Criptografia

Introdução

A criptografia já estava presente no sistema de escrita hieroglífica dos egípcios. Desde então vem sendo muito utilizada, principalmente para fins militares e diplomáticos. No âmbito da computação a criptologia é importante para que se possa garantir a segurança em todo o ambiente computacional que necessite de sigilo em relação às informações que manipula. Pode ser usada para se codificar dados e mensagens antes que esses sejam enviados por vias de comunicação, para que mesmo que sejam interceptados, dificilmente poderão ser decodificados.

Terminologias

A palavra criptografia vem do grego kryptos (em português, escondido) + grafo (grafia, escrita): arte ou ciência de escrever em cifra ou código; em outras palavras, é um conjunto de técnicas que permitem tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir normalmente que apenas o destinatário a decifre e compreenda. Quase sempre o deciframento requer uma chave, uma informação secreta disponível ao destinatário. Terceiros podem através de uma "escuta" ter acesso 'a mensagem cifrada e determinar o texto original ou mesmo a chave, quebrando o sistema. A criptoanálise (analisys = decomposição) é a arte ou ciência de determinar chave ou decifrar mensagens sem conhecer a chave. A criptologia é a ciência que reúne criptografia e criptoanálise. Uma ciência muito antiga, a criptologia já estava presente no sistema de escrita hieroglífica dos egípcios há quase quatro mil anos. Desde então vem sendo muito utilizada, principalmente para fins militares e diplomáticos (e por amantes também). Sua utilização durante a Segunda Guerra, e a conseqüentemente quebra dos códigos alemão e japonês, foi fundamental para o sucesso dos Aliados. O livro The Codebreakers (Kahn) apresenta a historia desta ciência ate a Segunda Guerra, inclusive.. Quase sempre o deciframento requer uma chave, uma informação secreta disponível ao destinatário. Criptoanálise (kriptós; análysis = decomposição) : e a arte ou ciência de determinar a chave ou decifrar mensagens sem conhecer a chave. Uma tentativa de criptoanálise e chamada ataque. Criptologia (kriptós; logo = estudo, ciência): e a ciência que reúne a criptografia e a criptoanálise.

A criptografia computacional é usada para garantir:

1 - Sigilo: somente os usuários autorizados têm acesso à informação.

2 - Integridade da informação: garantia oferecida ao usuário de que a informação correta, original, não foi alterada, nem intencionalmente, nem acidentalmente. Autenticação do usuário : é o processo que permite ao sistema verificar se a pessoa com quem está se comunicando é de fato a pessoa que alega ser. Autenticação de remetente: é o processo que permite a um usuário certificar-se que a mensagem recebida foi de fato enviada pelo remetente, podendo-se inclusive provar perante um juiz, que o remetente enviou aquela mensagem. Autenticação do destinatário: consiste em se ter uma prova de que a mensagem enviada foi como tal recebida pelo destinatário. Autenticação de atualidade: consiste em provar que a mensagem é atual, não se tratando de mensagens antigas reenviadas. Cifrar é o ato de transformar dados em alguma forma ilegível. Seu propósito é o de garantir a privacidade, mantendo a informação escondida de qualquer pessoa não autorizada, mesmo que esta consiga visualizar os dados criptografados. Decifrar é o processo inverso, ou seja, transformar os dados criptografados na sua forma original, inteligível.Para cifrarmos ou decifrarmos uma mensagem, necessitamos de informações confidenciais geralmente denominadas chaves ou senhas. Dependendo do método de criptografia empregado, a mesma chave pode ser utilizada tanto para criptografar como para decriptografar mensagens, enquanto outros mecanismos utilizam senhas diferentes.

A criptografia, hoje em dia, é mais que somente misturar e desembaralhar informações. Autenticação é fundamental para garantirmos privacidade. Usamos autenticação em nosso dia a dia, quando assinamos um cheque, por exemplo. O mesmo ocorre quando usamos meios eletrônicos de comunicação. Os processos criptográficos atuais nos fornecem mecanismos para implementarmos tal função. A assinatura digital garante a procedência do documento, enquanto o timestamp digital nos informa o momento da criação de um documento. Estes mecanismos podem ser usados para controlar, por exemplo, acessos a discos rígidos compartilhados ou controlar canais de TV pagas por tempo de uso.As aplicações para o campo da criptografia são muito amplas. Com algumas ferramentas básicas é possível elaborar esquemas e protocolos que nos permitam o uso do "dinheiro eletrônico", ou provar que se tem acesso a certa informação sem a necessidade de revelá-la, ou então dividir um contexto sigiloso de modo que não menos de 3 de um grupo de 5 pessoas, por exemplo, possam reconstruí-lo.

Sistemas Criptográficos

Criptossistemas podem ser tanto quando assimétricos. Num criptossistema simétrico a encriptação e a decriptação são feitas com uma única chave, ou seja, tanto o remetente quanto o destinatário usam a mesma chave. Num sistema assimétrico, ao contrário, duas chaves são empregadas. Em criptossistemas de uma chave, como por exemplo o DES (Data Encription Standart), ocorre o chamado "problema de distribuição de chaves". A chave tem de ser enviada para todos os usuarios autorizados antes que mensagens possam ser trocadas. Isso resulta num atraso de tempo e possibilita que a chave chegue a pessoas não autorizadas.

Criptossistemas assimétricos, ou de dua chaves, contormam o problema da distribuição de chaves através do uso de chaves públicas. A criptografia de chaves públicas foi inventada em 1976 por Whitfield diffie e Martin Hellman a fim de resolver o problema da distribuição de chaves. No novo sistema, cada pessoa tem um par de chaves chamadas : chave pública e chave privada. A chave pública é divulgada enquanto que a chave privada e deixada em segredo. Para mandar uma mensagem privada, o transmissor encripta a mensagem usando a chave públicado destinatário pretendido.

Segue um exemplo de como o sistema funciona.

Quando Ana quer mandar uma mensagem para Carlos, ela procura a chave pública dele em um diretório, a usa para encriptar a mensagem, e a envia. Carlos então usa a sua chave privada para decriptar a mensagem e lê-la. Este sistema também permite a autenticação digital de mensagens ,

ou seja é possível prover certeza ao receptor sobre a identidade do transmissor e sobre a integridade da mensagem.

Quando uma mensagem é encriptada com uma chave privada, ao invés da chave pública; o resultado é uma assinatura digital, ou seja, uma mensagem que só uma pessoa poderia produzir, mas que todos possam verificar. Normalmente autenticação se refere ao uso de assinaturas digitais : a assinatura é um conjunto inforjável de dados assegurando o nome do autor ou funcionando como uma assinatura de documentos , ou seja, que determinada pessoa concordou com o que estava escrito. Isso também evita que a pessoa que assinou a mensagem depois possa se livrar de responsabilidades, alegando que a mensagem foi forjada. Um exemplo de criptossistema de chave pública é o RSA (Rivest-Shamir-Adelman) . Sua maior desvantagem é a sua capacidade de canal limitada, ou seja, o número de bits de mensagem que ele pode transmitir por segundo. Enquanto um chip que implementa o algorítmo de uma chave DES pode processar informação em alguns milhões de bits por segundo, um chip RSA consegue apenas na ordem de mil bits por segundo.

Então vejamos , sistemas de uma chave são bem mais rápidos, e sistemas de duas chaves são bem mais seguros. Uma possível solução é combinar as duas, fornecendo assim um misto de velocidade e segurança. Simplesmente usa-se a encriptação de uma chave para encriptar a mensagem, e a chave secreta é transmitida usando a chave pública do destinatário. É importante não confundir chave privada com chave secreta.A primeira é mantida em segredo, enquanto que a segunda é enviada para as pessoas que efetivarão a comunicação.

Algorítmos

Algorítmos de Chave Única ou Secretas (Simétricos)

O exemplo mais difundido de cifrador computacional de chave única é o DES (Data Encryption Standard), desenvolvido pela IBM e adotado como padrão nos EUA em 1977. O DES cifra blocos de 64 bits (8 caracteres) usando uma chave de 56 bits mais 8 bits de paridade (o que soma 64 bits).O algoritmo inicia realizando uma transposição inicial sobre os 64 bits da mensagem, seguida de 16 passos de ciftagem e conclui realizando uma transposição final, que é a inversa da transposição inicial.Para os 16 passos de ciftagem usam-se 16 sub-chaves, todas derivadas da chave original através de deslocamentos e transposições.

Um passo de cifragem do DES, tem dois objetivos básicos: a difusão e a confusão. A difusão visa eliminar a redundância existente na mensagem original, distribuindo-a pela mensagem cifrada. O propósito da confusão é tomar a relação entre a mensagem e a chave tão complexa quanto possível.O DES pode ser quebrado pelo método da força bruta, tentando-se todas as combinações possíveis de chave. Como a chave tem 56 bits, tem-se um total de 2 exp 56 chaves possíveis.

Existem diversos algoritmos de cifragem de blocos de chave única, entre eles:

Triple-DES: O DES é aplicado 3 vezes, com sequências de cifragem e decifragem, combinando a utilização de 2 chaves.

WLucifer: precursor do DES.

Madryga: trabalha com 8 bits, usando ou-exclusivo e deslocamento de bits.

NewDES: blocos de 64 bits e chave de 120 bits.

FEAL-N: baseado no DES, pode-se especificar o número de passos da cifragem, fraco se utiliza-se menos de 8 passos.

LOKI: bloco e chave de 64 bits.

Khufu e Khafre: trabalham de forma semelhante ao DES, usam tabelas de substituição de 256 posições de 32 bits - contra as de 6 posições de 4 bits do DES - usam chaves de 512 bits e um número de passos flexíveis, múltiplo de 8.

IDEA: blocos de 64 bits com chave de 128 bits.

MMB: blocos e chave de 128 bits.

Skipjack: chave de 80 bits e 32 passos de processamento.

Estes e outros algoritmos podem ser encontrados em :

ftp://ftp.funet.fi:/pub/crypt/cryptography/symmetric

Algorítmos de Chave Pública (Assimétricos)

A chave de ciframento é públicada ou tornada acessível aos usuários, sem que haja quebra na segurança. Dessa forma cada usuário tem uma chave de ciframento, de conhecimento público, e outra de deciframento, secreta. Se um usuário A deseja mandar uma mensagem para um usuário B, ele utiliza a chave de ciframento pública PB e envia a mensagem para B, este de posse de sua chave de deciframento secreta SB decodifica a mensagem.

Um exemplo desse sistema é o RSA, anacronico de seus autores Rivest, Shamir e Adleman. Sua seguranca baseia-se na intrabilidade da fatoraçãao de produtos de dois primos. Um usuário B para determinar seu par (PB,SB), procede da seguinte maneira: escolhe ao acaso dois primos grandes "p" e "q" e computa o seu produto (n=p*q), e o número f(n)=(p-1)*(q-1); B escolhe ao acaso um número "c" relativamente primo com f(n) (ou seja, c e f(n) não possuem fatores em comum) e determinara "d" tal que c*d (módulo f(n)). Finalmente, o usuário B pública sua chave pública PB(c,n) e mantém secretos p, q, f(n) e d. A chave secreta SB(d,n) deve ser mantida em sigilo completo.

Cifragem de Blocos

Um algoritmo que realiza cifragem sobre blocos pode operar de diversas maneiras distintas. As mais conhecidas são:

1 - Modo do livro de Códigos (Electronic Code Book - ECB)

Cada bloco da mensagem original é individual e independentemente cifrado para produzir os blocos da mensagem cifrada. O bloco típico tem 64 bits, o que produz um livro de códigos de 2 exp 64 entradas. E note-se que para cada chave possível existe um livro de códigos diferentes. A vantagem do método é sua simplicidade e a independência entre os blocos. A desvantagem é que um criptoanalista pode começar a compilar um livro de códigos, mesmo sem conhecer a chave.

Um problema mais grave é a chamada repetição de bloco, onde um atacante ativo pode alterar parte de uma mensagem criptografada sem saber a chave e nem mesmo o conteúdo que foi modificado. Pode-se por exemplo interceptar uma transação bancária de transferência de saldo de qualquer pessoa, a seguir pode-se realizar uma transferência de saldo de uma conta para a conta do atacante e interceptar a mensagem, assim pode-se identificar os blocos correspondentes ao destinatário e dessa forma substituir em todas as mensagens o destinatário pelo atacante.

2 - Modo de Encadeamento de Blocos (Cipher Block Chaining - CBC)

CBC realimenta a cifragem do bloco atual com o resultado das cifragens dos blocos anteriores. A operação mais utilizada é o ou-exclusivo com o bloco anterior, dessa forma os blocos iguais serao normalmente cifrados de forma diferente, desde que no mínimo um dos blocos anteriores seja diferente da mensagem. Entretanto 2 mensagens iguais serao mapeadas para os mesmos blocos. E duas mensagens com início igual serão cifradas da mesma forma até que ocorra a diferença. A maneira empregada para evitar esse problema é a utilizacao de um vetor de inicializaçãao distinto para cada mensagem.

3 - Modo da Realimentação de Cifra (Cipher Feedback - CFB)

Quando há necessidade de enviar-se mensagens que possuem tamanho menor que um bloco usa-se o método CFB, que trabalha com grupos (8 bits por exemplo - 1 caracter), neste caso a realimentacao é feita sobre o grupo, utilizando-se também o ou-exclusivo.

4 - Cifras de Substituição

Troca cada caracter ou grupo de caracteres por outro, de acordo com uma tabela de substituição.Pode-se quebrar este método analisando-se a frequência de cada caracter no texto cifrado e comparando-se estas frequências com aquelas que normalmente aparecem em um determinado idioma.As vogais têm maior frequência que as consoantes e alguns caracteres possuem frequência baixíssima em relação aos demais. Para amenizar a frequência de caracteres, podemos utilizar várias tabelas para a cifragem de um texto. Para uma substituição monoalfabética podemos ter 261 Tabelas de Substituição. Tem-se uma chave que diz qual das tabelas será usada para cada letra do texto original. Portanto, quanto maior a chave mais seguro é o método. Entretanto, é suficiente descobrir o tamanho da chave k e analisar blocos de k caracteres no texto, verificando a frequência de repetição dos caracteres.

4.1 - Substituição Monoalfabética

Cada letra do texto original é trocada por outra de acordo com uma tabela e com sua posição no texto. A Substituição de César é um exemplo de substituição monoalfabética que consiste em trocar cada letra por outra que está 3 letras adiante na ordem alfabética. Ex: A=D. Pode-se usar outros valores ao invés de 3, o que constitui a chave de ciframento. Existem apenas 26 chaves, por isso é um método que visa proteger textos com pequeno grau de sigilo.

4.2 - Substituição por Deslocamentos

A chave indica quantas posições deve-se avançar no alfabeto para substituir cada letra. Diferente da substituição de César, as letras não são trocadas sempre por uma letra n posições a frente no alfabeto. Ex: Chave:020813, A primeira letra é trocada pela letra que está 2 posições a frente no

alfabeto, a segunda pela que está 8 posições a frente, e assim por diante, repetindo a chave se necessário. (P AI=RIV).

4.3 - Substituição Monofônica

Como a anterior, mas agora cada caracter pode ser mapeado para um ou vários caracteres na mensagem cifrada. Isso evita a linearidade da substituição.

4.4 - Substituição Polialfabética

A combinação no uso de várias substituições monoalfabéticas, usadas em rotação de acordo com um critério ou chave. Por exemplo, poderiam ser utilizadas 4 tabelas, usadas em alternância a cada 4 caracteres. Substituição por Polígramos: utiliza grupo de caracteres ao invés de um caracter individual. Se fossem considerados trigramas, por exemplo, ABA poderia ser substituído por RTQ ou KXS,

5 - Cifras de Transposição

Troca-se a posição dos caracteres na mensagem. Por exemplo, pode-se rescrever o texto percorrendo-o por colunas. Ou então definir o tamanho para um vetor de trocas e também uma ordem em que as trocas serão feitas. Pode-se usar chave para isso. Ex: em um vetor de tamanho 6 pode-se trocar o primeiro caracter pelo terceiro, o segundo pelo quinto e o quarto pelo sexto.Se a frequência dos caracteres for a mesma do idioma, temos substituição por transposição. Se for diferente, temos por substituição.Também é possível combinar substituição e transposição, ou vice-versa.

6 - Máquinas de Cifragem

Um código trabalha com grupos de caracteres de tamanho variável, ao contrário da cifra. Cada palavra é substituida por outra. Quebrar um código equivale a quebrar uma gigantesca substituição monoalfabética onde as unidades são as palavras e não os caracteres. Para isso deve-se usar a gramática da língua e analisar a estrutura das frases. Máquinas de cifragem baseiam-se em engrenagens que tem tamanhos diferentes e que giram a velocidades diferentes, obtendo um substituição polialfabética com chave de 26n, onde n é o número de engrenagens.

Sistemas Criptográfncos e Criptoanálise

Um criptossistema deve ser seguro mesmo quando os algoritmos de cifragem e de deciframento sejam conhecidos. Por esta razão são usadas chaves. Uma pessoa não autorizada que tem acesso a alguns dos elementos de um criptosistema é denominada de atacante. Um atacante passivo somente obtém cópias dos elementos, enquanto um atacante ativo pode alterar alguns desses elementos. Existem cinco tipos de ataque (ou criptoanálise) mais comuns.Todos eles supõe que o criptoanalista possui conhecimento total sobre os métodos de cifragem e decifragem utilizados, mas não sobre as chaves.

1 - Ataque do texto cifrado (cyphertext-only): o criptoanalista tem a sua disposição uma grande quantidade de mensagens cifradas, mas desconhece as originais e as chaves utilizadas. Sua tarefa é recuperar as mensagens normais (deduzir as chaves utilizadas).

2 - Ataque do texto conhecido (known-plaintext): o criptoanalista tem a sua disposição uma grande quantidade de mensagens cifradas e também as mensagens originais equivalentes. Sua tarefa é

deduzir as chaves usadas (ou um método para recuperar mensagens cifradas com a mesma chave).

3 - Ataque adaptativo do texto escolhido (adaptative-choosen-plaintext): no método anterior, o criptoanalista poderia ser capaz de fornecer somente uma grande quantidade de mensagens de uma só vez; agora ele pode fornecer um pequeno conjunto, analisar os resultados, fornecer outro conjunto e assim por diante. Sua tarefa é deduzir as chaves utilizadas. Alguns métodos de cifragem como o RSA são muito vulneráveis a este ataque.

4 - Ataque do texto cifrado escolhido (choosen-cyphertext): o criptoanalista não só tem uma grande quantidade de mensagens e seus equivalentes cifrados, mas pode produzir uma mensagem cifrada específica para ser decifrada e obter o resultado produzido. É utilizado quando se tem uma "caixa-preta" que faz decifragem automática. Sua tarefa é deduzir chaves utilizadas.

5 - Ataque da chave escolhida (choosen-key): o criptoanalista pode testar o sistema com diversas chaves diferentes, ou pode convencer diversos usuários legítimos do sistema a utilizarem determinadas chaves. Neste Ultimo caso, a finalidade imediata seria de decifrar as mensagens cifradas com essas chaves.

Segurança de criptosistemas

Um sistema é dito seguro se ele é teoricamente inquebrável, ou seja, não interessa qual a quantidade de texto normal ou decifrado a disposição, nunca se tem informação suficiente para deduzir as chaves utilizadas ou decifrar um texto qualquer cifrado. Só se conhece um método nesta categoria: a Cifra de Vernam ou One-time pad (cifra de uso único). Em essência dois elementos que desejam se comunicar possuem cópias idênticas de uma sequência randômica de valores, que são usados como chave. O método entretanto, exige que cada chave seja usada uma única vez e que o comprimento da sequência (chave) seja maior, ou no mínimo igual ao comprimento da mensagem a ser cifrada.

Chaves secretas

Funções Unidirecionais

Podemos dizer que uma uma função é unidirecional se for viável computá-la e computacionalmente inviável computar a sua inversa. Imagine que temos dois números primos da ordem de 10 exp lOO: multiplicá-los é uma questão de segundos com a tecnologia atual, no entanto, dado o seu produto da ordem de 10 exp 200, o melhor algoritmo conhecido leva hoje l bilhão de anos para fatorar o produto dado. Assim a função produto de dois primos é unidirecional. Uma funcao unidirecional é com segredo se existe uma informação que torna a computação da sua inversa possível. A funçao produto de dois primos é unidirecional sem segredo.
Há casos em que uma função unidirecional sem segredo é útil, um exemplo típico é na proteção de senhas, apresenta as senhas cifradas por uma função unidirecional sem segredo (e de inviável deciframento). Quando o usuário inicia sua sessão, fornece a senha que é então ciftada e comparada com a senha cifrada armazenada. Desta maneira, exige-se apenas a integridade do arquivo de senhas, não mais exigindo controle de acesso ao arquivo.

Ao selecionar uma função unidirecional como função de ciframento, o projetista deve supor que:

. o algoritmo de ciframento é de domínio público;

. o espião, através de escuta, tem acesso ao texto cifrado.

Diz-se então que a criptoanálise é de texto cifrado conhecido.

Protocolo para a Distribuição de Chaves Secretas

Quando se adota o método de chaves secretas, é recomendável não utilizar por muito tempo a mesma. Quando ideal é a cada nova sessão uma nova chave seja estabelecida. Mas como estabelecer a chave ao início de cada sessão? Como evitar as escutas? Cifrar a mensagem? Com que chave? Aqui apresenta-se uma solução para ilustrar o conceito de funções unidirecionais. A função a ser usada é a exponencial módulo de um número, isto é, dados os inteiros 'a', 'x' e 'n', seja ~x)=aAx mod n (n>O, x>=O). Assim, ftx) é o resto da divisão de aAx por n. O cálculo desta função é viável. O procedimento abaixo mostra uma maneira de calcular esta função :

```
Procedimento expomod (a,x,n,r:inteiro); {r possui o resultado da função}

declare y, c :  tipo inteiro

inicio

r:= l;
y:=x;
c:=a mod n;


   enquanto y>O faça inicio

      se ímpar(y) então

         r=r*c mod n;
         y=y div 2;
         C=C 2 mod n;

     fim;

fim;
```

Suponha que dois usuários A e B desejam manter uma conversa sigilosa através de chave secreta. As duas partes escolheram um número primo grande , p' da ordem de 10A 100, e já concordaram também em utilizar uma base , a'. Preferivelmente deve ser uma raiz primitiva de p, de modo que ffx)=aAx mod p é uma b~eção sobre o conjunto 1..p-l dos naturais x tais que l<=x<=p-l. Para iniciar o estabelecimento da chave, A gera ao acaso um expoente x no intervalo 1..p- l e B gera outro, y Usando expomod, A calcula ffx) e B ffy). Então A envia pela rede ffx) e B envia ffy). De posse de y e ffx), B calcula, usando

expomod :

K = [(ffx)]Ay mod p = (aAx mod p)Ay mod p = aA(xy) mod p = K.

Da mesma forma, A usa expomod e de posse de x e ffy) calcula:

k = [(ffy)]AX mod p = (aAy mod p)AX mod p = aA(xy) mod p - - K.

Assim A e B chegam a um número comum K, que será a chave de ciframento para as mensagens.

Suponha um espião bem informado que obtenha os valores de a e p e, através de escuta, os valores de f(f(x)) e de f(f(y)). Para determinar K, ele precisa determinar a função logaritmo módulo p, que é intratável. Mesmo A não é capaz de determinar o valor de y e B o valor de x. A função expomod é unidirecional sem segredo, permite a A e B trocarem uma chave secreta utilizando a própria rede.

Assinatura Digital

Nos sistemas com chave pública, qualquer pessoa pode cifrar uma mensagem, mas somente o destinatário da mensagem pode decifrá-la. Invertendo-se o uso das chaves podemos ter uma que só pode ser cifrada por uma pessoa e decifrada por qualquer um, obtendo-se assim umefeito de personalização do documento, semelhante a uma assinatura. Um sistema desse tipo é denominado assinatura digital. Assim para personalizar uma mensagem, um determinado usuário A codifica uma mensagem utilizando sua chave secreta e a envia para o destinatário. Somente a chave pública de A permitirá a decodificação sua chave secreta e a envia para o da mensagem, portanto é a prova de que A enviou a mensagem. A mensagem assim pode ser decodificada por qualquer um que tenha a chave pública de A. Para garantir o sigilo deve-se a primeira utilizando a própria chave secreta (para fazer a criptografia duas vezes a mensagem: a chave pública do destinatário, para que somente este possa ler a mensagem.

Propriedades

1 - a assinatura é autêntica: quando um usuário usa a chave pública de A para decifrar uma mensagem, ele confirma que foi A e somente A quem enviou a mensagem;

2 - a assinatura não pode ser forjada: somente A conhece sua chave secreta:

3 - o documento assinado não pode ser alterado : se houver qualquer alteração no texto criptografado este não poderá ser restaurado com o uso da chave pública de A;

4 - a assinatura não é reutilizável: a assinatura é uma função do documento e não pode ser transferida para outro documento;

5 - a assinatura não pode ser repudiada: o usuário B não precisa de nenhuma ajuda de A para reconhecer sua assinatura e A não pode negar ter assinado o documento.

Certificado digital

Certificado de Identidade Digital, também conhecido como Certificado Digital, associa a identidade de um titular a um par de chaves eletrônicas (uma pública e outra privada) que, usadas em conjunto, fomecem a comprovação da identidade. É uma versão eletrônica (digital) de algo

parecido a uma Cédula de Identidade - serve como prova de identidade, reconhecida diante de qualquer situação onde seja necessária a comprovação de identidade.

Certificado Digital pode ser usado em uma grande variedade de aplicações, como comércio eletrônico, groupware (Intranet's e Internet) e transferência eletrônica de fundos (veja o exemplo recente do Banco Bradesco S.A. na implantação do seu serviço Internet - o BradescoNet).

Dessa forma, um cliente que compre em um shopping virtual, utilizando um Servidor Seguro, solicitará o Certificado de Identidade Digital deste Servidor para verificar, a identidade do vendedor e o conteúdo do Certificado por ele apresentado. De forma inversa, o servidor poderá solicitar ao comprador seu Certificado de Identidade Digital, para identificá-lo com segurança e precisão.

Caso qualquer um dos dois apresente um Certificado de Identidade Digital adulterado, ele será avisado do fato, e a comunicação com segurança não será estabelecida. O Certificado de Identidade Digital é emitido e assinado (chancelado) por uma Autoridade Certificadora Digital(Certificate Authority), como a Thawte (certificadora da ArtNET), que emite o Certificado. Para tanto, esta autoridade usa as mais avançadas técnicas de criptografia disponíveis e de padrões internacionais (norma ISO X.509 para Certitncados Digitais), para a emissão e chancela digital dos Certificados de Identidade Digital.

Um certificado contem três elementos:

1 - Informação de atributo

Esta é a informação sobre o objeto que é certificado. No caso de uma pessoa, isto pode incluir seu nome, nacionalidade e endereço e-mail, sua organização e o departamento desta organização onde trabalha.

2 - Chave de informação pública

Esta é a chave públicada entidade certificada. O certificado atua para associar a chave pública à informação de atributo, descrita acima. A chave pública pode ser qualquer chave assimétrica, mas usualmente é uma chave RSA.

3 - Assinatura da Autoridade em Certificação (CA)

A CA assina os dois primeiros elementos e, então, adiciona credibilidade ao certificado.Quem recebe o certificado verifica a assinatura e acreditará na informação de atributo e chave públicaassociadas se acreditar na Autoridade em Certificação.

Selo Cronológico Digital

O Servico de Selo Cronológico Digital gera selos cronológicos que associam a data e a hora a um documento digital em uma forma de criptografia forte. O selo cronológico digital pode ser usado futuramente para provar que um documento eletrônico existia na data alegada por seu selo cronológico.

Por exemplo, um físico que tenha uma idéia brilhante pode descrevâ-la usando um processador de textos e selar este documento com o selo cronológico digital.O selo cronológico e o documento, juntos, podem mais tarde comprovar que este cientista é o merecedor do Prêmio Nobel, mesmo que um rival publique essa idéia primeiro.

Exemplo de uso do sistema: suponha que Paulo assine um documento e queira selá-lo cronologicamente. Ele calcula o resumo da mensagem usando uma função de hashing seguro e, então, envia este resumo (não o documento) para o DTS, que enviará de volta um seio cronológico digital consistindo do resumo da mensagem, da data e da hora em que foi recebida pelo DTS e da assinatura do DTS. Como o resumo da mensagem não revela qualquer informação a respeito do conteúdo do documento, o DTS não tem condições de saber o conteúdo do documento que recebeu o selo cronológico digital. Mais tarde, Paulo pode apresentar o documento e o selo cronológico, juntos, para provar a data em que este foi escrito. Aquele que vai comprovar a autenticidade do documento calcula o resumo da mensagem, verifica se as mensagens calculada e apresentada são iguais, e observa então a assinatura do DTS no selo cronológico. Para ser confiável, o selo cronológico não pode ser falsificável. Considere os requisitos para um DTS como descrito a seguir.

O DTS deve ser proprietário de uma chave longa (1.024 bits), se este desejar que os selos cronológicos sejam seguros por muitas décadas. A chave privativa do DTS deve ser armazenada em um local de máxima segurança, como, por exemplo, um cofre inviolável em um local seguro. A data e a hora vêm de um relógio que não possa ser alterado, (NIST) Deve ser impossível criar selos cronológicos sem usar um mecanismo que só aceite este relógio.

O uso do DTS parece ser extremamente importante, se não essencial, para manter a validade de documentos através dos anos. Suponha um contrato de leasing de vinte anos entre um proprietário de terras e um arrendatário. As chaves públicas usadas para assinar o contrato expiram após um ano. Soluções, como reafirmar as chaves ou reassinar o contrato a cada ano, com novas chaves, requerem a cooperação de ambas as partes durante vários anos enquanto durar o contrato. Se uma das partes se torna insatisfeita com o contrato, ela pode recusar-se a cooperar. A solução é registrar o contrato com o DTS na data da primeira assinatura deste. Ambas as partes recebem então uma cópia do selo cronológico, que pode ser usada anos mais tarde para comprovar a autenticidade do contrato original.

No futuro, o provável é que o DTS será usado para tudo, desde a assinatura de contratos a longo prazo até diários pessoais e cartas. Hoje, se um historiador descobrir algum manuscrito e atribuí-lo a um escritor famoso (já falecido), sua autenticidade poderá ser comprovada por meios físicos. Mas, se um achado semelhante ocorrer adqui a 100 anos, provavelmente será em arquivos de computador (disquetes ou fitas). Talvez a única forma de comprovar sua autenticidade seja através do selo cronológico digital.

Site seguro

Um site seguro é constituído por programas de computador que são executados em um servidor seguro para atender solicitações feitas pelos usuários finais, através de seus próprios programas (clientes seguros). Dotado de características que tornam as transações eletrônicas confidenciais, mediante criptografia, o servidor seguro utiliza-se de um protocolo especial de comunicação que é o SSL ((" Secure Socket Layer" - desenvolvido originalmente pela Netscape), que utiliza criptografia de chave assimétrica, tornando a comunicação entre as partes virtualmente inviolável. Desta forma, se houver interceptação das informações trafegadas entre o cliente e o servidor por parte de pessoas não autorizadas, estas informações serão de utilidade zero, já que seria necessário o conhecimento prévio das chaves privadas de criptografia.
Para que o sigilo e a inviolabilidade da comunicação realmente existam, é necessário um Certificado de Identidade Digital válido.

Formas de Pagamento Virtual

Para se comprar coisas pela internet é necessário arranjar uma forma adequada de efectuar o pagamento. No mundo real existem muitas maneiras de de pagar: dinheiro, cartões bancários, cartões de crédito, cheque, senhas, etc... Da mesma forma na internet foram criados vários sistemas de pagamento.

Cartões de Crédito

Uma das primeiras formas de pagamento na internet foi o uso de cartões de crédito. Trata-se de um sistema que já existe no mundo real, que é usado por milhões de pessoas e que permite efetuar compras em qualquer parte do mundo, desde que seja aceite pelo comerciante. Existem vários tipos de cartões, mas todos funcionam da mesma forma: o possuidor do cartão efetua um pagamento, as informações do cartão sao dadas e o dinheiro é movimentado do possuidor para o fornecedor dos serviços.

Assim o seu uso na internet é simples: basta ter um cartão de crédito, este ser aceite pelo fornecedor de serviços e enviar informações sobre o cartão para o fornecedor. O problema reside em questões de segurança : como garantir que o comprador é mesmo o dono do cartão? Para contornar este obstáculo existem várias formas. Uns usam sistemas de criptografia e autorizaçao do cartão online. Outros preferem o uso da confirmação pelo telefone ou e-mail.

Dinheiro Virtual

Como pagar para quem não possui ou não gosta de usar cartões de crédito? A resposta reside no dinheiro virtual. O dinheiro foi uma invencão espantosa pois antes todo sistema comercial se baseava em trocas. Para obter um bem era necessário trocá-lo por outro bem, o que tinha e números inconvenientes. No entanto o dinheiro só tem valor porque se lhe é reconhecido esse valor (pelo estado, entidades bancárias, ...). No início muitas pessoas prefiriam continuar com o sistema de trocas. Levou algum tempo para que os mais precavidos reconhececem o valor do dinheiro. Foram as vantagens deste (menor peso e volume) assim como uma intervenção por parte da entidade emissora que conduziram ao seu uso generalisado .

A criação de dinheiro virtual torna-se o passo seguinte nesta evolução financeira. O dinheiro virtual tem muitas vantagens: não ocupa espaço, não tem custos de emissão , não se desgasta e não se pode perder Mas para ser bem sucedido o dinheiro virtual precisa de ser seguro, rápido e simples de usar vários sistemas de dinheiro virtual foram criados, cada um tem as suas vantagens e não é claro qual será aceito. Como exemplo destes sistemas temos o NetCash, o Netbill, o Netchex, o Netcheque, o Netmarket e o Magic Money.

ecash

De momento o candidato mais provável é o ecash da empresa holandesa Digicash. Existe um banco emissor que dá o ecash aos utilizadores em troca de dinheiro real. O utilizador gasta quanto ecash quiser. Mais tarde o fornecedor de serviços pode trocar o ecash (se o quiser) depois (no tal banco) por dinheiro. Mais tarde o fomecedor de O dinheiro real. Em cada transação são usadas assinaturas digitais públicas para manter segurança. software cliente, usado pelos clientes para encriptar a transação, é gratuito e garante anonimato.Somente as lojas e serviços participantes têm de pagar uma pequena taxa e declarar todas transações (para evitar fugas ao fisco ou lavagem de dinheiro). Devido a ser um sistema simples o ecash tem bastantes probabilidades de ser bem sucedido.

NetCheque

O NetCheque, desenvolvido pela Universidade da Califórnia do Sul , usa-se da mesma forma que os cheques tradicionais. Os NetCheques são e-mails assinados pelo pagador autorizado com uma assinatura eletrônica (código criptográfico) e enviados para o receptor. Este processo é protegido pelo sistema de kerberos. A assinatura do utilizador cria o cheque enquanto que o endosso da pessoa a quem se paga o transforma numa ordem para o computador do banco.

LETSystem

Trata-se de um sistema mais ambicioso e complexo. Funciona na base de dinheiro local, tipos de unidades monetárias vagas e usadas em certas comunidades. Como exemplo desta unidades temos o Stroud, xxxx e pedras. Um utilizador nunca passa a dever dinheiro mas fica antes comprometido, i.e., devendo um serviço à comunidade. Este tipo de sistema depende bastante da confiança de todos que o usam.

PGP

PGP é um criptsistema híbrido que combina algorítmos de chaves públicas (assimétricas) com algorítmos convencionais (simétricos), com a vantagem de utilizar a velocidade da criptografia convencional e a seguranca da criptografia por chaves públicas. As chaves públicas são mantidas em arquivos que contém a identificação do usuário (i.e. o nome da pessoa), a hora (timestamp) da geração do par de chaves e as chaves propriamente ditas. São usados dois arquivos (key rings) diferentes, um para chaves públicas e outro para as secretas, que podem conter uma ou mais chaves cada um.

As chaves públicas são internamente referenciadas por uma Key JD, que é uma abreviação dessa chave (os 64 bits menos significativos). Enquanto muitas chaves podem ter a mesma identificação do usuário

(User JD), nenhuma chave pode ter a mesma Key JD.

PGP faz uso de "message digest para realizar as assinaturas. "Message digest é o nome que se dá a um conjunto de 128 bits fortemente cifrados, função da mensagem. É algo análogo ao checksum ou ao CRC, que é um código verificador de erros, e representa compactamente a mensagem, usada para detectar mudanças em seu conteúdo. Diferentemente do CRC, entretanto, é computacionalmente impraticável a qualquer pessoa descobrir uma outra mensagem que produza uma mesma " message digest", que ainda é criptografada pela chave secreta para formar a assinatura digital.

Os documentos são autenticados por um prefixo que contém o Key JD da chave secreta que foi usada para assiná-lo, o " message digest" do documento devidamente criptografado pela chave secreta doremetente e a hora (timestamp) de quando foi realizada a assinatura. O Key ID é utilizado pelo destinatário para relacioná-lo com a chave públicado remetente, afim de checar a assinatura. O software automaticamente procura a chave pública e a identificação do usuário remetente no arquivo de chaves públicas.

Arquivos cifrados são prefixados pelo Key ID da chave pública usada para cifrá-la. O receptor usa essa informação para relacionar a correspondente chave secreta que decifra a mensagem. Da mesma forma, o software do destinatário automaticamente localiza essa chave secreta no arquivo de chaves secretas.Esses dois tipos de arquivos são o principal método de armazenamento e gerenciamento das chaves públicas e privadas.

Vulnerabilidades

Nenhum sistema de segurança é impenetrável. PGP pode ser enganado de várias formas diferentes. Em qualquer sistema de segurança, temos que nos perguntar se a informação que escondemos é mais valiosa para um eventual agressor do que o custo que este teria para burlar o sistema de proteção. Isto ajudaria a nos proteger de ataques de baixo custo sem nos preocuparmos com meios mais sofisticados e caros de espionagem.

I - Comprometimento da passphrase e chave secreta:

Provavelmente o modo mais simples de quebrar o sistema é escrever em algum lugar sua passphrase. Se alguém a achar e também conseguir copiar seu arquivo de chave secreta, pode tranquilamente ler suas mensagens e enviar outras tantas com a sua assinatura, fazendo com que todos pensem que foi você o autor das tais mensagens.

Não usar passwords simples que possam ser facilmente descobertas como os nomes de esposa ou filhos já ajuda. Se você fizer de sua passphrase uma única palavra (tornando-se uma pas,S.word), ela poderá ser descoberta por um computador que teste todas as palavras do dicionário. Por isso uma passphrase é melhor do que uma password É claro que um agressor mais sofisticado poderia ter em seu computador um banco de dados com frases famosas para tentar achar sua passphrase. Uma passphrase fácil de lembrar e difícil de se descobrir poderia ser construída por alguns dizeres criativos sem sentido algum ou referências literárias obscuras.

2 - Falsificação da chave pública:

Este pode ser o ponto mais vulnerável de um criptossistema de chave pública, principalmente porque a maioria dos novatos na área não percebem a falsificação imediatamente. Quando você usar a chave públicade de alguém, esteja certo de que não foi falsificada. Só podemos confiar na chave pública de uma pessoa se a obtivermos diretamente dessa pessoa, ou se a recebemos em uma mensagem assinada por alguém em quem confiamos. Mantenha um controle fisico de seus arquivos de chave pública e secreta, mais preferivelmente em seu computador pessoal do que naqueles ligados em rede com acesso remoto.Tenha sempre uma cópia de ambos os arquivos.

3 - Arquivos não apagados completamente do disco:

Outro problema potencial é causado pelo modo de deleção de arquivos da maioria dos sistemas operacionais. Quando você criptografa um arquivo e apaga o texto original, o sistema operacional não destrói fisicamente o conteúdo do texto original. Ele apenas marca que aqueles blocos foram apagados do disco, permitindo que esse espaço seja reutilizado posteriormente. Esses blocos marcados ainda contém o texto original que queríamos destruir, e que será realmente apagado apenas quando outros dados forem gravados por cima. Se o agressor tiver acesso aos blocos marcados antes que eles sejam regravados, ele pode recuperar o texto original ou pelo menos parte dele, o que pode ser facilmente realizado com programas especializados.

De fato isto poderia até acontecer acidentalmente, se por alguma razão alguma coisa der errado na estrutura lógica de armazenamento de dados do disco e alguns arquivos forem acidentalmente apagados ou corrompidos. Programas de recuperação podem ser utilizados para tentar reaver os

arquivos danificados, mas isto frequentemente faz com que arquivos previamente deletados sejam ressucitados junto com os arquivos que realmente interessam. Daí, aquele arquivo confidencial que você achava ter sumido para todo o sempre pode reaparecer e ser lido pela pessoa que estava tentando consertar seu disco. Mesmo quando você está escrevendo sua mensagem com um processador de textos,o editor estar gerando várias cópias temporárias do seu texto no disco, apenas porque é texto ele trabalha internamente. Essas cópias temporárias são apagadas pelo próprio assim processador quando o finalizamos, mas os seus fragmentos ficam no disco, em algum lugar.

A única forma de se ter certeza que nossos textos originais não reaparecerão de uma hora pra outra, é, de algum jeito, apagar fisicamente do disco o conteúdo da mensagem. A menos que você tenha certeza de que todos os blocos marcados como apagados serão reutilizados brevemente, pode-se tomar providências para reescrevê-los, e assim, destruir qualquer vestígio do texto sigiloso deixado pelo seu editor de textos favorito. Pode-se fazê-lo utilizando qualquer programa especializado disponível no mercado, como por exemplo o Norton Utilities para DOS (WIPEINFO.EXE).

Mesmo tomadas todas as providências descritas acima, tavez ainda seja possível recuperar o conteUdo original do texto por alguém cheio de recursos. Resíduos magnéticos dos dados originais ficam no disco mesmo após serem regravados. Algum hardware sofisticado de recuperação de dados pode algumas vezes ter utilidade para reaver os dados (mais aí já é demais).

4 - Víroses e Cavalo de Tróia:

Outro tipo de ataque poderia envolver um vírus especial que infectaria o PGP ou o seu sistema operacional. Este vírus hipotético seria projetado para capturar sua passphrase ou chave secreta, e gravá-la em algum arquivo no disco ou enviá-la via rede para o 'proprietário' do referido vírus. Ele poderia até alterar o comportamento do PGP para que as assinaturas não sejam checadas corretamente, por exemplo.

Defender-se desse tipo de ataque nada mais é do que evitar contaminação por virus em geral. PGP não tem defesas contra vírus, ele assume que a sua máquina está livre de vermes, o que pode ser pelo menos tentado por versões atualizadas de produtos anti-vírus disponíveis no mercado. Se por acaso um vírus especial contra PGP aparecer, esperamos que todos tomemos conhecimento logo.

Outra forma de espionagem envolveria uma cópia do PGP parecida visualmente com a original, mas alterada para que não ftlncionasse a contento. Por exemplo, alguém poderia deliberadamente alterá-lo para que não checasse as assinaturas corretamente, permitindo a falsificação das mesmas. Esta versão tipo "Cavalo de Tróia" não seria difícil de ser desenvolvida, pois o código fonte do PGP é amplamente divulgado. Para evitar tais problemas, deve-se confiar na fonte de onde foi adquirida a cópia do PGP, ou pegá-la de várias fontes independentes e compará-las com um utilitário destinado para esse fim.

5 - Falha de segurança física:

Uma descuido do próprio usuário poderia permitir a alguém adquirir seus arquivos originais ou mensagens impressas. Um oponente determinado poderia utilizar meios tais como roubo, vasculhamento de lixo, sequestro, suborno, chantagem ou infiltração entre os funcionários.

Não se iluda com a falsa sensação de segurança só porque você tem uma ferramenta de criptografia. As técnicas criptográficas protegem a informação somente quando elas estão criptografadas, violações fisicas de segurança podem comprometê-las.

6 - Espionagem "Tempest".

Outra forma de espionagem tem sido utilizada por oponentes muito bem equipados que conseguem detectar os sinais eletromagnéticos emitidos pelo computador. Este tipo de ataque caro e de intensa monitoração pode ser realizado por um caminhão suprido da maquinaria necessária, estacionado próximo ao seu local de trabalho e remotamente captando todos os seus toques de teclado, assim como os textos jogados na tela, podendo comprometer seus passwords, mensagens, etc. Este tipo de ataque, conhecido como tempest, poderia ser evitado blindando-se computadores e cabos de rede, de modo que esses sinais não sejam mais emitidos.

7 - Análise de tráfico :

Mesmo que não seja possível ler o conteúdo das mensagens criptografadas, alguma informação útil ainda poderia ser deduzida observando-se de onde as mensagens chegam e para onde elas vão, o tamanho das mesmas e a hora em que foram enviadas. É a mesma coisa que olhar para uma conta telefônica de longa distância e ver para onde você ligou, quando e por quanto tempo ficou conversando, mesmo que o conteúdo da conversa seja desconhecido para um possível espião. A isto chamamos de análise de tráfico. Para resolver este tipo de problema, precisaríamos de protocolos de comunicação especialmente desenvolvidos para reduzir à exposição dessas análises, possívelmente com alguma assistência criptográfica.

8 - Exposição em sistemas multi-usuário:

PGP foi originalmente projetado para rodar em máquinas MSDOS mono-usuárias, sob seu controle fisico direto. Mas agora exitem versões do PGP que também rodam em sistemas multi-usuários como UNIX e VAXIVMS. Nesses sistemas, os riscos de descobrirem seus passwords, chaves secretas ou mensagens são maiores. Um intruso esperto o suficiente ou o próprio administrador de rede poderiam ter acesso aos seus arquivos originais, ou talvez utilizar-se de algum programinha especial para monitorar constantemente a digitação ou ver o que está aparecendo em sua tela. Os riscos reais de segurança dependem de cada situação em particular Alguns sistemas multi-usuários podem ser considerados seguros porque todos os usuários são confiáveis, ou porque não há interesse suficiente em espionar alguém. De qualquer modo, recomenda-se rodar o PGP de uma máquina isolada, em um sistema mono-usuário, diretamente sob seu controle fisico.

9 - Cripto-análise:

Um espião com acesso a supercomputadores poderia montar um formidável e caríssimo ataque para descobrir sua chave secreta, utilizando-se de algum novo método confidencial de análise da informação criptografada. Talvez fosse possível, mas note que o Governo Americano acredita suficientemente no algoritmo RSA a ponto de, em alguns casos, proteger informações a respeito de armas nucleares. Intensas tentativas de quebrar o algoritmo na RSA tiveram sucesso desde 1978.

Talvez o Governo Americano tenha algum método confidencial para quebrar o algoritmo de criptografia convencional utilizado no PGP (IDEA). Mas algum otimismo se justifica, pois os projetistas do algoritmo IDEA estão entre os melhores da Europa. Ele foi extensivamente analisado e revisado por alguns dos melhores cripto-analistas encontrados no mundo.

Além disso, mesmo que estes algoritmos tivessem alguma fraqueza desconhecida, o PGP comprime o texto original antes de criptografá-lo, o que deveria reduzir essas fraquezas quaisquer que fossem. Concluímos que o gasto computacional para quebrar uma mensagem provavelmente seria muito maior do que o valor da própria mensagem.