Fundação João Pinheiro
Escola de Governo de Minas Gerais
Mestrado em Administração Pública:

Criptologia

Uma ciência fundamental para tratamento de informações sigilosas

SUMÁRIO

INTRODUÇÃO

Desde que as sociedades humanas estruturam-se tem havido a necessidade de se ocultar informações entendidas, cada uma a seu tempo, como segredos. Sejam segredos familiares, segredos sentimentais, segredos pessoais, segredos religiosos, ou segredos militares ou governamentais. Tão forte quanto a necessidade de guardar estes segredos é o desejo de outros de desvendar esses mesmos segredos. Seja por dinheiro, poder, vingança, curiosidade, arrogância, ou qualquer outro sentimento essa tem sido uma batalha que, ao longo dos anos vem sendo travada entre aqueles que querem guardar segredos e os que querem desvendar esses segredos.

Na atualidade, com o avanço cada vez maior dos poderes das Redes de Computadores, as distâncias entre os vários agentes distribuídos ao longo do planeta tendem a ficar menores. À medida que isto acontece a tomada de decisões ressente-se em maior grau da velocidade em que estas decisões são tomadas. Contudo a qualidade das decisões tomadas continuam sendo determinadas pela qualidade das informações disponíveis para tal.

Neste contexto a disponibilidade, a qualidade e o controle sobre a informação ganham outro grau de magnitude na importância estratégica que esta sempre teve para os governos e para as empresas. Assim quanto maior o fluxo de informações em redes de telecomunicações, ou maior a quantidade de informação armazenada em meios computacionais, maior é a necessidade de empresas, governos (e até de pessoas físicas) de se protegerem contra uma velha ameaça que agora ganha outras feições com desenvolvimento da informática: o furto e a adulteração de informação.

Tendo em vista a necessidade de se criar ferramentas capazes de proteger a informação e de prover segurança aos documentos armazenados e transmitidos pelas organizações através do mundo, tem-se a motivação para se estudar Criptografia.

O que é Criptologia

A palavra Criptologia deriva da palavra grega *kryptos* (oculto) e *logos* (estudo). Este campo de estudo mais abrangente abarca as disciplinas da **Criptografia** e da **Criptoanálise** combinadas.

Um conceito que possa definir **Criptologia** em poucas palavras é que ela seria o estudo das escritas secretas.

Na verdade Criptologia é o estudo de **Códigos** e **Cifras** (não necessariamente secretos). Mensagens ocultas que não são nem codificadas nem cifradas são, simplesmente, ocultas. A técnica da tinta invisível é um exemplo de mensagem oculta.

Um **código** é um sistema preestabelecido 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, "ôi" em português equivale a "*hola*" em espanhol ou "*hi*" em inglês. A maioria dos códigos funcionam com um "livro de códigos" onde estão relacionadas as equivalências, como se fosse um dicionário.

Já a palavra **cifra** vem do hebraico *saphar*, que significa "dar número". A maioria das cifragens são intrinsecamente sistemáticas, freqüentemente baseadas em técnicas de sistemas numéricos.

Formada a partir da concatenação do termo grego *kryptos* (escondido, oculto) e da palavra *grapho* (grafia, escrita), a Criptografia apresenta-se como a ciência de escrever em códigos ou em cifras, ou seja, uma ciência capaz de prover meios através dos quais seja possível transformar um texto “em claro” (inteligível) em um texto “cifrado” (ininteligível).

Ao seu turno, o termo Criptoanálise é o estudo de como “quebrar” os mecanismos criptográficos, podendo assim revelar o conteúdo das mensagens cifradas.

Para muitos autores o 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 historia.

Dentro da Criptologia a ciência da Criptografia tem como seu objeto de estudos os processos de **Encriptação** ou seja, a transformação dos dados em uma forma que torna impossível a sua leitura sem o apropriado conhecimento. O seu propósito é assegurar privacidade da informação mantendo o entendimento da mensagem oculto de qualquer um a qual ela não seja destinada. A **Decriptação**, por outro lado, é o reverso da Encriptação; é a transformação de dados encriptados novamente em uma forma inteligível.

Encriptação e decriptação geralmente requerem o uso de uma informação secreta que atua como uma chave. Para alguns mecanismos de encriptação a mesma chave é usada para tanto para a cifragem dos dados quanto para a sua decifragem; para outros mecanismos as chaves usadas para a encriptação e decriptação são diferentes.

Na atualidade a aplicação da criptografia está ligada a uma propriedade tão fundamental de nossas vidas como a privacidade: a *Autenticação.* O uso da autenticação é algo comum no nosso cotidiano – quando assinamos algum documento – e como nos movemos para um mundo onde as decisões e contratos são feitos de forma eletrônica, necessitamos ter técnicas eletrônicas de provimento de autenticação.

A Criptografia provê mecanismos para tais procedimentos. Uma assinatura digital vincula um documento ao proprietário de uma chave particular, enquanto um "selo" digital vincula um documento ao momento de sua criação em um momento particular. Estes mecanismos criptográficos podem ser usados para o controle de acesso a um disco compartilhado, a uma instalação de alta segurança ou um canal privado de TV.

O campo da criptografia encobre ainda outros usos. Com o uso de ferramentas criptográficas básicas é possível a construção de elaborados esquemas e protocolos que permitem pagamentos com o uso do "dinheiro eletrônico", para comprovarmos nosso conhecimento de certas informações sem que tenhamos de revela-la.

Contudo, mesmo que o uso moderno da criptografia esteja crescendo em áreas diversas, a criptografia continua sendo fundamentalmente baseada em técnicas inspiradas em tipos de lógicas e problemas de difícil solução.

Algo sobre a história da Criptografia (e cômico sobre a Criptografia no Brasil)

A criptografia é tão antiga como a escrita. Desde que o *homo sapiens* iniciou sua jornada sobre este planeta, o mesmo tem necessitado comunicar-se com seus semelhantes mas em outras ocasiões não quer que outros se entendam. Em situações de guerra nenhum comandante deseja que seus inimigos conheçam suas estratégias caso viesse interceptar uma mensagem.

A despeito do fato de existirem pessoas cuja grafia faria qualquer médico se morder de inveja (e em muitos casos a própria pessoa não entende o que escreveu) esta "técnica" não pode ser classificada como Criptografia.

Os espartanos foram os primeiros a utilizar um sistema de criptografia militar, por volta do século V a.C. Eles cifravam e ocultavam mensagens usando um bastonete que eles chamavam de *skytalh* (**escútala**) e uma cinta enrolada nele, na qual a mensagem era escrita. A cinta era desenrolada e enviada ao destinatário, o qual tinha outra escútala, de igual diâmetro. Ele então enrolava de novo a cinta e lia a mensagem [Ric00]. Se o bastonete fosse do tamanho errado, a mensagem seria ilegível.

O general romano Júlio César também relatou o uso de mensagens cifradas em seu livro, sobre as Guerras Gálicas. A ele é atribuída a criação de um sistema simples de substituição de letras, que consistia em escrever o documento codificado com a terceira letra que seguiria a ela no alfabeto. Assim a letra A era substituída pela D, e a B pela E e assim sucessivamente. Por conseguinte seu nome foi dado a qualquer tipo de método de cifragem semelhante ao que usou:

```
alf. puro:   a b c d e f g h i j k l m n o p q r s t u v x y w z
alf. César:  D E F G H I J K L M N O P Q R S T U V X Y Z A B C D
```

Na Idade Média. os alquimistas, de forma geral, ficaram bastante conhecidos por escreverem suas receitas de forma cifrada.

Pulando alguns séculos, Leonardo da Vinci escreveu seus projetos, na época mirabolantes (e passíveis de serem premiados com um churrasco promovido pela Inquisição) através da escrita em forma reversa (ou especular), podendo ser lida colocando-se o original de frente a um espelho.

Nostradamus foi outro que também se preocupou com a possibilidade de virar churrasco e desenvolveu suas centúrias numa linguagem que até hoje tenta se descobrir. Descobre-se o que ele estava falando, na grande maioria das vezes, depois do fato ter acontecido.

Não obstante se atribui ao abade Johannes Trithemius as melhores referências sobre a criptografia neste período[Leo01]. Este religioso escreveu em 1530 a obra denominada “Poligrafía”, o primeiro livro impresso sobre o tema. Trithemius introduziu o conceito de Tabela Ajustada, na qual o alfabeto normal é permutado para codificar as mensagens.

São lendários, também, os mapas de tesouro escondidos durante os séculos XVII e XVIIII. Neles os piratas supostamente encriptavan a localização de tesouros, baseando-se principalmente em métodos de substituição de alfabeto.

O principal uso da criptografia na era moderna tem sido militar. Em 1917, por exemplo, o serviço de Inteligência Naval de Inglaterra 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 de Alemanha na Primeira Guerra Mundial. Em troca, os mexicanos receberiam os territórios de Novo México, Arizona e Texas, caso resultassem vencedores. O texto conhecido como Telegrama Zimmermann levou os norte americanos a participar dessa guerra contra Alemanha [Leo01].

Já na II Guerra Mundial os códigos da máquina Enigma, usada pelos mesmos alemães, foram quebrados pelos analistas norte americanos, o mesmo se dando com os códigos usados pelos japoneses.

Os alemães, na primeira guerra venceram os russos facilmente, por conta disso. Os EUA 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.

A aparição dos computadores, e a disponibilização de capacidade de processamento sempre crescente, fez 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 que seja particularmente difícil de ser rompido. Entretanto o DES depende de que tanto o remetente da mensagem como o receptor conheçam a chave com a qual ela foi encriptada. Neste sentido este mecanismo se parece com o sistema usado pelos espartanos, que necessitavam ter o cilindro com o qual se havia codificado o texto para que o mesmo pudesse ser lido. No caso do DES este “cilindro” se denomina “chave”. A segurança desta chave vai depender de seu tamanho. Quando temos uma mensagem cifrada ha um número “n” de possibilidades de descobrir a chave com a qual ela foi encriptada. Assim, a confiabilidade de uma chave depende de que esse número “n” seja tão grande que um “atacante” demande demasiado tempo para testar todas as possibilidades. Uma chave de 56 bits é atualmente o padrão no DES. Para ler uma mensagem cifrada com o DES é necessário usar a mesma chave com a qual ela foi encriptada.

Para fins de transações comerciais virtuais esta propriedade se torna pouco prática e insegura, porque a própria chave deve ser transmitida por meios eletrônicos.

Para resolver este problema se criou a criptografia de chave pública. Neste sistema existem duas chaves: uma privada e outra pública. Quando A quer enviar uma mensagem para B, este solicita sua chave pública (que como o nome indica pode ser conhecida por todo mundo). Com a chave pública A encripta a mensagem e a envia a B, que logo procede a descifragem aplicando sua chave privada, que não deve ser conhecida de mais ninguém. A vantagem deste método é que não requer que ambas as partes conheçam as chaves privadas deforma mútua.

As implementações mais conhecidas da criptografia de chave pública é o RSA e o PGP. Em 1977, Rivest, Shamir e Adelman desenvolveram o RSA e publicaram o algoritmo de encriptação a pesar da oposição do governo norte americano, que considera a criptografia um assunto de estado.

Mais tarde a patente do RSA e dada ao Instituto Tecnológico de Massachusetts (MIT) que logo a cede a um grupo denominado PKP (*Public Key Partners*). Em 1991, o programador Phil Zimmermann autoriza a publicação em boletins eletrônicos e grupos de noticias de um programa por ele desenvolvido e batizado como *Pretty Good Privacy* ou PGP. O PGP tem como base os algoritmos do RSA publicados em 1978.

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. A pesar 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.

A versão americana doPGPpode ser baixado a partir da URL http://web.mit.edu/network/pgp-form.html mas é necessário ser cidadão residente dos Estados Unidos ou Canadá para poder usá-lo.

Ao mesmo tempo, os 12 volumes (mais de 6.000 páginas) que contem o código fonte do PGP internacional, estão disponíveis na Página Internacional do PGP na URL http://www.ifi.uio.no/~staalesc/PGP/.

Mas por que é tão importante a criptografia na Internet? Se considerar-mos que atualmente os volumes de transações *on-line* apresentam perspectivas de movimentar centenas de milhões de dólares por ano entendemos a necessidade de tornar este canal de informação o mais seguro possível. A rede não é, na atualidade, suficientemente confiável.

O protocolo principal pelo qual se transmite a informação que viaja pela rede (TCP/IP, *Transfer Control Protocol/Internet Protocol*) não variou em sua essência desde a criação da Internet. Assim quando enviamos uma mensagem esta será dividida em vários datagramas, que viajarão de modo independente, para depois serem recompostos no computador de destino, sem que o receptor final possa saber que rota tomou cada um deles. Como nenhum destes datagramas está encriptado, qualquer um que os pegue em seu caminho pode le-los sem problema.

Desta forma a criptografia aparece como facilitador para o crescimento do comércio eletrônico. A idéia, portanto, é encontrar um sistema onde os dados comerciais e financeiros possam viajar de um modo seguro pela rede.

Na atualidade o SET (*Secure Electronic Transaction*) é o sistema utilizado para viabilizar este propósito. O SET é um sistema de criptografia baseado no mecanismo de chave pública e no qual participam as mais importantes companhias de cartões de crédito de nível mundial (Visa, Master Card e American Express) e várias empresas de informática (Microsoft, IBM, Netscape, dentre outros). SET cobre os três princípios básicos para assegurar o crescimento do comércio eletrônico:

- Que a informação transmitida seja confidencial;
- Que as transações ocorram total integridade, e sem perda de dados;
- Que compradores e vendedores possam ser autênticos.

Durante os períodos da ditadura no Brasil, coisa algo freqüente por aqui, sempre houve censura aos meios de comunicação. Nestes períodos não podia se dar o nome aos bois, não podia se falar palavras indevidas, não podia se contar o que estava acontecendo. O repórter que quisesse dar um colorido a sua matéria ou transmitir algo diferente, de conteúdo mais ideológico ou subversivo tinha que mascarar o conteúdo, para ver se "driblava" o censor, mas não o leitor. Se a notícia fosse muito forte, podia acontecer de toda a tiragem do jornal ser pura e simplesmente confiscada. É fácil de encontrar lembranças desse período, basta procurar em livros antigos, a mensagem "texto integral, sem cortes". Para garantir a vendagem dos jornais, durante o período da ditadura, alguns editores começaram a editar receitas culinárias. Imaginem jornais, do porte do Estado de São Paulo ou o Globo fazendo isso: na primeira pagina, ao invés de uma notícia sobre a queda de um ministro publicassem uma receita:

"Rabada á moda Magri”

Primeiro pegue uma carne de segunda ou de terceira, guarde o caldo, misture com um molho Volnei...".

Algumas vezes, os leitores escreviam cartas reclamando que as receitas não funcionavam, apesar do aviso de que essas receitas não significavam absolutamente nada. E o pior é que os jornais duplicavam a receita, quando imprimiam este tipo de coisa. Na musica popular, isso acontecia também, até a o artista ser obrigado a se asilar, antes de enfrentar cadeia. Dizer que determinado artista queria ou não transmitir essa ou aquela mensagem é algo meio forte. Mas era proibido abordar uma serie de temas, durante aquele período do milagre brasileiro, como a pobreza ou a repressão. Só prá se ter uma idéia, durante o bicentenário da independência dos EUA, comemorado em 1976, foi proibida a publicação de trechos da declaração dos direitos do homem nos meios de comunicação (coisas como "Todo homem tem direito a liberdade de opinião e expressão" eram consideradas subversivas). Pode-se

encontrar montes de mensagens de duplo sentido, na musica daquele tempo. Na literatura, o romance Zero, do Ignacio de Loyola Brandão, um verdadeiro diário de um "terrorista", que passou incólume pela censura, virou um sucesso de vendas e... foi proibido depois que esgotou e a censura descobriu do que se tratava de fato.

O livro "*The Codebreakers*", do autor americano David Kahn, é um livro obrigatório no que se refere a historia da criptografia. Lendo o livro, descobre-se que existiam no passado clubes dedicados ao estudo dessa matéria como *hobby* na maioria dos países centrais da época, desde o inicio do século, mas não no Brazil, que só aparece como referencia quando se fala que pais XXX conseguiu decodificar o código diplomático de pais YYY, e do Brazil. Quando se imagina o problema estratégico que isso representa é de se estranhar como é que não se pensa mais nisso por estes lados de cá.

Técnicas mais freqüentes de criptografia

Existem dois tipos de sistemas criptográficos: o de criptografia por Chave Privada (*secret-key* ou *private key*) e o de criptografia por Chave Pública (*public-key*).

Na criptografia por chave privada, também conhecida como criptografia simétrica, a mesma chave é usada para a encriptação e decriptação da mensagem. O sistema criptográfico mais popular baseado em chave privada em uso atualmente é o *Data Encriptação Standard* (DES).

Na criptografia por Chave Pública, cada usuário possui uma chave pública e uma chave privada. A chave pública é feita para ser francamente conhecida enquanto a chave privada permanece em segredo. A encriptação é feita com o uso da chave pública enquanto a decriptação é feita com o uso da chave privada. O sistema criptográfico de chave pública RSA é o sistema mais popular de método de criptografia por chave pública. A sigla RSA deriva das iniciais de Rivest, Shamir, and Adleman, os inventores deste sistema.

O Algoritmo de Assinatura Digital (*Digital Signature Algorithm* – DAS) é também um outro exemplo de técnica de chave pública, utilizada para assinaturas e não para outras aplicações de encriptação.

Os sistemas criptográficos baseados em Curvas Elípticas (*Elliptic Curve Cryptosystems* – ECC) são criptosistemas baseados em objetos matemáticos conhecidos como curvas elípticas.

A criptografia por curvas elípticas tem ganho recente popularidade. O protocolo Diffie-Hellman é uma técnica popular de chave pública para a definição de chaves secretas em canais inseguros.

Aplicações da Criptografia

A Criptografia apresenta-se como uma ferramenta de grande utilidade para uma série de aplicações. Uma aplicação típica da criptografia é a sua utilização em canais de tráfego de mensagens construídos a partir de tecnologias bem conhecidas. Tais sistemas podem ter diferentes níveis de complexidade. Dentre estas aplicações incluem segurança de comunicações, identificação e autenticação. Outras aplicações envolvem sistemas para comércio eletrônico, certificação, correio eletrônico seguro, recuperação de chaves e acesso seguro a sistemas de computação.

Segurança de Comunicações

As aplicações que envolvem segurança de comunicações são as que mais demandam o uso da criptografia. Duas pessoas podem se comunicar de forma segura encriptando as mensagens trocadas entre elas. Isto pode ser feito forma que uma terceira pessoa que esteja interceptando estas mensagens nunca possa ser capaz de decifra-las.

Atualmente graças ao desenvolvimento da criptografia com chaves públicas, uma serie de ferramentas estão disponíveis para a criação de grandes redes de comunicação que permitem às pessoas comunicarem-se seguramente mesmo que elas nunca tenham se comunicado antes, seja por meio de computadores, celulares ou outros dispositivos de comunicação de uso pessoal. Estas técnicas são usadas não só para a encriptação de dados, como também para a encriptação de voz.

Identificação e Autenticação

Identificação e Autenticação são as mais vastas aplicações da criptografia. Identificação é o processo de verificação da identidade de alguém ou de alguma coisa. Por exemplo, quando se retira dinheiro em um banco o caixa pede para que a pessoa se identifique para verificar a identidade do proprietário da conta. O mesmo processo pode ser feito de forma eletrônica com o uso da criptografia. Todos os cartões de terminais automáticos são associados a uma senha a qual vincula o proprietário do cartão ao proprietário da conta.

Quando o cartão é inserido em um terminal, a máquina pede a quem tem este cartão a senha. Caso esta senha esteja correta, a máquina infere que aquela pessoa seja o proprietário da conta e libera o acesso. Uma outra aplicação importante da criptografia é a Autenticação. A autenticação é similar à identificação, uma vez que ambos processos permitem a uma entidade o acesso a determinados recursos. Porém a autenticação é mais abrangente dado que ela não necessariamente envolve

a identificação da pessoa ou entidade. A autenticação meramente determina se dada pessoa ou entidade é autorizada para aquilo em questão.

Comércio Eletrônico

Ao longo de anos recentes tem havido um crescimento do número de negócios conduzidos via Internet. Esta forma de negócio é conhecido como Comércio Eletrônico ou *E-Commerce*. O comércio eletrônico envolve uma série de atividades realizadas de forma eletrônica dentre as quais se destacam as transferencias de fundos que são também realizadas desta forma.

Entretanto a simples apresentação de um número de cartão de crédito pode levar o seu proprietário a ser fraudado tendo o seu número de cartão de crédito usado sem sua permissão. O uso de mecanismos de transação segura na Internet, onde o número do cartão de crédito é enviado junto com outras informações de forma encriptada tem permitido que estes pagamentos possam se dar de forma segura.

Certification

Uma outra aplicação da criptografia é a Certificação. Certificação é um esquema pelo qual agentes confiáveis, tais como autoridades certificadoras, enviam um Certificado Eletrônico para um outro agente desconhecido, tal como no caso dos usuários.

PRINCÍPIOS BÁSICOS DA CRIPTOGRAFIA

Os princípios básicos da segurança são: a Autenticidade, Confidencialidade, Integridade e Disponibilidade das Informações. Os benefícios evidentes são reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas e, assim, consequentemente aumentar a produtividade dos usuários através de um ambiente mais organizado, maior controle sobre os recursos de informática e, finalmente, viabilizar aplicações críticas das empresas.

Autenticidade

O controle de autenticidade está associado com a identificação correta de um usuário ou computador. O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo. Normalmente, isso é implementado a partir de um mecanismo senhas ou de assinatura digital. A verificação de autenticidade é necessária após todo processo de identificação, seja de um usuário para um sistema, de um sistema para o usuário ou de um sistema para outro sistema. Ela é a medida de proteção de um serviço/informação contra a personificação por intrusos.

Um ataque contra a autenticidade envolve alguma forma personificação (*spoofing*). Um tipo comum de personificação consiste em um usuário externo assumir a identidade de um usuário interno, atuando no sistema no lugar deste usuário legítimo. A maneira mais simples de personificação está associada com infiltrações de senha, onde o intruso informa uma combinação de nome do usuário/senha, depois outra e assim por diante, até que uma determinada combinação permita sua entrada no sistema. Tal técnica (usualmente denominada como Força Bruta ou *Brute Force*) consome, com freqüência, um volume considerável de tempo e esforço de máquina. Assim classes de softwares como os *sniffers*, que possibilitam o rastreamento de senhas, estão sendo utilizados cada vez em maiores escalas.

Muitos tipos de sistemas não bloqueiam tentativas de *login* após um determinado número de insucessos. Essa fraqueza inerente em termos de segurança, permite que

um intruso dê início a um grande número de tentativas de *login* que não são impedidas. Consequentemente, possibilita aos violadores várias formas de invasão: acessando mensagens de correio eletrônico, os quais contêm senhas; ou decifrando-as com uma ferramenta que permite localizar e obter informações sobre senhas vulneráveis em sistemas. Na verdade, alguns invasores utilizam TFTP ou FTP para tentar obter a senha, em seguida o invasor deverá identificar as senhas verdadeiras. No Unix, as senhas contidas em /etc/passwd são cifradas através de um esquema de criptografia não-convencional, mas o algoritmo de criptografia em si está largamente disponível e pode ser até mesmo incorporado em algumas ferramentas utilizadas pelos invasores. Os invasores as utilizam para obter senhas em textos simples que serão informadas durante sessões de telnet ou de rlogin.

Confidencialidade

Confidencialidade significa proteger informações contra sua revelação para alguém não autorizado - interna ou externamente. Consiste em proteger a informação contra leitura e/ou cópia por alguém que não tenha sido explicitamente autorizado pelo proprietário daquela informação. A informação deve ser protegida qualquer que seja a mídia que a contenha, como por exemplo, mídia impressa ou mídia digital. Deve-se cuidar não apenas da proteção da informação como um todo, mas também de partes da informação que podem ser utilizadas para interferir sobre o todo. No caso da rede, isto significa que os dados, enquanto em trânsito, não serão vistos, alterados, ou extraídos da rede por pessoas não autorizadas ou capturados por dispositivos ilícitos.

O objetivo da confidencialidade é proteger informação privada (cidadãos, indústrias, governo, militar). Na comunicação, ela é obtida evitando-se a escuta (meio físico, topologia), ou se isto não for possível, evitando-se a inteligibilidade dos dados durante o processo de transmissão (cifra).

Uma rede de meios físicos compartilhados é uma rede na qual os pacotes são transmitidos para várias partes da rede à medida que trafegam dos pontos de origem para os de destino. As redes de meios físicos compartilhados impõem um tipo especial de risco de segurança, pois os pacotes podem ser interceptados em qualquer ponto dessas redes. A captura de pacotes dessa forma é conhecida como Rastreamento da Rede. Para o rastreamento de uma rede é preciso usar um dispositivo físico ou um programa. Normalmente, os dispositivos físicos de rastreamento são instalados onde há conexão de cabos, através de um conector dentado que penetra no isolamento do cabo, ou em interfaces de porta de máquina *host* individuais. Os programas de captura de pacotes proporcionam uma interface com um dispositivo de hardware que é executado no modo promíscuo (*sniffer*), ou

seja, copiando todos os pacotes que chegam até ele, independentemente do endereço de destino contido no pacote.

Se um *sniffer* for instalado em alguma parte da rota entre dois *hosts* de uma rede, senhas e informações confidenciais podem ser capturadas, causando transtornos e prejuízos. Tal ação pode proporcionar, também, a ocorrência de futuros ataques contra autenticidade, usando senhas, usernames e endereços de *host* capturados por *sniffers*.

Integridade

A integridade consiste em proteger a informação contra modificação sem a permissão explicita do proprietário daquela informação. A modificação inclui ações como escrita, alteração de conteúdo, alteração de status, remoção e criação de informações. Deve-se considerar a proteção da informação nas suas mais variadas formas, como por exemplo, armazenada em discos ou fitas de backup. Integridade significa garantir que se o dado está lá, então não foi corrompido, encontra-se íntegro. Isto significa que aos dados originais nada foi acrescentado, retirado ou modificado. A integridade é assegurada evitando-se alteração não detectada de mensagens (ex. tráfego bancário) e o forjamento não detectado de mensagem (aliado a violação de autenticidade).

Disponibilidade

Ter as informações acessíveis e prontas para uso representa um objetivo crítico para muitas organizações. No entanto, existem ataques de negação de serviços, onde o acesso a um sistema/aplicação é interrompido ou impedido, deixando de estar disponível; ou uma aplicação, cujo tempo de execução é crítico, é atrasada ou abortada.

Disponibilidade consiste na proteção dos serviços prestados pelo sistema de forma que eles não sejam degradados ou se tornem indisponíveis sem autorização, assegurando ao usuário o acesso aos dados sempre que deles precisar. Isto pode ser chamado também de continuidade dos serviços.

Um sistema indisponível, quando um usuário autorizado necessita dele, pode resultar em perdas tão graves quanto as causadas pela remoção das informações daquele sistema. Atacar a disponibilidade significa realizar ações que visem a negação do acesso a um serviço ou informação, como por exemplo: bloqueamento do canal de comunicação ou do acesso a servidores de dados.

ASPECTOS LEGAIS DO USO DA CRIPTOGRAFIA

Reza a Declaração Universal dos Direitos Humanos, art. 19:

> "Todo o homem tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferências, ter opiniões e de procurar, receber e transmitir informações e idéias por quaisquer meios, independentemente de fronteiras"

Todavia, o direito à livre expressão de opiniões e repasse ou guarda de informações, com a evolução dos meios de comunicação e com o advento da tecnologia da informação, vem sendo cerceado por mecanismos cada vez mais sofisticados de "invasão de privacidade", deixando muitas vezes impune o agente de tais ações.

As organizações tem enfrentado ações na justiça, muitas sem o sucesso desejado, visto que as leis de proteção ao patrimônio e dos direitos das pessoas, existentes até a década de 70, passaram a não mais atender às necessidades de penalidades para todos os tipos de crimes contra o direito das pessoas. Pela imaterialidade da informação - um bem muito adverso daqueles até então normalmente tratados como objeto de "roubo", "subtração" ou "destruição" - fica difícil aplicar o conceito de "coisa", deixando lacunas na lei que, ou não possibilitam aplicar penalidades aos agentes infratores ou exigem verdadeiras "ginásticas" de interpretação por advogados e juizes, para que os julgamentos tenham o resultado esperado em um crime envolvendo a informação. O exame dessas questões tem ocorrido em nível internacional e regional.

Neste particular pode ser citado o OECD (*Organisation for Economic Co-operation and Development*) e o *Council of Europe*, que têm produzido guias para legisladores e interessados no assunto, além de órgãos envolvidos em investigação. Em 1983, o OECD procedeu a um estudo que resultou na publicação, em 1986, de relatório que analisava as leis existentes e recomendava uma lista mínima de abusos contra a informação de modo geral, que os países deveriam considerar proibidos e passíveis de punições por leis criminais, por exemplo: fraudes e falsificações por computador, alteração de programas e dados, violação de copyright e interceptação de

comunicações. Além destas, outras proteções legais deveriam ser adotadas para outros tipos de abusos, incluindo o roubo de "Segredos de Negócios" e acesso não autorizado aos sistemas de computadores. O 8º Congresso das Nações Unidas Para Prevenção de Crimes e Tratamento aos Infratores produziu resolução, na qual cada Nação Membro intensificaria seus esforços no combate aos crimes por computador, observando as seguintes medidas:

- Modernização das Leis e procedimentos penais;
- Desenvolvimento de medidas de prevenção e segurança para computadores, no que concerne a respeitar os direitos humanos e as liberdades fundamentais;
- Adoção de medidas que sensibilizem o público e o judiciário para o problema e a importância de prevenir os crimes por computador;
- Adoção de treinamento para juizes, oficiais e agências responsáveis por prevenir, investigar e julgar os crimes por computador.
- Nesta resolução, recomenda-se que o Comitê de Prevenção e Controle de Crimes envide esforços no desenvolvimento e na disseminação de regras e padrões que auxiliem as Nações a tratar com crimes por computador.

Para subsidiar tais ações foi elaborada Lista Mínima de Infrações, concernente à crimes por computador, que deveriam ser tratadas pela legislação:

- Fraude por Computador

  Compreende a adulteração, dano ou supressão de dados ou programas de computador ou outras interferências no curso do processamento de dados, que influencie o resultado do processo, ocasionando perdas econômicas ou de propriedade, beneficiando os infratores ou terceiros;

- Falsificação por Computador

  Compreende a modificação de dados descrita no item acima, já protegidos por lei, caracterizando embuste ou imitação (fazer se passar por outro);

- Danos a dados ou programas de computador

  Deleção, modificação, deterioração ou supressão de dados ou programas sem autorização.

- Sabotagem computacional

  Introdução, alteração, deleção ou supressão de dados ou programas ou outras interferências em sistemas, com a intenção de dificultar o funcionamento de computadores ou sistemas de comunicação;

- Acesso não autorizado

Acesso a sistemas ou redes de computadores, sem autorização, burlando os controles de segurança implementados;

- Interceptação não autorizada

  Interceptação de comunicações de, para e de dentro dos sistemas e redes de computadores, feita sem autorização e por meios técnicos;

- Cópias não autorizadas de programas de computadores

  Reprodução, distribuição ou divulgação de programas de computador, sem autorização;

- Reprodução não autorizada de topografia

  Abrange a reprodução, exploração ou importação comercial não autorizada de topografia de semicondutores.

Ainda, a resolução propõe Lista Opcional abrangendo:

- Espionagem computacional

  Obtenção, transferência ou uso de segredos de negócio, de modo ilícito, sem autorização ou qualquer outra justificativa legal, com intenção tanto de causar perdas econômicas para o proprietário como de obter vantagens econômicas para si ou terceiros;

- Uso não autorizado de computadores

  Uso de sistemas ou rede de computadores, sem autorização, que:

  1. é feito com a admissão de riscos significativos de perdas para o proprietário, danos aos sistemas ou ao seu funcionamento;
  2. é feito com a intenção de causar perdas para o proprietário, danos aos sistemas ou ao seu funcionamento;
  3. causa perdas para o proprietário, danos aos sistemas ou ao seu funcionamento, mesmo não sendo intencional.

- Uso não autorizado de programa computacional

  Uso e reprodução não autorizados de programas protegidos por lei, com a intenção tanto de obter ganhos econômicos para si ou para terceiros, como causar danos ao proprietário do bem.

Meios Legais de Proteção da Informação

Atualmente, os principais meios invocados para proteger legalmente as informações são: COPYRIGHT, SEGREDO DE NEGÓCIO e CONTRATO.

Normalmente, aliam-se estes três métodos a outros não legais, a fim de obter-se maior nível de proteção contra cópias e divulgações indevidas de informações e sabotagens, visto que as leis não foram criadas observando os aspectos supracitados.

Copyright

Tem origem no art.1 parag.18 da Constituição dos EUA arbitrando poderes ao Congresso para: "Promover o progresso da ciência e das artes, assegurando por tempo determinado a autores e inventores os direitos exclusivos sobre seus escritos e descobertas". O principal problema é determinar se o trabalho possui ou não "originalidade" - ou seja, se mostra alguma criatividade e não somente cópia de trabalhos ou de informações já existentes. Por exemplo: um Banco de Dados com informações sobre cadastro de clientes: as informações não são consideradas "originais" pois qualquer um pode obter as mesmas informações. O trabalho despendido para obter as informações não qualifica o Banco de Dados a ser protegido por Copyright. A Lei brasileira no. 9609, de 18.02.98, somente "dispõe sobre a proteção de propriedade intelectual de programas de computador, sua comercialização no País...", obrigando o cadastramento prévio para a comercialização de programas de computador, tanto nacionais quanto estrangeiros; a celebração de contratos de distribuição com fornecedores de software de origem externa e o exame de similaridade entre produtos nacionais e estrangeiros. Referida Lei define o objeto a ser protegido, no caso programas e componentes do sistema; a autoria, tanto para softwares desenvolvidos internamente nas empresas quanto fora delas; e os direitos de proteção ao autor. No que tange à propriedade intelectual de programas de computador, a Lei 9609 elevou de 25 para 50 anos o prazo de proteção, equiparando-se ao regime de proteção conferido a obras literárias. Entretanto, esta Lei não faz nenhuma referência à proteção das informações processadas e armazenadas pelos sistemas.

Trade Secrecy Protecton

(Proteção do Negócio) Essencialmente, é a proteção legal ao conhecimento que pessoas ou companhias adquirem pelos seus esforços e que tem valor ou vantagem competitiva para elas. Tipicamente, estes conhecimentos são guardados dos seus concorrentes, pois sabe-se que estes obteriam vantagens ao possuir tais

informações. Exemplos: fórmulas, programas, metodologias, tecnologias, padrões etc.

Contrato

Acordos estabelecidos formalmente entre vendedores e compradores, definindo as condições de compra. Tipicamente assumem a forma de "Licenças de Uso" para proteger o direito das partes.

Proteções por Meios Não Legais

Trata-se da criação de mecanismos ou marcas específicas, como uma "assinatura", que possam comprovar a autoria de trabalhos. Exemplo: implantar erros ou omissões em bases de dados, de forma a obter evidências de cópias não autorizadas. Se alguns erros são implantados e os mesmos erros se mostram em base de dados de outrem, tem-se boas provas de que um competidor não obteve tais informações por seus próprios meios. Outro exemplo seria o estilo de programação, que eqüivale a um estilo de escrita. Os programadores podem esconder mensagens cifradas no código objeto ou adicionar linhas de programação desnecessárias. Estas idiossincrasias podem ser documentadas e servir de prova contra cópias ilegais.

Em resumo, embora os mecanismo acima garantam sustentação legal que favoreça ações contra os infratores, a necessidade de uma Lei específica, que defenda os autores e as companhias contra invasões, danos, divulgação não autorizada de informações ou topografias, dentre outros, e que defina claramente as respectivas penalidades é extremamente urgente e imperiosa. Alguns países já perceberam a importância de se legislar sobre este assunto - crimes por computador - oferecendo Leis abrangentes, consistentes e rigorosas quanto às penalidades imputadas aos infratores. O Brasil ainda é incipiente no tratamento do assunto. Um projeto de lei encontra-se em discussão, estando em vias de aprovação pelo Congresso Nacional. A lacuna deixada pela ausência de Lei específica sobre o assunto, tem obrigado advogados e juizes a enquadrar os crimes por computador em crimes comuns previstos em Leis penal e civil tais como:

- Lei de Escutas Telemáticas - art. 5o. Lei 9296/96;
- Lei do Estelionato e da Falsa Identidade - arts. 171 e 307 do Código Penal, respectivamente;
- Violação de Direitos - art. 18 da Lei 7492/86;
- Lei dos Direitos Autorais - Lei 5988/57;

- Lei de Crime Ambiental - art. 62, inciso II da Lei 9605/98;
- Lei de Proteção da Infância e da Juventude - art. 241 da Lei 8069/90,

dentre outras.

TAXONOMIA DOS RISCOS PARA AS ORGANIZAÇÕES

AMEAÇA

Possibilidade de exploração de fragilidades de sistemas, de forma intencional ou não. Podem originar-se interna ou externamente.

ATAQUE

Classificam-se em:

- Ataque ativo - informações são modificadas. São eles: interrupção, modificação e embuste;

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

As ameaças típicas, contra as quais as organizações despendem maior esforço e investimento em mecanismos de proteção das suas informações e estratégias de negócio são:

Ameaças	Descrição
Violação de autorização	Uso de autorização para outra finalidade.
Recusa de serviços	Não atendimento, sem motivo explícito, das requisições dos legítimos usuários.
Espionagem	Obter a informação, sem autorização do proprietário.
Vazamento	Revelação indevida de informação.
Violação de Integridade	Edição não autorizada de informação.
Mascaramento	Passar-se por outro, embuste.
Replay	Retransmissão ilegítima.

Repudiação	Negação imprópria de uma ação ou transação efetivamente realizada.
Exaustão	Sobrecarga de utilização de recurso.
Emulação	Imitação para conseguir informações sensíveis.
Roubo	Posse ilegítima de informações.
Porta dos fundos	Programação inserida e escondida no sistema, que possibilita a entrada de forma não convencional.
Cavalo de Tróia	Programa de captura indevida de informações.

Esses tipos de ameaças possibilitam ataques, que podem ser caracterizados como:

INVASÃO - acesso intencional e não justificado, por pessoa não autorizada pelo proprietário ou operadores dos sistemas.

INTERCEPTAÇÃO - acesso não autorizado à transmissões, possibilitando a cópia das mensagens transmitidas. É o ataque mais comum e de difícil detecção pelas partes legítimas.

MODIFICAÇÃO - é um agravante da interceptação, em que o conteúdo da mensagem é alterado.

FABRICAÇÃO ou EMBUSTE - simulação para o destino de uma origem legítima. O atacante faz-se passar por uma procedência legítima, inserindo objetos espúrios no sistema atacado.

INDISPONIBILIDADE ou INTERRUPÇÃO - ações não autorizadas ocasionado sobrecarga no processamento de sistemas, tornando-os inacessíveis aos legítimos usuários, por longos períodos ou por sucessões de pequenos intervalos.

Estes crimes carecem de legislação específica e, também, de apuração ou investigação detalhada que, devido às suas especificidades e meios utilizados, aliados à falta de capacitação dos investigadores e do judiciário, dificultam a comprovação do ato e de sua autoria. A situação se torna ainda mais crítica pelas características do mercado atual, com globalização da economia, levando pessoas e empresas a disputarem acirradamente sua fatia de mercado e "justificando" ações, mecanismos e técnicas não muito "éticas" adotadas por elas, para conhecimento de planos e produtos de concorrentes. A inadequação da legislação atual, não tratando tais ações como crime, favorece sua ocorrência, através de agentes internos ou externos ao país. Com esse cenário e as fragilidades criadas pela própria tecnologia de comunicação, as preocupações com a criação de uma Lei visando a proteção dos cidadãos e empresas contra crimes por computador são crescentes. É imperativo que haja normatização e definição de punições para os excessos, inclusive as

tentativas, que também afetam a prestação de serviços e disponibilidade do sistema para os usuários.

OS SISTEMAS CRIPTOGRÁFICOS

Podemos classificar os sistemas criptográficos em sistemas de criptografia clássica e sistemas de criptografia moderna.

Os sistemas de criptografia clássica são também conhecidos como sistemas convencionais, sistemas simétricos ou sistemas de chave secreta.

Por sua vez, os sistemas de criptografia moderna são ainda denominados de sistemas assimétricos ou de chave pública.

Técnicas Simples:

Transposição

Ordem Reversa:

A mensagem é escrita de trás para frente. Em seguida, reúne as letras em novos grupos.

```
Texto Puro:   Seu marido vai embora quando?
(1)           odnauq arobme iav odiram ues?
(2)           od nauqa rob me iavod ram ues?
```

Bi-reverso:

As letras são agrupadas em pares e os pares tem a ordem invertida.

```
Texto Puro:     seu marido vai embora quando?
(3)             (se) (um) (ar) (id) (ov) (ai) (em) (bo) (ra) (qu) (an) (do)
(4)             (es) (mu) (ra) (di) (vo) (ia) (me) (ob) (ar) (uq) (na) (od)
Texto cifrado:  esmu radi voiame obar uqna od
```

Grupo reverso

As letras são divididas em grupos que são colocados em ordem reversa.

```
Texto Puro:     seu marido vai embora quando
(1)             seuma ridov aiemb oraqu ando
(2)             amues vodir bmeia uqaro odna
Texto Cifrado:  amues vodir bmeia uqaro odna
```

Substituição

Alfabeto cifrado:

Alfabeto César

Como se pode ver, o alfabeto começa na letra D, mas poderia começar em qualquer outra. As letras iniciais são colocadas depois da letra Z.

```
alf. puro:   a b c d e f g h i j k l m n o p q r s t u v x y w z
alf. César:  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
Ex:    Texto puro: ganhei na loto
       Texto cifr: jdqkhl qd orwr
```

A partir desse método, pode-se colocar mais de um alfabeto, para dificultar a critpoanálise. Quando a mesma letra se repetir, usa-se a segunda cifra. Essa é a cifragem por substituição múltipla.

```
alf. puro:   a b c d e f g h i j k l m n o p q r s t u v x y w z
alf. Cifr1:  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
Alf. Cifr2:  F E G D J H I M K L P N O S Q R V T U Y W X B Z A C
Texto puro: ganhei na loto
Texto cifr: jdqkhl sf orwq
```

Transposição

Este método, projetado pelo grego Polybius, é anterior a César, mas continua difundido como método de criptografia. Funciona se ajuntando as letras do nosso alfabeto num quadrado 5X5. Para não complicar, a letra K é retirada e substituída por C:

```
     1 2 3 4 5
  --------------
1 I  a b c d e
2 I  f g h i j
3 I  l m n o p
4 I  q r s t u
5 I  v x y w z
```

Dessa forma, a letra E passa a ser representada por 15, a letra O pelo numero 34 e assim por diante.

Técnicas Simples de Criptoanálise:

Para praticar, o ideal são palavras cruzadas. Mas para tentar decifrar um texto feito com um dos métodos acima, sem saber qual, há varias formas. Primeiro e mais importante é não trabalhar com o texto original, mas fazer uma copia com espaço entre as linhas, para se trabalhar. Depois procurar as vogais, que estão presentes em todas as palavras. As consoantes duplas como ss e rr são outro bom alvo. Outras combinações comuns de letras são lh, ch, nh, br, cr, dr, gr, pr, tr, bl, cl, fl, gl, pl, tl. Saber sobre o que o texto fala pode ajudar, assim como ajuda saber o destinatário da carta. Palavras como amanha, que repetem a letra a varias vezes, também são bons indicadores.

Existem estudos que mostram a freqüência de ocorrência de letras e outros fonemas para as várias línguas. A analise da distribuição de freqüência de determinadas series de caracteres constitui a forma mais comum de quebra de mensagens cifradas.

Para os métodos mais sofisticados de cifragem a solução seria a descoberta da função inversa àquela usada para a cifragem da mensagem. Contudo os métodos atualmente em voga tornam esta tentativa impossível na prática.

Criptografia por Chaves

Criptografia por Chave Única

Na criptografia tradicional, tanto o remetente quanto o receptor de uma mensagem sabem e usam uma mesma chave secreta. Desta forma o remetente a usa para cifrar a mensagem e o receptor a usa para decifra-la. Esta forma é conhecida como **Criptografia por Chave Secreta** ou **Chave Única** ou **Criptografia Simétrica**.

O principal desafio (e fragilidade) deste método é garantir que ninguém mais saiba esta chave além do transmissor e receptor originais. Para tanto eles a devem trocar pessoalmente ou possuir um sistema de entrega, telefone ou outro meio de transmissão confiável capaz de garantir a confiabilidade do segredo.

Qualquer um que venha, de alguma forma, ter conhecimento desta chave pode mais tarde ler, modificar ou forjar mensagens encriptadas ou autenticadas que utilizem aquela chave. A geração, transmissão e armazenamento de chaves é denominado **Gerência de Chaves**. Dada a esta necessidade os sistemas de criptografia por chave única apresentam dificuldades em garantir plena segurança, especialmente em ambientes abertos com um grande número de usuários.

Em um sistema criptográfico simétrico ou de chave secreta, uma única chave é usada para criptografar e decriptografar.

A operação de criptografar compreende a transformação de um texto ou arquivo de dados, que esteja em claro, em algo ilegível ou irreconhecível, denominado **Texto Cifrado**, pela utilização de um algoritmo e de uma chave criptográfica. A operação de decriptografar é exatamente o inverso, ou seja, dado o texto cifrado, através do emprego do mesmo algoritmo e da mesma chave usados na criptografia, obtém-se o texto em claro original. Daí a denominação de Sistema Criptográfico Simétrico.

O grande segredo da criptografia simétrica é o sigilo a respeito da chave criptográfica que foi utilizada. Daí a denominação de Sistema Criptográfico de Chave Secreta.

Assim, o maior problema deste tipo de sistema é conseguir fazer com que o originador e o destinatário de uma mensagem cifrada pelo algoritmo, e somente eles, possam conhecer a chave secreta ora em uso, assim como combinar sobre futuras alterações da mesma. Isto requer a existência de um método pelo qual as duas partes possam se comunicar de modo seguro.

Dentre os meios possíveis de envio de chave secreta podemos citar o uso de mensageiros confiáveis e o emprego dos mecanismos da criptografia de chave pública.

Por sua vez, a grande vantagem da criptografia de chave secreta é que ela é muito mais rápida que a criptografia de chave pública.

Criptografia por Chave Pública e Chave Privada

Em 1976 Whitfield Diffie e Martin Hellman [RSA00] apresentaram o conceito de Criptografia por Chave Pública. Este sistema possui duas aplicações principais: Encriptação e Assinaturas Digitais.

Neste sistema cada pessoa possui um par de chaves, uma denominada Chave Pública e outra denominada Chave Privada. Enquanto a chave pública tem seu

conhecimento difundido, a chave privada deve ser mantida em segredo. Neste sistema a necessidade das partes comunicantes de trocar informações sigilosas é eliminada sendo que todas as comunicações irão envolver somente a chave pública não sendo necessária a troca de chaves secretas por nenhuma das partes. Ao mesmo tempo este sistema não exige credibilidade dos meios de transmissão envolvidos. O único requisito deste sistema é que a chave pública esteja associada aos seus usuários de uma forma autenticável.

Qualquer um dos possuidores da chave publica pode usa-la para enviar uma mensagem. Porém a mesma mensagem só pode ser lida mediante o uso da chave privada a qual é de uso restrito de seu proprietário.

Neste sistema criptográfico a chave privada é matematicamente derivada da chave pública. Se, em tese, é probalisticamente impossível a um atacante derivar a chave privada da chave pública, esta propriedade ainda não pode ser matematicamente comprovada [APS99].

Quais são as vantagens e desvantagens da criptografia baseada em chave pública e da baseada em chave privada?

A principal vantagem do uso de chave pública é o ganho de segurança e conveniência uma vez que a chave privada nunca tem que ser remetida ou revelada a ninguém. No sistema da chave secreta, por outro lado, esta deve ser transmitida (seja manualmente ou eletrônicamente) uma vez que a mesma é utilizada para a encriptação quanto para a decriptação. A principal desvantagem deste sistema é a possibilidade desta chave vir a ser interceptada e tornar-se de conhecimento de outros.

Uma outra vantagem do sistema de chave pública é a sua capacidade de prover assinaturas digitais que não podem ser repudiadas. A autenticação via um sistema de chave secreta requer o compartilhamento do segredo e algumas vezes requer a confirmação de terceiros. Como resultado, quem envia uma mensagem pode repudiar uma mensagem previamente autenticada alegando que o segredo compartilhado foi comprometido por outros que podem ter tido acesso à mesma chave.

Ao seu turno, o sistema de chave pública previne este tipo de repúdio, visto que cada usuário tem a responsabilidade de proteger sua chave. Esta propriedade da autenticação por chaves públicas também é conhecida como Não Repúdio [RSA00].

Porém a grande desvantagem do sistema de chave pública é a velocidade. Em geral os sistemas de criptografia por chave única são ordens de magnitude mais rápidos que os métodos de chave pública [APS99].

Em muitas situações o uso de criptografia por chave pública não se faz necessário e o sistema de chave única por si só é suficiente. Os ambientes onde a distribuição das chaves pode ser plenamente controlado por uma única autoridade certificadora, tal como em sistemas bancários fechados, são o exemplo típico deste tipo de aplicação.

Desde que a autoridade certificadora conhece todas as chaves não existe muita vantagem no uso de uma chave pública e outra privada. Entretanto mesmo que o conhecimento de todas as chaves possa se tornar impraticável se o número de usuários crescer em demasiado, ainda assim o uso do sistema de chave única pode continuar em uso.

Em geral a criptografia por chave pública mostra-se mais adequada para ambientes multi-usuários abertos. Este sistema usualmente é aplicado de forma suplementar o sistema de chave única para torna-lo mais seguro.

Cifragem de Blocos

A Cifragem de Blocos é um tipo de encriptação por algoritmo por chave simétrica que transforma um bloco de tamanho fixo de texto claro (texto não encriptado) em um bloco de texto encriptado de mesmo tamanho.

Um sistema simétrico cifrador de bloco transforma um bloco de texto em claro de tamanho fixo em um bloco de texto cifrado do mesmo tamanho, empregando o algoritmo de criptografar simétrico e uma determinada chave secreta, previamente combinada. O processo de decriptografia do texto assim cifrado é conseguido pela aplicação da transformação reversa da criptografia, ainda utilizando a mesma chave secreta. O tamanho do bloco fixo, na maioria dos sistemas simétricos de bloco atuais é de 64 bits sendo este o tamanho da chave usada. Com o avanço da tecnologia de processadores, tem-se alcançado tamanhos maiores de bloco, por exemplo 128 bits [RSA00].

Esta transformação tem lugar na medida em que uma chave é apresentada como parâmetro deste processo. A decriptação é efetuada pela aplicação reversa do algoritmo de cifragem utilizando-se a mesma chave usada para a encriptação.

Quando a mensagem a ser cifrada possui um comprimento arbitrário, a técnica de modularização da mensagem original em blocos de *n* caracteres é utilizada, onde *n* é o tamanho da chave de criptografia.

Cifragem de Cadeias

É um sistema simétrico, diferentemente do sistema cifrador de bloco, que opera tipicamente sobre unidades menores de texto em claro, normalmente sobre bits. Também ao contrário dos cifradores de bloco, onde sempre um determinado bloco de texto em claro irá originar o mesmo bloco cifrado, se a mesma chave for sempre usada, no caso do cifrador em cadeia as unidades menores de texto em claro poderão gerar textos cifrados diferentes, dependendo das suas posições durante o processo de criptografia.

Os sistemas simétricos cifradores de cadeia podem ser projetados para serem muito mais velozes do que qualquer sistema cifrador do bloco.

O mecanismo de cifragem de cadeias deve gerar o que é conhecido como *keystream*. A cifragem se dá então pela combinação da *keystream* com o texto em claro, usualmente por meio de uma operação binária XOR.

A geração da *keystream* deve se dar de forma independente do texto em claro e do texto cifrado.

O interesse no uso das *keystream* reside no seu apelo teórico do *one-time pad* [APS99]. Esta propriedade, também conhecida como cifragem *Vernam* [APS99], faz uso de uma cadeia de caracteres gerada de forma randômica. Assim uma chave randômica é aplicada sobre o texto em claro para a geração da *keystream* com base em uma operação XOR e esta é então aplicada sobre o texto em claro, novamente via operação XOR, para a produção do texto cifrado final.

Em última instância tudo se passa como se a chave de cifragem usada tivesse o mesmo tamanho do texto em claro, tornando a decifragem computacionalmente impossível [APS99].

Uma vez que a *keystream* parece ser randômica para que a intercepta, mesmo que o interceptador possua poder computacional infinito ele só poderá obter o texto em claro se puder ter todo o texto cifrado.

Até o momento nenhum método de cifragem de cadeia emergiu como um padrão. Entretanto o padrão RC4 [RSA00] tem sido o de maior aplicabilidade.

Conquanto os métodos de cifragem de cadeia contemporâneos não possam prover uma segurança matematicamente satisfatória, eles são de uso prático extremamente difundido [RSA00, APS99], tanto pela velocidade que proporcionam quanto pela segurança prática que apresentam.

Funções de Hash

Uma função de *hash* é um tipo de transformação que toma uma entrada *m* e retorna uma seqüência de tamanho fixo a qual é denominado de valor *hash* onde:

$$h = H(m).$$

Os requisitos básicos de uma função *hash* de criptografia são:

- As entradas devem possuir qualquer comprimento;
- As saídas devem possuir sempre o mesmo comprimento;
- h = H(m) deve ser fácil de calcular para qualquer *m* dado;
- $m = H^{-1}(h)$ deve ser impossível de ser obtida;
- H(x) deve ser livre de colisões (*colision free*) ou seja; não podem existir x e y onde $x \neq y$ tal que H(x) = H(y).

Um valor *hash* representa de forma concisa uma mensagem longa ou documento a partir do qual ele foi calculado. Este valor também é conhecido como *Message Digest*. Este valor pode ser entendido como sendo uma "impressão digital" do documento.

As principais aplicações das funções *hash* no campo da criptografia são a provisão da integridade de uma mensagem e nas assinaturas digitais [APS00]. Uma vez que as funções de *hash* são em geral mais rápidas que os algoritmos de encriptação ou assinatura digital, uma aplicação típica é a da verificação da integridade de um documento.

Sistemas Criptográficos baseados em Curvas Elípticas

Aspectos de Segurança

A base para a segurança de sistemas criptográficos baseados em curvas elípticas é a aparente intratabilidade do “problema do logaritmo discreto de curvas elípticas”, que pode ser resumido da seguinte forma: dada uma curva elíptica E definida sobre um corpo finito, um ponto P da curva de ordem n, e um ponto Q, determine o inteiro k, $0 < k < n-1$, tal que Q = kP.

Nos últimos 12 anos, o problema de logaritmos discretos de curvas elípticas tem recebido considerável atenção de matemáticos no mundo inteiro, e nenhum fraqueza significativa foi relatada. Um algoritmo devido a Pohlig e Hellman reduz a

determinação de k à determinação de k módulo cada um dos fatores primos de n. Logo, para se obter o máximo nível de segurança *n* deve ser primo.

O melhor algoritmo para quebrar os protocolos baseados em curvas elípticas, segundo Jurisic e Menezes [7], em geral, é o método RHO de Pollard que leva, aproximadamente, $\sqrt{\pi n / 2}$ passos, onde um passo significa uma adição de curva elíptica. Em 1993, Oorschot e Wiener [8] mostraram como o método RHO de Pollard pode ser distribuído em paralelo, tal que, se r processadores forem usados, o número esperado de passos por cada processador antes de um único logaritmo discreto ser obtido é

$$\sqrt{\pi n / 2} / r \quad (47)$$

Em seu trabalho, eles estimam que um atacante (bem financiado), considerando n > 1036 e < 2120, precisaria de uma máquina com 325.000 processadores (a um custo de US$10 milhões à época) para computar um único logaritmo discreto em 35 dias.

Comparemos, agora, a complexidade de algoritmos para quebra da chave. Algoritmos baseados em fatoração de inteiros, como o RSA, tem ataques bem conhecidos. O problema básico para este tipo de criptografia de chave pública é se encontrar dois primos grandes (p eq), cujo produto seja um inteiro grande N. O tempo necessário para fatorar este tipo de número é:

$$tempo_{fatoracao} \approx \exp(c\sqrt[3]{(\log N)(\log\log N)^2}) \quad (48)$$

Isto ocorre para um método em particular (por sinal, usando curvas elípticas). Pode haver métodos mais rápidos, em função do tamanho de N. Mas, de maneira geral, podemos considerar o problema da fatoração com complexidade:

$$\exp\left((\log N)^{\frac{1}{3}}\right) \quad (49)$$

Sua complexidade recai, assim, na classificação de sub-exponencial.

Sistemas criptográficos baseados em curvas elípticas usam pontos ou pares de números para esconder a informação. A idéia básica é que se tenha um número total de pontos disponíveis (m) bastante grande. O tempo necessário para encontrar um particular ponto é, aproximadamente, o seguinte:

$$tempo_{eliptica} \approx \exp(c\sqrt{m}) \quad (50)$$

Este tempo é completamente exponencial.

O resultado é que, segundo Rosing [9], embora a comparação não seja trivial, a quantidade de bits que um sistema usando curvas elípticas necessita, para ser

compatível com o RSA 1024 bits, está abaixo de 200 bits. Assim, apesar de precisar de dois elementos de 200 bits para representar cada ponto, a quantidade de hardware necessária para se atingir o mesmo nível de segurança é menor que o necessário para o mesmo nível de segurança usando métodos de fatoração de inteiros.

RSA - Rivest, Shamir and Adleman Algorithm (Algoritmo de Criptografia RSA baseado em chave pública e privada)

A descoberta de um novo paradigma em criptografia usando chave pública representada pelo popular sistema de criptografia RSA causou uma nova onda de interesse pela teoria de números e mais importante por processos computacionais. Entre os problemas que naturalmente aparecem achamos a fatoração de inteiros ou num termo mais genérico *primality proving*. Para lidar com tais problemas, precisamos achar um algoritmo bom, eficiente e rápido e isto causa um crescimento na área de teoria de números computacionais.

O RSA é um sistema de criptografia de chave pública tanto para cifrar quanto para autenticação de dados, foi inventado em 1977 por Ron Rivest, Adi Shamir e Leonard Adleman, pesquisadores do MIT. O RSA é combinado com a função *hashing* SHA1 (*secure hash algorithm*) para cifrar a mensagem. A principal vantagem da criptografia baseada em chave pública é a sua maior segurança em relação a criptografia baseada em chave secreta. No sistema baseado em chave pública as chaves privadas nunca precisam ser transmitidas ou recebidas a ninguém. Num sistema de chave secreta, ao contrário, sempre existe uma chance de que um intruso possa descobrir a chave secreta enquanto esta está sendo transmitida. Outra vantagem do sistema baseado em chave pública é que eles podem fornecer um método para assinaturas digitais, mas em contra partida existe uma como desvantagens principal: a velocidade. O método de chave pública é muito mais lento na cifragem do que o método de chave secreta.

SET - Secure Eletronic Transaction (Transações eletrônicas seguras com cartão de crédito)

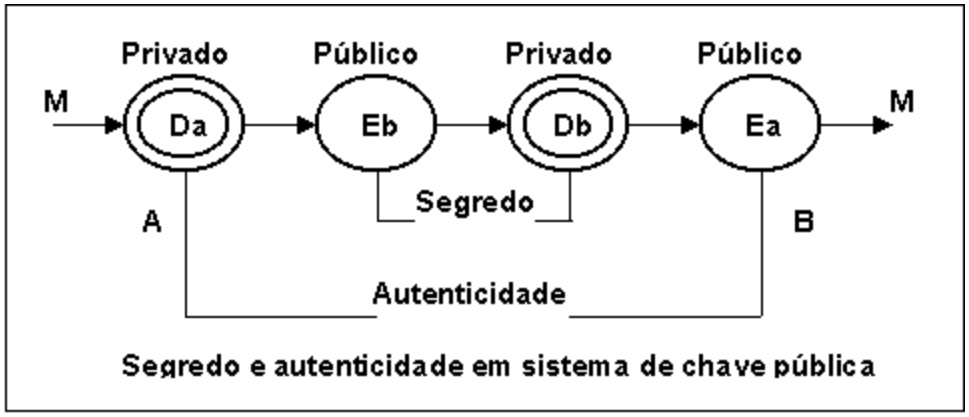
Internet

A Internet está alterando a maneira pela qual nos comunicamos e pagamos por serviços, acessamos as informações, pagamos e adquirimos mercadorias. Vários serviços financeiros como pagamentos de conta, corretagem, seguros, e *home banking* estão ou estarão disponíveis em larga escala na Internet.

Para que tais transações sejam efetuadas sem prejuízo para o lado do consumidor e até mesmo do servidor a criptografia na Internet se tornou mais que uma realidade e sim uma necessidade, sendo que a cada dia tenta-se implementar algoritmos cada vez mais poderosos e difíceis de serem decifrados por pessoas não autorizadas.

A autenticação num sistema digital é um processo por meio do qual o receptor de uma mensagem digital pode estar confiante da identidade do remetente e / ou da integridade da mensagem. Os protocolos de autenticação podem ser baseados tanto em sistemas criptográficos convencionais de chave secreta como DES ou em sistemas de chave pública como RSA; a autenticação em sistemas de chave pública utiliza assinaturas digitais. A necessidade de assinaturas digitais surgiu da proliferação das comunicações digitais.

Logo, a cifragem e autenticação acontecem sem compartilhamento de chaves privadas: cada pessoa usa apenas as chaves públicas de outras pessoas e sua própria chave privada. Qualquer um pode enviar uma mensagem cifrada ou verificar uma mensagem assinada, utilizando apenas chaves públicas, mas apenas a pessoa em posse da chave privada correta pode decifrar ou assinar uma mensagem (vide figura abaixo):



Segredo e autenticidade em sistema de chave pública

É necessário um prazo de validade de uma chave para prevenção contra tentativas de quebra a longo prazo. Logo, o tempo de validade deve ser muito menor do que o tempo esperado para que se consiga sua quebra, ou por outro lado, o comprimento da chave deve ser suficientemente grande para tornar as chances de se conseguir sua quebra antes do término da validade pequenas. A data de validade de uma chave acompanha a chave pública num certificado ou num diretório. O programa de verificação de assinatura deve verificar a validade da chave e não deve aceitar uma mensagem assinada por uma chave fora da validade.

A Certificação digital é uma aplicação na qual uma autoridade de certificação "assina" uma mensagem especial *m* contendo o nome de algum usuário *A* e sua chave pública, de forma que qualquer pessoa possa "verificar" que a mensagem foi assinada apenas pela autoridade de certificação e assim incrementa crédito na chave pública de *A*.

Uma implementação típica da certificação digital envolve um algoritmo de assinatura para assinar a mensagem especial, utilizada pelos certificados da X.509. Com uma assinatura digital comum, qualquer um pode verificar a qualquer hora, que a certificação foi assinada pela autoridade de certificação, sem acesso a informação secreta.

A CRL é outro tipo de mensagem especial com uma assinatura. A mensagem especial para um CRL contém uma lista de certificados revogados, onde os certificados são tipicamente referenciados indiretamente por um número serial. Um CRL habilita à autoridade da certificação a "desabilitar" suas assinaturas no certificado de "A" ou certificados estendidos, caso seja necessário quando o nome de "A" é alterado ou sua chave privada é comprometida.

A certificação digital possui seis aspectos adequados para padronização: uma sintaxe independente do algoritmo para requisições de certificações, para certificados, para certificados estendidos, para CRLs, e sintaxe de chave pública para algoritmos de chave pública específicos, e algoritmos de assinatura específicos.

O processo de assinatura e verificação consiste em quatro passos: digerir mensagens, codificação de dados, criptografia RSA, e conversão de cadeias de octetos a cadeia de bits. A entrada para o processo de assinatura pode ser uma cadeia de octetos M, a mensagem; e uma chave privada do assinante. A saída do processo de assinatura deve ser uma cadeia de bits S, a assinatura.

O processo de verificação para algoritmos de assinatura consiste em quatro passos: conversão de cadeia de bits em cadeia de octetos, decifragem do RSA, decodificação de dados, e mensagem digerida e comparação. O processo de assinatura deve ser desenvolvido com uma chave privada da entidade e o processo de verificação deve ser desenvolvido com uma chave privada da entidade. O processo de assinatura transforma uma cadeia de octetos (a mensagem) a uma cadeia de bits (a assinatura);

o processo de verificação determina se a assinatura é a assinatura de uma cadeia de octetos, a mensagem

Impacto da comércio eletrônico

Não há dúvidas que o comércio eletrônico, a exemplo da popularidade da Internet, está causando um grande impacto nos serviços fornecidos pelas instituições financeiras. Nenhuma instituição financeira deixará de ser afetada direta ou indiretamente pela explosão comércio eletrônico.

O número de compras com cartão de crédito realizadas através deste meio deve crescer com os pedidos online dos sistemas baseados na Internet.

Vários bancos estão planejando aderir a esta nova forma de comércio eletrônico oferecendo autorizações para pagamentos com cartões de crédito diretamente pela Internet.

Os sistemas de pagamento e suas instituições financeiras têm uma função significativa estabelecendo especificações abertas para transações com pagamentos em cartão que:

- Proporcionam transmissões confidenciais,
- Autenticam as partes envolvidas,
- Garantem a integridade das instruções de pagamento para bens e serviços, e
- Autenticam a identidade do portador do cartão e do vendedor mutuamente.

Confidencialidade da informação

Para facilitar e encorajar o comércio eletrônico usando os produtos com pagamento em cartão, será necessário garantir aos portadores de cartão que as suas informações de pagamento estão seguras e somente podem ser acessadas pelo destinatário. Portanto, a conta dos portadores de cartão e as informações de pagamento devem ser asseguradas em suas viagens pela rede, prevenindo a intercepção das números das contas e suas datas de expiração por indivíduos não autorizadas.

No ambiente de compras on-line atual, instruções contendo informações de pagamento são freqüentemente transmitidas pelos portadores de cartões aos comerciantes sobre redes abertas com poucas precauções de segurança, se houver. Contudo, esta informação da conta proporciona os elementos chave necessários para criar cartões falsificados e/ou transações fraudulentas.

Enquanto é possível obter informações de contas em outros ambientes, há um aumento sobre a facilidade de se fazer isso com transações em redes públicas. Esta

preocupação reflete o potencial para um alto volume de fraudes, fraudes automatizadas (como a utilização de filtros sobre todas as mensagens que passam sobre a rede para extrair todos os números de contas com pagamento em cartão do fluxo de dados na rede), e o potencial para "fraudes maliciosas" que parece ser características de alguns *hackers*.

Integridade dos dados

A informação do pagamento enviada dos portadores de cartão para os comerciantes inclui a informação do pedido, os dados pessoais, e as instruções de pagamento. Se qualquer componente for alterado na transição, a transação não será processada corretamente. Para eliminar esta fonte potencial de fraude e/ou erro, o SET deve proporcionar os meios para garantir que o conteúdo de cada pedido e a mensagem de pagamento recebida correspondem ao conteúdo da mensagem enviada.

Autenticação da conta do portador do cartão

Os comerciantes precisam de uma maneira para verificar que um portador de um cartão é o legítimo usuário da conta do cartão. Um mecanismo que usa tecnologia para ligar um portador de cartão a um número de uma conta de pagamento de um cartão específico reduzirá a incidência de fraude e por isso o custo global do processamento do pagamento.

Esta especificação define o mecanismo para verificar que o portador do cartão é um usuário legítimo de um número válido da conta de pagamento do cartão.

Nota: Esta especificação não define o processo usado por uma instituição financeira para determinar se um indivíduo é o legítimo usuário da conta.

Autenticação do comerciante

A especificação deve proporcionar uma maneira para os portadores de cartão de confirmar que o comerciante possui um relacionamento com uma instituição financeira que o permite aceitar pagamentos em cartão. Os portadores de cartão também precisam estar aptos a identificar os comerciantes com os quais ele pode conduzir seguramente o comércio eletrônico.

Interoperabilidade

A especificação deve ser aplicável em uma variedade de plataformas de hardware e software, e não deve incluir uma preferência de uma sobre a outra. Qualquer portador de um cartão de crédito com software compatível deve estar habilitado a se comunicar com o software do comerciante que também faz parte do padrão definido.

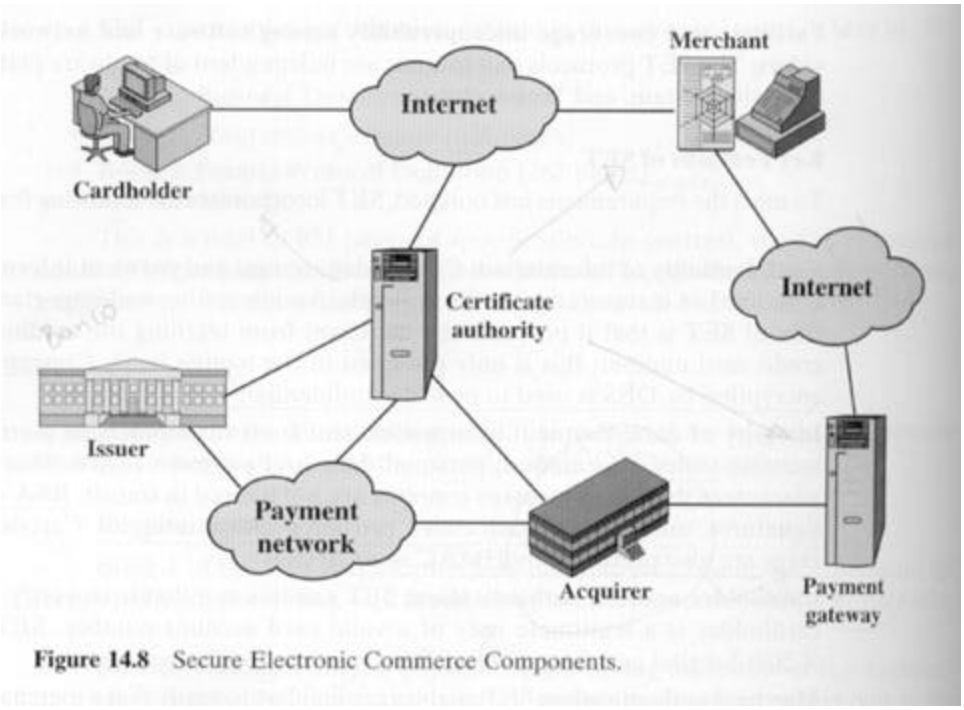


Figure 14.8 Secure Electronic Commerce Components.

Interação dos participantes

O SET altera a maneira que os participantes de um sistema de pagamento interagem. Em uma transação face-a-face pormenorizada ou em uma transação de um pedido por *e-mail*, um processamento eletrônico inicia-se com o comerciante ou com uma instituição financeira que processa as autorizações dos processos de pagamentos e os pagamentos propriamente ditos. Contudo, em uma transação SET, o processamento eletrônico inicia-se com o portador do cartão.

Portador do cartão de crédito

Em um ambiente de comércio eletrônico, os consumidores e os compradores corporativos interagem com os comerciantes através de computadores pessoais. Um portador de cartão usa um cartão que tenha sido emitido por uma instituição financeira - emissor. O SET assegura que nas interações dos portadores de cartão com os comerciantes, as informações da conta usada no pagamento permanece confidencial.

Emissor

Um Emissor é uma instituição financeira que estabelece uma conta para um portador de um cartão e emite o pagamento. O Emissor garante o pagamento para as transações autorizadas usando o cartão de pagamento em acordo com as regulações para cada tipo de cartão e com a legislação local.

Comerciante

Um comerciante oferece bens para venda ou fornece serviços em troca de pagamento. Com o SET, o comerciante pode oferecer interações eletrônicas seguras aos portadores de cartão. Um comerciante que aceita pagamento em cartão deve ter um relacionamento com um "Acquirer".

Acquirer

O "Acquirer" é uma instituição financeira que estabelece uma conta com o comerciante e processa as autorizações para pagamento em cartão e os pagamentos.

Gateway de pagamento

É um dispositivo operado pelo "Acquirer" ou uma terceira parte designada que processa as mensagens de pagamento do comerciante, incluindo as instruções de pagamento dos portadores de cartão.

Tipos de cartão

As instituições financeiras tem fundado marcas de cartão que protegem e anunciam a marca, estabelece e fazem cumprir regras para o uso e a aceitação dos seus cartões, e proporcionar redes para interconectar as instituições financeiras.

Terceiros

Os Emissores e os "Acquirers" algumas vezes escolhem associar o processamento das transações com pagamento em cartão aos processadores terceiros. Este documento não distingue entre as instituições financeiras e os processadores das transações.

Assinatura Dupla

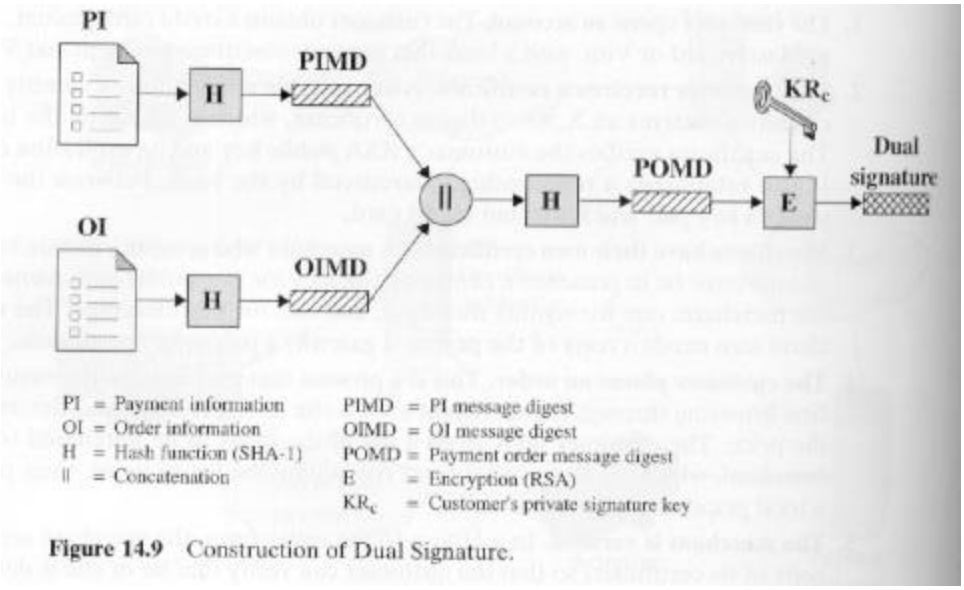


Figure 14.9 Construction of Dual Signature.

O propósito da assinatura dupla é ligar duas mensagens que são endereçadas para dois destinatários diferenças. Neste caso, o cliente quer enviar a informação de compra para o comerciante e a informação de pagamento para o banco. O comerciante não precisa saber o número do cartão de crédito do cliente e o banco não precisa saber os detalhes da compra. Ao cliente é oferecida uma proteção extra em termos de privacidade mantendo estes dois itens separados, entretanto estes dois itens precisam estar ligados de tal forma que possam ser usados para resolver qualquer dúvida, ou seja, essa ligação é necessária para que o cliente possa comprovar que aquela ordem de pagamento é destinada aquele pedido e não a qualquer outro bem ou serviço.

Para ver a necessidade dessa ligação, suponha que o consumidor envie duas mensagens para o comerciante - uma informação de compra (OI) assinada e uma informação de pagamento (PI) assinada - e o comerciante poderia afirmar que uma informação de compra pertence a um outro pedido. A ligação previne isso.

A figura acima mostra o uso da assinatura dupla para satisfazer as requisições do parágrafo anterior. O cliente O cliente usa o *hash* (usando SHA-1) do PI e o *hash* do OI. Estes dois *hashes* são concatenados e é gerado um novo *hash* desse resultado. Finalmente, o cliente cifra o *hash* resultante com a sua chave privada criando a assinatura dupla (DS). Esta operação pode ser resumida da seguinte maneira:

```
DS = Chave Privada [Hash ( Hash(PI) + Hash(OI) )
```

Agora suponha que o comerciante está de posse de uma assinatura dupla (DS), da informação de compra (OI) e do *hash* da mensagem para a informação de pagamento - Hash(PI) = PIMD. O comerciante também possui a chave pública do cliente, que foi obtida através do certificado do cliente. Então o comerciante pode calcular as duas quantidades:

```
Hash(PI) = PIMD

Chave Privada [Hash ( PIMD + Hash(OI) ) e a chave pública do cliente
```

Se estas duas quantidades forem iguais, então o comerciante verificou a assinatura do cliente. Similarmente, se o banco está de posse da assinatura dupla (DS), da informação de pagamento (PI), o *hash* da informação do pedido (OIMD), e a chave pública do cliente, então o banco pode calcular o seguinte:

```
Hash(OI) = OIMD

Chave Privada [Hash ( OIMD + Hash(PI) ) e a chave pública do cliente
```

Novamente, se essas duas quantidades forem iguais, então o banco verifica a assinatura.

Em resumo:

- comerciante recebeu a informação do pedido(OI) e verificou a assinatura.

- banco recebeu a informação do pagamento (PI) e verificou a assinatura.
- cliente ligou a OI e a PI e pode fornecer a ligação.

Por exemplo, suponha que o comerciante deseja-se substituir por outro pedido (OI) nesta transação, para tirar vantagem. Ele então teria que encontrar outro OI cujo *hash* fosse igual ao OIMD. Com o SHA-1, isto é considerado impossível. Sendo assim, o comerciante não pode ligar outro OI com este PI.

Processamento do Pagamento

Requisição de compra

Antes do início da requisição de compra, o portador do cartão completou a sua procura, seleção e o seu pedido. O final desta fase preliminar ocorre quando o comerciante envia um formulário completo para o consumidor. Todos os procedimentos anteriores ocorrem sem o uso do SET.

O processo da requisição de compra consiste de quatro mensagens:

- *Initiate Request,*
- *Initiate Response,*
- *Purchase Request,* e
- *Purchase Response*.

Para enviar mensagens ao comerciante, o portador do cartão deve ter uma cópia do certificado do comerciante e do *gateway* de pagamento. O cliente requisita um certificado na mensagem *Initiate Request,* enviada para o comerciante. Esta mensagem inclui o tipo ou marca do cartão de crédito usado pelo comerciante. A mensagem também inclui uma identificação (ID) assinada para este par de requisição/resposta.

O comerciante gera uma resposta e a assina com sua chave privada. Além da resposta assinada, a mensagem de *Initiate Response* inclui o certificado de assinatura do comerciante e o certificado do *gateway* de pagamento.

O portador do cartão verifica o certificado do comerciante e do *gateway* de pagamento por meio de suas respectivas assinaturas na autoridade certificadora (CA) e então cria a informação do Pedido (OI) e a informação do pagamento (PI). A identificação da transação (ID) assinada pelo comerciante é colocada em ambos os OI e PI. O OI não contém os dados explícitos do pedido como o número e o preço dos itens. Em vez disso, o OI contém uma referência do pedido gerado na troca entre o comerciante e o consumidor durante a fase de compra antes da primeira mensagem SET.

Após isso, o portador do cartão prepara a mensagem *Purchase Request.* Para este propósito, o portador do cartão gera uma chave simétrica uma vez, Ks. A mensagem inclui o seguinte:

1. Informação relacionada a compra: essa informação será encaminhada para o "gateway" de pagamento pelo comerciante e consiste de:
   - A informação do pagamento (PI)
   - A assinatura dupla (DS), calculada entre a PI e a OI assinada com a chave privada do consumidor
   - hash da OI
   - envelope digital

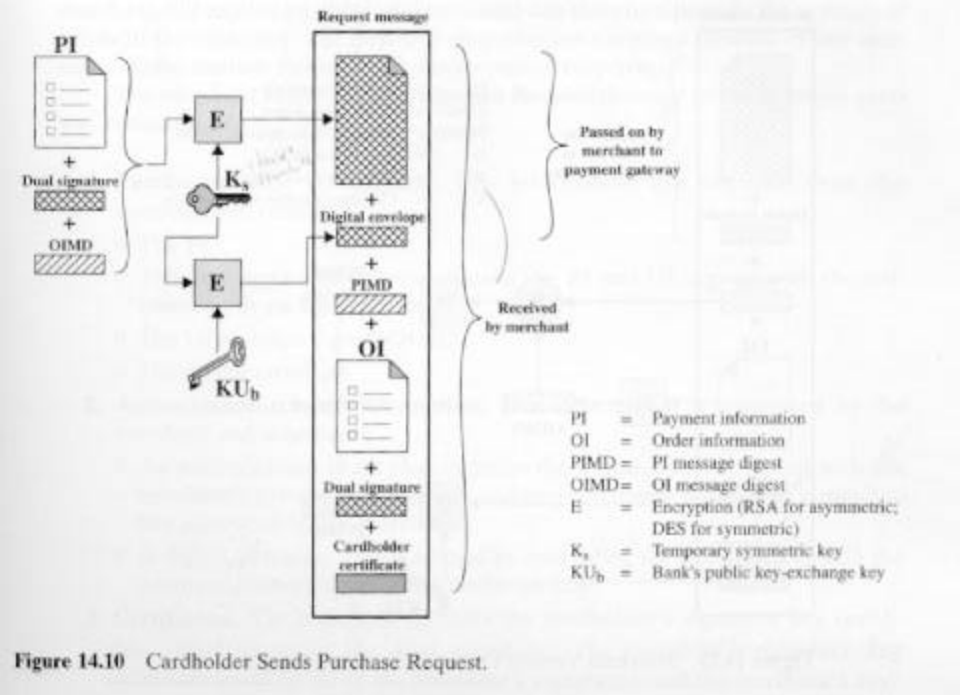


Figure 14.10 Cardholder Sends Purchase Request.

2. Informação relacionada ao pedido: essa informação é necessária para o comerciante e consiste de:
   - A informação do pedido (OI)
   - A assinatura dupla (DS), calculada entre a PI e a OI assinada com a chave privada do consumidor
   - hash da PI
3. O certificado do portador do cartão: contém a chave pública do portador do cartão.

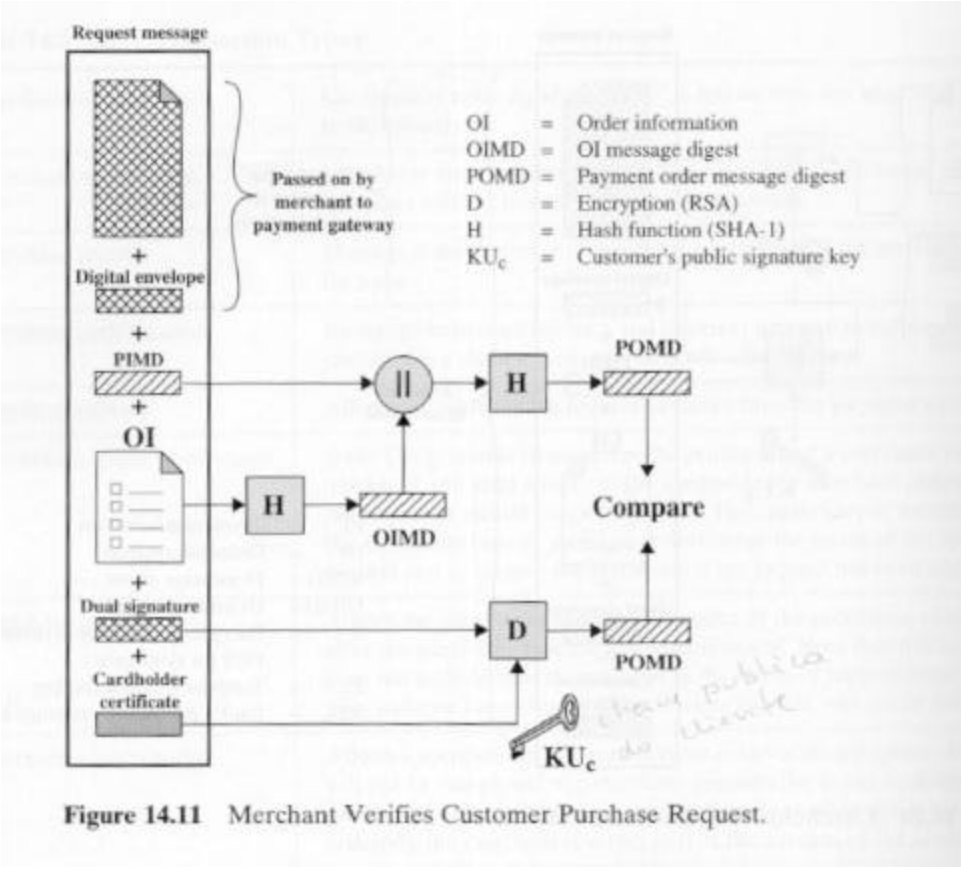


Figure 14.11 Merchant Verifies Customer Purchase Request.

Quando o comerciante recebe a mensagem de pedido de compra ele realiza as seguintes ações:

- Verifica o certificado do portador do cartão pela sua assinatura da autoridade certificadora
- Verifica a assinatura dupla usando a chave pública do cliente. Isto garante que o pedido não foi modificado na transmissão e que foi assinado usando a chave privada do portador do cartão
- Processa o pedido e encaminha a informação de pagamento para o *gateway* de pagamento
- Envia a resposta da compra para o portador do cartão

A resposta da compra (*Purchase Response*) inclui um bloco de reconhece o pedido e referencia o número da transação correspondente. Este bloco é assinado com a chave pública do comerciante. O bloco e sua assinatura são enviados para o cliente, juntamente com o certificado de assinatura do comerciante.

Quando o software do portador do cartão recebe a mensagem de resposta da compra, ele verifica o certificado do comerciante e então verifica a assinatura no bloco de resposta. Finalmente, são realizadas algumas ações como atualizar o banco de dados e de mostrar a mensagem para o usuário.

Algoritmo Criptográfico Blowfish

Blowfish é um algoritmo criptográfico de chave simétrica desenvolvido por Bruce Schneier. Consiste de um cifrador em blocos de 64 bits com chaves de tamanho variável (até 448 bits). O *Blowfish* ganhou uma grande aceitação no mercado sendo utilizado em diversas aplicações, dentre elas, o Nautilus e o PGPfone. Ainda não são conhecidos ataques contra ele.

Possui:

- Cifragem em blocos de 64 bits;
- Chave de tamanho variável: 32 à 448 bits;
- Desenvolvido por Bruce Schneier;
- Mais rápido que o DES e o IDEA;
- Não patenteado e totalmente grátis;
- Não necessita de licença;
- *Código fonte* disponível para download.

O algoritmo criptográfico Blowfish

O *Blowfish* é um algoritmo criptográfico simétrico de blocos que pode ser usado em substituição ao DES ou IDEA. Ele toma uma chave de tamanho variável, de 32 a 448 bits, tornando-o ideal para aplicações tanto domésticas, quanto comerciais. O *Blowfish* foi desenvolvido em 1993 como uma alternativa grátis mais rápida para os algoritmos criptográficos existentes. Desde então ele vem sendo analisado de forma considerável e está conquistando a aceitação do mercado como um algoritmo forte. O *Blowfish* não é patenteado, tem sua licença grátis e está a disposição para todos.

Qualquer pessoa é bem vinda para efetuar o "download" do Blowfish e fazer uso em suas aplicações.. Não há regras de uso do código. Bruce Schneier pede, somente, que seja notificado de aplicações comerciais para que possam ser listadas em seu *website*.

Uma implementação que serve como referência do Blowfish (nos modos ECB, CBC, CFB e OFB) está disponível em ftp://ftp.psy.uq.oz.au/ ou em *ftp.ox.ac.uk*.

Uma *implementação em Java* pode ser encontrada como parte do *Cryptix*.

GLOSSÁRIO

TEXTO PURO	É o texto destinado a ser colocado de forma secreta ou ininteligível para o publico comum.
TEXTO CIFRADO	É o texto puro após ser alterado pela cifra ou palavra-chave.
CIFRAR, CODIFICAR:	Ato de transformar o texto puro em texto cifrado.
DECIFRAR, DECODIFICAR:	Ato de transformar o texto cifrado em texto puro.
QUEBRAR A SENHA OU SEGREDO:	Conseguir decifrar um texto cifrado sem possuir a senha.
TRANSPOSICAO	Alterar a ordem das letras, tal como transformar segredo em esoderg.
SUBSTITUICAO	Substituir letras especificas por outras, ou por números ou símbolos. Escrever SOS em código morse seria uma substituição. ex: texto puro: SOS código morse: ...---... Vários músicos também usavam linguagem de duplo sentido, para poder transmitir sua mensagem (isso, antes de terem que se asilar para escaparem a repressão).
ALFABETO CIFRADO:	Um alfabeto para ser usado para transposição. ex: Alfabeto puro: a b c d e f g h i j k l m n o p q r s t u v x y z Dessa forma, inimigo viraria TQTPTCE. Pode-se usar mais de um alfabeto, quando então o sistema se chama polialfabético.
CODIGOS	Essa é mais ou menos, a forma favorita do brasileiro de criptografia. Consiste em se utilizar palavras-de-codigo ou números- de-codigo para representar o texto, como acontece com as gírias. ex: numero-codigo texto-puro 11 muito bom (ver filme "mulher nota 10") 10 bom 1 ruim 5 medio 24 homossexual 171 estelionato Obs: Usei exemplos ja' incorporados a cultura popular, mas esse tipo de código é muito usado pela policia. A gíria usada por um grupo especifico, tal como usar "foca" para designar repórter iniciante na imprensa também pode ser chamada de código.

VOCABULARIO Nesse texto, o conjunto de palavras que compõem um código, tal como visto acima.

PALAVRA-CHAVE: A expressão ou código que permite o deciframento do texto cifrado.

BIBLIOGRAFIA

[BEL95] BARATA ELETRICA, número 2 São Paulo, 15 de abril de 1995.

[Leo01] *Criptografia - Historia y Métodos Clásicos*. Disponível na URL http://leo.worldonline.es/jlquijad/histo.htm. [15/04/2001]

[Ign01] MENDVIL. Ignacio, *El ABC de los Documentos Electrónicos Seguros*. Disponível na URL http://www.seguridata.com [15/04/2001]

[APS99] MENEZES. Alfred J., OORSCHOT Paul C. van, VANSTONE. Scott A., *Handbook of Applied Cryptography*. CRC Press; 4ª ed. jul 1999. Disponível na URL http://www.cacr.math.uwaterloo.ca/hac/index.html. [15/04/2001]

[Ric00] MENEZES. Ricardo, *Escrita Secreta: Criptologia.* 23 nov 2000. Disponível na URL http://www.gecm.org.br/!cripto/EscritaSecreta.html [15/04/2001]

[RSA00] RSA Laboratories. *RSA Laboratories' Frequently Asked Questions About Today's Cryptography*. maio 2000. RSA Security Inc.

[SP01] SOUSA Jr, Rafael T. de., PUTTINI, Ricardo S. *Criptografia e Segurança de Redes de Computadores*. UnB - Departamento de Engenharia Elétrica. Brasília. Disponível na URL http://webserver.redes.unb.br/security/introducao/aspectos.html [15/04/2001]