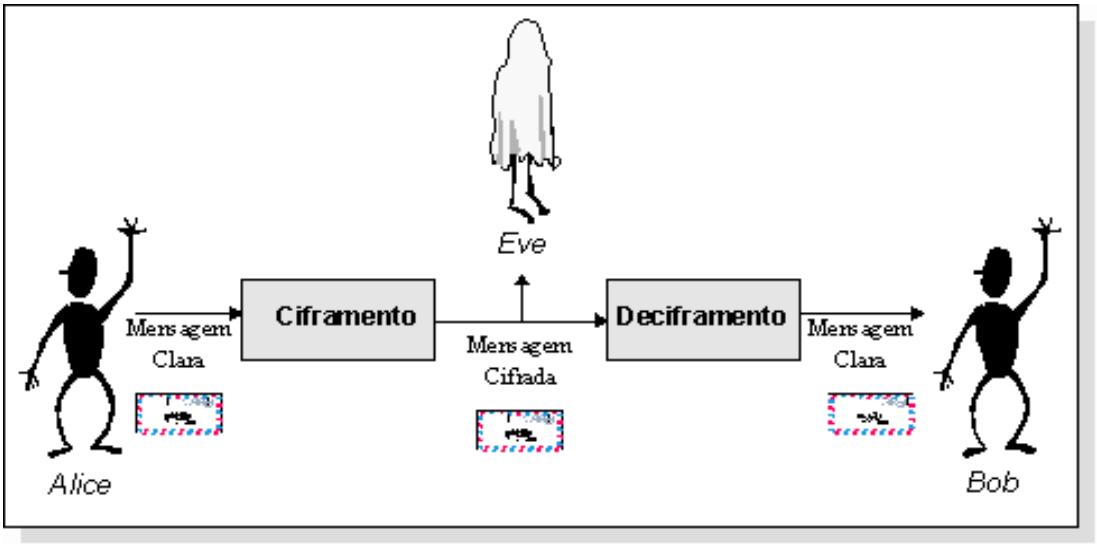
Criptografia e Certificação Digital

Serviços Oferecidos

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

Criptografia Simétrica

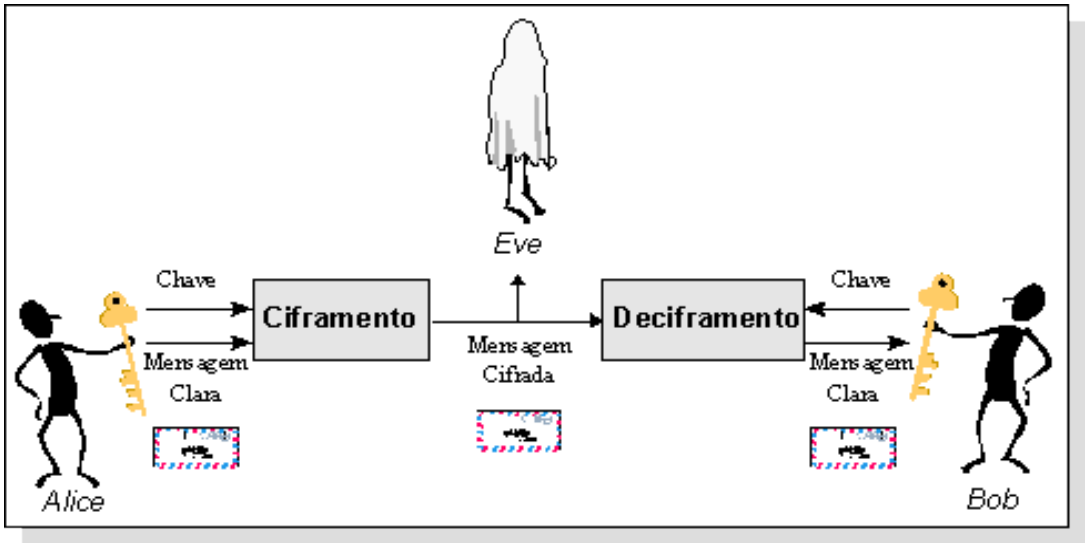
Antigamente, a segurança do ciframento estava baseada somente no sigilo do algoritmo criptográfico.



A utilização de um algoritmo e uma chave oferece duas importantes vantagens.

- A primeira é permitir a utilização do mesmo algoritmo criptográfico para a comunicação com diferentes receptores, apenas trocando a chave.

- A segunda vantagem é permitir trocar facilmente a chave no caso de uma violação, mantendo o mesmo algoritmo.



Criptografia *simétrica* ou de chave secreta : 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 destinatário, antes de se estabelecer o canal criptográfico desejado, utilizando-se um canal seguro e independente do destinado à comunicação sigilosa.

Algoritmo Simétrico	Bits	Descrição
DES	56 (bloco de 64 bits)	O Data Encryption Standard (DES) é o algoritmo simétrico mais disseminado no mundo. Foi criado pela IBM em 1977 e, apesar de permitir cerca de 72 quadrilhões de combinações (2^{56}), 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 (National Institute of Standards and Technology), que lançou o desafio mencionado, recertificou o DES pela última vez em 1993 e desde então está recomendando o 3DES. O NIST está também propondo um substituto ao DES que deve aceitar chaves de 128, 192 e 256 bits, operar com blocos de 128 bits, ser eficiente, flexível e estar livre de "royalties". O padrão, denominado AES (Advanced Encryption Standard), está sendo estudado desde 1997 a partir de vários algoritmos apresentados pela comunidade. O AES foi anunciado pelo NIST (Instituto Nacional de Padrões e Tecnologia dos EUA) como U.S. FIPS PUB (FIPS 197) em 26 de Novembro de 2001, depois de 5 anos de um processo de padronização. Tornou-se um padrão efetivo em 26 de Maio de 2002. Em 2006, o AES já é um dos algoritmos mais populares usados para criptografia de chave simétrica. Dos candidatos, 5 finalistas: MARS, RC6, Rijndael, Serpent e Twofish. Em 2000, é conhecido o vencedor: Rijndael. O algoritmo, criado pelos belgas. Vincent Rijmen e Joan Daemen, foi escolhido com base em qualidades como segurança, flexibilidade, bom desempenho em software e hardware etc.

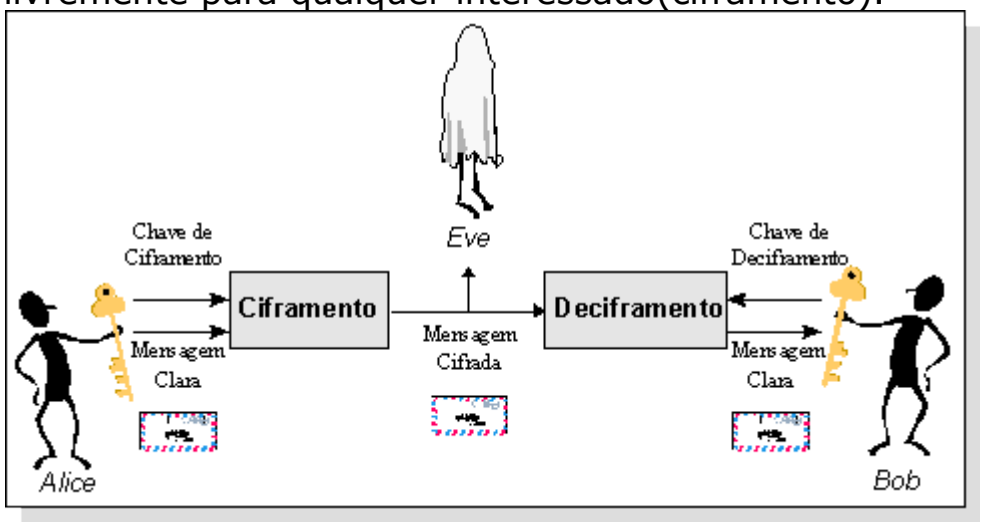
Triple DES	112 ou 168	O 3DES é uma simples variação do DES, utilizando-o em três ciframentos sucessivos, podendo empregar um versão com duas ou com três chaves diferentes. É seguro, porém muito lento para ser um algoritmo padrão.
IDEA	128	O International Data Encryption Algorithm foi criado em 1991 por 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 escolhe entre maior segurança ou desempenho através de chaves de tamanho variável. O autor aperfeiçoou-o no Twofish, concorrente ao AES.
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 do RC4, RC5 e RC6, este último concorrente ao AES.

Apesar de sua simplicidade, existem alguns problemas na criptografia simétrica:

- 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 a identidade de quem enviou ou recebeu a mensagem (autenticidade e não-repudiação).

Criptografia Assimétrica ou chave pública

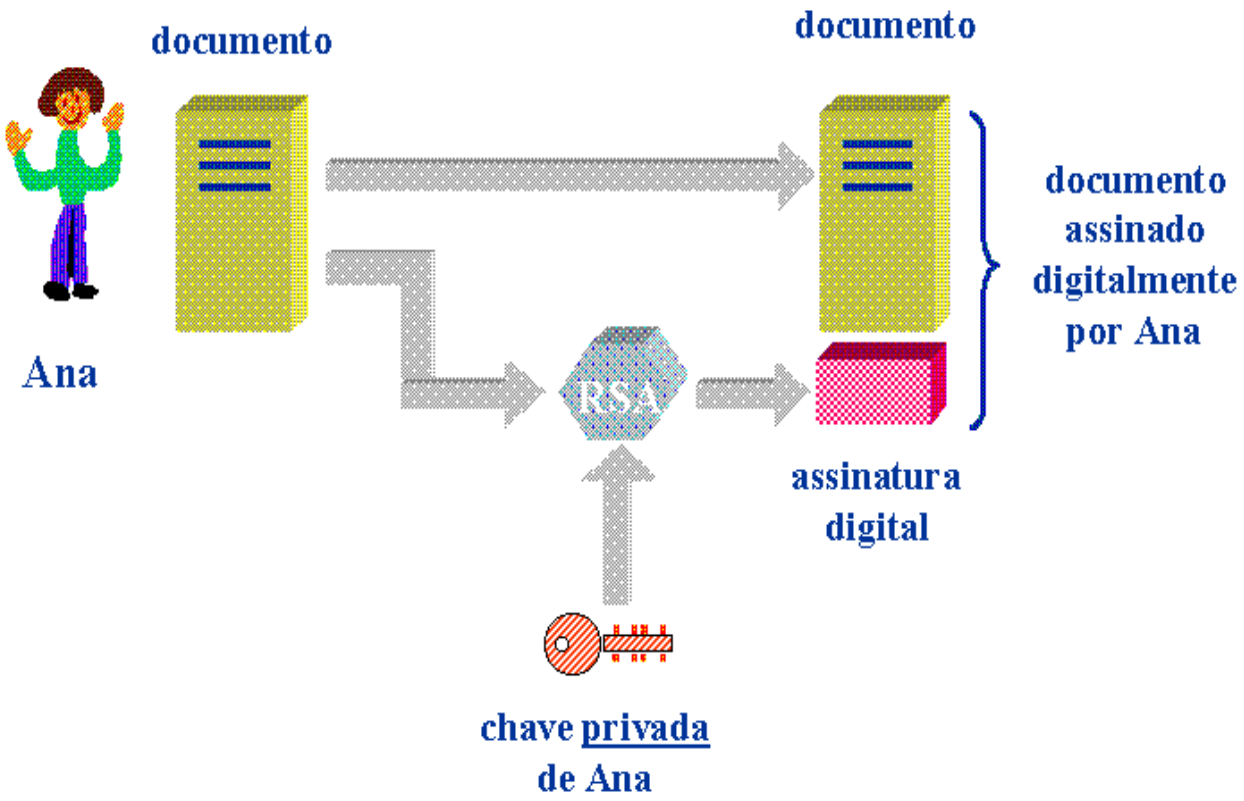
Baseada no conceito de par de chaves: uma chave privada e uma chave pública. Qualquer uma das chaves é utilizada para cifrar uma mensagem e a outra para decifrá-la. As mensagens cifradas com uma das chaves do par só podem ser decifradas com a outra chave correspondente. A chave privada deve ser mantida secreta (deciframento), enquanto a chave pública disponível livremente para qualquer interessado(ciframento).



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. O RSA utiliza números primos. A premissa por trás do RSA é que é fácil multiplicar dois números primos para obter um terceiro número, mas muito difícil 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.
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 se 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 e 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.

Assinatura Digital

Garantir a autenticidade de quem envia a mensagem, associada à integridade do seu conteúdo**.**



É importante perceber que a assinatura digital, como descrita no exemplo anterior, não garante a confidencialidade da mensagem. Qualquer um poderá acessá-la e verificá-la, mesmo um intruso (Eve), apenas utilizando a chave pública de Alice. Para obter confidencialidade com assinatura digital, basta combinar os dois métodos. Alice primeiro assina a mensagem, utilizando sua chave privada. Em seguida, ela criptografa a mensagem novamente, junto com sua assinatura, utilizando a chave pública de Bob. Este, ao receber a mensagem, deve, primeiramente, decifrá-la com sua chave privada, o que garante sua privacidade. Em seguida, "decifrá-la" novamente, ou seja, verificar sua assinatura utilizando a chave pública de Alice, garantindo assim sua autenticidade.

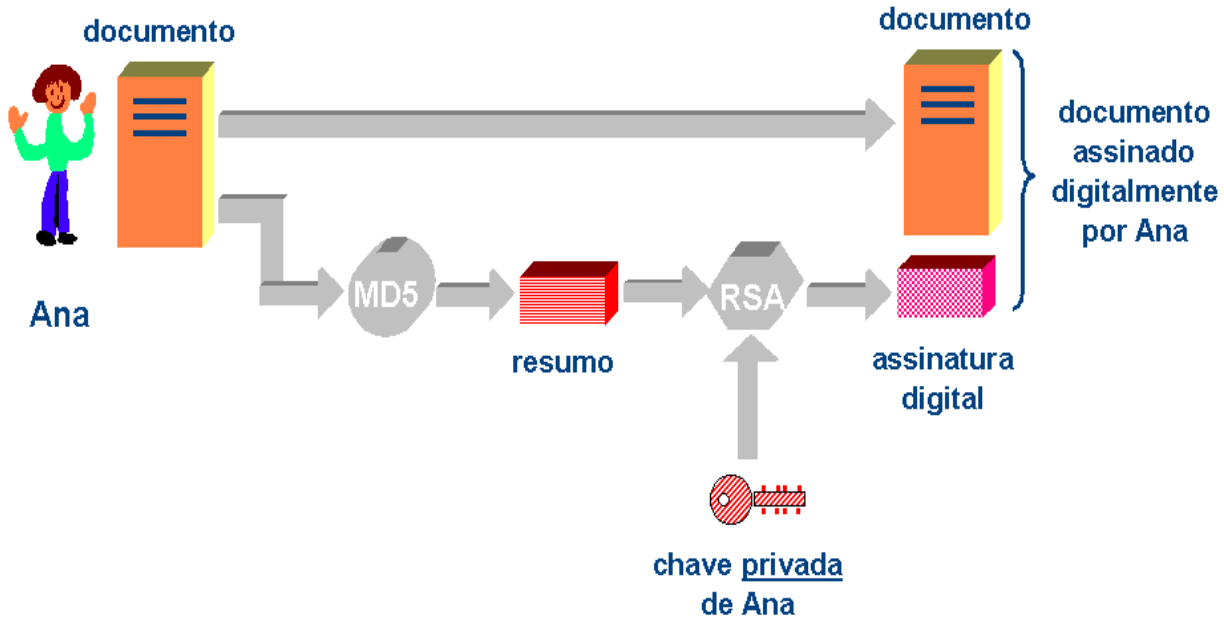
Algoritmo	Descrição
RSA	Como já mencionado, o RSA também é comutativo e pode ser utilizado para a geração de assinatura digital. A matemática é a mesma: há uma chave pública e uma chave privada, e a segurança do sistema baseia-se na dificuldade da fatoração de números grandes.
ElGamal	Como o RSA, o ElGamal 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	O Digital Signature Algorithm, unicamente destinado a assinaturas digitais, foi proposto pelo NIST em agosto de 1991, para utilização no seu padrão DSS (Digital Signature Standard). Adotado como padrão final em dezembro de 1994, trata-se de uma variação dos algoritmos de assinatura ElGamal e Schnorr. Foi inventado pela NSA e patenteado pelo governo americano.

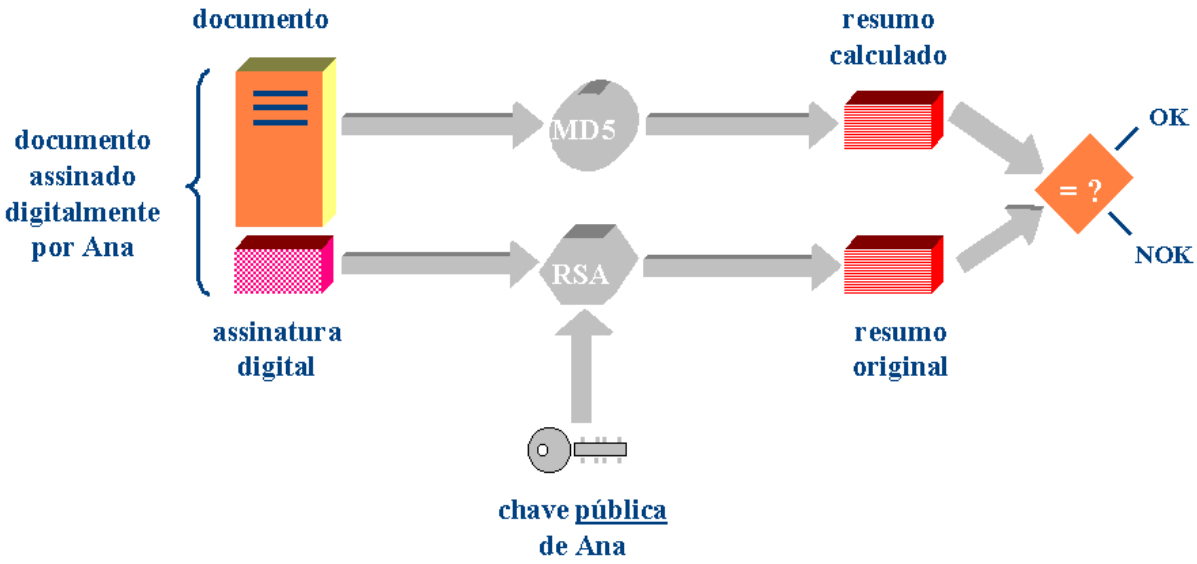
Função Hashing

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. Assim, a função Hashing oferece agilidade nas assinaturas digitais, além de integridade confiável, conforme descrito a seguir.

Também denominada Message Digest, One-Way Hash Function, Função de Condensação ou Função de Espalhamento Unidirecional, a função Hashing funciona como uma impressão digital de uma mensagem gerando, a partir de uma entrada de tamanho variável, um valor fixo pequeno: o digest ou valor hash.

Este valor está para o conteúdo da mensagem assim como o dígito verificador de uma conta-corrente está para o número da conta ou o check sum está para os valores que valida. Serve, portanto, para garantir a integridade do conteúdo da mensagem que representa. Assim, 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.





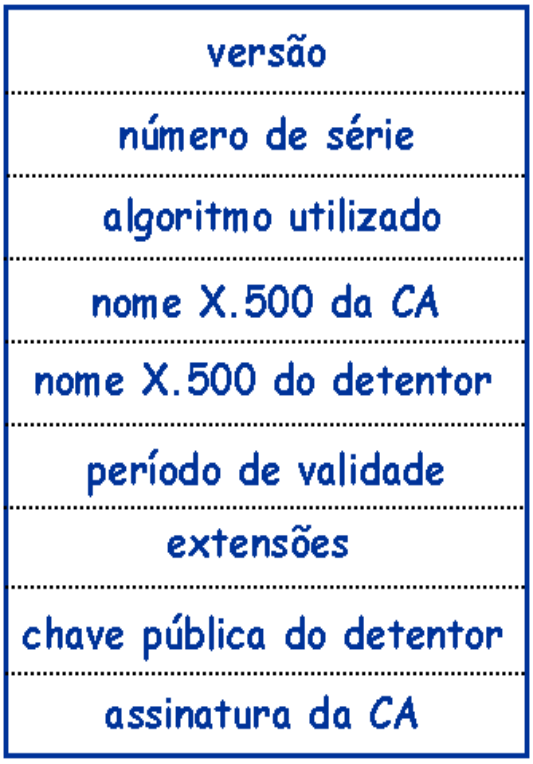
Funções	Descrição
MD5	É uma função de espalhamento unidirecional inventada por Ron Rivest, do MIT, que também trabalha para a RSA Data Security. A sigla MD significa Message Digest. Este algoritmo produz um valor hash de 128 bits, para uma mensagem de entrada de tamanho arbitrário. Foi inicialmente proposto 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.
SHA-1	O Secure Hash Algorithm, 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, citada anteriormente, descoberta após o SHA-1 ter sido proposto, não ocorre no SHA-1. Atualmente, não há nenhum ataque de criptoanálise conhecido contra o SHA-1. Mesmo o ataque da força bruta torna-se impraticável, devido ao seu valor hash de 160 bits. Porém, não há provas de que, no futuro, alguém não possa descobrir como quebrar o SHA-1.
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 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.

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.

Seguem exemplos de protocolos que empregam sistemas criptográficos 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 funçãoHashing 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. Permite Virtual Private Network fim-a-fim. Futuro padrão para todas as formas de VPN.
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	Inventado por Phil Zimmermman em 1991, é um programa criptográfico famoso e bastante difundido na Internet, destinado a criptografia de e-mail pessoal. Algoritmos suportados: hashing: MD5, SHA-1, simétricos: CAST-128, IDEA e 3DES, assimétricos: RSA, Diffie-Hellman/DSS. Versão mais recente: 6.5.3.
S/MIME	O S/MIME (Secure Multipurpose Internet Mail Extensions) consiste em um esforço de um consórcio de empresas, liderado pela RSADSI e pela Microsoft, para adicionar segurança a mensagens eletrônicas no formato MIME. Apesar do S/MIME e PGP serem ambos padrões Internet, o S/MIME deverá se estabelecer no mercado corporativo, enquanto o PGP no mundo do mail pessoal.
SET	O SET é um conjunto de padrões e protocolos, para realizar transações financeira 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).

Certificados de chave pública: garantia para evitar ataque. Consistem em chaves públicas assinadas por uma pessoa de confiança, geralmente no formato padrão ITU X.509v3. Servem para evitar tentativas de substituição de uma chave pública por outra. O certificado de Pessoa1 contém algo mais do que sua chave pública: contém informações como seu nome, endereço e outras dados pessoais - e é assinado por alguém em quem Pessoa2 deposita sua confiança: uma *autoridade de certificação* ou *CA* (*Certification Authority*), que funciona como um cartório eletrônico.



Assim, um certificado digital pode ser definido como um documento eletrônico, assinado digitalmente por uma terceira parte confiável, que associa o nome (e atributos) de uma pessoa ou instituição a uma chave criptográfica pública.

Autoridades de certificação, como Verisign, Cybertrust e Nortel, assinam certificados digitais garantindo sua validade. Uma CA também tem a responsabilidade de manter e divulgar uma lista com os certificados revogados (Certificate Revocation List - CRL). Certificados nesta lista podem ter sido roubados, perdidos ou, simplesmente, estar sem utilidade. As CAs podem estar encadeadas em hierarquias de certificação, onde a CA de um nível inferior valida sua assinatura com a assinatura de uma CA mais alta na hierarquia.

Material retirado de:

Algoritmos de Criptografia. Tecnologiadarede. 2010. Disponível em: <http://tecnologiadarede.webnode.com.br/news/noticia-aos-visitantes/ >. Acesso em: 13/05/2010.

MAIA, Luiz Paulo; PAGLIUSI, Paulo Sergio. Criptografia e Certificação Digital. Disponível em: <http://www.training.com.br/lpmaia/pub_seg_cripto.htm >. Acesso em: 13/05/2010.

FISHER, Dennis. RSA 2010: Experts esperam que sistemas sejam quebrados. 02/03/2010. Disponível em: <http://threatpost.com/pt_br/blogs/rsa-2010-experts-esperam-que-sistemas-sejam-quebrados-030210 >. Acesso em: 13/05/2010.