www.leitejunior.com.br
Informática para Concursos Públicos
leitejuniorbr@yahoo.com.br
leitejuniorbr@hotmail.com

ÍNDICE

CRIPTOGRAFIA

(Do Grego kryptós, "escondido", e gráphein, "escrever") é o estudo dos princípios e das técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, a menos que seja conhecida uma "chave secreta", o que a torna difícil de ser lida por alguém não autorizado.

TERMOS DA CRIPTOGRAFIA

MENSAGEM ORIGINAL
É a mensagem em si, escrita em linguagem compreensível.

CIFRAR(ENCRIPTAR)
É o processo de embaralhar a mensagem original transformando-a em mensagem cifrada.

DECIFRAR(DECRIPTAR)
É o processo de transformar a mensagem cifrada de volta em mensagem original.

ALGORITMO DE CRIPTOGRAFIA
É o programa(seqüência de passos) usado para realizar a encriptação e a decriptação.

MENSAGEM CIFRADA(OU ENCRIPTADA)
É a mensagem embaralhada, incompreensível, que passou pelo processo de encriptação.

CHAVE
É um número(binário) que é usado para cifrar e/ou decifrar a mensagem. É o código que o programa deve conhecer para embaralhar ou desembaralhar a mensagem.

TAMANHO DA CHAVE
É a medida em bits do tamanho do número usado como chave. Quanto maior a chave, mais complexa ela será para ser descoberta(mais segura).

- Uma chave criptográfica de 40 bits, sorteada elatoriamente por um programa qualquer, resulta em 2^{40} possibilidades.
- Quer dizer que, para discobrir uma chave de 40 bits, é necessário testar o equivalente a 1.099.511.627.776 possibilidade.
- Imagina hoje, uma chave de 128 a 1024 bits.

CRIPTOANALISTA
Aquele que desenvolve ou tenta quebrar uma criptografia(código-chave).

FORÇA BRUTA
Forma de ataque aos sistemas criptográfico que se baseia em testar todas as possibilidades de chaves(tentativa e erro) em uma mensagem cifrada. Quanto maior a chave, mais tampo demora para a quebra.

SERVIÇOS OFERECIDOS

As técnicas de criptografia oferecem seis tipos de serviços básicos. Sem estes predicados não é possível realizar o comércio eletrônico seguro na Internet:

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-Repúdio	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 OU CRIPTOGRAFIA DE CHAVE PRIVADA

Utiliza apenas uma chave para encriptar e decriptar as mensagens. Também conhecida como Criptografia Convencional(ou criptografia de chave secreta).

- Fácil implementação.
- Velocidade no processamento.
- O nível de segurança depende do tamanho da chave.

Veja um exemplo. Tomemos um número de cartão de crédito hipotético, **1424 3135 2435 1556** e escolhemos o número 12 para ser a nossa chave. Poderíamos encriptar o segredo assim: Chave menos número do cartão.

Chave	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
Segredo	-1	-4	-2	-4	-3	-1	-3	-5	-2	-4	-3	-5	-1	-5	-5	-6
Cifrado	**11**	**8**	**10**	**8**	**9**	**11**	**9**	**7**	**10**	**8**	**9**	**7**	**11**	**7**	**7**	**6**

Para "abrir a caixa" e ver o segredo, temos que subtrair novamente só que desta vez subtraímos o a mensagem cifrada da chave:

Chave	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
Cifrado	-11	-8	-10	-8	-9	-11	-9	-7	-10	-8	-9	-7	-11	-7	-7	-6
Segredo	**1**	**4**	**2**	**4**	**3**	**1**	**3**	**5**	**2**	**4**	**3**	**5**	**1**	**5**	**5**	**6**

ALGORITMOS SIMÉTRICOS

Algoritmo Simétrico	Bits	Descrição
DES	56	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, 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.
Triple DES ou 3DES	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 escolha entre maior segurança ou desempenho através de chaves de tamanho variável.
RC2	8 a 1024	Projetado por Ron Rivest 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:

- 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-repúdio).

CRIPTOGRAFIA ASSIMÉTRICA OU CRIPTOGRAFIA DE CHAVE PÚBLICA

Utiliza duas chaves diferentes, uma privada e uma pública.

- **Pública:** conhecida por todos, é usada para encriptar as mensagens que se deseja enviar para o usuário.
- **Privada:** (ou secreta) é conhecida apenas pelo seu proprietário (o usuário). É usada para decriptar as mensagens enviadas a ele(usuário).

- 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, enquanto a chave pública disponível livremente para qualquer interessado.

- Há somente um par de chave que combina; uma chave compartilhável(pública) e outra intransferível(privada).
- Utiliza números gigantescos, de 300 dígitos.
- Não é possível usar ataques de **força bruta** para descobrir a chave privada.

ALGORITMOS ASSIMÉTRICOS

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 (Massachusetts Institute of Technology). É, atualmente, 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 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. Um fato preocupante: cerca de 95% dos sites de comércio eletrônico utilzam chaves RSA de 512 bits.
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.

HASH

- Consiste em gerar um valor, chamado de "message digest- MD", a partir de um texto qualquer.
- O tamanho do MD depende do algoritmo escolhido (MD1, MD2, ..., MD5 ou SHA1), que é medido em bits.
- O SHA1 é o mais recente. Usado em certificados e assinaturas digitais. Cria hash de 20 caracteres (160 bits). É o mais seguro, pois ninguém conseguiu quebra-lo.

- Na criptografia, o hash serve para garantir a integridade da mensagem, onde o gerador (ou emissor) da mensagem, submete-a a um algoritmo hash, o qual produzirá um "valor hash" (este é outro nome pelo qual é conhecido o MD).
- Este valor é enviado junto com a mensagem para o destinatário. O destinatário fará a verificação da integridade da mensagem aplicando o mesmo algoritmo na mensagem original e obterá um valor hash que deverá ser igual ao valor hash gerado na origem. Se for diferente, a mensagem foi alterada no "caminho" - é claro que a mensagem juntamente com o MD terão que ser encriptados para dificultar a intervenção de terceiros.

- O algoritmo hash é composto por fórmulas matemáticas complexas, para poder garantir a irreversibilidade e a unicidade do MD gerado - textos diferentes não produzem o mesmo MD. A alteração de um simples bit na mensagem gera um MD completamente diferente.
-
- Não há limite quanto ao tamanho do texto a ser submetido a um algoritmo hash, porém, o resultado obtido será sempre do tamanho determinado pelo algoritmo escolhido. Por isso é praticamente impossível descobrir a mensagem original através do MD. O MD possui tamanho fixo, conforme os algoritmos hash MD1, MD2, ..., MD5 e SHA1, e o texto a ser "hasheado" possui tamanho indeterminado.

- Hoje em dia o hash é utilizado em muitos setores da informática e eletrônica específica. Por exemplo, na autenticação de usuários através da assinatura ou dos dados contidos em um smartcard. Em ambos os casos, o que é armazenado é apenas o MD e a informação fica contida no mundo externo. Toda vez que é necessário a autenticação, o sistema coletará os dados e fará o cálculo do hash para comparar com o hash armazenado no banco de dados ou no smartcard.

- A principal característica do hash é a irreversibilidade e integridade.

ALGORITMOS HASH

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. O algoritmo foi projetado para ser rápido, simples e seguro. 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.
SHA1	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. 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.

ASSINATURA DIGITAL

- Permite garantir a autenticidade de quem envia a mensagem, associada à integridade do seu conteúdo. Utiliza chaves públicas e privadas(criptografia assimétrica).

- A assinatura digital é um mecanismo criado para atribuir confiabilidade a um documento eletrônico, da mesma forma que uma assinatura de punho (ou firma) atribui confiabilidade a um documento papel.

- A assinatura digital soluciona aspectos fundamentais à confiabilidade dos documentos eletrônicos:
  - Permite autenticar a identidade da assinatura, desta forma pode-se confirmar quem participou de uma determinada transação eletrônica.
  - Proteger a integridade do documento, pode-se saber se o documento recebido sofreu alterações, quer acidental, quer maliciosamente.
  - Provar quem participou da transação (não-repúdio), eliminando a possibilidade de que o autor venha a negar sua assinatura.

- Uma assinatura digital, é criada utilizando-se a chave privada do certificado do autor da assinatura, deste modo, a mesma pode ser conferida através da chave pública que encontra-se no seu certificado digital do autor.

- Para assinar digitalmente qualquer tipo de informação eletrônica, a fim de comprovar inequivocamente a autoria(não-repúdio), o autor deverá possuir um certificado digital, único e pessoal, que comprove indubitavelmente a sua identidade no mundo eletrônico e que tenha sido emitido por uma autoridade certificadora de confiança.

ALGORITMOS DA 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	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.

PROTOCOLOS CRIPTOGRÁFICOS

- Qual o modelo de criptografia que devemos utilizar? Simétrico ou Assimétrico? A resposta é simples: devemos utilizar os dois, em um modelo denominado híbrido.
- O algoritmo simétrico, por ser muito mais rápido, é utilizado no ciframento da mensagem em si.
- Enquanto o assimétrico, embora lento, permite implementar a distribuição de chaves e a assinatura digital.
- Além disso, como já exposto no item anterior, deve-se utilizar também o mecanismo de Hashing para complemento da assinatura digital.

Criptografia Simétrica.	**Criptografia Assimétrica.**
Rápida.	Lenta.
Gerência e distribuição das chaves é complexa.	Gerência e distribuição simples.
Não oferece assinatura digital	Oferece assinatura digital.

- 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).

O QUE É A ICP- BRASIL?

- A Infra-estrutura de Chaves Públicas brasileira(ICP-Brasil) - PKI(Public Key Infraestructure) é um conjunto de técnicas, práticas e procedimentos que foram traçadas pelo seu Comitê Gestor com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública.

Acesse o link abaixo para saber mais:
http://www.icpbrasil.gov.br/
http://www.iti.br/.

CERTIFICADO DIGITAL

- Um certificado digital, ou identidade digital, pode ser visto como uma carteira de identidade para uso na internet.
- Com ele é possível comprovar a identidade tanto do internauta como do site.
- Por exemplo, ao acessar uma conta bancária o certificado de servidor do banco assegura que você está realmente acessando o site do banco, da mesma forma que o certificado de cliente garante ao banco que o internauta que está acessando os dados de uma determinada conta é realmente o titular da conta.

- O certificado digital pode também ser utilizado para atribuir integridade e autenticidade aos documentos eletrônicos -mensagens, textos, dados, etc-.
- Por exemplo: quando você envia uma mensagem de e-mail para alguém, o programa de e-mail pode utilizar seu certificado para "assinar" digitalmente sua mensagem. Deste modo, a pessoa que receber a mensagem tem certeza que a mesma foi realmente enviada por você, além de ter a garantia de que o conteúdo da mensagem não foi alterado entre o envio e o recebimento.

- Tecnicamente, um certificado digital é um conjunto de dados (um arquivo), assinado digitalmente pela autoridade certificadora e contento tipicamente informações como:
  - chave pública do certificado.
  - nome e endereço de e-mail do dono do certificado.
  - nome e assinatura digital da autoridade certificadora.
  - privilégios de acesso a sites seguros.
  - outras.

DIFERENÇA ENTRE O CERTIFICADO TIPO A1 E A3?

TIPO A1

- O par de chaves pública/privada é gerado em seu computador, no momento da solicitação de emissão do certificado. A chave pública será enviada para a Autoridade Certificadora(AC) com a solicitação de emissão do certificado, enquanto a chave privada ficará armazenada em seu computador, devendo, obrigatoriamente, ser protegida por senha de acesso. Este certificado é instalado no mesmo computador onde foi efetuada a solicitação do certificado e tem validade de 1 (um) ano.

TIPO A3

- Oferece mais segurança, justamente porque o par de chaves é gerado em hardware específico, isto é num cartão inteligente ou token que não permite a exportação ou qualquer outro tipo de reprodução ou cópia da chave privada. Também no certificado tipo A3 a chave pública será enviada para a AC junto com a solicitação de emissão do certificado, enquanto a chave privada ficará armazenada no cartão ou token, impedindo tentativas de acesso de terceiros. Com este método, você poderá transportar a sua chave privada e o seu certificado digital de maneira segura, podendo realizar transações eletrônicas onde desejar. O certificado tipo A3 tem validade de 3 (três) anos.

O QUE É UM SMARTCARD?

- É um cartão criptográfico capaz de gerar e armazenar as chaves criptográficas que irão compor os certificados digitais.

Mesmo que o computador seja atacado por um vírus ou, até mesmo, um hacker essas chaves estarão seguras e protegidas, não sendo expostas a risco de roubo ou violação.

Os múltiplos níveis de proteção que compõem a solução - incluindo recursos físicos e lógicos - asseguram a identificação do assinante, permitirão que a integridade e o sigilo das informações sejam protegidos e impossibilitarão o repúdio do documento em momento posterior.

O QUE É UMA LEITORA?

Uma leitora é um dispositivo projetado para conectar um cartão inteligente a um computador. A leitora se encarregará de fazer a interface com o cartão, enquanto o computador suporta e gerencia as aplicações.

Uma vez instalada, a leitora permitirá o acesso seguro a serviços na Internet já preparados para a certificação digital, como o Receita 222 e aplicações de Internet Banking.

O QUE É UM TOKEN?

O token é um hardware capaz de gerar e armazenar as chaves criptográficas que irão compor os certificados digitais. Uma vez geradas estas chaves estarão totalmente protegidas, pois não será possível exportá-las ou retirá-las do token (seu hardware criptográfico), além de protegê-las de riscos como roubo ou violação.

São características do token, incluindo recursos físicos e lógicos: assegurar a identificação do portador (que precisa de uma senha pessoal e intransferível para utilizá-lo), permitir que a integridade e o sigilo das informações contidas nele, proteger e armazenar essas informações (as chaves e os certificados) e impossibilitar a separação da chave criptográfica do hardware criptográfico.

PARA QUE SERVE O eCPF?

O documento eletrônico de identidade e-CPF é utilizado para garantir a autenticidade dos remetentes e destinatários de documentos e dados que trafegam pela Internet, assegurando sua inviolabilidade. O e-CPF foi criado para facilitar o relacionamento entre os contribuintes brasileiros e a Secretaria da Receita Federal-SRF.

O e-CPF pode também ser utilizado para assinar digitalmente documentos eletrônicos.