualisado o esquema de ciframento e deciframento de fluxo.

[3] XOR ou OU Exclusivo: Operador lógico muito útil na criptografia, visto que em 50% dos casos o resultado é 1 e os outros 50% é igual a 0. A operação com bits iguais é igual a 0 e com bits diferentes é igual a 1: 0 XOR 0 = 0 e 0 XOR 1 = 1 e 1 XOR 0 = 1 e 1 XOR 1 = 0 [5].

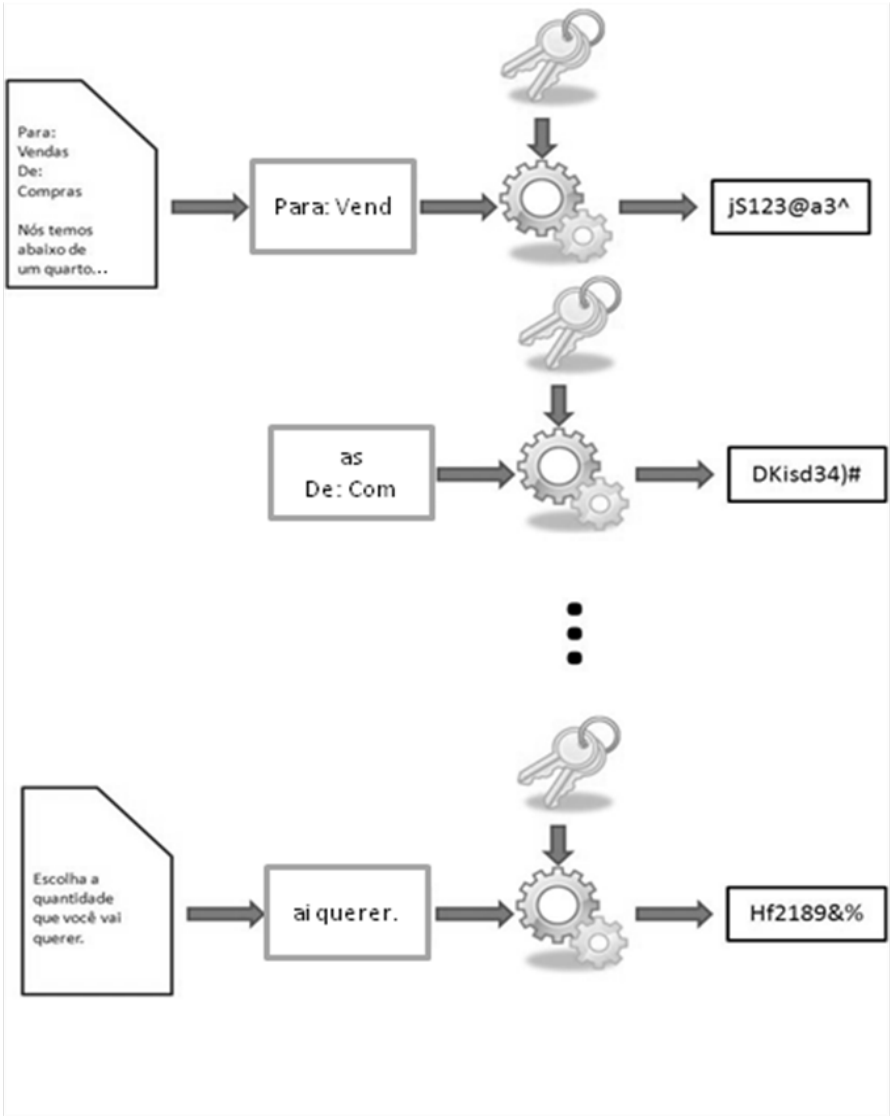

Figura 5 – Esquema de cifragem em bloco. Fonte: O autor.

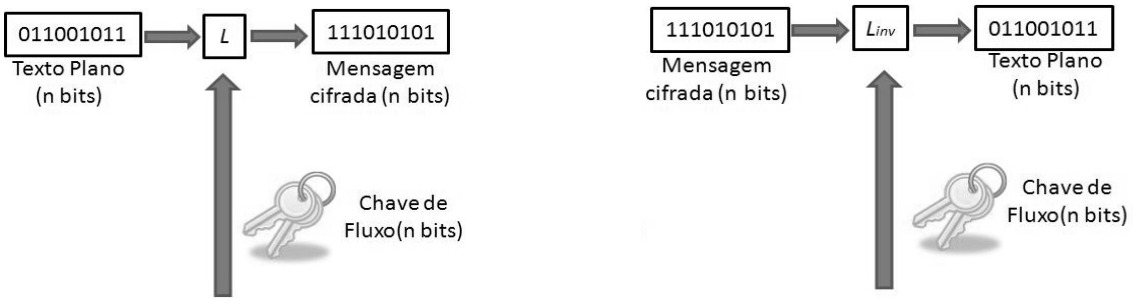

Figura 6 – Esquema de cifragem de fluxo. Fonte: O autor.

Ciframento de bloco X ciframento de fluxo

A ciframento de fluxo é quase sempre mais rápida e geralmente utiliza bem menos código do que as de bloco [5].

Por outro lado, com a ciframento de blocos, você pode reutilizar as chaves. No ciframento de fluxo utilizar-se a chave apenas uma vez, o que torna o gerenciamento dessas chaves difícil.

Nenhum tipo é melhor que o outro. Se for preciso reutilizar as chaves, o ciframento de blocos é mais adequado. Se for preciso velocidade não precisando reutilizar a chave, o ciframento de fluxo provavelmente é mais indicado.

Na tabela 1, podem-se verificar exemplos dos tipos de ciframento de bloco ou fluxo, conforme a aplicação.

A criptografia simétrica atinge ao objetivo de confidencialidade, mantendo os dados seguros, e suas principais vantagens sobre a criptografia de chave pública [3]:

a) velocidade, pois os algoritmos são muito rápidos, permitindo cifrar uma grande quantidade de dados em pouco tempo;

b) as chaves são relativamente pequenas e relativamente simples, permitindo gerar cifradores extremamente robustos;

Enquanto desvantagens podem-se citar [3]:

a) a chave secreta deve ser compartilhada entre emissor e receptor, o que dificulta o gerenciamento de chaves;

b) não permite autenticação do remetente, uma vez que qualquer pessoa poderá enviar uma mensagem criptografada com qualquer chave que esteja em seu domínio;

c) não permite o não-repúdio do remetente, o que é decorrência direta do item anterior.

Os principais algoritmos desta classe são [3]:

a) *Data Encryption Standard* (DES): É o algoritmo simétrico mais difundido no mundo. Criado pela IBM em 1977, com um tamanho de chave de 56 bits, relativamente pequeno para os padrões atuais, por “força bruta” em 1997;

Aplicação/Tipo de ciframento	Exemplo
Banco de dados/Bloco	A interoperabilidade com outro software não é uma questão, mas será preciso reutilizar as chaves.
E-mail/Bloco (AES)	Embora cada mensagem de e-mail tenha sua própria chave e possa ser utilizado um ciframento de fluxo, há um ganho de interoperabilidade em todos os pacotes de e-mail utilizando o AES padrão.
SSL em conexões *Web*[4]/Fluxo (RC4[5])	A velocidade é extremamente importante, cada conexão pode ter uma nova chave e praticamente todos os navegadores e servidores *Web* utilizam o algoritmo criptográfico simétrico RC4.
Ciframento de Arquivos/Bloco	A interoperabilidade não é uma questão, porém pode-se cifrar cada arquivo com a mesma chave e então proteger essa chave.

Tabela 1: Utilização do ciframento de bloco ou fluxo em algoritmos de chave simétrica. Fonte: [5].

b) *Triple* DES: Uma variação do DES que utiliza três ciframentos em seqüência, empregando chaves com tamanho de 112 ou 168 bits, sendo recomendado no lugar do DES desde 1993;

c) *International Data Encryption Algorithm* (IDEA): Criado em 1991, segue as mesmas idéias do DES, mas tem execução mais rápida que o mesmo.

d) *Advanced Encryption Standard* (AES): É o padrão atual para ciframento recomendado pelo *National Institute of Standards and Technology* (NIST). Trabalham com chaves de 128, 192 e 256 bits, que adotou o cifrador *Rijndael* após a avaliação de vários outros;

[4] *Web* – Termo usado para referir-se à rede mundial de computadores
[5] RC4 – É um algoritmo de ciframento de fluxo para chave simétrica desenvolvido por Ron Rivest [35].

e) RC6 (*Rivest Chipher 6*): A última versão de uma série de cifradores (RC2, RC3, RC4, RC5) desenvolvidos por Rivest. Concorreu à adoção pelo padrão AES.

3.5 Gerador de números aleatórios

Como pode ser visto anteriormente, a chave é um número gerado aleatoriamente. Mas como são gerados esses números? Existem duas formas de gerá-los:

R*andom Number Generator* (RNG): São dispositivos que agrupam números de diferentes tipos de entradas imprevisíveis como a medição da desintegração espontânea de radioatividade, o exame das condições atmosféricas na vizinhança ou o cálculo de minúsculas variâncias na corrente elétrica. Esses números passam por teste de aleatoriedade [5].

P*seudo-Random Number Generator* (PRNG): São algoritmos que recebem sementes[6] para gerar números estatisticamente aleatórios. O que torna esses números pseudo-aleatórios e não aleatórios é a possibilidade de serem repetidos [5].

3.6 Criptografia de chaves públicas

A criptografia de chaves públicas, também conhecida por criptografia assimétrica, é baseada no uso de pares de chaves para cifrar/decifrar mensagens [3].

As duas chaves são relacionadas através de um processo matemático, usando funções unidirecionais com segredo para a codificação da informação. Uma das chaves, chamada de chave pública, como o nome já diz, qualquer um pode conhecer e ter acesso, é utilizada para cifrar, enquanto a outra, chamada chave privada (secreta), é utilizada para decifrar (figura 7).

---

[6] Semente: Valor retirado de um sistema do computador que é utilizado para alimentar a entrada do PRNG tais como: hora do dia em milissegundos, estado do computador, número de processos, coordenadas do cursor do mouse entre outros [5].

Uma mensagem cifrada com uma chave pública somente poderá ser decifrada com o uso da chave privada com a qual está relacionada.

Segue a tabela 2:

Função da Chave	Qual Chave?	De Quem?
Cifrar os dados para um destinatário	Chave Pública	Do Destinatário
Assinar a mensagem	Chave Privada	Do Signatário
Decifrar os dados para ler a mensagem	Chave Privada	Do Destinatário
Verificar a assinatura da mensagem	Chave Pública	Do Signatário

Tabela 2 - Resumo do uso de chaves públicas e privadas na criptografia assimétrica. Fonte: [3].

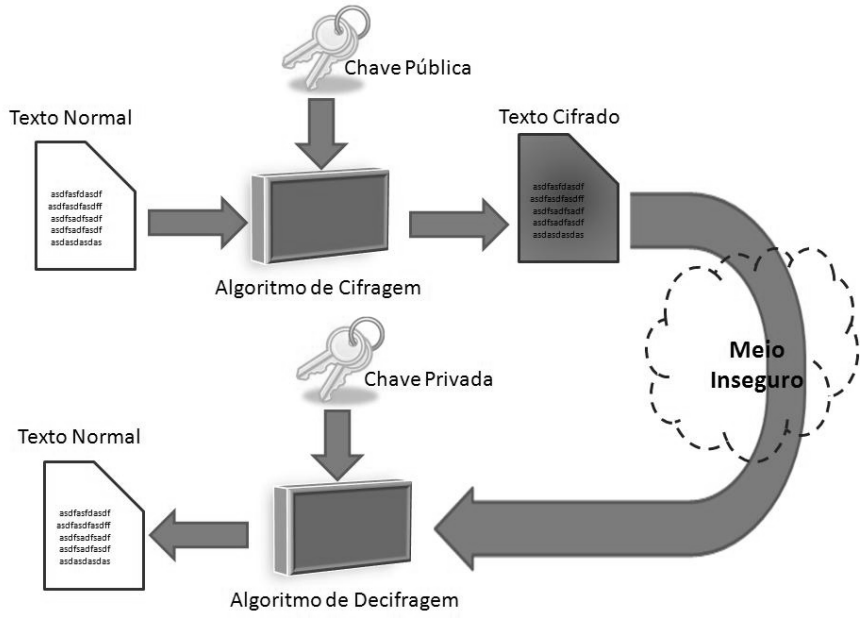

Figura 7 - Esquema de criptografia assimétrica. Fonte: O autor.

Os sistemas criptográficos de chave assimétrica baseiam-se na dificuldade que existe em se calcular a operação inversa de determinadas operações matemáticas. Atualmente existem três categorias de problemas matemáticos a partir dos quais são construídos os algoritmos de chaves públicas [3]:

a) fatoração inteira (IFP - *Integer Factorization Problem*): Dado um número n resultado da multiplicação de dois números primos *p* e *q*, a dificuldade consiste em

encontrar *p* e *q* tendo-se somente *n*, sendo, todos, números inteiros positivos. Para números pequenos, um ataque de força bruta pode facilmente encontrar a solução, mas para valores maiores de *n* (da ordem de 1024 bits), encontrar a solução não é computacionalmente tratável. Um dos algoritmos criptográficos baseados neste problema é o RSA;

b) problema logaritmo discreto (DLP - *Discrete Logarithm Problem*): Dada a equação $y = g^x \bmod p$, onde *g* é um número inteiro positivo e *p* um número primo, ambos conhecidos, a dificuldade é dado o valor de *y* calcular o valor de *x*. Da mesma forma que a fatoração inteira, para valores grandes de *p*; *x*; *y* e *g*, da ordem de centenas de bits, este cálculo torna-se muito difícil. Os esquemas criptográficos ElGamal e Diffie-Hellman são baseados neste problema;

c) problema logaritmo discreto sobre curvas elípticas (ECDLP - *Elliptic Curve Discrete Logarithm Problem*). Dada a equação $Q = l.P \bmod n$, onde *P* é um ponto sobre a curva elíptica *E*, *n* a ordem do ponto *P*, e *l* um inteiro no intervalo $0 \leq l \leq n$ -1, a dificuldade está em se encontrar *l* sabendo-se *P* e *Q*. Basicamente os mesmos algoritmos desenvolvidos para DLP, podem ser aplicados sobre curvas elípticas.

As principais vantagens da criptografia de chave pública sobre a simétrica são [3]:

a) a chave secreta não é compartilhada, uma vez que basta a chave pública – de conhecimento geral – para a troca segura de mensagens;

b) provê autenticação, já que é possível validar assinatura com a chave privada através da chave pública, partindo-se do princípio que a chave privada não foi distribuída (uma vez que isso não é necessário) para ninguém;

c) permite o não-repúdio, pois é possível verificar as chaves;

d) é escalável, possibilitando que exista uma hierarquia de controle e distribuição de chaves, que pode ser facilmente ampliada.

Em contrapartida, existem pelo menos duas grandes desvantagens [3]:

a) é lenta, pois os algoritmos, pela sua natureza matemática, apresentam auto custo de processamento;

b) requer uma autoridade de certificação, para que se possa garantir a identidade e ter-se chaves públicas confiáveis.

A criptografia assimétrica não substitui a criptografia simétrica. É importante reconhecer e identificar as limitações de cada método, de forma a utilizar os dois tipos de maneira complementar para prover a segurança necessária às partes envolvidas.

A distribuição de chaves públicas é feita através de uma infra-estrutura de chaves públicas, que será apresentada a frente.

3.7 O que a criptografia não pode fazer

A criptografia tem um papel importante na segurança da informação, porém alguns fatores fazem com que ela torne-se vulnerável, tais como [2]:

1. A criptografia não protege arquivos não-criptografados: Mesmo que se tenha um servidor *Web* configurado para utilizar uma forte criptografia no tráfego dos dados, se os arquivos originais armazenados no servidor não estiverem criptografados, os mesmos se tornam vulneráveis.
2. A criptografia não pode proteger contra chaves criptográficas roubadas: É preciso ter uma infra-estrutura segura para a armazenagem da chave criptográfica, pois se o atacante tiver acesso à chave e conhecer qual foi o algoritmo utilizado na ciframento, ele pode facilmente decifrar um dado.
3. A criptografia não pode proteger contra ataques ao serviço: Mesmo os dados estando criptografados, o atacante pode ter outro objetivo do que o de roubar dados. Ele pode ter como objetivo lançar ataques do tipo de DoS[7], a fim de deixar o acesso ao serviço, por exemplo, de um banco, indisponível.
4. A criptografia não pode proteger de programas modificados: Um atacante pode modificar programas utilizados em um sistema criptográfico para produzir resultados de seu conhecimento. Por exemplo: a Universidade da Califórnia em Berkeley desenvolveu um ataque onde o Internet Explorer foi modificado para sempre gerar a mesma chave criptográfica.

[7] *Denial of Service* (DoS) ou ataque de negação de serviços, consistem em tentativas de impedir usuários legítimos de utilizarem um determinado serviço de um computador [1].

CAPÍTULO 4

4 CERTIFICAÇÃO DIGITAL

A Certificação Digital é um conjunto de técnicas e processos que propiciam mais segurança às comunicações e transações eletrônicas, permitindo também a guarda segura de documentos [17].

4.1 Assinatura digital

O mesmo método de autenticação dos algoritmos de criptografia de chave pública operando em conjunto com um resumo da mensagem, também conhecido como função de *hash*[8], é chamado de assinatura digital (figura 8) [16].

O resumo criptográfico é o resultado retornado por uma função de *hash*. Este pode ser comparado a uma impressão digital, pois cada documento possui um valor único de resumo e até mesmo uma pequena alteração no documento, como a inserção de um espaço em branco, resulta em um resumo completamente diferente.

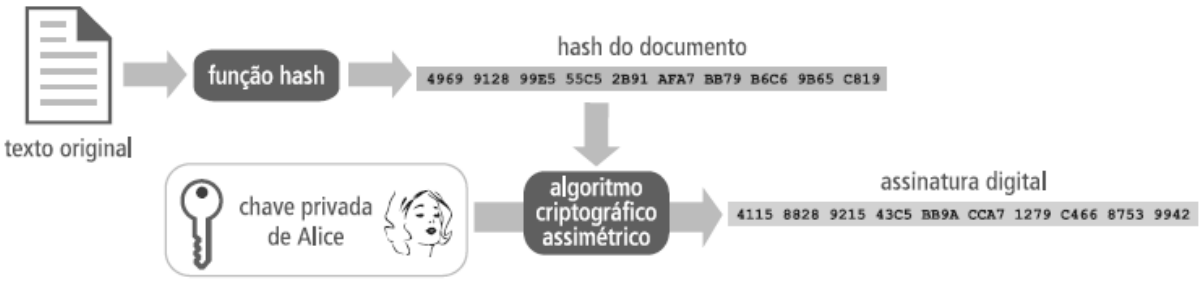

Figura 8 - Esquema de assinatura digital. Fonte: [16].

A vantagem da utilização de resumos criptográficos no processo de autenticação é o aumento de desempenho, pois os algoritmos de criptografia

[8] A função de *hash* é uma função que recebe um conjunto de bits que pode ter tamanho variado e devolve um conjunto de bits de tamanho fixo [37].

assimétrica são muito lentos. A submissão de resumos criptográficos ao processo de ciframento com a chave privada reduz o tempo de operação para gerar uma assinatura por serem os resumos, em geral, muito menores que os documentos em si. Assim, consomem um tempo baixo e uniforme, independente do tamanho do documento a ser assinado.

Na assinatura digital, o documento não sofre qualquer alteração e o *hash* cifrado com a chave privada é anexado ao documento.

4.1.1 Propriedades da assinatura digital

São propriedades da assinatura digital [25].

1. A assinatura é autêntica: quando um usuário usa a chave pública de A para verificar uma mensagem, ele confirma que foi A e somente A quem assinou a mensagem;
2. A assinatura não pode ser forjada: somente A conhece sua chave secreta;
3. O documento assinado não pode ser alterado: se houver qualquer alteração no texto criptografado este não poderá ser restaurado com o uso da chave pública de A;
4. A assinatura não é reutilizável: a assinatura é uma função do documento signatário e não pode ser transferida para outro documento;
5. A assinatura não pode ser repudiada: o usuário B não precisa de nenhuma ajuda de A para verificar sua assinatura e A não pode negar ter assinado o documento.

4.1.2 Verificação da assinatura digital

Para comprovar uma assinatura digital é necessário realizar duas operações: calcular o resumo da mensagem do documento e verificar a assinatura com a chave pública do signatário. Se forem iguais, a assinatura está correta, o que significa que foi gerada pela chave privada corresponde à chave pública utilizada na verificação e que o documento está íntegro. Caso sejam diferentes, a assinatura está incorreta, o que significa que pode ter havido alterações no documento ou na assinatura pública [16].

4.1.3 Validade jurídica da assinatura digital

A técnica de assinatura digital é uma forma eficaz de garantir autoria de documentos eletrônicos. Em agosto de 2001, a Medida Provisória (MP) 2.200 garantiu no Brasil a validade jurídica de documentos eletrônicos e a utilização de certificados digitais para atribuir autenticidade e integridade aos documentos. Este fato tornou a assinatura digital um instrumento válido juridicamente [16].

4.2 Infra-estrutura de chaves públicas

Infra-estrutura de chaves públicas (ICP) ou *Public Key Infrastructures* (PKI) é um ambiente para prover aos negócios eletrônicos condições de viabilidade a fim de que tenham os mesmos resultados daqueles conferidos aos contratos fora da rede. Tal recurso viabiliza a autenticação oficial e a integridade do documento, assim como sua elaboração e a confidencialidade nas operações e na assinatura digital, garantindo o valor jurídico e precavendo os envolvidos nas negociações da recusa do que foi firmado anteriormente. Além dos requisitos de segurança, a ICP conta com leis e decretos elaborados pelo governo federal que possibilitam a legitimidade do negócio digital, quebrando definitivamente o paradigma do uso da *Internet* para transações financeiras entre empresas e/ou pessoas físicas [31].

4.2.1 ICP-Brasil

É o órgão que regula um conjunto de entidades governamentais ou de iniciativa privada que são responsáveis por assegurar que determinado par de chaves, privada e pública, pertence ao indivíduo correto [37].

A ICP-Brasil foi instituída pela MP 2.200-2, de 24 de agosto de 2001, que cria o Comitê Gestor da ICP-Brasil, a Autoridade Certificadora (AC) Raiz Brasileira e define as demais entidades que compõem sua estrutura. A partir dessa MP foram elaborados os regulamentos que regem as atividades das entidades integrantes da ICP-Brasil: são as Resoluções do Comitê Gestor da ICP-Brasil, as Instruções Normativas e outros documentos, que podem ser consultados em legislação [13].

A utilização da tecnologia de assinatura de digital e chave assimétrica pode ser utilizada sem a necessidade certificação, mas juridicamente ela só é valida com a certificação de uma AC.

4.2.2 Autoridade Certificadora e Registradora

Uma AC é uma entidade, pública ou privada, que estabelece previamente a identidade do futuro portador do certificado digital (pessoa física ou jurídica), por meio dos documentos necessários, e emite esse certificado. No âmbito do Governo Federal, a AC, para ter seus certificados legalmente reconhecidos, o que é obrigatório para transações com órgãos públicos, tem de ter sido certificada pela AC Raiz, ou seja, pelo Instituto Nacional de Tecnologia da Informação (ITI), que é a autoridade responsável por credenciar as demais AC's, supervisionar e fazer auditoria dos processos para garantir o cumprimento das exigências de segurança.

O estabelecimento prévio da identidade da pessoa e a aprovação da solicitação de certificado são feitos por uma Autoridade Registradora (AR), credenciada por uma AC. Cabe à AC estabelecer e fazer cumprir, pelas AR's a ela vinculadas, as políticas de segurança necessárias para garantir a autenticidade da identificação feita, bem como emitir os certificados e publicá-los em repositório público, ou ainda, renová-los e revogá-los, conforme seja o caso [14].

4.2.3 Estrutura hierárquica da AC do Brasil

No topo da estrutura hierárquica encontra-se a AC Raiz (AC Raiz) e, abaixo dela, as diversas entidades (AC's de primeiro e segundo nível e AR). Na ICP-Brasil, a AC Raiz é o ITI, que é responsável também pela emissão de seu próprio par de chaves e pela supervisão de todos os processos que envolvem a certificação (figura 9) [29].

Atualmente, a ICP Brasil tem credenciadas oito Autoridades Certificadoras de primeiro nível (Presidência da República, Secretaria da Receita Federal, Serpro, Caixa Econômica Federal, AC Jus, Certisign, Imprensa Oficial de São Paulo - Imesp e Serasa).

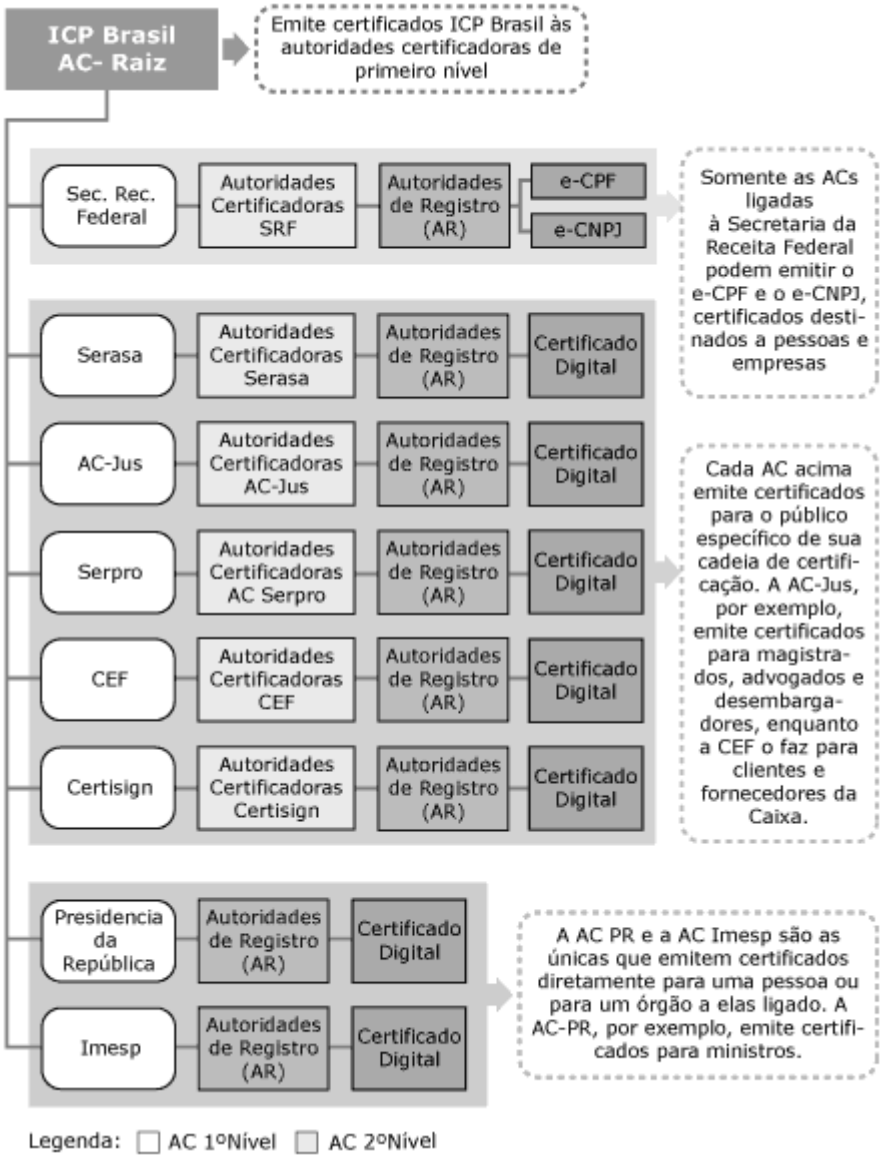

Figura 9 – Estrutura Hierárquica da AC do Brasil. Fonte: [29].

4.3 Certificado digital

O certificado digital é um arquivo eletrônico que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade. Este arquivo pode estar armazenado em um computador ou em outra mídia, como um *token* ou um *smartcard* (figura 10) [7].

Um certificado digital tem dois objetivos: estabelece a identidade do proprietário e torna disponível a chave pública do proprietário [12].

Figura 10 - *Token* e *Smartcard*. Fonte: [6].

4.3.1 Padrão X.509

Na certificação digital, os certificados seguem um padrão internacional. A especificação X.509 é um padrão internacional que especifica o formato dos certificados digitais, de tal maneira que se possa amarrar firmemente um nome a uma chave pública. Na ICP-Brasil utiliza-se certificados no padrão X.509 v3 [7].

4.3.2 Estrutura de um certificado digital

Um certificado digital normalmente apresenta as seguintes informações [16]:

- Nome da pessoa ou entidade a ser associada à chave pública;
- Período de validade do certificado;
- Chave pública;
- Nome e assinatura da entidade que assinou o certificado e
- Número de série.

A figura 11 apresenta a estrutura de um certificado digital:

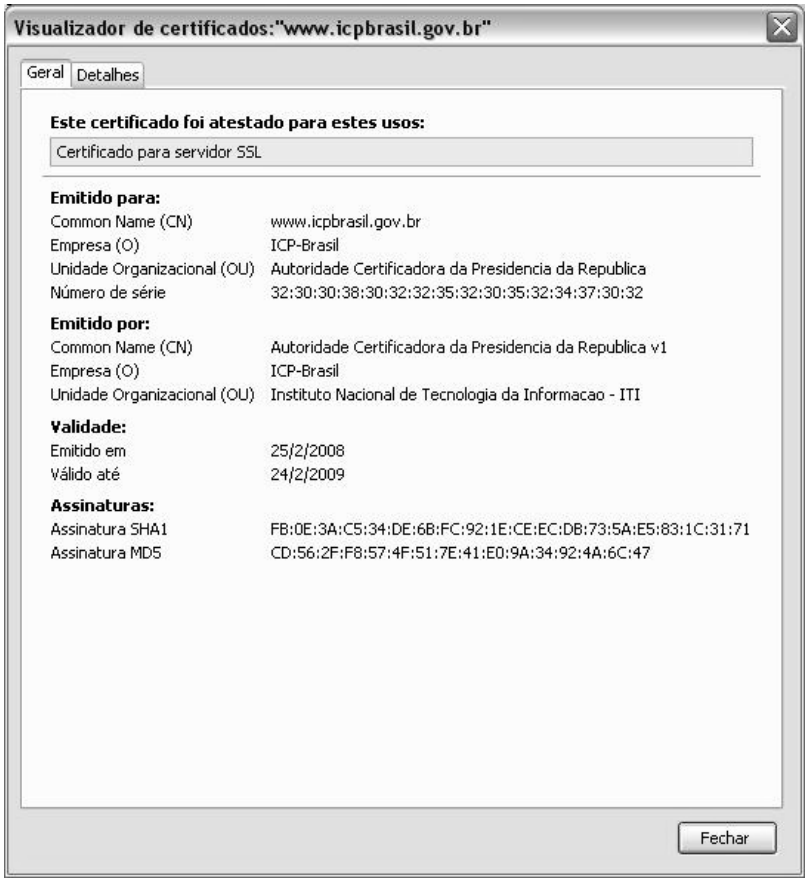

Figura 11 - Certificado Digital. Fonte: O autor.

4.3.3 Aplicações da certificação digital

Um exemplo do uso de certificados digitais é o serviço bancário provido via *internet.* Os bancos possuem certificado para autenticar-se perante o cliente, assegurando que o acesso está realmente ocorrendo com o servidor do banco. E o cliente, ao solicitar um serviço, como por exemplo, acesso ao saldo da conta corrente, pode utilizar o seu certificado para autenticar-se perante o banco.

As dez mais populares aplicações da certificação digital atualmente são [15]:

1 - A Receita Federal permite que o contribuinte acompanhe o andamento da declaração de Imposto de Renda pela rede, bem como verifique e regularize a situação fiscal, via *web*.

2 - Alguns cartórios brasileiros, por meio do sistema de certificação digital, permitem a solicitação remota de ofícios, certidões de escrituras de imóveis, contratos registrados, certidões de nascimento, de casamento ou óbito, garantindo a autenticidade, a integridade, a segurança e a eficácia jurídica de todos eles.

3 - Vários bancos utilizam os certificados digitais para garantir mais segurança aos clientes e usuários dos serviços.

4 - Diversas empresas e órgãos públicos usam certificados digitais para garantir que o sítio que o internauta está acessando é realmente o buscado, evitando, por exemplo, que o interessado negocie em um sítio clonado.

5 - Com o uso do certificado, pode-se assinar digitalmente mensagem de e-mail, garantindo ao destinatário a autoria do remetente e que o conteúdo não foi adulterado entre o envio e o recebimento.

6 - Processos judiciais foram acelerados com a criação da Autoridade Certificadora do Judiciário (AC-JUS), que facilitou a utilização da certificação digital nos tribunais, conferindo segurança e agilidade aos processos.

7 - O Sistema de Pagamentos Brasileiros (SPB) usa a certificação digital da ICP-Brasil.

8 - A Nota Fiscal Eletrônica (e-NF) já nasceu atrelada à certificação digital. Essa iniciativa está sendo testada em grandes empresas e deverá ser estendida a todas às pessoas jurídicas. Com isso, haverá maior segurança na arrecadação, redução de custos em todo o processo, além da enorme economia de papel.

9 - No ProUni (Programa Universidade para Todos), cada entidade participante é digitalmente autenticada.

10 - O INSS (Instituto Nacional de Seguridade Social), em novembro de 2006, anunciou que vai usar certificação digital nos escritórios para evitar fraudes.

CAPÍTULO 5

5 PROTOCOLOS CRIPTOGRÁFICOS

Qualquer sistema criptográfico quando utilizado apenas para ciframento e deciframento tem uma utilidade limitada. Para obter uma solução completa, deve haver a união da tecnologia criptográfica com outras que possibilite solução para algum tipo de problema (como envio de mensagens com segurança, autenticação de usuários, etc.) [34]. Surgiu então a necessidade de serem criados protocolos que solucionassem esses problemas. Um protocolo, na ciência da computação, nada mais é que uma padronização de procedimentos computacionais para haja uma comunicação entre dois ou mais computadores.

Entende-se por protocolos criptográficos, aqueles protocolos que se utilizam de criptografia em um ou mais de seus passos [34]. Têm por objetivo satisfazer requisitos de segurança e permitir que dois ou mais usuários possam trocar conteúdo eletrônico, sem que algum deles possa ter alguma vantagem ilegítima sobre os demais ou que terceiros consigam acessar indevidamente as informações transmitidas entre as entidades [26].

5.1 Protocolo SSL

Secure Sockets Layer (SSL) é um protocolo de comunicação que fornece confidencialidade e integridade na comunicação entre um cliente e um servidor, através do uso de criptografia [7].

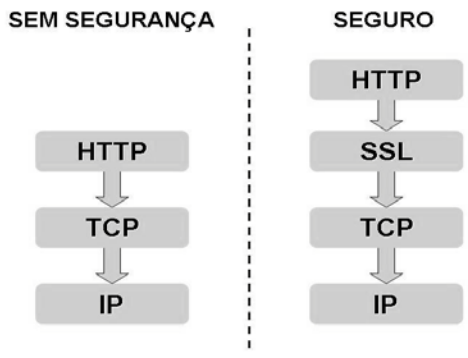

Figura 12 – Esquema sem e com SSL. Fonte: [35].

A Netscape Communications foi a desenvolvedora do SSL a versão inicial foi lançada em julho de 1994. Distribuído junto os navegadores *Netscape* e *Internet Explorer* e os servidores *web* mais comuns Apache, NCSA HTTPD, IIS, *Netscape Server* etc. [21].

O SSL é um protocolo proprietário, ou seja, seu código fonte é restrito ao desenvolvedor, por isso em 1997 foi criado um grupo de trabalho na *internet Engineering Task Force* (IETF), que é uma organização que desenvolve os padrões da *Internet*, para construir um padrão, aberto, que garanta conexões seguras na *internet*. Foi padronizado pela RFC2246 e RFC4346. O nome escolhido para esta versão foi *Transport Layer Security* (TLS) e é baseado no SSL v3 da Netscape, a seguir algumas diferenças entre os protocolos [8]:

- TLS usa o algoritmo *keyed-Hashing for Message Authentication Code* (HMAC) enquanto o SSL apenas *Message Authentication Code* (MAC). O algoritmo HMAC produz *hashes* mais seguros que o algoritmo MAC;
- No TLS nem sempre é necessário recorrer à raiz de uma AC para usar uma certificação. Pode ser usada uma autoridade intermediária;
- O TLS apresenta novas mensagens de alerta [8];

SSL será o termo utilizado na continuação deste trabalho e é aplicado para ambos os protocolos, exceto se comparados.

5.1.1 Objetivos

Os objetivos do protocolo SSL, em ordem de prioridade, são [8]:

1. Segurança com criptografia: SSL deve ser usado para estabelecer uma conexão segura entre duas entidades.

2. Interoperabilidade: Programadores independentes devem conseguir desenvolver aplicações utilizando SSL que possam trocar parâmetros criptográficos sem um conhecer o código do outro.

3. Extensibilidade: SSL busca o fornecimento de uma estrutura (*framework*), em que novos métodos de criptografia simétrica e assimétrica podem ser adicionados, sem a necessidade da implementação de uma nova biblioteca de segurança.

4. Eficiência Relativa: Operações de criptografia, principalmente de chave pública, exigem um alto processamento. Sendo assim, o protocolo SSL incorporou

um mecanismo de armazenamento para evitar que toda conexão ao ser estabelecida não precise processar operações de criptografia. Com isso, reduz-se também a atividade da rede.

5.1.2 SSL e a pilha de protocolos TCP/IP

Como o próprio nome indica (Camada de Soquete Seguro), conexões SSL agem como soquetes conectados por TCP. Portanto, pode-se pensar a conexão SSL como conexões TCP seguras desde que o lugar do SSL na pilha de protocolos é imediatamente acima do TCP e logo abaixo da camada de aplicação, como mostra a figura 13 [30].

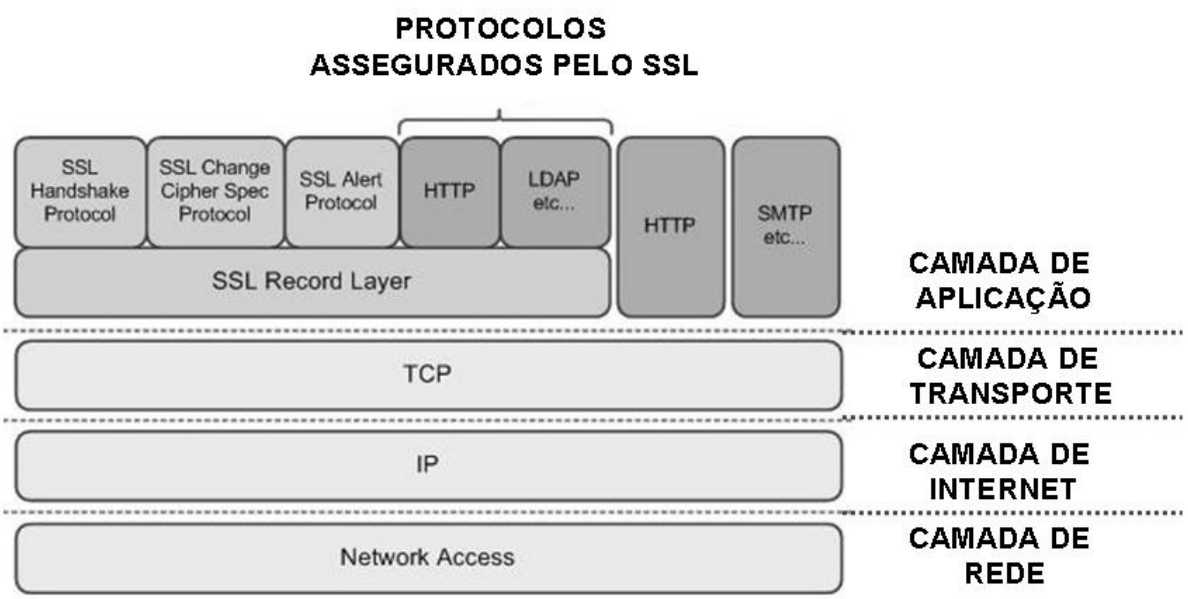

Figura 13 - SSL e a pilha de protocolos TCP/IP. Fonte: [20].

O TLS/SSL possui três subprotocolos que permitem às partes chegarem a um acordo sobre os parâmetros de segurança que serão utilizados na camada de registro para autenticação, comunicação e para reportar condições de erro entre as partes.

5.1.3 Protocolo *Handshake*

O protocolo de *Handshake* é responsável pelos seguintes itens [8]:

- Identificador da sessão: uma seqüência de bytes escolhida pelo servidor para identificar uma sessão ativa ou uma sessão reiniciável.
- Método de compressão: qual o método de compressão que será utilizado antes da criptografia dos dados.
- *Cipher Spec*: especifica qual o algoritmo de criptografia vai ser utilizado, por exemplo, DES. Qual algoritmo de MAC (MD5, SHA) que vai ser utilizado. E define alguns atributos criptográficos como, por exemplo, o tamanho do *hash.*
- Chave Mestre (*master key*): chave secreta de 48 bytes que será compartilhada entre o cliente e o servidor.
- *Is Resumable*: *semáforo* que indica se a sessão pode ser utilizada para iniciar novas conexões.

Com os itens acima são criados os parâmetros de segurança para serem usados pela Camada de Registro para proteger os dados. Muitas conexões podem ser retomadas usando a mesma sessão, caso essa característica seja suportada pela mesma. Isso evita que todos os parâmetros de segurança tenham que ser novamente negociados.

5.1.4 Protocolo *Change Cipher Spec*

O protocolo *Change Cipher Spec* existe para sinalizar mudanças nas estratégias de criptografia que estavam sendo utilizadas. Este protocolo é formado por apenas uma mensagem, a qual é cifrada e comprimida com os parâmetros que estavam previamente estabelecidos [8].

A mensagem Change Cipher Spec é enviada por ambos, cliente e servidor, para que cada um deles passe a usar as novas regras de criptografia que foram negociadas.

Um cuidado deve ser tomado ao fazer as alterações nas estratégias de criptografia, pois existe a possibilidade de que o primeiro a receber a mensagem de troca de estratégia possa ainda estar computando uma mensagem que recebeu

anteriormente, já que os algoritmos de chave pública demandam muito processamento. Para resolver isso, deve ser esperado um tempo antes de mandar essa mensagem para garantir que o outro lado não perderá informações.

5.1.5 Protocolo de Alerta

Um dos tipos de conteúdo suportado pela camada de registros do SSL é o conteúdo de alerta [8].

As mensagens de alerta transportam a importância do alerta e a descrição do alerta. Mensagens com importância denominada fatal resultam imediatamente no encerramento da conexão. Nesse caso outras conexões correspondendo à mesma sessão podem continuar, mas o identificador da sessão deve ser invalidado, prevenindo que essa sessão seja utilizada posteriormente para estabelecer novas conexões.

Assim como as outras mensagens do SSL os alertas também são cifrados e comprimidos de acordo com os parâmetros de segurança que estão ativos no momento em que a mensagem é enviada.

Tipos de mensagem de alerta:

1. Alertas de Encerramento: São utilizados para informar às partes que a conexão será encerrada, evitando assim ataques por truncamento. Todos os dados recebidos após o recebimento de uma mensagem de encerramento são descartados.

2. Alertas de Erro: O tratamento de erros pelo SSL *Handshake Protocol* é muito simples. Quando um erro é detectado, quem detectou o erro envia um alerta para o outro lado. Se for um alerta fatal, imediatamente ambos terminam a conexão. Clientes e servidores devem esquecer quaisquer identificadores de sessões e chaves secretas associados com uma conexão que falhou. Por conseguinte qualquer conexão que tenha sido encerrada por um alerta fatal não pode ser restabelecida.

Exemplos de mensagem de erro são [5]:

- *unexpected_message*: fatal, indica o recebimento de uma mensagem fora de ordem;
- *close_warning*, sinaliza o fechamento de uma conexão SSL;

- *bad_record_mac*: fatal, indica que a verificação do MAC da mensagem recebida não coincidiu;
- *decompression_failure*: fatal, indica que o processo de descompactação resultou num bloco maior que 214 bytes;
- *handshake_failure*: fatal, indica algum problema na negociação das informações de segurança;
- *no_certificate*: indica que o cliente não possui nenhum certificado que coincida com os tipos pedidos;
- *bad_certificate*: indica que o certificado recebido possui uma assinatura não válida;
- *unsupported_certificate*: indica recepção de certificado não é suportado;
- *certificate_revoked*: indica que o certificado foi revogado por quem o assinou;
- *certificate_expired*: indica que a data de validez do certificado expirou ou, de que este ainda não esta válido;
- *certificate_unknown*: indica qualquer outro problema relacionado com falhas no certificado;
- *illegal_parameter*: fatal, indica que algum campo de alguma mensagem trafegada durante o *handshake* está fora do seu intervalo ou incoerente com outro campo.

5.1.6 Camada de Registro

O SSL utiliza esta camada para encapsular todas as mensagens dos demais protocolos das camadas superiores, explicando a sua independência com os protocolos de aplicação, facilitando o desenvolvimento de aplicações que necessitam de conexões seguras [8]. Enquanto os protocolos *handshaking* realizam a negociação de parâmetros de segurança, o protocolo de Registro é quem realmente efetua as operações necessárias para garantir a segurança da conexão. O protocolo de Registro recebe as mensagens para serem transmitidas, fragmenta os dados em blocos, opcionalmente realiza a compressão dos dados, aplica o MAC, cifra e transmite o resultado. Logicamente, com os dados recebidos, o protocolo de Registro realiza a decriptação, verificação da integridade, realiza descompressão, reagrupa os blocos e os entrega para as camadas superiores.

5.1.7 Como funciona o início da conexão

O cliente envia uma *“hello message*” (figura 14) para a qual o servidor deve responder com uma outra *“hello message*”, caso contrário um erro fatal ocorrerá e a conexão falhará. O “*hello*” do cliente e o do servidor é utilizado para estabelecer capacidades de segurança entre o cliente e o servidor [30].

Esses *hello's* estabelecem os seguintes atributos: versão do protocolo, identificação da sessão, conjunto de cifras e métodos de compressão. Adicionalmente, dois valores randômicos são gerados e trocados: *ClientHello.random* e *ServerHello.random.*

A seguir, o servidor enviará o seu certificado, se este for autenticado. Adicionalmente, uma mensagem de trocas de chave do servidor pode ser enviada, se necessário (por exemplo, se o servidor não possuir certificado ou se o seu certificado for apenas para assinatura). Se o servidor está autenticado, ele pode solicitar um certificado do cliente.

Agora o servidor enviará uma mensagem “*hello”* concluído, indicando que a fase “*hello message”* do *handshake* está completa. O servidor irá, então, esperar por uma resposta do cliente.

Se o servidor tiver enviado uma mensagem de solicitação de certificado, o cliente deve enviar o seu certificado ou uma mensagem de alerta de que não há certificado (*no_certificate alert*). A mensagem de troca de chaves do cliente é, então, enviada, e o conteúdo desta mensagem dependerá do algoritmo assimétrico escolhido durante o “*hello”* do cliente e o “*hello”* do servidor. Se o cliente enviou um certificado com possibilidade de assinatura, uma mensagem de verificação digital do certificado (*digitally-signed cerfiticate verify message*) é enviada para verificar, explicitamente, o certificado.

Nesse momento, uma mensagem de mudança de especificação da cifra é enviada pelo cliente, e o cliente copia a Especificação de Cifra (*Cipher Spec*) da cifra pendente na Especificação atual. O cliente envia, então, imediatamente a mensagem de finalização, juntamente com os novos algoritmos, chaves e segredos.

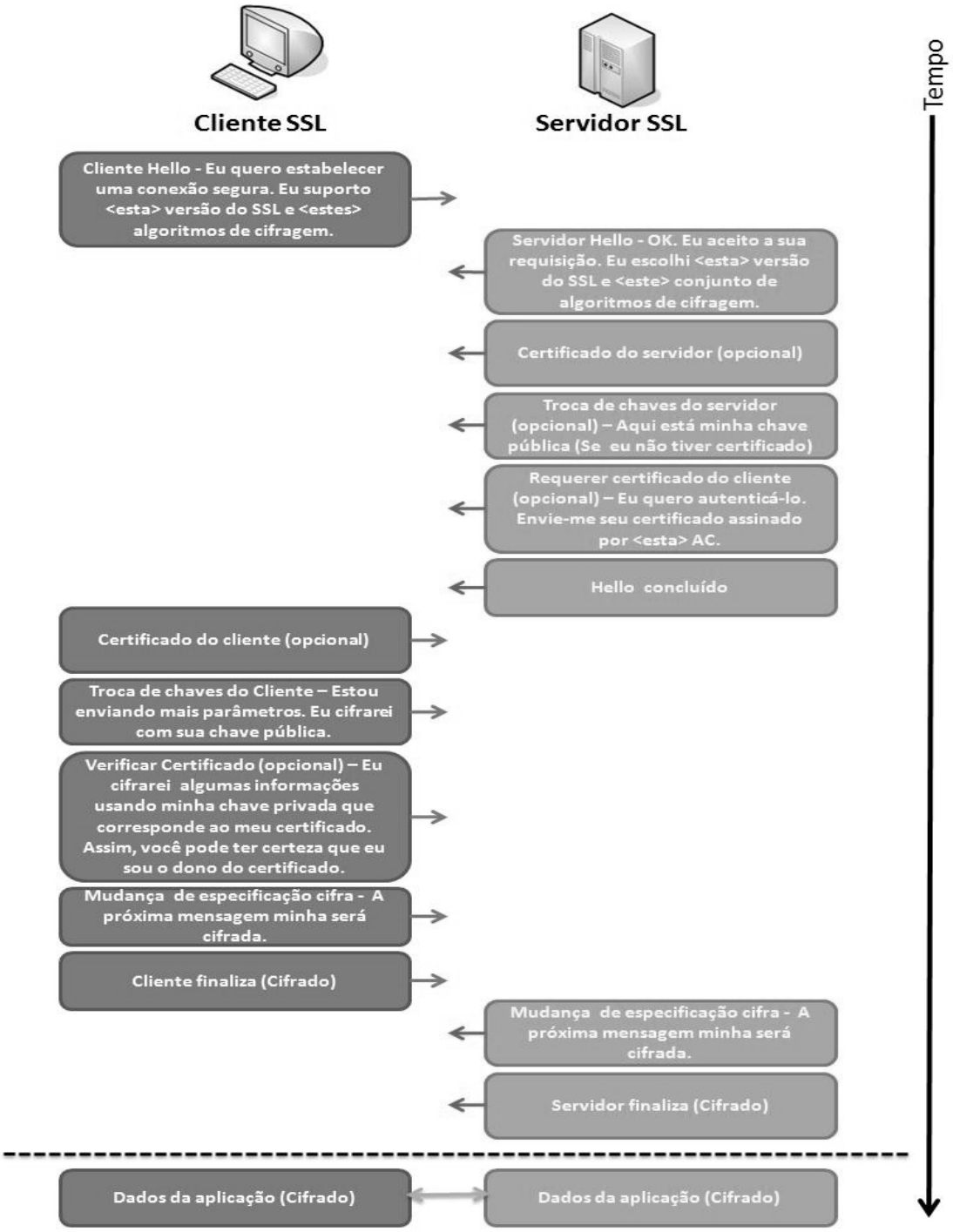

Figura 14 - Conexão Inicial SSL. Fonte: [20].

Em resposta, o servidor enviará sua mensagem de mudança de *Cipher Spec*, transferindo a cifra pendente para a Especificação atual e envia sua mensagem de finalização juntamente com a nova *Cipher Spec*.

Nesse momento, o *handshake* está completo e o cliente e o servidor podem começar a trocar dados na camada de aplicação.

5.1.8 Identificando um sítio com SSL

Existem pelo menos dois itens que podem ser visualizados na janela do seu navegador, e que significam que os dados transmitidos entre o navegador e o sítio visitado estão dentro de uma sessão segura:

- Na parte superior, na barra de endereços, pode se observar que o endereço digitado começa com HTTPS[9] ao invés do HTTP (figura 15);
- Na parte inferior, na barra de status, deve aparecer o cadeado (figura 16);

Nos Browsers atuais, existem mais elementos que mostram o acesso a um sítio seguro como a mudança de cor e a presença do cadeado na barra de endereços.

Figura 15 – Barra de endereços com SSL. Fonte: O autor

Figura 16 – Barra de *status* com SSL. Fonte: O autor

Ao clicar sobre o cadeado é possível visualizar as propriedades de segurança: identidade do sítio, tipo de criptografia utilizada e o certificado de segurança (figura 17).

[9] HTTPS é a combinação do protocolo HTTP com o SSL. É a maneira mais comum atualmente de trafegar documentos via HTTP de maneira segura. Provê cifragem de dados, autenticação de servidor, integridade de mensagem e autenticação de cliente [22].

Figura 17 – Propriedades de segurança de um sítio. Fonte: O autor

5.1.9 Certificado gerado pelo OpenSSL

O OpenSSL é um kit de ferramentas que implementa os protocolos SSL e o TLS, além de prover diversas ferramentas de criptografia. Apêndice A apresenta como gerar certificados no OpenSSL.

Na figura 18, é apresentado um exemplo de um certificado criado no OpenSSL.

5.2 IPSec

O *Internet Protocol Security* (IPSec) define um conjunto de protocolos para implementação de serviços de segurança na camada de rede. A figura 19 mostra a localização deste protocolo na pilha do TCP/IP.

Figura 18 - Certificado gerado a partir do SSL. Fonte: O autor

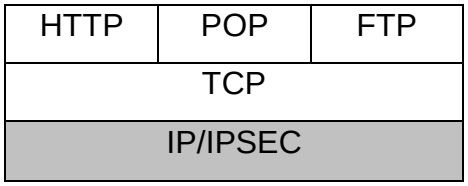

Figura 19 – Localização do IPSec na pilha de protocolo TCP/IP. Fonte: O autor.

Baseado em padrões desenvolvidos pela IETF o IPSec busca garantir confidencialidade, integridade e autenticidade na comunicação entre dois

computadores, mesmo que as informações trafeguem por um meio não seguro, como por exemplo, a *internet* [5].

5.2.1 *Security Association*

Para transferências dos dados entre a origem e o destino, o IPSec trabalha com o conceito de S*ecurity Association* (SA), trata-se de um túnel no qual serão enviadas as informações entre os computadores ou *gateways.* As SA's são limitadas a um protocolo por conexão, logo no processo de comunicação entre duas entidades pode ter mais de uma SA.

Para estabelecer as SA's o IPsec utiliza o protocolo *Internet Key Exchange* (IKE), que realiza a negociação entre as entidades e a troca das chaves criptográficas, que serão utilizadas nas transações.

5.2.2 Protocolos

Os serviços de segurança oferecido pelo IPSec através de seus protocolos são:

- Estabelecer a conexão segura entre origem e destino;
- Controle de acesso;
- Autenticação da origem dos dados;
- Não aceita pacotes repetidos;
- Criptografia dos pacotes.

Além do protocolo IKE citado no item de SA, tem-se:

Protocolo AH

Authentication Header (AH) implementa os serviços de integridade e autenticação dos dados, usando algoritmos de chave publica como MD5 e o SHA-1, com isso ataques do tipo “homem-ao-meio[10]” são evitados. Uma desvantagem do

10 Homem-ao-Meio – O atacante se coloca entre as duas entidades recebendo e falsificando a mensagens.

AH é que ele não realiza a cifragem dos dados, essa desvantagem pode ser corrigida com o uso de outro protocolo o ESP. A figura 20 mostra os campos do AH [5].

Próximo Cabeçalho	Tamanho do conteúdo AH	Reservado
Parâmetros de Segurança		
Número de seqüência		
Dados de Autenticação		

Figura 20 – Protocolo AH. Fonte: O autor.

Protocolo ESP

Encapsulating Security Payload (ESP) implementa o serviço de cifragem dos dados, confidencialidade, o que garante que somente o destinatário terá acesso ao conteúdo da mensagem, porém o protocolo ESP não verifica a integridade do cabeçalho do pacote, já o protocolo AH faz essa checagem. A figura 21 mostra os campos do ESP.

Parâmetros de Segurança		
Número de seqüência		
Dados de Carga		
Enchimento		
	Tamanho do enchimento	Próximo Cabeçalho
Dados de Autenticação		

Figura 21 – Protocolo ESP. Fonte: O autor.

Para estabelecer uma conexão IPSec com maior segurança, pode-se implementar os dois protocolos, AH e ESP, mas como as SA's são simplex, ou seja, os dados só são transferidos em um sentido e suportando, apenas um protocolo, por

isso, deve ter uma SA para cada protocolo. Segue a figura 22 com uma ilustração das SA's criadas em uma conexão IPSec.

5.2.3 Funcionamento do protocolo

O IPSec opera de duas formas: Transporte e Túnel. A diferença entre os modos de trabalho é que, no modo transporte a SA é estabelecida de *host*[11] para *host*, já o modo túnel a SA é estabelecida entre os *Gateways*[12] de cada *host*. A figura 23 ilustra o funcionamento do IPSec das duas formas [4].

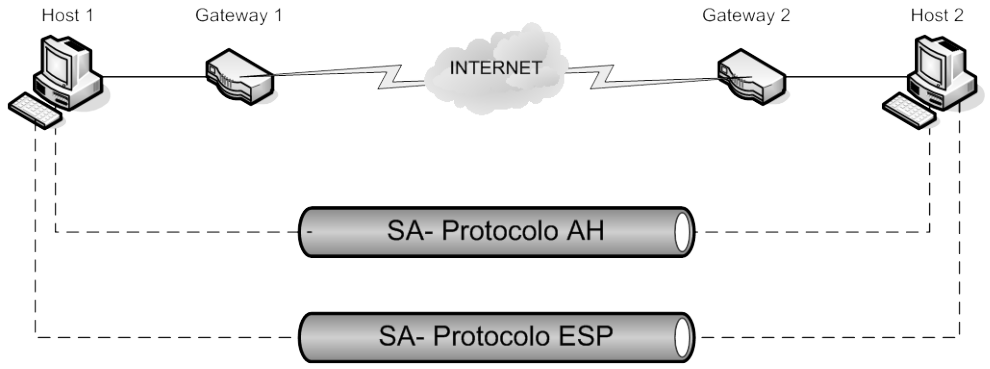

Figura 22 – SA's criadas em conexão IPSec. Fonte: O autor

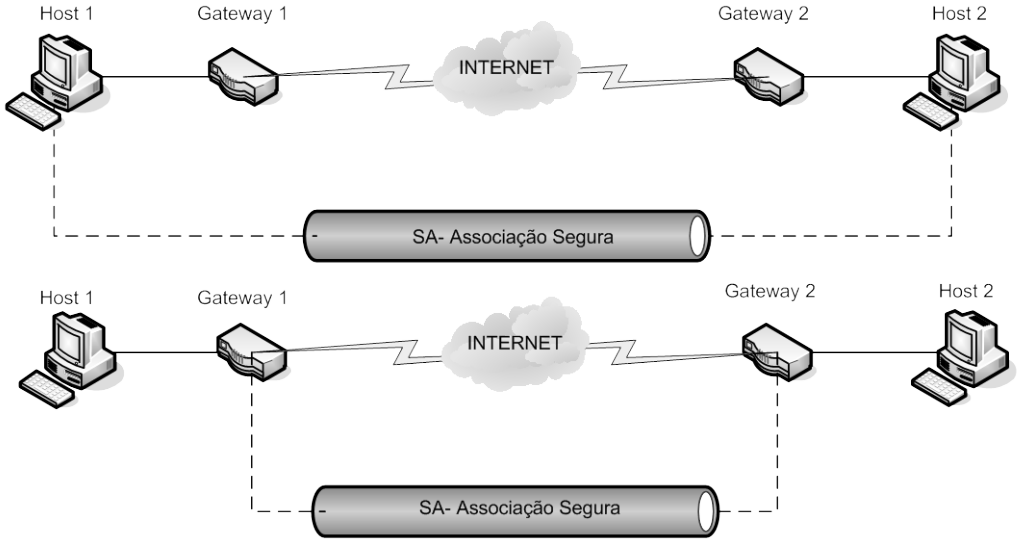

Figura 23 – Formas de funcionamento do IPSec. Fonte: O autor

[11] Host – Computador conectado a rede.
[12] Gateway – Equipamento que interliga duas redes.

No modo de transporte, a mensagem é cifrada, mas o cabeçalho IP não. A vantagem é que como os dispositivos da rede pública tem acesso nas informações de origem e destino do pacote, processamentos sobre o pacote que visão melhorar o desempenho do tráfego, podem ser implementados. A desvantagem é que nesse modo um atacante pode analisar o tráfego, mesmo ela estando cifrada.

No modo de túnel todo o datagrama[13], mensagem e cabeçalho são cifrados. O que permite que um dispositivo de rede, o *gateway* de origem, implemente a segurança do IPSec nos pacotes, realizando a cifragem no lugar dos hosts, e enviando, através da SA, ao *gateway* de destino que decifra e repassa ao *host*. A primeira vantagem é que as entidades de destino não precisam ser modificadas para suportar o IPSec e a segunda é proteger contra a análise de tráfego [28].

5.2.4 Tecnologias de Criptografia

São tecnologias empregadas pelo IPSec para garantir a segurança [28]:

- Mecanismo de troca de chaves de *Diffie-Hellman*;
- Criptografia de chave pública para assinar as trocas de chave de *Diffie-Hellman*, garantindo assim a identidade das duas partes e evitando ataques do tipo “homen-ao-meio”;
- Algoritmos simétricos para cifragem para grandes volumes de dados, como o DES;
- Algoritmos para cálculo de *hash* com utilização de chaves, com o HMAC, combinado com os algoritmos de *hash* tradicionais como o MD5 ou SHA, autenticando os pacotes;
- Certificados digitais assinados por uma autoridade certificadora, que agem como identidades digitais.

5.3 SET

O protocolo *Secure Eletronic Transaction* (SET), que em português significa transações eletrônicas seguras, foi desenvolvido por um conjunto de empresa,

[13] Datagrama – bloco de informações que trafega em uma rede.

dentre elas, Visa, Mastercard, IBM e Microsoft. Este protocolo oferece uma estrutura para proteger as transações do comercio eletrônico, pois autentica os donos de cartões de crédito, comerciantes e bancos, define os protocolos e algoritmos para garantir a integridade e confidencialidade dos dados [24] [5].

O protocolo SET é de fácil implementação e não demanda muitas alterações nos sistemas das operadoras, bancos e clientes, o que facilita a aceitação no mercado [24].

5.3.1 Requisitos de negócio

- Fornecer confidencialidade para as informações de pagamento e pedido;
- Garantir a integridade dos dados transmitidos;
- Autenticar que o usuário do cartão é realmente dono da conta vinculada a ele;
- Montar a estrutura de autenticação entre o comerciante e a sua instituição financeira, para que o vendedor possa aceitar a transação de pagamento do cliente, via cartão de crédito;
- Garantir o uso das melhores práticas e técnicas de sistemas que protejam as transações;
- Desenvolver um protocolo que não dependa de segurança no nível de transporte e nem evite a utilização;
- Facilitar e incentivar a interoperabilidade para adaptação de softwares e da rede de comunicação.

5.3.2 Recursos do protocolo

Os recursos necessários para garantir os requisitos citados acima são:

- Confidencialidade garantida com o uso do algoritmo DES;
- Integridade garantida com uso de assinaturas digitais utilizando o algoritmo RSA;
- Autenticação do portador do cartão realizada com assinaturas digitais e certificados X.509 v3;
- Interoperabilidade permite a utilização do SET em diversas plataformas de hardware e software.

5.3.3 Entidades do protocolo

Emissor: Instituição financeira que fornece o cartão para cliente, ele é responsável por realizar o pagamento das compras.

Cliente: Pessoa autorizada a utilizar o cartão, o protocolo SET fornece os serviços de confidencialidade para as transações *on-line* como os comerciantes.

Comerciante: Qualquer entidade que venda produtos e ou serviços via *internet* e para aceitar o pagamento eletrônico, o comerciante precisa de um banco.

Banco do comerciante: Fornece os serviços de processamentos dos pagamentos para o comerciante, de forma resumida, o banco paga o comerciante e o emissor paga o banco.

Portal de Pagamento: Processam as mensagens de pagamento do comerciante, este papel pode ser desempenhado por um terceiro, porém em algum momento deverá existir a interação entre o comerciante e seu banco [5].

A figura 24 ilustra as interações das entidades do protocolo SET.

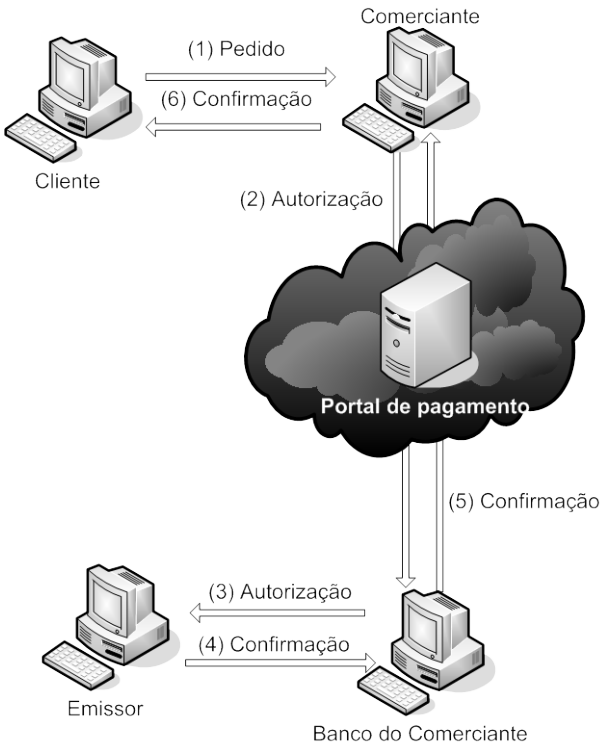

Figura 24 – Interação SET. Fonte: O autor.

5.3.4 Assinatura dupla

Este conceito, também conhecido como assinatura dual, foi introduzido pelo protocolo SET, este tipo de assinatura permite que duas informações sejam enviadas para duas entidades diferentes em uma mesma mensagem. Essa técnica é aplicada quando o cliente envia o pedido para o comerciante, junto com o pedido o cliente envia também as informações de pagamento, que são destinadas ao portal de pagamento. Com isso o cliente não pode negar que fez um pedido e nem comerciante pode cobrar por produtos que não foram solicitados.

5.3.5 Certificados

Os certificados do SET são privados e apenas os sistemas que compatíveis com SET podem interpretá-los. Todas as entidades possuem um certificado, para utilizarem nas transações. O SET define também que os certificados devem ser gerenciados por uma hierarquia, ilustrada na figura 25. Desta forma, as entidades podem checar os certificados entre si, utilizando para isso, a chave pública emitida pela certificadora de raiz.

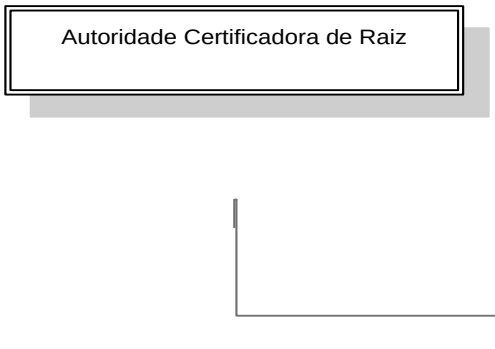

Figura 25 – Hierarquia de certificados. Fonte: [5].

Com o SET as transações *on-line* de compra pela *internet* ficaram mais seguras, pois a arquitetura utilizada implementa duas soluções importantíssimas:

1. Todas as mensagens do processo de compra entre as entidades estão criptografas, o que impede o acesso à informação por elementos que não façam parte do processo.
2. Implementar a confiança na transação, ou seja, uma entidade ao receber uma informação pode confirmar a veracidade da mesma, graças ao esquema de assinaturas digitais.

CAPÍTULO 6

6 CONCLUSÕES

Ao longo da história, o homem sempre necessitou ocultar informações. Um exemplo são as guerras, onde as informações não podem cair em mãos inimigas. Surgiu-se então a necessidade de garantir a segurança da informação. Uma tecnologia utilizada para este fim é a criptografia, que transforma uma informação legível a qualquer interessado, em uma informação cifrada.

Com o surgimento dos computadores, desenvolveu-se a criptografia computacional, tendo em vista manter seguro as informações geradas e armazenadas em computadores e assim possibilitar que os objetivos da segurança da informação sejam alcançados.

A *internet* e a capacidade de processamento sempre crescente fizeram com que, a criptografia isoladamente não resolvesse todos os problemas com a segurança da informação. Impulsionado por esse problema, surgiram então os protocolos criptográficos. Assim, a *internet* tornou-se um canal seguro para uma diversa gama de serviços.

A certificação digital veio para garantir a autenticidade dos usuários na *Internet* e fez com que os protocolos precisassem de adequações, tornando-os cada vez mais seguros.

A criptografia é um elemento essencial nos protocolos criptográficos para garantir a confidencialidade dos dados durante o tráfego na rede, sendo utilizada tanto a criptografia de chave pública como a simétrica, assim como as funções de *hash* criptográficos.

Há uma infinidade de protocolos criptográficos. Não há um melhor que o outro. Deve ser levada em consideração a aplicação a ser processada sobre ele. Nesse trabalho foram abordados os protocolos: SSL, IPSec e SET. Os três, basicamente, têm o mesmo conceito, mas diferem em alguns aspectos mais específicos, tais como: O SSL situa-se entre a camada de aplicação e a de transporte e um *software* faz a sua implementação, já o IPSec está situado sob a camada de rede, ele permite o tráfego de alguns tipos de dados que o SSL não permite e sua implementação é realizada pelo sistema operacional.

No exemplo prático apresentado nesta monografia, foi adotado o protocolo SSL, pois ele é largamente utilizado por sítios na *internet*. Foi utilizado a ferramenta OpenSSL para implementar o protocolo e o servidor *web* mais utilizado do mundo, o Apache. O Apêndice A orienta na instalação e a configuração do Apache para suportar o SSL, visando apresentar uma maneira de ser instalado e configurado um servidor seguro para hospedar um sítio seguro.

O objetivo desse trabalho foi demonstrar como a *internet*, que é um meio inseguro, pode tornar-se um ambiente seguro, o que é possível graças ao surgimento e aperfeiçoamento contínuo dos protocolos criptográficos.

Este trabalho teve uma limitação de aprofundamento técnico devido à complexidade do tema em relação ao curto espaço de tempo disponível e pela dificuldade de se encontrar exemplos reais e atuais de uso dos protocolos criptográficos, devido à confidencialidade que as empresas adotam em suas políticas de segurança da informação. Trabalhos futuros poderão fazer uma abordagem mais prática de determinado protocolo, a partir deste, não necessitando abordar toda a teoria envolvida e podendo assim se focar, por exemplo, em uma implementação em linguagem de programação, como: Java, PHP ou .NET.

REFERÊNCIAS

[1] ALECRIM, Emerson. Ataques DoS (Denial of Service) e DDoS (Distributed DoS). Disponível em: <http://www.infowester.com/col091004.php>. Acesso em: 15 mai. 2008.

[2] ALMEIDA, André L. de Souza; SILVA, Jussara R. Freitas. Chave de segurança. Trabalho de Conclusão de Curso (Pós Graduação em Projeto, Suporte e Administração de Rede de Computadores) – Centro Universitário de Volta Redonda, Volta Redonda.

[3] AMARO, George. Criptografia simétrica e criptografia de chave pública: Vantagens e desvantagens. Disponível em: <http://publica.fesppr.br/index.php/rnti/article/viewFile/33/20>. Acesso em: 06 mar. 2008.

[4] ASSIS, João Mário de. Implementando VPN em Linux. 2003. 76 f. Monografia (Pós-graduação em Informática) – Universidade Federal de Lavras, Lavras, 2003.

[5] BURNETT, S.; PAINE, S. Criptografia e segurança – O guia oficial RSA. 1. ed. Rio de Janeiro: Campus, 2002.

[6] CERTISIGN. E-CPF. Disponível em: <www.certisign.com.br>. Acesso em: 29 mar. 2008.

[7] CGI.BR. Cartilha de Segurança para Internet. Disponível em: <http://cartilha.cert.br>. Acesso em: 22 mar. 2008.

[8] COUTINHO, Gustavo Lacerda; SILVA, Renan G. Machado e. SSL e TLS. Disponível em: <http://gta.ufrj.br/grad/06_1/ssl/>. Acesso em: 20 abr.2008.

[9] Criptografia baseada em identidade. Disponível em: <http://www.linux.ime.usp.br/~cef/mac499-04/monografias/rec/cesarse/monografia.html>. Acesso em: 25 fev. 2008.

[10] FILHO, Antonio M. da Silva. Segurança da Informação: Sobre a necessidade de proteção de Sistemas de Informações. Revista Espaço Acadêmico. n 42, nov. 2004.

[11] História e aplicação da Criptografia. Disponível em: <http://www.absoluta.org/cripty/cripty_h.htm>. Acesso em: 14 mar. 2008.

[12] IBM. Certificados digitais. Disponível em: <http://publib.boulder.ibm.com/tividd/td/TRM/GC32-1323-00/pt_BR/HTML/admin230.htm>. Acesso em: 15 mai. 2008.

[13] ICP-Brasil (Brasil). Apresentação. Disponível em: <https://www.icpbrasil.gov.br/apresentacao>. Acesso em: 28 mar. 2008.

[14] _____. O que é uma autoridade certificadora. Disponível em: <https://www.icpbrasil.gov.br/duvidas/faq/o-que-e-uma-autoridade-certificadora>. Acesso em: 28 mar. 2008.

[15] INTEL. Curso on-line de Certificação digital. Disponível em: <http://www.nextg.com.br>. Acesso em: 31 mar. 2008.

[16] ITI (Brasil). O que é certificação digital? Disponível em: <http://www.iti.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf>. Acesso em: 28 fev. 2008.

[17] _____. Certificação digital. <acraiz.gov.br/twiki/pub/Certificacao/CartilhasCd/CertificacaoDigital.pdf>. Acesso em: 19 fev. 2008.

[18] KUNZ, Leonardo. Esteganografia em imagens usando codificação de Huffman. Disponível em: <http://www.inf.ufrgs.br/~lkunz/cpd/> Acesso em: 29 fev. 2008.

[19] LAUREANO, Marcos A. Pchek. Gestão de Segurança da Informação. Disponível em: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acesso em: 22 mar. 2008.

[20] MAJ, Artur. Apache 2 with SSL/TLS: Step-by-Step, Part 1. Disponível em: <http://www.securityfocus.com/infocus/1818&h=778&w=576&sz=64&hl=pt-BR&start=2&um=1&tbnid=gJYubZb34HfZeM:&tbnh=142>. Acesso em: 01 mai. 2008.

[21] MENDES, Hammurabi das Chagas. Uma implementação livre do protocolo SSL. 2003. Trabalho da disciplina Segurança de dados – Universidade de Brasília, Brasília, 2003.

[22] PASTORE, Pablo. HTTPS. Disponível em: <http://www.gta.ufrj.br/grad/03_1/http/https.html>. Acesso em: 03 mai. 2008.

[23] PEREIRA, Samáris Ramiro. O Sistema criptográfico de Chave Pública RSA. 2008. 222 f. Dissertação (Mestrado em Informática) – Universidade Católica de Santos, Santos, 2008.

[24] PETRY, Helô. Protocolo SET: Uma solução para segurança em comércio eletrônico. Departamento de Informática e estatistica – Universidade Federal de Santa Catarina, Florianópolis.

[25] PISTELLI, Daniela. Criptografia. Disponível em: <www.geekbrasil.com.br>. Acesso: 8 fev. 2008.

[26] PIVA, Fabio; DAHAB, Ricardo. Verificação formal de protocolos. Disponível em: <http://www.prp.unicamp.br/pibic/congressos/xiiicongresso/paineis/016013.pdf>. Acesso em: 30 mai. 2008.

[27] RAPOPORT, Eduardo. VPN – Conceitos. Disponível em: <http://www.gta.ufrj.br/~rezende/cursos/eel879/trabalhos/vpn/conceitos.html>. Acesso em: 28 fev. 2008.

[28] _____. IPSec – Protocolo de segurança IP. Departamento de Engenharia Eletrônica e de Computação (DEL) - Escola Politécnica/Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2003.

[29] RIBEIRO, Gisele. Como funciona o certificado digital? Disponível em: <http://informatica.hsw.uol.com.br/certificado-digital3.htm>. Acesso em: 13 abr. 2008.

[30] SILVA, André T. Souza. Uma implementação SSL utilizando JSSE. 2004. Trabalho da disciplina Segurança de dados – Universidade de Brasília, Brasília, 2004.

[31] SILVA, Lino Sarlo da. *Public Key Infrastructure* – PKI. Novatec, 2004.

[32] SINGH, Simón. *Los códigos secretos – El arte y la ciência de la criptografia, desde el antiguo Egipto a la era Internet.* Disponível em: <personal.telefonica.terra.es/web/jms32/cifra/codsecretos>. Acesso em: 22 mar. 2008.

[33] STREBE, Matthew; PERKINS, Charles. Firewall. 1. ed. São Paulo: Makron Books, 2002. 411 p.

[34] TAROUCO, Liane M. Rockenbach. Protocolos. Disponível em: <http://penta.ufrgs.br/gere96/segur2/protocol.htm>. Acesso em: 02 mai. 2008.

[35] THOMAS, Stephen, *SSL and TLS Essencials – Securing the Web.* Estados Unidos da América: Wiley, 2000.

[36] VELOSO, Caio J. Martins. Criptologia – Uma ciência fundamental para tratamento de informações sigilosas. Disponível em: <http://www.modulo.com.br/index.jsp?page=3&catid=17&objid=23&pagenumber=0&idiom=0>. Acesso em: 14 fev. 2008.

[37] VERISSIMO, Fernando. Um estudo sobre a ICP-Brasil. Rio de Janeiro, 2002. Disponível em: <http://www.abc.org.br/~verissimo/textos/icpbrasil.pdf>. Acesso em: 26 mar. 2008.

[38] VILLELA, S. M.; CARVALHO, L. A. V. O resfriamento simulado no projeto ótimo de autômatos celulares para a geração de chaves criptográficas de fluxo. Disponível em: <http://www.cos.ufrj.br/~ines/enia07_html/pdf/27815.pdf> Acesso em: 23 mar. 2008.

APÊNDICE A - Tutorial de instalação e configuração Apache+SSL em ambiente Windows

A.1 Introdução

Esse tutorial visa mostrar a configuração do servidor Apache, o qual é o servidor HTTP mais utilizado no mundo, para trabalhar com o protocolo SSL.

Para realizar a configuração, será necessário fazer o *download* dos arquivos de instalação do servidor Apache, OpenSSL, para gerar o certificado e as chaves que serão utilizadas e o módulo SSL utilizado no Apache.

Links para *download*:

apache_2.2.8-win32-x86-no_ssl - http://ftp.unicamp.br/pub/apache/httpd/binaries/win32/apache_2.2.8-win32-x86-no_ssl.msi

Win32OpenSSL-0_9_8g.exe - http://www.slproweb.com/download/Win32OpenSSL-0_9_8g.exe

mod_ssl.so - http://conteudo.imasters.com.br/3465/mod_ssl.so

A.2 Instalação

Servidor Apache

Após realizado os *downloads,* o próximo passo será instalar o Apache.

1. Execute o arquivo de instalação do Apache;
2. Leia e caso concorde com o termo de uso o aceite;
3. A seguir a um breve resumo sobre o *Apache,* avance para o próximo passo;
4. Configurar os parâmetros iniciais do Apache (figura 26).

Network Domain: Domínio do sítio (Ex.: apache.org);

Server Name: Nome do servidor (Ex.: www.apache.org);

Administrator's E-mail Address: E-mail do administrador do sítio (Ex.: admin@apache.org).

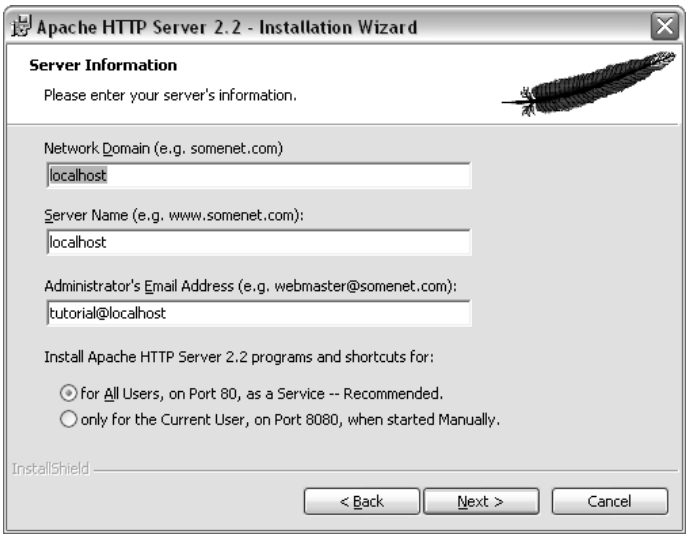

Figura 26 – Tela de configuração inicial do servidor. Fonte: O autor

5. Escolha instalação típica (instalação padrão);
6. Escolha o diretório a ser instalado;
7. Clique em instalar e aguarde o término.

OpenSSL

Da mesma forma após realizado o *download* execute o arquivo de instalação do OpenSSL e siga os passos:

1. Leia e caso concorde com o termo de uso aceite-o;
2. Escolha o diretório onde será instalado;
3. Criação do atalho no menu iniciar, avance;
4. Clique em instalar e aguarde o término.

A.3 Criando Certificado SSL de teste

Antes de começar a configuração do SSL no Apache, é necessário criar um certificado de teste para a sessão segura. Este certificado não tem juridicamente nenhuma validade, pois ele não é gerado por uma AC. Para ter validade será necessário adquirir um certificado SSL para servidor com uma AC.

Abra o "*Prompt* de comando", execute o comando para ir até o diretório do *OpenSSL*: "C:\Documents and Settings\Administrador> cd c:\OpenSSL\bin".

Em seguida, crie o certificado que será utilizado no servidor com seguinte comando: "openssl req -config openssl.cnf -new -out cert_tcc.csr". O "cert_tcc.csr" pode ser substituído pelo nome que você deseja dar ao certificado. Após a execução do comando, será gerada a chave privada. Em seguida será pedida a criação de uma senha e a confirmação dela. O programa irá verificar e entrará automaticamente no próximo passo que é o preenchimento das propriedades do certificado:

- Nome do país (2 letras): BR;
- Nome do estado (nome completo): São Paulo;
- Nome da cidade: São Bernardo do Campo;
- Nome da organização: TCC Protocolo Criptográfico;
- Nome da unidade organizacional: Tutorial SSL;
- Nome comum: www.tccpc.com.br;
- Endereço de e-mail: admin@tccpc.com.br;
- Atributos extras: challenge pass: segredo;
- Nome opcional da companhia: tcc.

Depois de gerado o certificado vá até o diretório "/bin" do *OpenSSL*, e apague um arquivo ".rnd", porque tem a semente que foi utilizado para gerar a chave.

Retornando ao *prompt*, execute o comando: "openssl rsa -in privkey.pem -out tccpc.key", para remover a senha da chave ("tccpc.key" é o nome da sua chave para o servidor, pode ser usado qualquer nome). Será pedido a senha que foi utilizada na geração da chave privada.

Agora execute o comando: "openssl x509 -in cert_tcc.csr -out cert_tcc.cert -req -signkey tccpc.key -days 365". Esse comando assina o certificado e configura o tempo de validade do certificado.

Após esse comando, vá na pasta “/bin” do *OpenSSL* e copie os arquivos “tccpc.key” e “cert_tcc.cert” para o diretório “/conf” do *Apache*.

A.4 Configurando Apache para suportar o SSL

Após gerar o certificado SSL de teste para o servidor, é necessário configurar o Apache para suportar o SSL.

Antes de abrir o arquivo de configuração, copie para “/modules” do Apache o módulo SSL “mod_ssl.so” que foi baixado.

Abra o arquivo de configuração do Apache “httpd.conf”, que está dentro da pasta “/Apache2.2/conf”. Localize as linha “#LoadModule ssl_module modules/mod_ssl.so” e “#Include conf/extra/httpd-ssl.conf” e descomente as linha, ou seja, retire o caractere “#” no inicio das linhas. Verifique se no arquivo há o bloco de PRNG abaixo:

```
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>
```

Salve o arquivo e vá até o diretório “/conf/extra/” e abra o arquivo “httpd-ssl.conf”.

Localize a linha “SSLCertificateFile” e troque o certificado padrão pelo gerado anteriormente ”cert_tcc.cert".

Localize a linha ”SSLCertificateKeyFile” e troque a chave padrão pela a gerada “tccpc.key”.

Após essa configuração salve o arquivo e reinicie o serviço do Apache (utilize o Apache *Service Monitor*).

A.5 Testando o servidor Apache+*SSL*

Para testar se o serviço foi configurado corretamente, abra o seu navegador e na barra de endereços digite: “*https://localhost”*.

Se o servidor estiver funcionando, ele deverá abrir uma janela de “Certificado de uma AC desconhecida” (figura 27), já que o certificado gerado não tem valor legal.

Nessa tela, tem a opção de visualizar o certificado antes de aceitá-lo ou recusá-lo. Clique em “Examinar certificado”. Deverá aparecer o certificado conforme foi configurado na geração dele (figura 28).

Figura 27 – Alerta de certificado desconhecido. Fonte: O autor.

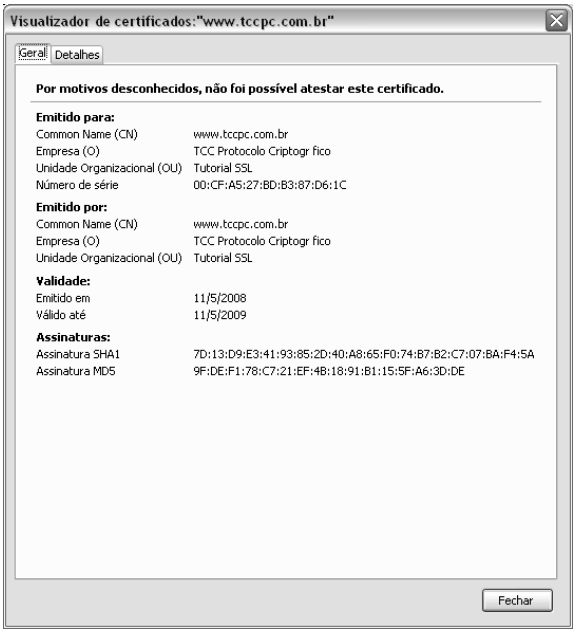

Figura 28 – Certificado gerado para o servidor Apache. Fonte: O autor.

Voltando a tela de “Certificado desconhecido”, há as seguintes opções: Aceitar permanentemente, aceitar temporariamente e não aceitar o certificado. Escolha uma das opções de aceite, para iniciar a sessão segura.

Deverá aparecer em seguida outra janela de erro (figura 29). Esse erro é devido ao *Common Name* (CN) ser diferente ao domínio do sítio (www.tccpc.com.br é diferente de localhost), clique em “OK”.

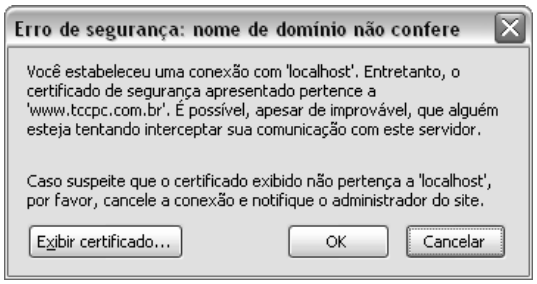

Figura 29 – Erro de verificação de domínio. Fonte: O autor

Deverá exibir a página padrão do Apache com a mensagem *“It works”*. Pronto! O servidor Apache+*SSL* está funcionando e pronto para hospedar sítios para operar em ambiente seguro.