Criptografia simétrica e assimétrica: os principais algoritmos de cifragem

Ronielton Rezende Oliveira, MBA, PMP®, ronielton@ronielton.eti.br

Resumo

A palavra criptografia provém dos radicais gregos kriptos (oculto) e grapho (escrita) e é o nome dado à ciência ou arte de codificar mensagens usando uma fórmula, que também será utilizada depois para decodificar a mesma mensagem. Na criptografia moderna, esta fórmula é chamada de algoritmo. Usada há milênios pela humanidade, a criptografia se tornou essencial para garantir a privacidade das comunicações no mundo atual, principalmente em redes de computadores públicas como a internet, por onde circulam dados pessoais, comerciais, bancários e outros. Conhecer, difundir e utilizar algoritmos criptográficos é essencial ao profissional de Tecnologia da Informação que no mundo moderno, entre suas atribuições deve proteger e garantir a privacidade das transações comerciais realizadas através de meios eletrônicos, assim é fundamental o entendimento das técnicas, seus algoritmos, protocolos e finalmente a maneira como estes lidam com a informação a ser mantida segura.

Palavras chave: Criptografia; Algoritmo; Segurança.

1. Introdução

Quando falamos de informação e transportamos este conceito para o meio digital, particularmente na utilização das redes públicas de computação como a internet, e diversos são os serviços realizados é relevante ao ser humano à credibilidade nos sistemas computacionais, estes que inseridos nos fundamentos da segurança da informação, são definidos pela disponibilidade, integridade, controle de acesso, autenticidade, não-repudiação e finalmente a privacidade, os quais devem ser de livre compreensão e facilmente perceptíveis ao se efetuar transações computacionais:

- Disponibilidade - garantir que uma informação estará disponível para acesso no momento desejado.
- Integridade - garantir que o conteúdo da mensagem não foi alterado.
- Controle de acesso - garantir que o conteúdo da mensagem somente será acessado por pessoas autorizadas.
- Autenticidade - garantir a identidade de quem está enviando a mensagem.
- Não-repudiação - prevenir que alguém negue o envio e/ou recebimento de uma mensagem.
- Privacidade - impedir que pessoas não autorizadas tenham acesso ao conteúdo da mensagem, garantindo que apenas a origem e o destino tenham conhecimento.

O exemplo clássico é uma compra pela internet, todos os requisitos são encontrados neste processo de troca de informações: A informação que permite a transação - valor e descrição do produto - precisa estar disponível no dia e na hora que o cliente desejar efetuá-la (disponibilidade), o valor da transação não pode ser alterado (integridade), somente o cliente que está comprando e o comerciante devem ter acesso à transação (controle de acesso), o

cliente que está comprando deve ser realmente quem diz ser (autenticidade), o cliente tem como provar o pagamento e o comerciante não têm como negar o recebimento (não-repúdio) e o conhecimento do conteúdo da transação fica restrito aos envolvidos (privacidade).

Assim é fundamental que técnicas computacionais sejam empregadas para que os requisitos de proteção da informação sejam atendidos. Neste cenário apresentam-se os dois tipos básicos de criptografia: a simétrica ou chave privada, e a assimétrica ou chave pública.

2. Criptografia simétrica ou chave privada

O modelo mais antigo de criptografia, em que a chave, isto é, o elemento que dá acesso à mensagem oculta trocada entre duas partes, é igual (simétrica) para ambas as partes e deve permanecer em segredo (privada). Tipicamente, esta chave é representada por uma senha, usada tanto pelo remetente para codificar a mensagem numa ponta, como pelo destinatário para decodificá-la na outra.

Essencialmente, quando a origem (ALFA) cifra uma mensagem, ele utiliza um algoritmo de ciframento para transformar o conteúdo em claro da mensagem em texto cifrado. Quando o destino (BRAVO) decifra uma mensagem, ele utiliza o algoritmo de deciframento correspondente para converter o texto cifrado de novo em uma mensagem clara. Se um intruso (CHARLIE) conhecer o algoritmo de ciframento, ele poderia decifrar uma mensagem cifrada tão facilmente quanto o destino (BRAVO). A solução no uso da criptografia de chave privada propõe que quando a origem (ALFA) cifra uma mensagem, ele utilize um algoritmo de ciframento e uma chave secreta para transformar uma mensagem clara em um texto cifrado. O destino (BRAVO), por sua vez, ao decifrar a mensagem, utiliza o algoritmo de deciframento correspondente e a mesma chave para transformar o texto cifrado em uma mensagem em claro. O intruso (CHARLIE), por não possuir a chave secreta, mesmo conhecendo o algoritmo, não conseguirá decifrar a mensagem. A segurança do sistema passa a residir não mais no algoritmo e sim na chave empregada. É ela (chave privada) que agora, no lugar do algoritmo, deverá ser mantida em segredo pela origem (ALFA) e destino (BRAVO).

A principal vantagem é a simplicidade, esta técnica apresenta facilidade de uso e rapidez para executar os processos criptográficos. Entenda que se as chaves utilizadas forem complexas a elaboração de um algoritmo de chave privada se torna bastante fácil, porém as possibilidades de interceptação são correlatas aos recursos empregados, entretanto sua utilização é considerável no processo de proteção da informação, pois quanto mais simples o algoritmo, melhor é a velocidade de processamento e facilidade de implementação.

O principal problema residente na utilização deste sistema de criptografia é que quando a chave de ciframento é a mesma utilizada para deciframento, ou esta última pode facilmente ser obtida a partir do conhecimento da primeira, ambas precisam ser compartilhadas previamente entre origem e destino, antes de se estabelecer o canal criptográfico desejado, e durante o processo de compartilhamento a senha pode ser interceptada, por isso é fundamental utilizar um canal seguro durante o compartilhamento, este independente do destinado à comunicação sigilosa, uma vez que qualquer um que tenha acesso à senha poderá descobrir o conteúdo secreto da mensagem. Outras lacunas são interpostas a este sistema:

- Como cada par necessita de uma chave para se comunicar de forma segura, para um uma rede de n usuários precisaríamos de algo da ordem de n^2 chaves, quantidade esta que dificulta a gerência das chaves;
- A chave deve ser trocada entre as partes e armazenada de forma segura, o que nem sempre é fácil de ser garantido;

- A criptografia simétrica não garante os princípios de autenticidade e não-repudiação.

Tabela 1 - Principais algoritmos de chave privada ou criptografia simétrica

Algoritmo	Bits	Descrição
AES	128	O Advanced Encryption Standard (AES) é uma cifra de bloco, anunciado pelo National Institute of Standards and Technology (NIST) em 2003, fruto de concurso para escolha de um novo algoritmo de chave simétrica para proteger informações do governo federal, sendo adotado como padrão pelo governo dos Estados Unidos, é um dos algoritmos mais populares, desde 2006, usado para criptografia de chave simétrica, sendo considerado como o padrão substituto do DES. O AES tem um tamanho de bloco fixo em 128 bits e uma chave com tamanho de 128, 192 ou 256 bits, ele é rápido tanto em software quanto em hardware, é relativamente fácil de executar e requer pouca memória.
DES	56	O Data Encryption Standard (DES) foi o algoritmo simétrico mais disseminado no mundo, até a padronização do AES. Foi criado pela IBM em 1977 e, apesar de permitir cerca de 72 quadrilhões de combinações, seu tamanho de chave (56 bits) é considerado pequeno, tendo sido quebrado por "força bruta" em 1997 em um desafio lançado na internet. O NIST que lançou o desafio mencionado, recertificou o DES pela última vez em 1993, passando então a recomendar o 3DES.
3DES	112 ou 168	O 3DES é uma simples variação do DES, utilizando o em três ciframentos suscessivos, podendo empregar uma versão com duas ou com três chaves diferentes. É seguro, porém muito lento para ser um algoritmo padrão.
IDEA	128	O International Data Encryption Algorithm (IDEA) foi criado em 1991 por James Massey e Xuejia Lai e possui patente da suíça ASCOM Systec. O algoritmo é estruturado seguindo as mesmas linhas gerais do DES. Mas na maioria dos microprocessadores, uma implementação por software do IDEA é mais rápida do que uma implementação por software do DES. O IDEA é utilizado principalmente no mercado financeiro e no PGP, o programa para criptografia de e-mail pessoal mais disseminado no mundo.
Blowfish	32 a 448	Algoritmo desenvolvido por Bruce Schneier, que oferece a escolha, entre maior segurança ou desempenho através de chaves de tamanho variável. O autor aperfeiçoou o no Twofish.
Twofish	128	É uma das poucas cifras incluídas no OpenPGP. O Twofish é uma chave simétrica que emprega a cifra de bloco de 128 bits, utilizando chaves de tamanhos variáveis, podendo ser de 128, 192 ou 256 bits. Ele realiza 16 interações durante a criptografia, sendo um algoritmo bastante veloz. A cifra Twofish não foi patenteada estando acessível no domínio público, como resultado, o algoritmo Twofish é de uso livre para qualquer um utilizar sem restrição.
RC2	8 a 1024	Projetado por Ron Rivest (o R da empresa RSA Data Security Inc.) e utilizado no protocolo S/MIME, voltado para criptografia de e-mail corporativo. Também possui chave de tamanho variável. Rivest também é o autor dos algoritmos RC4, RC5 e RC6.
CAST	128	É um algoritmo de cifra de bloco, sendo criado em 1996 por Carlisle Adams e Stafford Tavares. O CAST-128 é um algoritmo de Feistel, com 12 a 16 iterações da etapa principal, tamanho de bloco de 64 bits e chave de tamanho variável (40 a 128 bits, com acréscimos de 8 bits). Os 16 rounds de iteração são usados quando a chave tem comprimento maior que 80 bits.

3. Criptografia assimétrica ou chave pública

Modelo de criptografia criado na década de 1970 - pelo matemático Clifford Cocks que trabalhava no serviço secreto inglês, o GCHQ - na qual cada parte envolvida na comunicação usa duas chaves diferentes (assimétricas) e complementares, uma privada e outra pública. Neste caso, as chaves não são apenas senhas, mas arquivos digitais mais complexos (que eventualmente até estão associados a uma senha). A chave pública pode ficar disponível para qualquer pessoa que queira se comunicar com outra de modo seguro, mas a chave privada

deverá ficar em poder apenas de cada titular. É com a chave privada que o destinatário poderá decodificar uma mensagem que foi criptografada para ele com sua respectiva chave pública.

Para entender o conceito, basta pensar num cadeado comum protegendo um determinado bem. A mensagem é este bem, e o cadeado, que pode ficar exposto, é a chave pública. Apenas quem tiver uma chave particular (privada) que consiga abrir o cadeado poderá acessar a mensagem. A principal vantagem deste método é a sua segurança, pois não é preciso (nem se deve) compartilhar a chave privada. Por outro lado, o tempo de processamento de mensagens com criptografia assimétrica é muitas vezes maior do que com criptografia simétrica, o que pode limitar seu uso em determinadas situações.

Essencialmente, o destino (BRAVO) e todos os que desejam comunicar-se de modo seguro geram uma chave de ciframento e sua correspondente chave de deciframento. Ele mantém secreta a chave de deciframento, esta é chamada de sua chave privada. Ele torna pública a chave de ciframento, esta é chamada de sua chave pública. A chave pública realmente condiz com seu nome. Qualquer pessoa pode obter uma cópia dela. O destino (BRAVO) inclusive encoraja isto, enviando-a para seus amigos ou publicando-a na internet. Assim, O intruso (CHARLIE) não tem nenhuma dificuldade em obtê-la. Quando a origem (ALFA) deseja enviar uma mensagem ao destino (BRAVO), precisa primeiro encontrar a chave pública dele. Feito isto, ela cifra sua mensagem utilizando a chave pública do destino (BRAVO), despachando-a em seguida. Quando o destino (BRAVO) recebe a mensagem, ele a decifra facilmente com sua chave privada. O intruso (CHARLIE), que interceptou a mensagem em trânsito, não conhece a chave privada do destino (BRAVO), embora conheça sua chave pública. Mas este conhecimento não o ajuda a decifrar a mensagem. Mesmo a origem (ALFA), que foi quem cifrou a mensagem com a chave pública do destino (BRAVO), não pode decifrá-la agora.

A grande vantagem deste sistema é permitir a qualquer um enviar uma mensagem secreta, apenas utilizando a chave pública de quem irá recebê-la. Como a chave pública está amplamente disponível, não há necessidade do envio de chaves como feito no modelo simétrico. A confidencialidade da mensagem é garantida, enquanto a chave privada estiver segura. Caso contrário, quem possuir acesso à chave privada terá acesso às mensagens.

O óbice deste sistema é a complexidade empregada no desenvolvimento dos algoritmos que devem ser capazes de reconhecer a dupla de chaves existentes e poder relacionar as mesmas no momento oportuno, o que acarreta num grande poder de processamento computacional.

Tabela 2 - Principais algoritmos de chave pública ou criptografia assimétrica

Algoritmo	Descrição
RSA	O RSA é um algoritmo assimétrico que possui este nome devido a seus inventores: Ron Rivest, Adi Shamir e Len Adleman, que o criaram em 1977 no MIT. Atualmente, é o algoritmo de chave pública mais amplamente utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecidas até o momento. O RSA utiliza números primos. A premissa por trás do RSA consiste na facilidade de multiplicar dois números primos para obter um terceiro número, mas muito difícil de recuperar os dois primos a partir daquele terceiro número. Isto é conhecido como fatoração. Por exemplo, os fatores primos de 3.337 são 47 e 71. Gerar a chave pública envolve multiplicar dois primos grandes; qualquer um pode fazer isto. Derivar a chave privada a partir da chave pública envolve fatorar um grande número. Se o número for grande o suficiente e bem escolhido, então ninguém pode fazer isto em uma quantidade de tempo razoável. Assim, a segurança do RSA baseia se na dificuldade de fatoração de números grandes. Deste modo, a fatoração representa um limite superior do tempo necessário para quebrar o algoritmo. Uma chave RSA de 512 bits foi quebrada em 1999 pelo Instituto Nacional de Pesquisa da Holanda, com o apoio de cientistas de mais 6 países. Levou cerca de 7 meses e foram utilizadas 300 estações de trabalho para a quebra. No Brasil, o RSA é utilizado pela ICP-Brasil, no seu sistema de emissão de certificados digitais, e a partir do dia 1º de janeiro de 2012, as chaves utilizadas pelas autoridades certificadoras do país, passam a serem emitidas

	com o comprimento de 4.096bits, em vez dos 2.048bits atuais.
ElGamal	O ElGamal é outro algoritmo de chave pública utilizado para gerenciamento de chaves. Sua matemática difere da utilizada no RSA, mas também é um sistema comutativo. O algoritmo envolve a manipulação matemática de grandes quantidades numéricas. Sua segurança advém de algo denominado problema do logaritmo discreto. Assim, o ElGamal obtém sua segurança da dificuldade de calcular logaritmos discretos em um corpo finito, o que lembra bastante o problema da fatoração.
Diffie-Hellman	Também baseado no problema do logaritmo discreto, e o criptosistema de chave pública mais antigo ainda em uso. O conceito de chave pública, aliás foi introduzido pelos autores deste criptosistema em 1976. Contudo, ele não permite nem ciframento nem assinatura digital. O sistema foi projetado para permitir a dois indivíduos entrarem em um acordo ao compartilharem um segredo tal como uma chave, muito embora eles somente troquem mensagens em público.
Curvas Elípticas	Em 1985, Neal Koblitz e V. S. Miller propuseram de forma independente a utilização de curvas elípticas para sistemas criptográficos de chave pública. Eles não chegaram a inventar um novo algoritmo criptográfico com curvas elípticas sobre corpos finitos, mas implementaram algoritmos de chave pública já existentes, como o algoritmo de Diffie-Hellman, usando curvas elípticas. Assim, os sistemas criptográficos de curvas elípticas consistem em modificações de outros sistemas (o ElGamal, por exemplo), que passam a trabalhar no domínio das curvas elípticas, em vez de trabalharem no domínio dos corpos finitos. Eles possuem o potencial de proverem sistemas criptográficos de chave pública mais seguros, com chaves de menor tamanho. Muitos algoritmos de chave pública, como o Diffie-Hellman, o ElGamal e o Schnorr podem ser implementados em curvas elípticas sobre corpos finitos. Assim, fica resolvido um dos maiores problemas dos algoritmos de chave pública, o grande tamanho de suas chaves. Porém, os algoritmos de curvas elípticas atuais, embora possuam o potencial de serem rápidos, são em geral mais demorados do que o RSA.

4. Certificado digital

Com um sistema de chave pública, o gerenciamento de chaves passa a ter dois novos aspectos: primeiro, deve-se previamente localizar a chave pública de qualquer pessoa com quem se deseja comunicar e, segundo, deve-se obter uma garantia de que a chave pública encontrada seja proveniente daquela pessoa. Sem esta garantia, um intruso pode convencer os interlocutores de que chaves públicas falsas pertencem a eles. Estabelecendo um processo de confiança entre os interlocutores, o intruso pode fazer-se passar por ambos. Deste modo, quando um emissor enviar uma mensagem ao receptor solicitando sua chave pública, o intruso poderá interceptá-la e devolver-lhe uma chave pública forjada por ele. Ele também pode fazer o mesmo com o receptor, fazendo com que cada lado pense que está se comunicando com o outro, quando na verdade estão sendo interceptados pelo intruso, então este pode decifrar todas as mensagens, cifrá-las novamente ou, se preferir, até substituí-las por outras mensagens. Através deste ataque, um intruso pode causar tantos danos ou até mais do que causaria se conseguisse quebrar o algoritmo de ciframento empregado pelos interlocutores.

A garantia para evitar este tipo de ataque é representada pelos certificados de chave pública, comumente chamados de certificado digital, tais certificados consistem em chaves públicas assinadas por uma pessoa de confiança. Servem para evitar tentativas de substituição de uma chave pública por outra. O certificado contém algo mais do que sua chave pública, ele apresenta informações sobre o nome, endereço e outros dados pessoais, e é assinado por alguém em quem o proprietário deposita sua confiança, uma autoridade de certificação (certification authority - CA). Assim, um certificado digital pode ser definido como um documento eletrônico, assinado digitalmente por uma terceira parte confiável.

No Brasil, o órgão da autoridade certificadora raiz é o ICP-Brasil (AC-Raiz), ele é o executor das políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. São autoridades certificadoras no país: Serpro (AC-SERPRO), Caixa Econômica Federal (AC-CAIXA), Serasa Experian (AC-SERASA), Receita Federal do Brasil

(AC-RFB), Certsing (AC-Certisign), Imprensa Oficial do Estado de São Paulo (AC-IOSP), Autoridade Certificadora da Justiça (AC-JUS), Autoridade Certificadora da Presidência da República (AC-PR) e Casa da Moeda do Brasil (AC-CMB).

Assim, a AC-Raiz tem autoridade de emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu, sendo também encarregada de emitir a lista de certificados revogados e de fiscalizar e auditar as autoridades certificadoras, autoridades de registro e demais prestadores de serviço habilitados na ICP-Brasil. Além disso, verifica se as autoridades certificadoras (ACs) estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor.

5. Assinatura digital

O sistema de criptografia assimétrica ou de chave pública também é utilizado como um meio de assinatura digital. A pessoa que assina usa sua chave privada para criptografar uma mensagem conhecida, e o texto cifrado pode ser decifrado por qualquer um usando a chave pública desta pessoa, assim como uma assinatura em papel, consiste em um bloco de informação adicionado à mensagem que comprova a identidade do emissor, confirmando quem ele diz ser.

O processo se baseia em uma inversão do sistema, onde o funcionamento da assinatura digital pode ser descrito como: o emissor cifra (ou seja, atesta autenticidade) a mensagem com sua chave privada e a envia, em um processo denominado de assinatura digital. Cada um que receber a mensagem deverá verificar a validade da assinatura digital, utilizando para isso a chave pública do emissor, reconhecendo de fato, que a mensagem não foi adulterada.

Como a chave pública do emissor apenas decifra (ou seja, verifica a validade) mensagens cifradas com sua chave privada, obtém-se a garantia de autenticidade, integridade e não-repudiação da mensagem, o que é apoiado pela função hashing, pois se alguém modificar um bit do conteúdo da mensagem ou se outra pessoa assiná-la ao invés do próprio emissor, o sistema de verificação não irá reconhecer a assinatura digital dele como sendo válida.

É importante perceber que a assinatura digital, como descrita, não garante a confidencialidade da mensagem. Qualquer um poderá acessá-la e verificá-la, mesmo um intruso, apenas utilizando a chave pública do emissor, assim, ao empregar o uso da técnica de assinatura digital o que se busca é a garantia de autenticidade, integridade e não-repudiação da mensagem.

Tabela 3 - Principais algoritmos de assinatura digital

Algoritmo	Descrição
RSA	Como já mencionado, o RSA também é comutativo e pode ser utilizado para a geração de assinatura digital. A matemática é a mesma, há uma chave pública e uma chave privada, e a segurança do sistema baseia se na dificuldade da fatoração de números grandes.
ElGamal	Como o RSA, o ElGamal também é comutativo, podendo ser utilizado tanto para assinatura digital quanto para gerenciamento de chaves; assim, ele obtém sua segurança da dificuldade do cálculo de logaritmos discretos em um corpo finito.
DSA	Inventado pela NSA e patenteado pelo governo americano, o Digital Signature Algorithm (DSA), unicamente destinado a assinaturas digitais, foi proposto pelo NIST em agosto de 1991, para utilização no seu padrão Digital Signature Standard (DSS). Adotado como padrão final em dezembro de 1994, trata de uma variação dos algoritmos de assinatura ElGamal e Schnorr.

6. Função hashing

A assinatura digital obtida através do uso da criptografia assimétrica ou de chave pública infelizmente não pode ser empregada, na prática, de forma isolada, é necessário o emprego de

um mecanismo fundamental para o adequado emprego da assinatura digital. Este mecanismo é a função hashing.

Assim, na prática é inviável e contraproducente utilizar puramente algoritmos de chave pública para assinaturas digitais, principalmente quando se deseja assinar grandes mensagens, que podem levar preciosos minutos ou mesmo horas para serem integralmente cifradas com a chave privada de alguém, ao invés disso, é empregada uma função hashing, que gera um valor pequeno, de tamanho fixo, derivado da mensagem que se pretende assinar, de qualquer tamanho, para oferecer agilidade nas assinaturas digitais, além de integridade confiável.

Serve, portanto, para garantir a integridade do conteúdo da mensagem que representa, por isto, após o valor hash de uma mensagem ter sido calculado através do emprego de uma função hashing, qualquer modificação em seu conteúdo - mesmo em apenas um bit da mensagem - será detectada, pois um novo cálculo do valor hash sobre o conteúdo modificado resultará em um valor hash bastante distinto.

Tabela 4 - Principais funções hashing

Funções	Descrição
SHA-2	O Secure Hash Algorithm (SHA-2) por outro lado significativamente difere da função hash SHA-1, desenhado pelo NSA é uma família de duas funções hash similares, com diferentes tamanhos de bloco, conhecido como SHA-256 e SHA-512. Eles diferem no tamanho, o SHA-256 utiliza 256 bits e o SHA-512 utiliza 512 bits. Há também versões truncadas de cada padrão, conhecidos como SHA-224 e SHA-384. O ICP-Brasil em suas mudanças anunciadas adotadas para o novo padrão criptográfico do sistema de certificação digital, esta implantando em 2012, o uso do SHA-512 em substituição ao seu antecessor, o SHA-1. Um novo padrão proposto de função de hash ainda está em desenvolvimento, pela programação do NIST a competição que apresentará esta nova função hash tem previsão de termino, com a seleção de uma função vencedora, que será dado o nome de SHA-3, ainda em 2012.
SHA-1	O Secure Hash Algorithm (SHA-1), uma função de espalhamento unidirecional inventada pela NSA, gera um valor hash de 160 bits, a partir de um tamanho arbitrário de mensagem. O funcionamento interno do SHA-1 é muito parecido com o observado no MD4, indicando que os estudiosos da NSA basearam-se no MD4 e fizeram melhorias em sua segurança. De fato, a fraqueza existente em parte do MD5, descoberta após o SHA-1 ter sido proposto, não ocorre no SHA-1. Em 2005, falhas de segurança foram identificados no SHA-1, ou seja, que uma fraqueza matemática pode existir, o que indica que o uso de uma função hash mais forte é recomendável, o que motiva o uso preferencial de SHA-2.
MD5	É uma função de espalhamento unidirecional inventada por Ron Rivest, do MIT, que também trabalha para a RSA Data Security. A sigla MD significa message digest. Este algoritmo produz um valor hash de 128 bits, para uma mensagem de entrada de tamanho arbitrário. Foi inicialmente proposto em 1991, após alguns ataques de criptoanálise terem sidos descobertos contra a função hashing prévia de Rivest: a MD4. O algoritmo foi projetado para ser rápido, simples e seguro. Seus detalhes são públicos, e têm sido analisados pela comunidade de criptografia. Foi descoberta uma fraqueza em parte do MD5, mas até agora ela não afetou a segurança global do algoritmo. Entretanto, o fato dele produzir uma valor hash de somente 128 bits é o que causa maior preocupação; é preferível uma função hashing que produza um valor maior.
MD2 e MD4	O MD4 é o precursor do MD5, tendo sido inventado por Ron Rivest. Após terem sido descobertas algumas fraquezas no MD4, Rivest escreveu o MD5. O MD4 não é mais utilizado. O MD2 é uma função de espalhamento unidirecional simplificada, e produz um hash de 128 bits. A segurança do MD2 é dependente de uma permutação aleatória de bytes. Não é recomendável sua utilização, pois, em geral, é mais lento do que as outras funções hash citadas e acredita-se que seja menos seguro.

7. Sistemas híbridos

Em resumo, os algoritmos criptográficos podem ser combinados para a implementação dos três mecanismos criptográficos básicos: o ciframento, a assinatura e o hashing. Estes mecanismos são componentes dos protocolos criptográficos, embutidos na arquitetura de segurança dos produtos destinados ao comércio eletrônico.

Estes protocolos criptográficos, portanto, provêm os serviços associados à criptografia que viabilizam o comércio eletrônico: disponibilidade, sigilo, controle de acesso, autenticidade, integridade e não-repúdio, usualmente apoiado por sistemas híbridos.

Tabela 5 - Protocolos com Sistemas Híbridos

Protocolo	Descrição
IPSec	Padrão de protocolos criptográficos desenvolvidos para o IPv6. Realiza também o tunelamento de IP sobre IP. É composto de três mecanismos criptográficos: Authentication Header (define a função hashing para assinatura digital), Encapsulation Security Payload (define o algoritmo simétrico para ciframento) e ISAKMP (define o algoritmo assimétrico para gerência e troca de chaves de criptografia). Criptografia e tunelamento são independentes, e permite Virtual Private Network (VPN) fim-a-fim.
SSL e TLS	Oferecem suporte de segurança criptográfica para os protocolos NTTP, HTTP, SMTP e Telnet. Permitem utilizar diferentes algoritmos simétricos, message digest (hashing) e métodos de autenticação e gerência de chaves (assimétricos).
PGP	O Pretty Good Privacy (PGP), foi inventado por Phil Zimmermman em 1991, é um programa criptográfico famoso e bastante difundido na internet, destinado à criptografia de e-mail pessoal. Algoritmos suportados: hashing: MD5, SHA-1 - simétricos: CAST-128, IDEA e 3DES - assimétricos: RSA, Diffie-Hellman e DSS.
S/MIME	O Secure Multipurpose Internet Mail Extensions (S/MIME) consiste em um esforço de consórcio de empresas, liderado pela RSADSI e Microsoft, para adicionar segurança a mensagens eletrônicas no formato MIME. Apesar do S/MIME e PGP serem ambos padrões para a internet, o S/MIME tem sua maior utilização no mercado corporativo, enquanto o PGP é utilizado em e-mail pessoal.
SET	O SET é um conjunto de padrões e protocolos, para realizar transações financeiras seguras, como as realizadas com cartão de crédito na internet. Oferece um canal de comunicação seguro entre todos os envolvidos na transação. Garante autenticidade X.509v3 e privacidade entre as partes.
X.509	Recomendação ITU-T, a especificação X.509 define o relacionamento entre as autoridades de certificação. Faz parte das séries X.500 de recomendações para uma estrutura de diretório global, baseada em nomes distintos para localização. Utilizado pelo S/MIME, IPSec, SSL/TLS e SET. Baseado em criptografia com chave pública (RSA) e assinatura digital (com hashing).

8. Conclusão

Qual o modelo de criptografia que devemos utilizar, simétrico ou assimétrico? A resposta é simples, devemos utilizar os dois, em um modelo denominado híbrido. Um exemplo de combinação de emprego é encontrado ao utilizar o PGP, que combina um sistema de chave pública (Diffie-Hellmam ou RSA) com um sistema de chave privada (CAST, IDEA ou 3DES).

O algoritmo simétrico, por ser muito mais rápido, é utilizado no ciframento da mensagem em si, enquanto o algoritmo assimétrico, cerca de 1.000 vezes mais lento, permite implementar a distribuição de chaves e a assinatura digital, permitindo garantir a autenticidade de quem envia a mensagem, associada à integridade do seu conteúdo, complementado com a utilização do mecanismo de hashing para assegurar a integridade da assinatura digital.

Tabela 6 – Quadro comparativo

Criptografia simétrica ou chave privada	Criptografia assimétrica ou chave pública
Rápida	Lenta
Gerência e distribuição das chaves é complexa	Gerência e distribuição das chaves é simples
Não oferece assinatura digital	Oferece assinatura digital

Em síntese, proteger a informação é uma máxima que persiste a cada instante quando se incrementa diariamente o número de transações comerciais e financeiras realizadas através de meios eletrônicos, em particular através da internet, neste contexto é necessário o emprego de meios e recursos para que os dados sigilosos estejam a salvo de intrusos, por isto a

importância de conhecer as ferramentas e técnicas oferecidas pela criptografia, afinal desde os primórdios dos tempos o homem vem trabalhando de maneira persistente na elaboração de rotinas, que se transformaram em algoritmos poderosos, e bem empregados propiciam a proteção desejada à informação, aumentando a segurança dos dados e minimizando o impacto dos ataques submetidos às informações que trafegam através das redes de computadores, pelos seus inúmeros dispositivos conectados e muitas vezes vulneráveis.

9. Referências Bibliográficas

COSTA, Celso José da e FIGUEIREDO, Luiz Manoel Silva de. **Criptografia Geral**. 2 ed. Rio de Janeiro : UFF / CEP - EB, 2006. 192p. – (Curso de Criptografia e Segurança em Redes).

FIGUEIREDO, Luiz Manoel Silva de. **Números primos e criptografia de chave pública**. Rio de Janeiro : UFF / CEP - EB, 2006. 180p. – (Curso de Criptografia e Segurança em Redes).

OLIVEIRA, Ronielton Rezende. **Criptografia tradicional simétrica de chave privada e criptografia assimétrica de chave pública: análise das vantagens e desvantagens**. Niterói : Trabalho da pós-graduação Criptografia e Segurança em Redes da UFF, 2006. 20p.