FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Alexandra Meca Bernardo da Silva

O USO DA CRIPTOGRAFIA NA SEGURANÇA DA INFORMAÇÃO EM E-COMMERCE

Americana, S.P.

2013

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Alexandra Meca Bernardo da Silva

O USO DA CRIPTOGRAFIA NA SEGURANÇA DA INFORMAÇÃO EM E-COMMERCE

Trabalho monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec Americana, sob orientação do(a) Prof$^{o(a)}$ Msc. Alexandre Garcia Aguado
Área temática: Segurança da Informação

Americana, S. P.

2013

Alexandra Meca Bernardo da Silva

FICHA CATALOGRÁFICA elaborada pela

BIBLIOTECA – FATEC Americana – CEETPS

Silva, Alexandra Meca Bernardo da

S578u O uso da criptografia na segurança da informação em e-commerce. / Alexandra Meca Bernardo da Silva. – Americana: 2013.

48f.

Monografia (Graduação de Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.

Orientador: Prof. Me. Alexandre Garcia Aguado

1. Segurança em sistemas de informação I. Aguado, Alexandre Garcia II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

Bibliotecária responsável pela FC: Ana Valquiria Niaradi – CRB-8 região 6203

O USO DA CRIPTOGRAFIA NA SEGURANÇA DA INFORMAÇÃO EM E-COMMERCE

Trabalho de Conclusão de Curso apresentado à Faculdade de Tecnologia de Americana como parte dos requisitos para obtenção do título de Tecnólogo em Segurança da Informação.

Americana, 16 de Dezembro de 2013.

Banca Examinadora:

_____
Alexandre Garcia Aguado – (Presidente)
Mestre
Fatec Americana

_____
Edson Roberto Gaseta – (Membro)
Especialista
Fatec Americana

_____
Thaís Godoy Vasquez – (Membro)
Doutora
Fatec Americana

RESUMO

Este trabalho foi desenvolvido com o objetivo de ressaltar a importância da criptografia na garantia da segurança da informação em sites de comércio eletrônico ou E-commerce como também é conhecido. Para tanto, primeiramente foram realizadas pesquisas em livros de autores reconhecidos na área explorada. Pesquisa essa que trouxe definições de assuntos como: histórico da Internet, comércio eletrônico ou E-commerce, segurança da informação, criptografia, certificação digital e HTTPS. Cada qual com suas respectivas categorias que aprofundam melhor a explicação do assunto. Além disso, foram usados mais dois métodos de levantamento de dados para a realização da pesquisa de campo que colaborou na complementação das informações anteriormente já expostas. O primeiro trata-se de um questionário contendo perguntas pertinentes ao campo de estudo que é direcionado ao uso da criptografia na garantia da segurança da informação em um site de E-commerce. O mesmo foi respondido por um profissional de TI que atua na gerência do desenvolvimento de sites de E-commerce. O segundo mecanismo utilizado foi uma coleta de dados realizada nos sites dos cinco E-commerces mais acessados na atualidade com o intuito de colher informações como: algoritmos de criptografia utilizados e autoridades certificadoras. Os resultados das três pesquisas mencionadas acima são discutidos ao final do trabalho.

Palavras-chave: E-commerce; criptografia; segurança da informação.

ABSTRACT

This paper was developed with the objective of highlighting the importance of cryptography to garantee information security in E-commerce sites. To do so, primarily, research was conducted using books from renowned authors in the area explored. This research brought definitions of subjects such as Internet history, commerce or E-commerce, information security, cryptography, digital certification and HTTPS. Each with their respective categories deepening the subject's explanation. Furthermore, two additional data collection methods were used to assist the field research that collaborated in complementing the information previously given above . The first one is a questionnaire containing relevant questions to the field of study that is directed to the use of cryptography in ensuring information security in an E-commerce site. It was answered by an IT professional who works managing the development of E-commerce sites. The second mechanism used was a data collection held on the five most accessed E-commerce websites today in order to gather information such as: cryptography algorithms used and certifying authorities. The results of the three studies mentioned above are discussed at the end of the paper.

Keywords: E-commerce, cryptography, information security.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

1.1 Justificativa

O uso da Internet vem se tornando cada vez mais comum a cada dia. A facilidade de acesso a informações, cultura, educação, comunicação, realização de pesquisas sobre diversos assuntos e obtenção de maneira rápida o que se procura, são alguns dos fatores que mais atraem usuários.

Com a evolução da mesma, outro serviço da Web que se torna cada vez mais comum é o comércio eletrônico. Usuários conseguem visitar sites específicos que listam de maneira bem atraente seus produtos comercializáveis, escolhem os que pretendem comprar e com apenas alguns cliques é possível efetuar a compra. Sem complicações, sem filas, sem ao menos precisar sair do conforto de casa e após um prazo estipulado pelo vendedor, a mercadoria chega à casa do comprador entregue por um serviço de Correios.

Porém, quanto mais cresce a quantidade de vendas feitas por meios digitais, mais surgem ataques com a finalidade de obtenção de números de cartão de crédito, número de contas, senhas de sistemas, entre outros roubos de informações.

Garantir que as informações dos clientes permanecerão intactas e seguras, é algo crucial para o sucesso da venda através de meios eletrônicos. Se o consumidor não tem confiança ao ceder seus dados bancários ao site de E-commerce, fica claro que a compra não será consumada.

Para que acorra de fato a segurança das informações dos compradores, proprietários de lojas on-line estão investindo cada vez mais em sistemas de segurança eficazes, além de investirem em softwares e hardwares, assuntos que serão tratados ao longo do trabalho.

1.2 Objetivos

Expor vários aspectos relacionados ao uso da criptografia na obtenção da segurança da informação em sites de E-commerce ou comércio eletrônico, desde definições sobre o tema, meios mais utilizados para garantir a segurança dos clientes que optam por realizar suas compras através do uso da Internet até a discussão e conclusão de resultados obtidos através de duas ferramentas de pesquisa relacionadas ao assunto.

1.3 Metodologia

Este trabalho, com base em pesquisas realizadas em fontes como livros impressos e via Internet on-line, tem como principal objetivo detalhar e apresentar vantagens e desvantagens relacionadas ao uso de ferramentas que garantam a segurança aos dados de clientes que optam por realizar suas compras através da Internet, dando ênfase principalmente no uso da Criptografia.

Com o intuito de aumentar a credibilidade das informações que são expostas ao longo do trabalho, além de serem utilizadas estas pesquisas, optou-se por adicionar também mais duas outras ferramentas de pesquisa:

- Um questionário que contém perguntas pertinentes ao uso da criptografia para garantir a segurança da Informação em sites de E-commerce, respondido por um profissional de TI que atua na gerência do desenvolvimento de comércios eletrônicos.
- Uma pesquisa realizada nos sites dos cinco E-commerces mais acessados no Brasil atualmente, que visa colher dados como: algoritmos de criptografia utilizados e autoridades certificadoras.

Todos os dados colhidos através das ferramentas citadas acima, assim como as informações obtidas através dos livros, são comparados entre si e discutidos ao longo do trabalho.

2. HISTÓRICO DA INTERNET

Segundo Limeira (2007), em 1957, durante a guerra fria entre Estados Unidos e União Soviética, o Departamento de Defesa (DoD) dos Estados Unidos criou a agência Advanced Research Projects Agency (ARPA), que tinha como intuito "estabelecer a liderança norte-americana em ciência e tecnologia na área militar." A ARPA apoiou vários projetos na área de informática, principalmente os assuntos relacionados a redes de computadores e a sistemas operacionais.

Um desses projetos foi a criação de uma rede que fosse capaz de conectar vários computadores diferentes, a distância, de um jeito que a informação pudesse trafegar (em pacotes separados e roteados entre esses computadores) de maneira que não fosse necessário haver disponibilidade de qualquer ponto dessa rede - ou seja, "caso algum ponto da rede ficasse desconectado, essa não era paralisada como um todo."

A rede mencionada acima teve iniciada sua operação em setembro de 1969 e foi chamada de ARPANET.

Em 1986, a National Science Foundation (NSF) criou a NSFNET, rede que era mantida pelo governo norte-americano e formada com a ajuda das empresas IBM, MCI e Merit, inicialmente com um backbone, ou infraestrutura.

Em 1989, a Arpanet teve suas operações encerradas e a NSFNET tornou-se o backbone da 'rede das redes'. Desenvolvida e projetada para ligar cinco super-computadores de universidades e centros de pesquisa acadêmicos, a NSFNET começou a incluir outras redes distribuídas pelo mundo, o que acabou ampliando o seu uso que não era mais exclusivamente acadêmico.

Dessa maneira surge a Internet, que, com a popularização dos computadores pessoais (PCs, abreviatura de personal computers), tornou possível o crescimento do número de equipamentos, de pessoas e de países conectados.

O autor Laudon (2011) explica também que, a Internet tornou-se o mais abrangente sistema de comunicação público, que hoje, rivaliza com o sistema telefônico global em alcance e amplitude. Além de ser o maior exemplo de redes interconectadas e computação cliente/servidor no mundo, realizando a conexão de centenas de milhares de redes individuais em todo o planeta.

A maioria das residências conecta-se à Internet por meio de um provedor de serviços (ISP - Internet Service Provider), que nada mais é que "uma organização comercial com conexão permanente com a rede que vende conexões temporárias a assinantes."

A forma mais comum de conexão pelo mundo era feita através de uma linha telefônica tradicional e de um modem, com a velocidade de 56,6 quilobits por segundo (Kbps). Mas esse tipo de conexão acabou dando lugar às conexões banda larga, que são oferecidas por conexões via linha digital de assinante (DSL), cabo e satélite e linhas T.

Fornecedores de televisão a cabo também oferecem as conexões de Internet a cabo, que usam cabos coaxiais a cabos digitais para disponibilizar acesso à Internet a empresas e residências.

Vale lembrar que nas regiões nas quais os serviços DSL e a cabo não estão disponíveis, existe a possibilidade de acessar a Internet via satélite, apesar de "algumas conexões via Internet apresentarem velocidade de *upload* inferiores às dos serviços de banda larga."

3. O COMÉRCIO ELETRÔNICO OU E-COMMERCE

O comércio eletrônico ou E-commerce é definido pela autora Limeira (2007) como "uma aplicação da Internet que se expandiu aceleradamente desde o ano de 2000 e que deve desenvolver-se a taxas elevadas nos próximos anos." (LIMEIRA, 2007, pag. 37).

A autora utiliza ainda outra definição para o termo segundo a Organisation for Economic Co-operation and Development[1]:

> "...engloba a realização de negócios por meio da Internet, incluindo a venda não só de produtos e serviços físicos, entregues off-line, isto é, por meios tradicionais, mas de produtos como softwares, que podem ser digitalizados e entregues on-line, por meio da Internet." (LIMEIRA, 2007, pag. 37).

Segundo Laudon (2011), o comércio eletrônico ou E-commerce diz respeito ao fato de utilizar a Internet ou a web para conduzir negócios. De maneira mais formal, "diz respeito às transações comerciais realizadas digitalmente entre organizações e indivíduos ou entre duas ou mais empresas."

O mesmo surgiu em 1995, quando o Netscape.com, considerado um dos primeiros portais da Internet, concordou com a exibição de anúncios de grandes corporações, difundindo e popularizando a ideia de que a Internet poderia sim ser um poderoso canal de mídia para propaganda e vendas.

Em 2009, as vendas de comércio tradicional estavam diminuindo cinco por cento ao ano, enquanto as vendas através da Internet mantinham-se estáveis. Foi nessa época que se considerou uma recessão, quando o crescimento do comércio eletrônico 'desacelerou'.

Em 2001, explica Laudon, um grande número de empresas de E-commerce faliu. Mas muitas outras, como Amazon, eBay, Expedia e Google, tiveram resultados muito positivos, como faturamento recorde, modelos de negócios bem estruturados e lucrativos e preços de ações em elevação. Em 2006, "o faturamento do comércio eletrônico voltou a experimentar um sólido crescimento e continuou a ser a forma de venda de varejo que mais crescia nos Estados Unidos, na Europa e na Ásia."

Já os autores Kotler e Keller (2006) explicam que existem dois tipos de empresas na Internet: as inteiramente virtuais e as virtuais e reais (do inglês: brick-and-click companies).

[1]ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. E-commerce: impacts and policy challenges. Economic Outlook 2000. Disponível em: <http://www.oecd.org/dataoecd/42/48/208733.pdf>.

Empresas inteiramente virtuais

São aquelas que começaram em um site sem nenhuma existência previa como empresa tradicional (Kotler; Keller, 2006). Existem vários tipos de empresas que seguem essa modalidade, como sites de busca, provedores de serviços de Internet, sites comerciais, sites de transação, sites de conteúdo e sites capacitadores.

Como exemplos, é possível citar os sites comerciais mais proeminentes: Amazon, eBay e Expedia.

Empresas virtuais e reais

Os autores Kotler e Keller (2006) definem como empresas virtuais e reais aquelas que já existiam fisicamente (empresas tradicionais) e que decidiram também realizar vendas através da Internet.

No início, muitas empresas tradicionais tinham receio em acrescentar um canal de comércio eletrônico, pensando que causariam conflitos de canal já que estariam competindo com seus varejistas, com seus representantes ou com suas próprias lojas físicas.

Porém, existem ao menos três maneiras de ganhar a aceitação por parte de varejistas, corretores, representantes e outros intermediários:

> **"**Uma delas é oferecer marcas ou produtos diferentes na Internet. Outra é oferecer aos parceiros off-line comissões maiores para amortecer o impacto negativo sobre as vendas. A terceira é receber pedidos no site, mas delegar a entrega e a cobrança aos varejistas.**"** (KOTLER;KELLER, 2006, pag. 491).

3.1 Algumas vantagens e desvantagens do uso do E-commerce

Segundo os autores Kotler e Keller (2006), utilizar a Internet como meio de realização de compras é útil quando o comprador busca maior comodidade na compra para produtos como livros e músicas, bem como preço mais baixo como negociação de ações ou leitura de notícias.

Porém, já passa a ser menos útil nas compras de produtos que necessitam ser experimentados ou examinados antes da compra. Mas segundo o autor, até esses casos possuem exceções, já que é possível encomendar móveis no site da EthanAllen, eletrodomésticos no site da Sears e computadores caros da Dell ou Gateway sem experimentá-los previamente.

A autora Limeira (2007) cita ainda mais alguns motivos pelos quais algumas pessoas ainda se encontram resistentes com o fato de realizar compras através da Internet:

- A preocupação com a segurança e a privacidade transacional, referente a fraudes e ao mau uso de informações financeiras pessoais, como as do cartão de crédito;

- A preocupação com a privacidade não transacional, referente ao mau uso por terceiros de informações pessoais, ao vírus de computador indesejáveis, ao recebimento de e-mails sem permissão, ao excesso de propaganda, entre outros aspectos.

A autora também comenta que:

> "Para os consumidores que estão avaliando a possibilidade de realizar compras e pagamentos pela Internet, mais importantes são a segurança das informações e a política de devolução de mercadorias por parte das empresas vendedoras, caso esses produtos não correspondam às expectativas deles." (LIMEIRA, 2007, pag. 89).

4. CATEGORIAS DO COMÉRCIO ELETRÔNICO

Segundo Laudon (2011), existem três principais categorias de comércio eletrônico, que são:

- **Comércio eletrônico empresa-consumidor (B2C):** venda de produtos e serviços no varejo diretamente a compradores individuais. A BarnesandNoble.com, que vende livros, software e música a consumidores individuais, é um exemplo de e-commerce B2C.
- **Comércio eletrônico empresa-empresa (B2B):** venda de bens e serviços entre empresas. O site da ChemConnect, que vende produtos químicos e plástico, é um exemplo de e-commerce B2B.
- **Comércio eletrônico consumidor-consumidor (C2C):** venda eletrônica de bens e serviços por consumidores, diretamente a outros consumidores. Por exemplo, o eBay, gigantesco site de leilões, permite que pessoas vendam suas mercadorias a outros consumidores levando-as a leilão por preço mais alto ou por um preço fixo. A Craigslist é a plataforma mais largamente utilizada por consumidores para comprar e vender diretamente.

Existe ainda outro tipo de classificação para vendas realizadas através da Internet: o **comércio móvel (mobile commerce)** ou **m-commerce**, aquele em que são utilizados equipamentos portáteis sem fio para comprar bens e serviços em qualquer lugar. Nessa categoria, é possível realizar transações tanto empresa-empresa quanto empresa-consumidor.

Já Limeira (2007) explica que o e-commerce envolve a realização de trocas de produtos, de serviços e de informações entre diferentes agentes, a saber:

- Trocas entre consumidores (consumer-to-consumer - C2C), como ocorrem nos leilões virtuais;

- Trocas entre consumidores e empresas e vice-versa (consumer-to-business - C2C ou B2C), por exemplo, a realização de compras em lojas virtuais, ou atendimento ao cliente on-line;

- Trocas entre consumidores e governos e vice-versa (consumer-to-government - C2G ou G2C), como o pagamento de taxas e impostos, a solicitação de serviços públicos, as reclamações, etc.

- Trocas entre empresas (business-to-business - B2B), como a venda de produtos agrícolas ou fornecimento de matérias-primas para indústrias;

- Trocas entre empresas e governo e vice-versa (business-to-governament - B2B ou G2B), por exemplo, venda de produtos e serviços para órgãos do governo em licitações públicas;

Trocas entre órgãos de governo (government-to-government - G2G), como a coordenação de políticas e programas entre os diversos níveis de governo.

Tabela 1: Exemplos de Aplicações de comércio eletrônico

	Governo	**Empresa**	**Consumidor**
Governo	G2G Ex. coordenação	G2B Ex. informação	G2C Ex. informação
Empresa	B2G Ex. aquisição	B2B Ex. e-commerce	B2C Ex. loja virtual
Consumidor	C2G Ex. imposto	C2B Ex. comparação de preços	C2C Ex. leilão

Fonte: ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. E-commerce: impacts and policy challenges. Economic Outlook 2000. Disponível em: <http://www.oecd.org/dataoecd/42/48/208733.pdf>.

5. SEGURANÇA DA INFORMAÇÃO

A segurança da informação, segundo o que definem Coelho e Araújo (2013), "compreende a proteção das informações, sistemas, recursos e demais ativos contra desastres, erros (intencionais ou não) e manipulação não autorizada, objetivando a redução da probabilidade e do impacto de incidentes de segurança."

Os autores citam ainda que a norma ABNT NBR ISO/IEC 27002:2005, define segurança da informação como:

> "...a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades de negócio. A segurança da informação é obtida como resultado da implementação de um conjunto de controles, compreendendo políticas, processos, procedimentos, estruturas organizacionais e funções de hardware e software." (COELHO; ARAÚJO, 2013, pag. 2).

Segundo Stallings (2007), o Internet Architecture Board (IAB), em 1994, emitiu um relatório chamado de “Security in the Internet architecture” – segurança na arquitetura da Internet - (RFC 1636), revelando que a Internet necessitava de mais e melhor segurança, além de identificar as principais áreas para mecanismos de segurança. Entre as quais estavam:

- A necessidade de proteger a infra-estrutura da rede contra monitoração e controle não autorizados do tráfego da rede;

- A necessidade de proteger o tráfego de usuário final para usuário final usando mecanismos de autenticação e de criptografia.

O autor menciona ainda os principais incidentes relacionados à segurança informados ao CERT (Computer Emergency Response Team). Os quais incluem:

- Ataques de negação de serviços;

- Falsificação de IP, em que os intrusos criam pacotes com endereços IP falsos e exploram aplicações que usam a autenticação baseada em IP;

- Diversas formas de bisbilhotagem e farejamento de pacote, em que os atacantes lêem informações transmitidas, incluindo informações de logon e conteúdo de banco de dados.

Conforme acontece o aumento do uso da Internet e também os aumentos na complexidade dos protocolos, aplicações e da própria Internet, aumenta proporcionalmente a quantidade de ataques na Internet e em sistemas conectados a ela. Como solução para agir

contra essa ameaça que cresce a cada dia, é necessário que haja uma gama de ferramentas e tecnologias que auxiliem nessa problemática.

O autor afirma que “em um nível básico, os algoritmos criptográficos para confidencialidade e autenticação assumem maior importância. Além disso, os projetistas precisam focalizar os protocolos baseados na Internet e as vulnerabilidades dos sistemas operacionais e das aplicações atacadas.”

5.1 Formas de ataque

O ataque, conforme explicam os autores Coelho e Araújo (2013), é "um ato deliberado de tentar se desviar dos controles de segurança com o objetivo de explorar as vulnerabilidades." Eles podem ser classificados de duas maneiras:

- **Ataques passivos**

Segundo os autores, os ataques passivos são aqueles baseados em escutas e monitoramento de transmissões, com a finalidade de se conseguir informações que estão sendo transmitidas. Como exemplo pode-se citar uma escuta telefônica. Esse tipo de ataque é de difícil detecção porque não envolve alteração dos dados, porém é possível fazer sua prevenção com a utilização de criptografia.

- **Ataques ativos**

Os ataques ativos, segundo Coelho e Araújo (2013), "envolvem a modificação de dados, criação de objetos falsificados ou negação de serviço, e possuem propriedades opostas às dos ataques passivos." Prevenir esse tipo de ataque é difícil, em função da necessidade de proteção completa de todas as facilidades de comunicação e processamento, feito o tempo todo. Mas depois de detectados, é possível aplicar uma medida para recuperação de prejuízos causados.

Segundo o autor Stallings (2007), um ataque pode ser definido como:

> “Um ataque à segurança do sistema, derivado de uma ameaça inteligente, ou seja, um ato inteligente que é uma tentativa deliberada (especialmente no sentido de um método ou técnica) de burlar os serviços de segurança e violar a política de segurança de um sistema.” (STALLINGS, 2007, pag. 6).

5.2 Serviços de segurança da informação

Segundo o padrão ISO 7498-2, que compreende os aspectos relacionados à segurança no modelo Open System Interconnection (OSI), conforme afirmam Coelho e Araújo (2013), os serviços de segurança "são medidas preventivas escolhidas para combater ameaças identificadas." Esses serviços aumentam a segurança da informação contra ataques fazendo uso de um ou mais mecanismos de segurança. Em algumas literaturas os serviços de segurança também são chamados de princípios básicos de segurança.

É importante lembrar que esses serviços de segurança devem ser aplicados de acordo com as necessidades de cada organização estando em equilíbrio com os custos que as mesmas estão dispostas a ter para garantir a segurança das suas informações.

Abaixo estão as categorias de serviços de segurança:

- **Confidencialidade:** protege a transmissão de dados contra ataques passivos, ou seja, acessos não autorizados, empregando medidas como controle de acesso e criptografia. Quando acontece a quebra de sigilo de uma determinada informação ocorre a perda de Confidencialidade, como por exemplo a senha de um usuário ou administrador de sistema, o que permite a exposição de informações que deveriam ser acessadas apenas por um determinado grupo de usuários.

- **Autenticidade:** tem por objetivo garantir que uma comunicação é de fato autêntica, ou seja, é possível que origem e destino verifiquem a identidade uma da outra e que a outra parte é realmente quem alega ser. Origem e destino podem ser usuários, dispositivos ou processos.

- **Integridade:** garante que não ocorrerão ataques ativos por meio de alterações ou remoções não autorizadas. É importante o uso de um esquema que permita a verificação da integridade dos dados armazenados e em transmissão. A perda da integridade acontece quando uma determinada informação fica exposta a manuseio por uma pessoa não autorizada, que faz modificações não autorizadas e não estão sob o controle do proprietário (corporativo ou privado) da informação.

- **Não repúdio:** previne que uma origem ou destino neguem a transmissão de uma mensagem, ou seja, quando determinada mensagem é enviada, o destino consegue provar que esta foi realmente enviada por determinada origem, e vice-versa.

- **Conformidade:** garante o cumprimento de regulamentos internos e externos impostos às atividades da organização. Estar em conformidade significa estar de acordo, seguindo e fazendo cumprir leis e regulamentos internos e externos.
- **Controle de acesso:** limita e controla o acesso lógico/físico aos ativos de uma organização através dos processos de identificação, autenticação e autorização, com o intuito de proteger os recursos contra acessos não autorizados.
- **Disponibilidade:** garante a disponibilidade dos recursos para acesso por entidades autorizadas, sempre que solicitados, representando a proteção contra perdas ou degradações. A perda da Disponibilidade ocorre quando a informação deixa de estar acessível por quem necessita dela. Um exemplo seria a perda de comunicação com um sistema importante para a empresa, que ocorreu devido a queda de um servidor ou de uma aplicação crítica de negócio, que apresentou uma falha devido a um erro causado por motivo interno ou externo ao equipamento ou por ação não autorizada de pessoas com ou sem má intenção.

5.3 Visão geral da segurança da informação

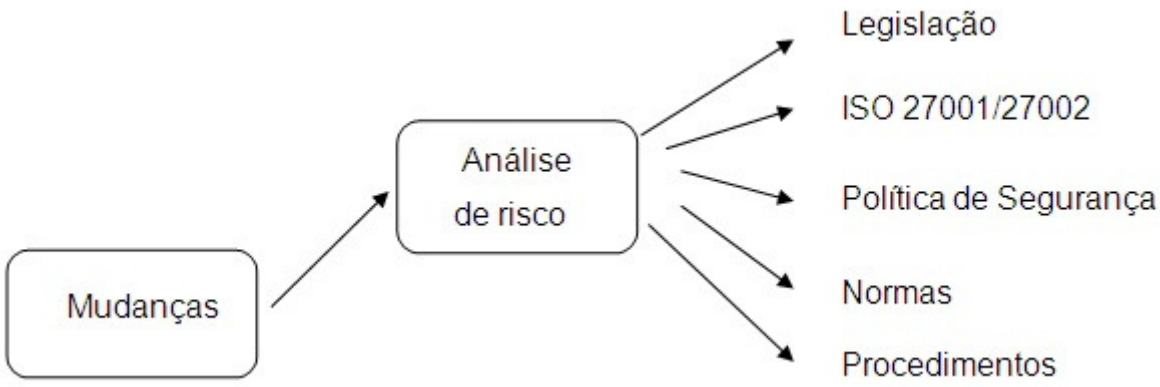

Figura 1: Visão geral da Segurança da Informação
(Fonte: Gestão da Segurança da Informação NBR 27001 e 27002, página 8)

Os autores Coelho e Araújo (2013), comentam que constantemente são lançadas no mercado novas mudanças tecnológicas que acabam fazendo surgir novas vulnerabilidades e riscos, ou ainda aumentando os já existentes. É então necessário que haja um acompanhamento dessas mudanças através de uma análise de riscos dinâmica e atualizada, o que permite o levantamento dos níveis dos riscos e da forma de tratá-los.

Juntamente a isso, é necessário:

> "...conhecer a legislação que a organização é obrigada a seguir e a levantar os requisitos de segurança necessários para atendê-la, e a partir desses requisitos legais, identificar os controles necessários e aqueles apontados pela análise de risco, com o uso das normas de segurança. A partir dos controles identificados, é necessário gerar as políticas, normas e procedimentos para a implementação dos controles." (COELHO; ARAÚJO, 2013, pag. 8).

5.4 O uso da criptografia

Conforme afirmam os autores Coelho e Araújo (2013), nas organizações é recomendável o uso da criptografia que deve ser feito conforme a legislação, regulamentos, contratos e acordos. Dessa maneira, a norma ABNT NBR ISSO/IEC 27002:2005 faz as seguintes recomendações, em conformidade com a legislação nacional vigente:

- Restringir o uso de criptografia;
- Restringir importação e/ou exportação de hardware e software cujo objetivo é a execução de funções de criptografia;
- Restringir importação e/ou exportação de hardware e software projetados com funções de criptografia embutidas;
- Definir métodos de acesso à informação cifrada por hardware ou software a serem utilizados por autoridades de outros países.

6. CRIPTOGRAFIA

A criptografia é uma ciência que usa a matemática (em forma de algoritmos) para ocultar dados (embaralhar informações). (MONTEIRO; MIGNONI, 2006, pag. 22).

A palavra criptografia é originária do grego, "Kriptos = escondido, oculto e grifo = escrita". Monteiro e Mignoni comentam ainda que a criptografia consiste na arte de escrever em cifras ou em códigos Não decifráveis a olhos nus, chamados de cifragem. Para tornar a mensagem legível novamente, o destinatário aplica o processo inverso, a decifragem.

Segundo a Cartilha de Segurança para Internet (2013), disponibilizada no site do Cert (Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil), a criptografia pode ser considerada como "a ciência e a arte de escrever mensagens em forma cifrada ou em código", além de ser considerada um dos principais mecanismos de segurança, usada para garantir a proteção contra os riscos associados ao uso da Internet.

Por meio do uso da criptografia é possível:

- Proteger os dados sigilosos armazenados em seu computador, como o seu arquivo de senhas e a sua declaração de Imposto de Renda;
- Criar uma área (partição) específica no seu computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas;
- Proteger backups contra acesso indevido, principalmente aqueles enviados para áreas de armazenamento externo de mídias;
- Proteger as comunicações realizadas pela Internet, como os e-mails enviados/recebidos e as transações bancárias e comerciais realizadas.

Alguns termos serão utilizados durante os próximos capítulos, para isso alguns deles serão explicados na tabela a seguir:

Tabela 2: Termos empregados em criptografia e comunicações via Internet

Termo	Significado
Texto claro	Informação legível (original) que será protegida, ou seja, que será codificada
Texto codificado (cifrado)	Texto ilegível, gerado pela codificação de um texto claro
Codificar (cifrar)	Ato de transformar um texto claro em um texto codificado
Decodificar (decifrar)	Ato de transformar um texto codificado em um texto claro
Método criptográfico	Conjunto de programas responsável por codificar e decodificar informações
Chave	Similar a uma senha, é utilizada como elemento secreto pelos métodos criptográficos. Seu tamanho é geralmente medido em quantidade de *bits*
Canal de comunicação	Meio utilizado para a troca de informações
Remetente	Pessoa ou serviço que envia a informação
Destinatário	Pessoa ou serviço que recebe a informação

Fonte: Cartilha de Segurança para Internet. Cert.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), 25 de setembro de 2013 às 15:00h. Disponível em: <http://cartilha.cert.br/criptografia/>.

6.1 Criptografia de chave simétrica

Segundo a Cartilha de Segurança para Internet (2013), também chamada de criptografia de chave secreta ou única, esse tipo de criptografia "utiliza uma mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados."

Caso a informação seja codificada e decodificada por uma única pessoa, não existe a necessidade de compartilhamento da chave secreta. Já quando essas operações envolvem mais de uma pessoa ou é feita em equipamentos distintos, é necessário que a chave secreta seja combinada antecipadamente por meio de um canal de comunicação seguro.

Dessa maneira, a confidencialidade da chave não fica comprometida.

Alguns exemplos de algoritmos de criptografia de chave simétrica: AES, Blowfish, RC4, 3DES e IDEA.

Por esse método de criptografia ter sido usado durante muito tempo e utilizar apenas uma chave, Monteiro e Mignoni (2007), explicam que houve a necessidade da adoção de uma Política de Segurança para troca e guarda das chaves, com o intuito de evitar que intrusos raptem a chave e passem a usá-la, bem como distribuir a chave a um novo membro do grupo.

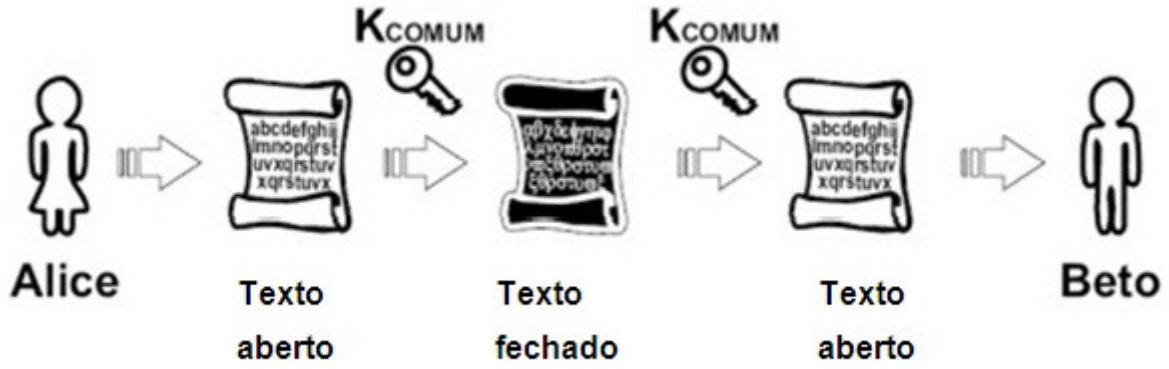

Figura 2: Criptografia de chave simétrica
(Fonte: Certificados digitais conceitos e práticas, página 23).

A criptografia simétrica, segundo Stallings (2007), chamada também de criptografia convencional ou criptografia de chave única, permaneceu sendo o único tipo de criptografia utilizado antes do desenvolvimento da criptografia por chave pública, por volta da década de 1970. Segundo o autor o modelo de criptografia simétrica possui cinco ingredientes:

1. **Texto claro:** É a mensagem ou dados originais, inteligíveis, alimentados no algoritmo como entrada;
2. **Algoritmo de criptografia:** Realiza diversas substituições e transformações no texto claro;
3. **Chave secreta:** É a entrada para o algoritmo de criptografia. A chave é um valor independente do texto claro e do algoritmo. Dependendo da chave específica que esteja sendo utilizada no momento, o algoritmo produzirá uma saída diferente. As substituições e transformações exatas realizadas pelo algoritmo dependem da chave;
4. **Texto cifrado:** Produzida como saída, essa é a mensagem embaralhada. Ela depende do texto claro e da chave secreta. Para determinada mensagem, duas chaves diferentes produzirão dois textos cifrados diferentes. O texto cifrado é um fluxo de dados aparentemente aleatório e, nesse formato, é inteligível;
5. **Algoritmo de decriptografia:** Esse é basicamente o algoritmo de criptografia executado de modo inverso. Ele toma o texto cifrado e a chave secreta e produz o texto claro original.

> Nesse tipo de criptografia, não é necessário manter em segredo o tipo de algoritmo utilizado no processo de criptografia, porém é imprescindível que a chave seja mantida secreta. Devido a essa característica, a criptografia simétrica torna-se viável para o uso generalizado. (STALLINGS, 2007, pag.19).

O autor ainda comenta que existem duas técnicas gerais para o ataque a um esquema de criptografia convencional:

- **Criptoanálise:** Os ataques criptoanalíticos contam com a natureza do algoritmo e talvez mais algum conhecimento das características gerais do texto claro, ou ainda alguns pares de amostra de texto claro e texto cifrado. Esse tipo de ataque explora as características do algoritmo para tentar deduzir um texto claro específico ou deduzir a chave utilizada.

- **Ataque por força bruta:** O atacante experimenta cada chave possível em um trecho do texto cifrado, até obter uma tradução inteligível para texto claro. Na média, metade de todas as chaves possíveis precisam ser experimentadas para se obter sucesso.

Existem ainda as técnicas de substituição, conhecidas também como técnicas de criptografia clássicas, que podem ser feitas, no caso da criptografia simétrica, através de substituição e transposição.

A técnica de substituição mais antiga e mais simples que se tem conhecimento é a Cifra de César, que consiste em substituir cada letra do alfabeto pela letra que fica três posições adiante no alfabeto. Dessa maneira, é possível ilustrar o alfabeto da seguinte maneira:

Texto claro:	a b c d e f g h i j k l m n o p q r s t u v w x y z
Texto cifrado:	d e f g h i j k l m n o p q r s t u v w x y z a b c

Dessa maneira, o algoritmo de César pode ser expresso da seguinte forma:

Para cada letra em texto claro *p*, substitua-a pelo texto cifrado *C*:

- Para cada letra em texto claro em p, substitua-a pelo texto cifrado C:
  C = E(e,p) = (p+3) mod 26
- Um deslocamento pode ser de qualquer quantidade, de modo que o algoritmo de César geral é:
  C = E(k,p) = (p+k) mod 26. Onde k assume um valor no intervalo de 1 a 25.
- O algoritmo de decriptografia é simplesmente:
  p = D(k,C) = (C-k) mod 26

Segundo Stallings, uma cifra de transposição bem simples de se entender é a técnica de *rail fence* na qual o texto claro é escrito como uma sequência de diagonais e depois lido como uma sequência de linhas.

É possível considerar o exemplo a seguir:

Cifrar a mensagem: *meet me after the toga party*, com a cifra de *rail fence* de profundidade 2:

m e m a t r h t g p r y

e t e f e t e o a a t

Mensagem criptografada: M E M A T R H T G P R Y E T E F E T E O A A T

6.2. Criptografia de chave assimétrica

Segundo a Cartilha de Segurança para Internet (2013), a criptografia de chave assimétrica é também conhecida como criptografia de chave pública, e "utiliza duas chaves distintas: uma pública que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono".

Nesse tipo de criptografia, a informação é codificada por uma das chaves e apenas a outra chave pode decodificá-la.

A chave privada pode ser armazenada de várias maneiras, como: um arquivo no computador, um *smartcard*, um *token*.

Alguns exemplos de algoritmos de criptografia de chave assimétrica: RSA, DSA, ECC e Diffie-Hellman.

A criptografia de chave assimétrica, segundo Monteiro e Mignoni (2007), permite a utilização de dois tipos de serviços:

- Assinatura Digital: é criada através do uso da chave privada e sua verificação é feita utilizando a chave pública.
- Sigilo: utiliza a chave pública do destinatário, o qual deve utilizar sua chave privada para decifrar uma mensagem.

O serviço de Sigilo é representado na imagem abaixo, já o de Assinatura Digital, no capítulo 7:

Figura 3: Criptografia de chave assimétrica, garantindo Sigilo
(Fonte: Certificados digitais conceitos e práticas, página 24)

Segundo Stallings (2007), os algoritmos de criptografia assimétrica possuem uma chave para criptografia e uma chave diferente, porém relacionada, para a decriptografia. Esses algoritmos têm como característica importante o fato de ser "computacionalmente inviável determinar a chave de decriptografia dado apenas o conhecimento do algoritmo de criptografia e da chave de criptografia."

Alguns algoritmos, como o de RSA, por exemplo, possui como característica o fato de "qualquer uma das duas chaves relacionadas pode ser usada para criptografia, com a outra usada para a decriptografia."

Conforme o autor afirma, o modelo de criptografia assimétrica possui cinco ingredientes:

1. **Texto claro:** Essa é a mensagem ou dados legíveis que são alimentados no algoritmo como entrada;
2. **Algoritmo de criptografia:** Algoritmo de criptografia realiza várias transformações no texto claro;
3. **Chaves pública e privada:** Esse é um par de chaves que foi selecionado de modo que, se uma for usada para criptografia, a outra será usada para decriptografia. As transformações exatas realizadas pelo algoritmo dependem da chave pública ou privada que é fornecida como entrada;
4. **Texto cifrado:** Essa é a mensagem codificada produzida como saída. Ela depende do texto claro e da chave. Para uma determinada mensagem, duas chaves diferentes produzirão dois textos cifrados diferentes;
5. **Algoritmo de decriptografia:** Esse algoritmo aceita o texto cifrado e a chave correspondente e produz o texto claro original.

O algoritmo de RSA é tido como um dos exemplos de técnicas de substituição dos algoritmos de criptografia assimétrica. Ele é considerado a técnica de uso geral mais aceita e implementada para a criptografia de chave pública.

De maneira mais resumida, o RSA pode ser ilustrado da seguinte maneira:

Para geração de chaves:

1. Selecione p e q (lembrando que os dois devem ser primos e diferentes entre si;
2. Calcular: $n = p \times q$;
3. Calcular: $\phi(n) = (p - 1) \times (q - 1)$;
4. Selecionar o inteiro e

   $mdc(\phi(n), e) = 1$; sendo que $1 < e < \phi(n)$;
5. Calcular d

   $d = e^{-1} (\text{mod } \phi(n))$;

Assim,

Chave Pública: PU = (e,n) e Chave Privada: PR = (d,n).

Para Criptografar:

Texto claro: $M < n$

Texto cifrado: $C = M^e \bmod n$

Para Decriptografar:

Texto cifrado: C

Texto claro: $M = C^d \bmod n$

6.3. Função de resumo (hash)

Uma função de resumo, segundo a Cartilha de Segurança para Internet (2013), pode ser definida como "um método criptográfico que, quando aplicado sobre uma informação, independente do tamanho que ela tenha, gera um resultado único e de tamanho fixo, chamado hash."

O hash é gerado de tal forma que não é possível realizar o processamento inverso para se obter a informação original e que qualquer alteração na informação original produzirá um hash distinto.

Em um cenário perfeito, deveria ser impossível que informações diferentes gerassem o mesmo hash, mas infelizmente isso não é fato. A probabilidade de dois valores diferentes gerarem o mesmo hash é chamada de probabilidade de colisão, ou seja, a probabilidade de dois valores diferentes, tendo hashs gerados por este determinado algoritmo, terem como saída o mesmo valor.

É possível utilizar o hash para:

- Verificar a integridade de um arquivo armazenado em um computador ou em *backups*;
- Verificar a integridade de um arquivo obtido da Internet (alguns sites, além do arquivo em si, também disponibilizam o *hash* correspondente, para que seja possível verificar se o arquivo foi corretamente transmitido e gravado);
- Gerar assinaturas digitais (descrita no capítulo 7).

Alguns exemplos de algoritmos de *hash*: SHA-1, SHA-256 e MD5.

A função de resumo pode ser comparada ao dígito verificador do CPF, explicam Monteiro e Mignoni (2007), já que se qualquer número do CPF for modificado, modificará também o dígito verificador. Essa função produz um resumo de tamanho fixo, que representa o conteúdo da mensagem.

Os autores comentam ainda que, com o resultado gerado por uma Função de resumo é possível garantir a integridade de uma mensagem, pois o resumo gerado no destino por uma função de resumo terá que ser igual ao resumo gerado na origem. Qualquer alteração que tenha sido feita reflete no resultado, indicando que a mensagem original foi alterada.

Exemplo:

> Alice quer enviar uma mensagem para Bob. A integridade da mensagem poderá ser garantida quando Alice enviar para Bob uma mensagem e o resumo da mesma criptografado com a sua chave privada. Bob irá decifrar o resumo com a chave pública de Alice e calcular novamente o resumo, baseado na mensagem recebida e realizando a comparação entre os dois resumos, se os dois estivem iguais, significa que não houve violação de informações e a integridade da mensagem é garantida. (MONTEIRO; MIGNONI, 2007, pag. 25).

7. ASSINATURA DIGITAL

Quando é necessário efetivar uma ligação entre uma informação que está impressa no papel e a assinatura propriamente dita, ocorre o ato de assinar um documento. Quando se assina à mão um documento, existe uma ligação entre a pessoa que assina e o documento, pois são impressas no papel as biocaracterísticas que cada indivíduo possui e que o torna único.

> Eletronicamente não é possível acontecer isso, já que não existe um meio físico que estabeleça uma ligação entre a pessoa que assina e a assinatura. O que acontece é a assinatura digital, que nada mais é que um algoritmo de autenticação, que possibilita o criador de um objeto, unir ao objeto criado, um código que irá agir como uma assinatura. (MONTEIRO; MIGNONI, 2007, pag. 26).

O processo de assinatura digital esta ilustrado na figura abaixo:

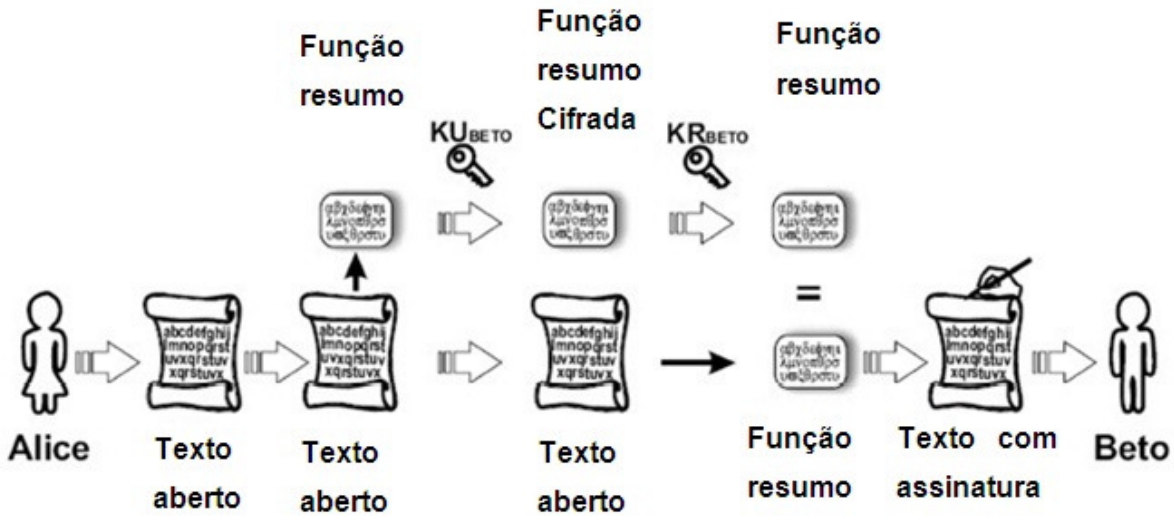

Figura 4: Processo de assinatura digital
(Fonte: Certificados digitais conceitos e práticas, página 26).

Explicação:

> Para criar a assinatura digital de um documento, Alice executa a função resumo dele e cifra o resultado com sua chave privada. O resumo cifrado é enviado para Beto juntamente com o documento. Beto decifra o resumo com a chave Pública de Alice, executa novamente a Função Resumo do documento e compara os dois resultados. Se forem iguais a assinatura é válida. (MONTEIRO; MIGNONI, 2007, pag. 26).

A assinatura digital, segundo a Cartilha de Segurança para Internet (2013) "permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isto e que ela não foi alterada."

A assinatura digital leva em consideração que apenas o dono deve conhecer a chave privada, assim, se ela foi usada para codificar uma informação, o único que pode ter feito isto seria o mesmo.

Usa-se a chave pública para realizar a verificação da assinatura, pois se o texto foi codificado com a chave privada, a decodificação só poderá ser feita utilizando a chave pública correspondente.

Uma assinatura digital é um mecanismo de autenticação que permite ao criador de uma mensagem anexar um código que atue como uma assinatura. A assinatura é formada tomando o hash da mensagem e criptografando-a com a chave privada do criador. A assinatura garante a origem e a integridade da mensagem. (STALLINGS, 2007).

Ainda segundo o autor, uma assinatura digital é semelhante à assinatura escrita a mão e precisa ter as características descritas abaixo:

- Deve verificar o autor, a data e a hora da assinatura.
- Deve autenticar o conteúdo no momento da assinatura.
- Deve ser verificável por terceiros, para resolver disputas.

O autor ainda cita os seguintes requisitos para uma assinatura digital:

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

8. CERTIFICAÇÃO DIGITAL E HTTPS

A chave pública, segundo a Cartilha de Segurança para Internet (2013), pode ser divulgada livremente, porém isso pode ocasionar um sério problema: caso não tenha como comprovar a quem a chave pública pertence, pode-se pensar estar se comunicando com uma pessoa, de forma cifrada e segura, mas na verdade a pessoa pode ser um impostor.

Segundo a Cartilha de Segurança para Internet (2013), o certificado digital é "um registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave pública."

Pode ser comparado a um documento de identidade, no qual constam os dados pessoais e a identificação de quem o emitiu. A entidade responsável pela emissão e pela veracidade dos dados do certificado digital é uma Autoridade Certificadora (AC).

Um certificado digital pode ser emitido tanto por uma autoridade certificadora quanto emitido pela própria pessoa ou instituição. Este certificado que não é assinado por uma AC recebe o nome de certificado auto-assinado. É possível encontrar este tipo de certificado em dois momentos:

- Quando a organização é uma AC Raiz, assim ela assina seu próprio certificado. Como é o caso do Google, que assina seu próprio certificado;
- Quando alguma pessoa ou empresa gera seu próprio certificado utilizando alguma ferramenta de criptografia.

Os navegadores possuem uma lista das autoridades certificadoras existentes, sendo que no momento em que algum cliente acessa um site que usa um certificado auto-assinado, recebe um alerta devido ao não reconhecimento daquele certificado, conforme pode ser visto na figura abaixo:

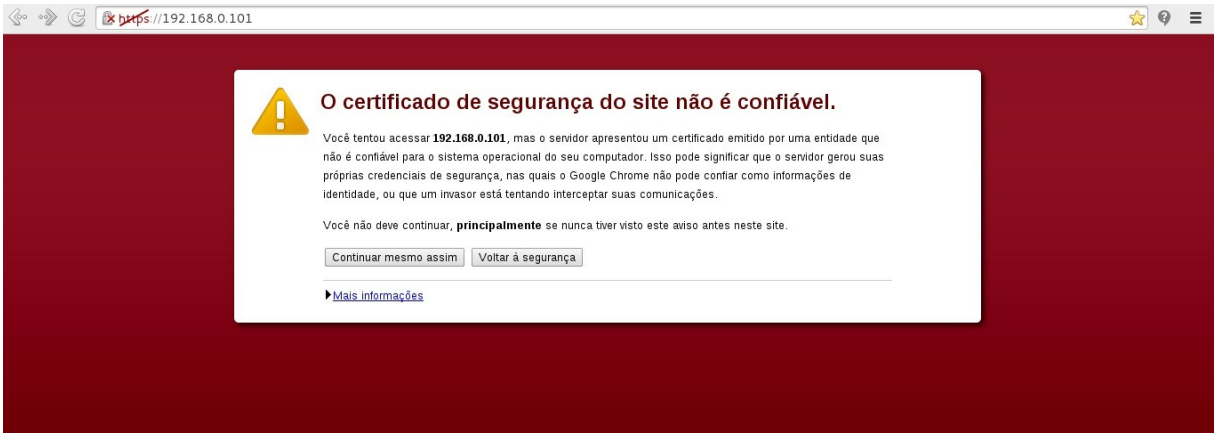

Figura 5: Certificado de Segurança não confiável

É importante salientar que é a existência de um terceiro confiável que garante segurança ao protocolo https, ou seja, as autoridades certificadoras assumem um papel essência nesse processo.

8.1 Autoridades certificadoras (AC)

Os autores Monteiro e Mignoni explicam autoridades certificadoras – AC como sendo:

> "...entidades de Confiança, que emitem certificados digitais para outras entidades, empresas, indivíduos, que precisam se identificar e garantir as suas Operações no mundo digital. Cada certificado digital emitido é certificado e garantido pela AC responsável pela sua Emissão. A AC recebe e autentica a solicitação de certificado, emite e chancela digitalmente o certificado e gerência os certificados emitidos. (MONTEIRO; MIGNONI, 2007, pag. 34).

O requerente ao solicitar o certificado, envia para a AC um formulário assegurado por ela mesma suas informações pessoais além da chave pública. A AC tem como responsabilidade verificar a veracidade dessas informações antes de emitir o certificado.

As ACs podem oferecer outros tipos de serviços, como: Autenticação de data, serviço de gerenciamento de chaves e LCR (Lista de Certificados Revogados).

O DPC – Declaração de Práticas de Certificação é o termo no qual devem ser expressas as responsabilidades, regras e obrigações legais da AC e dos usuários de certificados. As ACs estão divididas em três categorias:

- **Interna:** operacionalizada por uma instituição, para a Emissão de certificados digitais internos;
- **Terceirizada:** contratada por uma instituição ou empresa para emitir certificados internos e para clientes;
- **Autônoma:** governamental e privada, que comercializa Serviços de Certificação aos usuários finais.

8.2 Certificado digital - padrão x.509

O X.509, conforme afirma Stallings (2007), define uma estrutura para a provisão de serviços de autenticação pelo diretório X.500 aos seus usuários. O diretório pode servir como um repositório de certificados de chave pública. Cada certificado possui a chave pública de um usuário e é assinado com a chave privada de uma autoridade certificadora confiável. Além disso, o X.509 define protocolos de autenticação alternativos com base no uso de certificados de chave pública.

De maneira mais resumida, o X.509 é o padrão que determina o formato que um certificado digital deve seguir.

O autor ainda cita que o formato de certificado X.509 é usado em vários contextos, como por exemplo, em S/MIME, IP Security e SSL/TLS e SET.

O padrão X.509 não define o uso de um algoritmo específico, mas cita o RSA. Além disso, é esperado que o esquema de assinatura digital necessite do uso de uma função hash, mas novamente o padrão não especifica o uso de um algoritmo hash específico.

Abaixo estão descritos os principais campos de um certificado padrão X.509, segundo o autor Stallings (2007):

Nome do Campo	Descrição
Versão	Número da versão X.509 do certificado, tendo como valor válido apenas 1, 2 e 3.
Número de série	Identificador único do certificado e representado por um número inteiro. Não deve haver mais de um certificado emitido com o mesmo número de série por uma mesma autoridade certificadora.
Algoritmo de Assinatura	Identificador do algoritmo usado para assinatura do certificado pela autoridade certificadora.
Emissor	Nome da autoridade certificadora que produziu e assinou o certificado.
Período de Validade	Intervalo de tempo de duração que determina quando um certificado deve ser considerado válido pelas aplicações.
Assunto	Identifica o dono da chave pública do certificado. O assunto deve ser único para cada assunto no certificado emitido por uma autoridade certificadora.
Chave Pública	Contém o valor da chave pública do certificado junto com informações de algoritmos com o qual a chave deve ser usada.
Identificador Único de Emissor(opcional)	Campo opcional para permitir o reuso de um emissor com o tempo.
Identificador Único de Assunto(opcional)	Campo opcional para permitir o reuso de um assunto com o tempo.
Extensões (opcional)	Campos complementares com informações adicionais personalizadas.

Figura 6: Principais campos de um certificado padrão X.509

(Fonte: Criptografia e segurança de redes, página 303).

8.3 Http e Https

O HTTP (HyperText Transfer Protocol, ou Protocolo de transferência de Hipertexto,em português), segundo os autores Kurose e Ross (2008), trata-se de um protocolo de aplicação da Web que é implementado em um programa cliente e outro programa servidor. Esses dois programas conversam entre si por meio da troca de mensagens HTTP que é quem define também a estrutura que essas mensagens devem ter e a maneira como cliente e servidor as trocam.

Os autores também explicam que o HTTP usa o TCP como seu protocolo subjacente. O TCP fornece ao HTTP um serviço confiável de transferência de dados, dessa maneira o cliente primeiramente inicia uma conexão TCP com o servidor. Estabelecida a conexão, os processos do browser e do servidor acessam o TCP por meio de suas interfaces sockets.

A interface socket, pelo lado do cliente, pode ser definida como a porta entre o processo cliente e a conexão TCP; já pelo lado do servidor, ela é a porta entre o processo servidor e a conexão TCP.

Com o surgimento do comércio eletrônico, houve a necessidade de essa troca de mensagens entre cliente e servidor ser mais efetivamente segura. É nesse momento que entra o SSL como um protocolo seguro que, implementado ao HTTPS fornece essa segurança quando se trata de transferência de dados como, por exemplo, o número do cartão de crédito de um cliente.

O exemplo a seguir fornece base para a explicação do SLL e TSL:

Cenário típico de comércio eletrônico pela Internet.

> "Bob está navegando pela Web e encontra o site Alice Incorporated, que vende um produto. Esse site apresenta um formulário no qual Bob deve informar a quantidade desejada, seu endereço e o número de seu cartão de crédito. Bob registra essas informações, clica em 'apresentar' e, então, aguarda o recebimento do produto (por exemplo, pelo correio convencional); ele também espera receber a cobrança da mercadoria na próxima fatura do seu cartão de crédito." (KUROSE; ROSS, 2008, pag. 556).

Como afirmam os autores, toda a comodidade de poder comprar o que se deseja sem ao menos existir a necessidade de sair de casa, é algo muito bom, mas se durante esse processo não fossem tomadas algumas medidas de segurança, Bob poderia ter algumas surpresas desagradáveis:

- Um intruso pode interceptar o pedido de compra, obter informações sobre o cartão de crédito e, então, fazer compras na conta de Bob.

- O site pode apresentar a estrutura já conhecida do site de Alice Incorporated, mas na verdade ser mantido por uma terceira pessoa mal intencionada que se faz passar por

Alice Incorporated. Essa pessoa poderia simplesmente tomar posse do dinheiro de Bob e fugir. Ou ainda realizar outras compras e enviar a fatura para a conta de Bob.

Como meio de enfrentar esses e muitos outros problemas que possam surgir, o comércio eletrônico usa o protocolo SSL.

> A SSL (secure sockets layer - camada de sockets de segurança), originalmente desenvolvida pela Netscape, é um protocolo projetado para fornecer criptografia de dados e autenticação entre um cliente e um servidor Web. (KUROSE; ROSS, 2008, pag. 555).

O protocolo inicia com uma apresentação mútua entre cliente e servidor. Primeiro é negociado um algoritmo de criptografia (que pode ser o DES, por exemplo) e chaves, assim é realizada a autenticação do servidor para o cliente. Opcionalmente, ocorre a autenticação do cliente para o servidor. Quando concluída a apresentação mútua e iniciada a transmissão de dados, todos os dados são criptografados usando chaves de sessão negociadas durante a fase de apresentação mútua.

O comércio eletrônico amplamente utiliza o protocolo SSL que é implementado em praticamente todos os browsers populares e servidores Web. Além disso, é a base do protocolo TLS (transport layer security - segurança da camada de transporte). Os autores ainda explicam que:

> "A camada SSL pode ser vista como uma camada que se situa entre a camada de aplicação e a camada de transporte. No lado remetente, o protocolo SSL recebe dados, criptografa-os e direciona os dados criptografados a um socket TCP. No lado receptor, o SSL lê socket TCP, decripta os dados e os direciona à aplicação." (KUROSE; ROSS, 2006, pag. 555).

Na verdade em todas as compras realizada pela Internet com o uso de cartão de crédito, comentam Kurose e Ross (2008), a comunicação entre o browser do cliente e o servidor foi feita por meio do protocolo SSL. É possível verificar o uso do SSL pelo browser quando a URL iniciar-se por https: ao invés de http.

Os autores apresentam uma visão de alto nível da SSL, explicada em sete etapas:

1. O browser envia ao servidor a versão da SSL utilizada e também as preferências criptográficas, que são enviadas pois browser e servidor negociam qual algoritmo de chave simétrica será usado.

2. Agora é o servidor quem envia ao browser o número da versão da SSL, as preferências criptográficas e seu certificado digital.

3. O browser tem uma lista de Autoridades Certificadoras (ACs) totalmente confiáveis e uma chave pública para cada uma delas. Quando o browser recebe o certificado do servidor, ele verifica se a AC está na sua lista. Se o browser encontrá-la, utilizará sua chave pública para

validar o certificado e obter a chave pública do servidor. Caso contrário, o usuário será avisado do problema ocorrido e informado de que não será possível começar uma conexão segura criptografada e autenticada.

4. Uma chave de sessão simétrica é gerada pelo browser que a criptografa com a chave pública do servidor e envia ao servidor.

5. Uma mensagem é enviada ao servidor pelo browser informando que as futuras mensagens do cliente serão criptografadas com a chave de sessão. Ele envia então uma mensagem separada (criptografada) indicando que a sua parte na apresentação mútua está encerrada.

6. Agora o servidor envia uma mensagem ao browser informando que todas as mensagens futuras serão criptografadas com a chave de sessão. Ele também envia uma mensagem separada (criptografada) indicando que a sua parte na apresentação mútua está encerrada.

7. Nesse momento, a apresentação mútua está concluída e tem inicio a sessão SSL. Browser e servidor utilizam as chaves de sessão para criptografar e decriptar os dados que enviam um ao outro e para validar sua integridade.

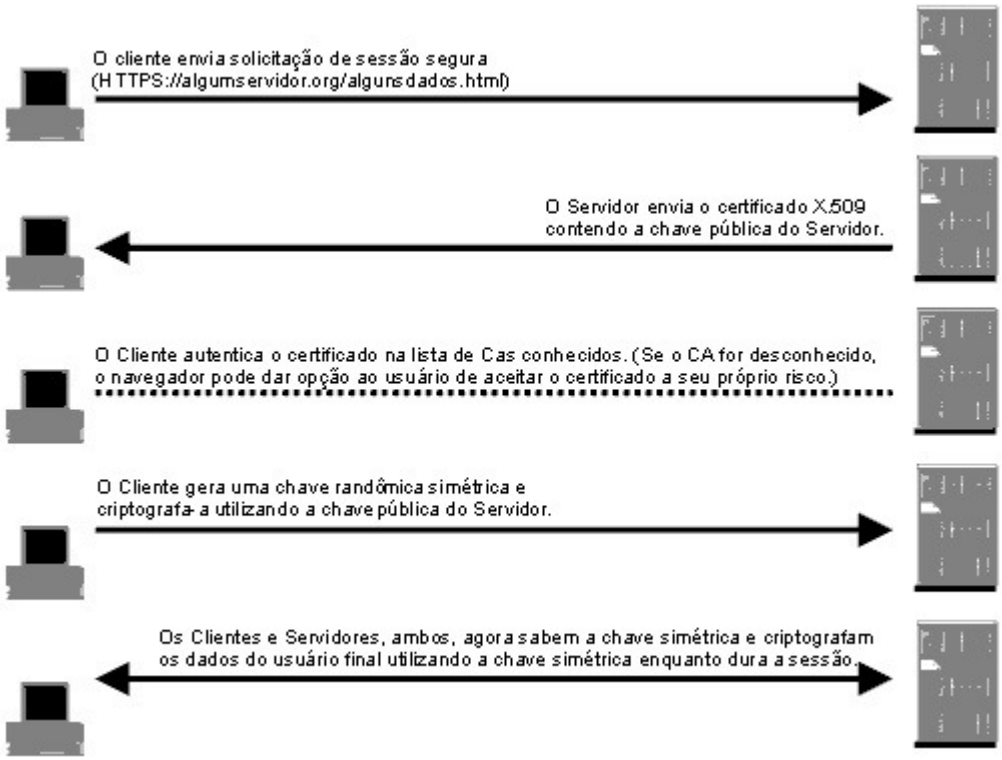

Figura 7: Protocolo de recebimento SSL

Existem ainda muitas outras etapas na apresentação mútua, mas de maneira mais geral as principais são estas apresentadas acima. Kurose e Ross (2006) comentam ainda que, a SSL pode ser usada para outras transações financeiras além das compras feitas com cartão de crédito, como home banking e comércio de ações.

9 PESQUISA DE CAMPO

A presente pesquisa de campo foi realizada levando em consideração dois mecanismos de pesquisa para alcançar o objetivo esperado. O primeiro trata-se de um questionário contendo perguntas pertinentes ao campo de estudo que é direcionado ao uso da criptografia na garantia da segurança da informação em um site de E-commerce. O mesmo foi respondido por um profissional de TI que atua na gerência do desenvolvimento de sites de E-commerce.

O segundo mecanismo mencionado acima trata-se de uma pesquisa realizada nos sites dos cinco E-commerces mais acessados na atualidade com o intuito de colher informações como: algoritmos de criptografia utilizados, autoridades certificadoras, entre outras que serão descritas com detalhes nas próximas seções.

9.1 Detalhamento da Pesquisa

A empresa escolhida para participar do estudo de caso desse trabalho optou por ter seu nome preservado, assim como o nome do gerente que respondeu ao questionário.

Trata-se de uma empresa que atua no ramo de desenvolvimento de software, principalmente voltados à WEB, juntamente a isso está o desenvolvimento dos E-commerces. Um cliente ao comprar o desenvolvimento do seu site, opta por inserir ou não o comércio eletrônico a ele. O formulário de pesquisa respondido pelo gerente pode ser visto no APÊNDICE A.

Com a finalidade de complementar o questionário respondido, houve também uma pesquisa realizada na Internet buscando um ranking dos cinco sites de E-commerce mais acessados no Brasil.

Rank	Sites	% de participação
1°	Mercado Livre/ Mercadolivre.com.br	10.11%
2°	Americanas /Americanas.com.br	4.80%
3°	Buscapé / buscape.com.br	3.47%
4°	Dafiti / Dafiti.com.br	3.45
5°	Bom Negócio / Bomnegocio.com	3.05%

Figura 8: Ranking dos cinco sites de E-commerce mais acessados no Brasil
Disponível em: http://top10mais.org/top-10-maiores-sites-de-compras-e-commerce-do-brasil/. Acesso: 12/11/2013 – às 18h.

Nesta pesquisa buscou-se encontrar informações como quais autoridades certificadoras esses sites utilizam, quais algoritmos de criptografia são utilizados por eles, com o objetivo de realizar uma comparação entre os dados colhidos e as informações apresentadas ao longo desse trabalho.

É possível encontrar essas informações acessando a parte segura do site, geralmente a área de login que passa a trafegar os dados através da conexão HTTPS. Clicando sobre o cadeado que aparece antes da palavra HTTPS, na segunda aba chamada Conexão, existe um link Informações do Certificado que quando clicado exibe a seguinte caixa de informações:

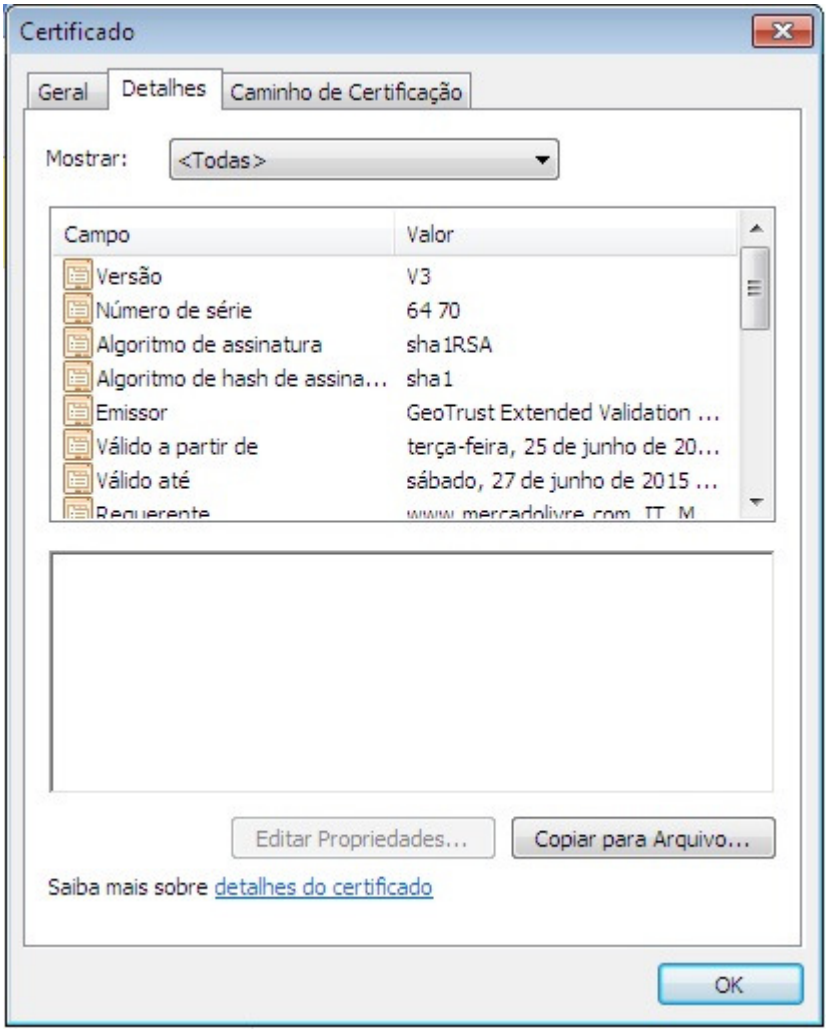

Figura 9: Informações do Certificado

Disponível em: https://www.mercadolivre.com/jms/mlb/lgz/login?syi=true&new_syi=true&go=https%3A%2F%2Fsyi.mercadolivre.com.br%2Fsell. Acessado em: 12/11/2013 – às 21:30h.

Navegando entre as abas é possível encontrar todas as informações que estão presentes na **Tabela 3: Dados Coletados**, do próximo capítulo.

9.2 Resultados e Discussões

Esta seção busca apresentar uma relação dos dados coletados através dos dois mecanismos de pesquisa mencionados anteriormente. Tais informações encontram-se discriminadas na Tabela 3: Dados Coletados.

Além disso, ela está subdividida em três categorias:

- **Algoritmos de Criptografia:** relaciona os tipos de algoritmos de criptografia que são usados pelos sites envolvidos na pesquisa, assim como os mencionados como resposta no questionário aplicado a empresa de desenvolvimento WEB;
- **Autoridades Certificadoras:** da mesma maneira cita as autoridades certificadoras presentes nos cinco principais sites de E-commerce citados no ranking. E também as ACs presentes nas respostas do questionário aplicado a empresa de desenvolvimento WEB.
- **Outros Aspectos:** engloba os demais aspectos pertinentes apenas ao questionário respondido pelo gerente de desenvolvimento de sites de E-commerce.

Tabela 3: Dados Coletados

Nomes / Perguntas	Mercado Livre	Americanas	Buscapé	Dafiti	Bom Negócio	Questionário
Algoritmos de Hash para Assinatura	SHA-1	SHA-1	SHA-1	SHA-1	SHA-1	SHA-1
Algoritmo de criptografia assimétrica	RSA (2048 bits)	RSA (2048 bits)	RSA (2048 bits)	RSA (2048 bits)	RSA (2048 bits)	X
Algoritmo de criptografia simétrica	RC4_128	AES_256_CBC	RC4_128	RC4_128	RC4_128	DES e AES
Autoridades Certificadoras (ACs)	Equifax Secure Certificate Authority	Baltimore Cyber Trust Root	GlobalSign Root CA	AddTrust External CA Root	VeriSign Class 3 Public Primary Certification Authority – G5	CertiSign
Dados Armazenados	X	X	X	X	X	Senha dos usuários
Informações que trafegam sob HTTPS	Informações de login (autenticação)	Informações de login (autenticação)	Informações de login (autenticação)	Informações de login (autenticação)	Informações de login (autenticação)	Dados de clientes
Treinamento de Funcionários	X	X	X	X	X	Apenas Engenheiros de Software
Principais Ameaças	X	X	X	X	X	Lista da OWASP com as 10 principais ameaças

9.2.1 Algoritmos de Criptografia

Conforme informações encontradas na pesquisa realizada nos cinco sites de comércio eletrônico mais acessados no Brasil, a grande maioria utiliza como algoritmo de hash de assinatura o SHA-1, assim como o RSA para criptografia de chave pública. Já na empresa que trabalha com o desenvolvimento de sites de E-commerce, são utilizados os algoritmos DES, AES e também o já mencionado SHA-1.

Como pode ser observado, o RSA é muito utilizado atualmente, principalmente por ser um dos métodos mais conhecidos de criptografia de chave pública, além de ser um dos algoritmos mais seguros de encriptação de informações.

Em 1999, o NIST (National Institute of Standards and Tecnology), lançou um concurso para adotar um novo algoritmo de criptografia simétrica para proteger informações confidenciais. Este novo algoritmo escolhido que seria chamado de AES, substituiria o DES, que como pode ser notado também é mencionado na tabela de dados coletados.

Por sua vez, o DES acabou sendo, por motivos de falta de segurança, também substituído pelo algoritmo 3DES que possui duas características principais que garantem o seu uso por um bom tempo: primeiro que ele possui uma chave de 168 bits, o que contorna a vulnerabilidade do ataque de força bruta ao DES. Segundo que o algoritmo básico no 3DES é igual ao do DES, este algoritmo foi submetido a mais análises detalhadas que qualquer outro algoritmo de criptografia por um longo período, e nenhum ataque criptoanalítico eficaz contra o algoritmo, inclusive o ataque de força bruta, obteve sucesso. (STALLINGS, 2007).

Por esse motivo é possível concluir que provavelmente o algoritmo realmente utilizado pela empresa de desenvolvimento WEB, seja o 3DES, umas vez que o uso do algoritmo DES foi descontinuado, como explicado acima.

O algoritmo de criptografia AES acaba sendo mais leve que o 3DES, o mesmo é capaz de cifrar em blocos de 128 bits com chaves de 128, 192 ou 256 bits, além de ser também mais rápido que o 3DES, apesar dessas características não deixa de ser seguro.

Outro algoritmo muito encontrado tanto na pesquisa quanto no questionário, é o de hash SHA-1. Apesar de ser muito utilizado, é facilmente possível encontrar uma de suas falhas de segurança realizando um procedimento simples na Internet:

1. Acessar o site: http://www.sha1-online.com/
2. Digitar uma palavra e gerar o seu hash usando o algoritmo SHA-1;

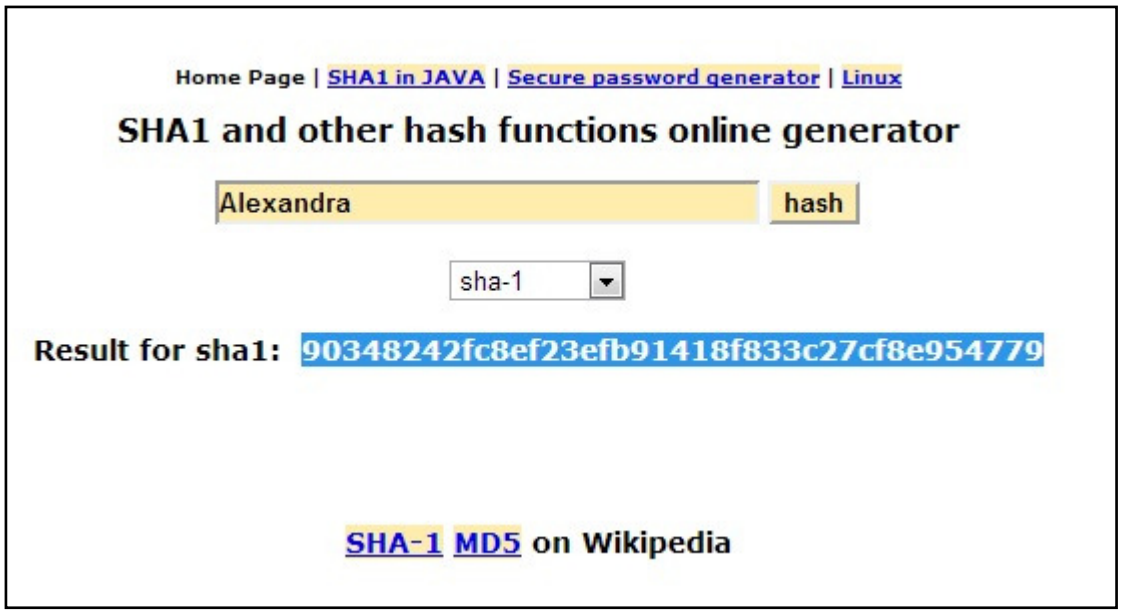

Figura 10: Criptografia usando SHA-1

3. Copiar o hash e acessar outro site: http://www.md5decrypter.co.uk/sha1-decrypt.aspx

4. Colar no local indicado, digitar corretamente o Captcha e decriptografar.

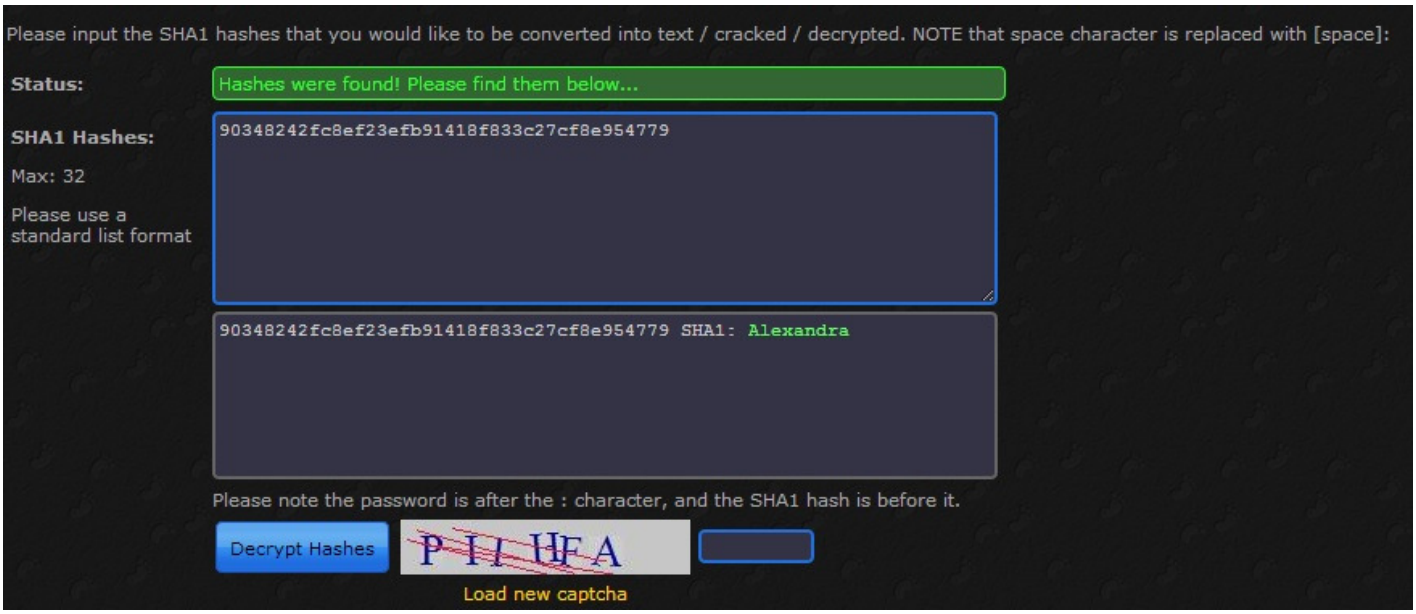

Figura 11: Decriptografia usando SHA-1

Com esse procedimento fica fácil perceber que existem métodos prontos disponíveis na Internet que realizam a criptografia de uma informação, assim como sua decriptografia, todas utilizando o SHA-1.

9.2.2 Autoridades Certificadoras

Os cinco sites de E-commerce mais acessados no Brasil possuem autoridades certificadoras distintas, assim como a autoridade certificadora que a empresa desenvolvedora de sites de comércio eletrônico utiliza, sendo escolhida na época através de uma pesquisa que constatou que 80% dos sites de bancos utilizavam certificados da CertiSign.

A CertiSign é uma empresa que atua no ramo de certificação digital digital, situada em São Paulo, pioneira nessa atividade no país há 16 anos. Foi a terceira autoridade certificadora a entrar em operação no mundo e a primeira da América Latina. A rede Certisign, possui mais de 950 pontos de atendimento distribuídos pelo país e alcançou a marca de mais de três milhões de certificados emitidos.

A tecnologia da certificação digital tem sido aplicada por organizações públicas e privadas para desmaterialização dos processos o que gera melhoria na prestação de serviços e redução de custos com insumos para impressão de documentos, com recursos humanos e com estoque de documentação física. O Selo de Site Seguro Certisign é reconhecido pelos usuários brasileiros de internet como a maior referência de confiança para relacionamento na rede.

9.2.3 Outros Aspectos

Segundo respostas encontradas no questionário, algumas informações trafegam sob a conexão HTTPS, já que são mais sensíveis e necessitam serem mantidas em segurança. Tais informações são de maneira geral dados de clientes, como informações pessoais, de acesso, de contrato, etc. Caso, acidentalmente, essas informações forem acessadas por uma pessoal mal intencionada, muitos problemas podem surgir, por essa razão trafegam por um canal seguro, como explicado na categoria 8.3 HTTP e HTTPS desse trabalho.

A empresa é autorizada a armazenar em seu banco de dados informações de seus clientes, mas dados como o número de cartão de crédito não podem ser guardados. A empresa armazena as senhas dos seus usuários de maneira criptografada a fim de garantir a segurança das mesmas. Os algoritmos utilizados nesse processo são: DES, AES e SHA-1.

Informações como essa são passadas aos funcionários responsáveis pela segurança do site de E-commerce, no caso os Engenheiros de Software, através de treinamentos aos quais os mesmos são submetidos.

Para finalizar, o gerente de desenvolvimento de sites de comércio eletrônico cita que durante a fase de desenvolvimento, foi realizada uma pesquisa e encontrou-se um relatório da OWASP que listava os dez principais ataques realizados em sites dessa categoria nos últimos dez anos. Dessa maneira, trabalham para garantir a segurança em relação a eles.

10 CONSIDERAÇÕES FINAIS

Este trabalho buscou apresentar de forma concisa informações pertinentes ao tema escolhido como pesquisa. Utilizou-se de pesquisas realizadas através de livros que buscavam principalmente definições e conceitos dos principais assuntos abordados ao longo do mesmo, assim como dois outros métodos de pesquisa que permitiram colher dados significativos de ambientes reais a fim de serem utilizados em discussões e comparação de resultados.

Com a sua finalização, é possível concluir que a segurança dos dados que clientes confiam aos sites de E-commerce é um dos fatores mais importantes, se não for o mais importante na decisão de qual comércio eletrônico optar na hora de realizar compras on-line. Preocupados com essa questão, donos de sites de E-commerce confiáveis buscam cada vez mais mecanismos que garantam tal segurança.

O uso da criptografia acaba sendo crucial, já que dessa maneira é possível preservar as informações dos clientes de maneira que terceiros mal intencionados não consigam ter acesso fácil a informações que devem ser sigilosas. A criptografia está presente nas definições deste trabalho, assim como seus termos encontram-se mencionados no questionário respondido pelo gerente de desenvolvimento de sites de E-commerce e também nos próprios sites que compõem o ranking dos cinco sites de comércio eletrônico mais acessados no Brasil.

Apesar de este trabalho abordar o uso da criptografia na garantia da segurança da informação em sites de E-commerce, é importante salientar que a segurança em transações online estão relacionadas a outros fatores: letramento informacional, que permite as pessoas saberem utilizar as informações e evitarem ataques de engenharia social; programação segura, que evite invasões através do código fonte do site, armazenamento seguro e utilizando a criptografia, entre outros, que podem ser melhor explorados em trabalhos futuros.

REFERÊNCIAS

Cartilha de Segurança para Internet. Disponível em: <http://cartilha.cert.br/criptografia/>. Acesso em: 25 de set. 2013.

COELHO, Flávia Estélia Silva; ARAÚJO, Luís Geraldo Segadas de. **Gestão da Segurança da Informação – NBR 27.001 e 27.002.** 12.ed. Disponível para download, 2013.

KOTLER, Philip; KELLER, Kevin Lane. **Administração de marketing.** 12.ed. Pearson, 2006.

KUROSE; James F.; ROSS, Keith W.. **Redes de computadores e a Internet – Uma abordagem top-down.** Pearson, 2006.

LAUDON, Kenneth; LAUDON, Jane. **Sistemas de Informação Gerenciais.** 12.ed. Pearson, 2011.

LIMEIRA, Tania M. Vidigal. **E-marketing. O marketing na Internet com casos brasileiros.** Saraiva, 2007.

MONTEIRO, Emiliano S.; MIGNONI, Maria Eloisa. **Certificados Digitais – conceitos e práticas.** Brasport, 2006.

Norma Brasileira ABNT NBR 14724. Disponível em: <http://www.ufvjm.edu.br/site/revistamultidisciplinar/files/2011/09/NBR_14724_atualizada_abr_2011.pdf>. Acesso em: 27 de set. 2013.

STALLINGS, William. **Criptografia e segurança de redes – princípios e práticas.** 4.ed. Pearson, 2007.

APÊNDICE A – Questionário destinado a entrevista com profissional da área de gestão de sites de E-commerce

1. **Em geral, em um site de e-commerce que vocês desenvolvem, quais informações trafegam sob uma conexão https?**
   Dados de cliente, como dados pessoais, acesso, contrato e etc.

2. **Quais algoritmos geralmente são usados em um projeto de E-commerce que vocês desenvolvem?**
   DES, AES e SHA-1

3. **Existe uma autoridade certificadora específica que fornece os certificados digitais utilizados pelo seu E-commerce? Por que a escolha dela?**
   Sim, CertiSign, na época da escolha fizemos uma análise rápida nos sites de bancos, e cerca de 80% utilizavam certificados da CertiSign.

4. **Quais informações são guardadas geralmente em banco de dados de forma criptografada? Quais algoritmos mais usados por vocês neste processo?**
   Apenas a senha dos usuários, dados como cartão de crédito não ficam armazenados na nossa base de dados. Os algoritmos são DES, AES e SHA-1.

5. **Os seus funcionários responsáveis pelo desenvolvimento e manutenção dos sites de E-commerce são submetidos a treinamentos?**
   Normalmente os responsáveis pela segurança são os Arquitetos de Software, que são devidamente treinados. Outras pessoas do time não recebem treinamentos.

6. **Quais as principais ameaças as quais um site de E-commerce está exposto quanto a sua segurança?**
   Durante a fase de planejamento pegamos o relatório da OWASP que listava os 10 principais ataques utilizados nos últimos anos, e trabalhamos para estarmos seguros deles.