FELIPE CHAVES FROSSARD
FERNANDO HAFNER

DISTRIBUIÇÃO DE CHAVES DIGITAIS E CERTIFICAÇÃO DIGITAL

Pontifícia Universidade Católica de Campinas
Faculdade de Engenharia da Computação
Junho/2005

FELIPE CHAVES FROSSARD RA: 01068477
FERNANDO HAFNER RA: 01056209

DISTRIBUIÇÃO DE CHAVES DIGITAIS E CERTIFICAÇÃO DIGITAL

Trabalho apresentado como exigência da Disciplina Tópicos de Engenharia da Computação A, ministrada no Curso Engenharia de Computação na PUC-Campinas,sob orientação do professor Ricardo Freitas.

Pontifícia Universidade Católica de Campinas
Faculdade de Engenharia da Computação
Junho/2005

SUMÁRIO

ÍNDICE DE FIGURAS

INTRODUÇÃO

Amores proibidos, comunicação em tempo de guerra e transações financeiras são as necessidades dos seres humanos comumente citadas quando assunto é segurança.

Embora a criptografia tenha uma longa história que remonta, no mínimo, a Júlio César (logo examinaremos uma cifra chamada César), as modernas técnicas de criptografia, incluindo muitas das usadas na Internet de hoje, são baseadas em progressos feitos nos últimos 30 anos.

Veremos nessa monografia que a desvantagem da criptográfica de chaves simétrica era a necessidade de que as duas partes comunicantes concordem com sua chave secreta previamente.

Veremos como as principais ferramentas de segurança em rede estão sendo utilizada para garantir a segurança na internet. É interessante o fato de que é possível fornecer serviços de segurança em qualquer uma das 4 camadas superiores da pilha de protocolos da Internet.

Para ilustrar a segurança em uma camada inferior, a camada de transporte, usaremos o comércio pela Internet como estudo de caso. Chamamos de comércio pela Internet a compra de ‘bens’ pela Internet. Nesse contexto, consideraremos o termo ‘bens’ em um sentido muito mais amplo, que engloba desde livros, CDs, hardwares, softwares, passagens aéreas e assim por diante.

1. O que é Segurança na Rede

Vamos apresentar Alice e Bob, duas pessoas que desejam se comunicar 'com segurança'. Gostaríamos de observar que Alice e Bob podem ser dois roteadores que querem trocar tabela de roteamento com segurança, dois hospedeiros que querem estabelecer uma conexão de transporte segura ou duas aplicações de e-mail que querem trocar e-mails seguros. Amores proibidos, comunicação em tempo de guerra e transações financeiras são as necessidades dos seres humanos comumente citadas quando assunto é segurança.

1.1. Comunicação Segura

Dissemos que Alice e Bob querem se comunicar 'com segurança', mas o que isso significa exatamente? Com certeza, Alice quer que Bob entenda a mensagem que ela enviou, mesmo que eles estejam se comunicando por um meio 'inseguro', em que um intruso (Trudy, a intrusa) pode interceptar, ler e registrar qualquer dado que seja transmitido de Alice a Bob. Bob também quer ter certeza de que a pessoa cm quem está se comunicando é de fato Bob. Alice e Bob também querem ter certeza de que o conteúdo da mensagem de Alice não foi alterado em trânsito. Dada essas considerações, podemos identificar as seguintes propriedades desejáveis da Comunicação segura:

- *Sigilo.* Somente o remetente e o destinatário pretendido devem poder entender o conteúdo da mensagem transmitida. O fato de intrusos poderem interceptar a mensagem exige, necessariamente, que esta seja cifrada de alguma maneira (que seus dados sejam disfarçados) para impedir que a mensagem interceptada seja decifrada (entendida) por um interceptador. Esse aspecto de sigilo é, provavelmente, o significado mais percebido em 'comunicação segura'. Note, contudo, que essa não é apenas uma definição limitada de comunicação segura (relacionamos a seguir aspectos adicionais de segurança), mas também uma definição bastante restrita de sigilo. Por exemplo, Alice poderia também querer que o mero fato de ela estar se comunicando com Bob (ou os horários ou a freqüência de suas comunicações) fosse também um segredo.

- *Autenticação.* O remetente e o destinatário precisam confirmar a identidade da outra parte envolvida na comunicação, confirmar que a outra parte é realmente quem alega ser. A comunicação pessoal entre seres humanos resolve facilmente este problema com o reconhecimento visual. Quando entidades comunicantes trocam mensagens por um meio pelo qual não podem 'ver' a outra parte, a autenticação é assim tão simples. Por que, por exemplo, você deveria acreditar que o e-mail que você recebeu e que contém uma sentença afirmando que aquele e-mail veio de um amigo seu realmente veio daquele amigo? Se alguém o chama ao telefone dizendo ser de um banco e perguntando qual é o número da sua conta, sua senha e seu saldo bancário, alegando finalidades de verificação, você dá essas informações? Esperamos que não.
- *Integridade da mensagem.* Mesmo que o remetente e o destinatário consigam se autenticar reciprocamente, eles querem assegurar que o conteúdo de sua comunicação não seja alterado, por acidente ou por má intenção, durante a transmissão.

Agora que estabelecemos o que significa comunicação segura nesse contexto, vamos considerar o que quer dizer exatamente 'canal seguro'. A que informações um intruso tem acesso e que ações podem ser tomadas sobre os dados transmitidos?

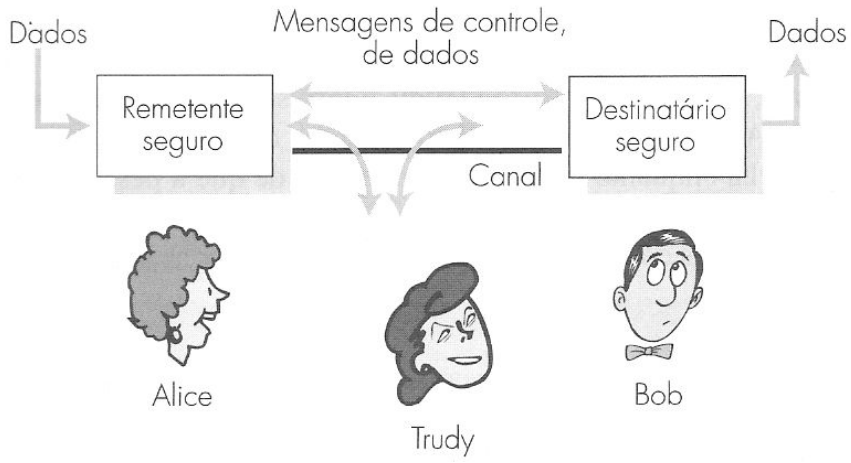

Figura 1 – Remetente, destinatário e intruso (Alice, Bob e Trudy)

Alice, a remetente, quer enviar dados a Bob, o destinatário. A fim de trocar dados com segurança, além de atender aos requisitos de sigilo, autenticação e integridade das

mensagens, Alice e Bob trocarão mensagens de controle e de dados (de maneira muito semelhante ao modo como os remetentes e os destinatários TCP trocam segmentos de controle e segmentos de dados). Todas ou algumas dessas mensagens serão cifradas de modo típico. Um intruso passivo pode ouvir e gravar as mensagens de controle e de dados do canal; um intruso ativo pode remover mensagens do canal e/ou adiciona-las a ele.

2. Princípios da Criptografia

Embora a criptografia tenha uma longa história que remonta, no mínimo, a Júlio César (logo examinaremos uma cifra chamada César), as modernas técnicas de criptografia, incluindo muitas das usadas na Internet de hoje, são baseadas em progressos feitos nos últimos 30 anos. O livro de Kahn *The Codebreakers* [Kahn, 1967] nos oferece um fascinante panorama dessa longa história. [Kaufman, 1995] apresenta uma discussão técnica detalhada sobre criptografia, sobretudo do ponto de vista da rede. [Diffie,1998] fornece uma análise atraente e atualizada das questões políticas e sociais (a respeito, por exemplo, da privacidade) que hoje estão relacionadas à criptografia. Uma discussão completa sobre a criptografia exige um livro inteiro; portanto, apenas trataremos de seus aspectos essenciais, em particular do modo como as técnicas criptográficas são postas em prática na Internet hoje em dia.

As técnicas criptográficas permitem que um remetente disfarce os dados de modo que um intruso não consiga obter nenhuma informação com base nos dados interceptados. O destinatário, é claro, deve estar habilitado a recuperar os dados originais a partir dos dados criptografados. A figura 2 apresenta alguns dos mais importantes componentes criptográficos.

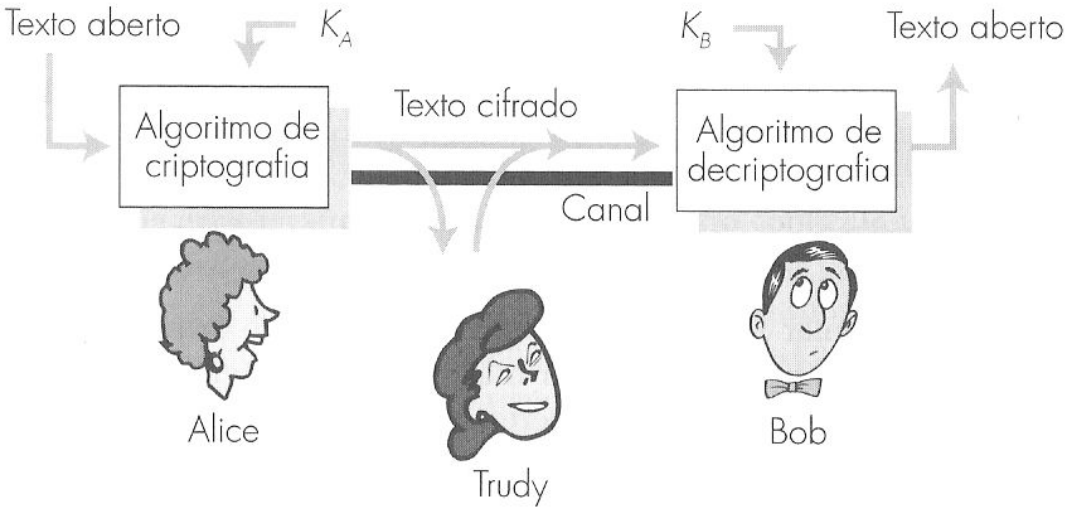

Figura 2 – Componentes Criptográficos

Suponha agora que Alice queira enviar uma mensagem a Bob. A mensagem de Alice em seu modelo original é conhecida como **texto aberto** ou **texto claro**. Alice criptografa sua mensagem em texto aberto usando um **algoritmo de criptografia**, de

modo que a mensagem criptografada, conhecida como **texto cifrado**, pareça ilegível para qualquer possível intruso. O interessante é que em muitos sistemas criptográficos modernos, incluindo os usados na Internet, a técnica de codificação é conhecida, publicada, padronizada e disponível para qualquer um, mesmo um intruso em potencial. Evidentemente, se todos conhecem o método para codificar os dados, então deve haver algum pedaço de informação secreta que impede que um intruso decifre os dados transmitidos. Para resolver esse problema, existe o segredo da chave. Na Figura 2, Alice fornece uma chave, K_A, uma cadeia de números ou de caracteres como entrada para o algoritmo de criptografia. O algoritmo de criptografia pega essa chave e o texto aberto como entrada e produz o texto cifrado como saída. De maneira semelhante, Bob fornecerá uma chave K_B, ao **algoritmo de decriptografia** que pega o texto cifrado e a chave de Bob como entrada e produz o texto original como saída. Nos sistemas conhecidos como **sistemas de chaves simétricas**, as chaves de Bob e Alice são idênticas e secretas. Nos sistemas de **chaves públicas**, é usado um par de chave. Uma das chaves é conhecida por Bob e por Alice, enquanto a outra chave é conhecida por um dos dois, mas nunca por ambos.

2.1 Criptografia – Chaves Simétricas

Todos os algoritmos criptográficos envolvem a substituição de um dado por outro, como, por exemplo, tomar um trecho de um texto e então, calculando e substituindo esse texto por outro cifrado apropriado, criar uma mensagem cifrada. Antes de examinarmos o sistema criptográfico moderno baseado em chaves, vamos examinar um algoritmo de chaves simétricas bastante simples, conhecido como *cifra de César*, atribuído a Júlio César.

A cifra de César funciona tomando cada letra da mensagem do texto aberto e a substituindo pela k-ésima letra sucessiva do alfabeto (permitindo a alternância das letras do alfabeto, isto é, a letra ‘z’ seria seguida novamente da letra ‘a’). Por exemplo, se k=3, então a letra ‘a’ do texto aberto fica sendo ‘d’ no texto cifrado; a letra ‘b’ se torna ‘e’, e assim por diante. Nesse caso, o valor de k serve como chave. Embora o texto cifrado

utilizando a cifra de César parece sem nexo, não levaria muito tempo para quebrar o código, uma vez que existem apenas 25 chaves possíveis.

Um aprimoramento da cifra de César, é a **cifra monoalfabética**, que também substitui uma letra do alfabeto por outra. No entanto, em vez de substituir as letras seguindo um padrão regular, qualquer letra pode ser substituída por qualquer outra letra, contanto que cada letra tenha uma letra substituta exclusiva e vice-versa. Novamente um texto cifrado parece sem nexo, mas nesse caso, existe uma melhoria considerável no número de chaves possíveis, pois há 10^{26} possíveis pares de letras. Usar a força bruta para experimentar 1026 pares demandaria um esforço incrivelmente grande e portanto, excluindo que esse fosse um método utilizável para quebrar esse algoritmo criptográfico e decodificar a mensagem. Contudo, fazendo-se a análise estatística do texto aberto, por exemplo, e sabendo quais letras e grupos de letras são mais freqüentes nos textos do idioma em questão, torna-se relativamente fácil quebrar esse algoritmo.

Existem 3 estratégias diferentes para a quebra de um algoritmo criptográfico. Em uma primeira situação, o intruso tem acesso somente ao texto cifrado, sem ter nenhum conhecimento a respeito do que se trata a informação, nesse caso, dados estatísticos podem ajudar na quebra do algoritmo criptográfico, como mencionado anteriormente, quando foi falado a respeito da cifra monoalfabética. Em um segundo cenário, temos o ataque à um texto do qual o conteúdo já é conhecido anteriormente. Se tivermos, por exemplo, 2 palavras; ‘meia’ e ‘branca’, podemos determinar os pares (texto cifrado, texto aberto) para as letras a,b,c,e,i,m,n e r. Chamamos essa técnica de ataque ao esquema criptográfico a partir do texto aberto conhecido. Em um último caso, o intruso pode escolher a mensagem em texto aberto e obter o seu modelo cifrado correspondente. Para os algoritmos criptográficos vistos até o momento, se o intruso conseguisse que uma pessoa mandasse a mensagem “The quick fox jumps over the lazy dog”, ela poderia decifrar o esquema por completo (a frase utilizada no exemplo, contém todas as letras do alfabeto).

Quinhentos anos atrás foram inventadas técnicas que aprimoravam a cifra monoalfabética. Conhecidas hoje como **cifras polialfabéticas**, essas técnicas foram chamadas de **cifras de Vigenere**. O princípio das cifras de Vigenere é usar múltiplas cifras monoalfabéticas e uma cifra monoalfabética específica para codificar uma letra em uma posição específica no texto aberto da mensagem. Assim, a mesma letra, quando aparece em posições diferentes no texto aberto da mensagem, pode ser codificada de maneira diferente.

2.2 Criptografia – Chaves Públicas

Por mais de 2.000 anos, a comunicação cifrada exigia que as duas partes comunicantes compartilhassem um segredo em comum; a chave simétrica, usada para cifrar e decifrar. Uma dificuldade dessa abordagem é que as duas partes têm que escolher, conjuntamente, de alguma maneira, qual é a chave; mas, para fazê-lo, é preciso comunicação entre os lados. Talvez as partes poderiam se encontrar, e escolher as chaves pessoalmente e mais tarde, comunicar a cifra. No atual mundo em rede, contudo, o mais provável é que as partes comunicantes nunca possam se encontrar e portanto jamais poderiam conversar a não ser pela rede. Seria então possível que 2 pessoas se comunicassem sem utilizar uma chave em comum ? Em 1976, Diffie e Hellman apresentaram um algoritmo conhecido como Troca de Chaves Diffie Hellman, que faz exatamente isso.

O uso da criptografia utilizando chaves públicas é bastante simples. Suponha que Alice queira se comunicar com Bob. Bob, tem 2 chaves; uma chave pública, que está disponível a todos (inclusive à um intruso em potencial), e uma chave privada que apenas Bob conhece. Para se comunicar com Bob, Alice busca primeiramente a chave pública de Bob. Em seguida, ela criptografa sua mensagem usando a chave pública de Bob e um algoritmo criptográfico conhecido. Bob recebe a mensagem criptografada de Alice e usa sua chave privada e um algoritmo de decriptografia conhecido para decifrar a mensagem de Alice. Dessa maneira, Alice pode enviar uma mensagem secreta a Bob sem que nenhum deles tenham que enviar a chave secreta pela rede.

O uso da criptografia de chave pública é, portanto, conceitualmente simples. Mas apresenta duas preocupações. A primeira diz respeito ao conhecimento público da chave e do algoritmo de criptografia, isto é, embora um intruso que intercepta a mensagem cifrada de Alice veja apenas os dados criptografados, ele conhece tanto a chave pública quanto o algoritmo que Alice usou para a criptografia. Assim, um intruso pode montar um ataque ao texto aberto utilizando o algoritmo criptográfico conhecido e a chave pública de Bob para codificar a mensagem que quiser. Para que a criptografia de chaves públicas funcione de forma eficaz, a escolha de chaves e de códigos deve ser feita de tal maneira que seja impossível para um intruso determinar a chave privada de Bob ou conseguir decifrar ou adivinhar a mensagem de Alice a Bob. A segunda preocupação se

refere ao envio da mensagem cifrada, ou seja, como a chave criptográfica de Bob é pública, qualquer um pode enviar uma mensagem cifrada a Bob, incluindo Alice ou alguém se passando por Alice. No caso de uma única chave secreta compartilhada, o fato de o remetente conhecer a chave secreta identifica implicitamente o remetente para o destinatário. No caso da criptografia de chave pública, contudo, isso não acontece, já que qualquer um pode enviar uma mensagem cifrada a Bob usando a chave dele, que está publicamente disponível a todos. É preciso então, de uma assinatura digital, para vincular um remetente à mensagem (o conceito de assinatura digital será melhor abordado no item de Integridade).

3. Distribuição de chaves e certificação

No tópico anterior, vimos que uma desvantagem da criptográfica de chaves simétrica era a necessidade de que as duas partes comunicantes concordem com sua chave secreta previamente. Com a criptografia de chaves públicas, a priori esse acordo quando a um valor secreto não é necessário. Contudo, como a criptografia de chaves públicas também tem suas dificuldades, em particular o problema de obter a chave pública verdadeira de alguém. Ambos os problemas, determinação de uma chave compartilhada para a criptografia de chaves simétricas e obtenção de uma chave pública segura, no caso da criptografia de chaves públicas, podem ser solucionados usando-se um intermediário de confiança. Para a criptografia de chaves simétricas, esse intermediário de confiança é chamado de central de distribuição de chaves (*key distribution center – KDC)*, uma entidade de rede única e de confiança com quem o usuário estabelece uma chave secreta compartilhada. Veremos que a KDC pode ser usada para obter as chaves compartilhadas necessárias para uma comunicação segura com todas as outras entidades de rede, evitando algumas armadilhas. No caso da criptografia de chaves públicas, o intermediário de confiança é chamado de autoridade certificadora (*certification authority – CA).* Uma CA certifica que uma chave pública pertence a uma determinada entidade (uma pessoa ou uma rede). No caso de uma chave pública certificada, se a confiança depositada na CA que certificou a chave for absoluta, poderemos ter certeza quanto a quem pertence a chave pública. Uma vez que uma chave pública é certificada, ela pode ser distribuída de qualquer lugar, incluindo um servidor de chave pública, uma página Web pessoal ou um disquete.

3.1. KDC (Central de Distribuição de chaves)

Suponha novamente que Bob e Alice queiram se comunicar usando criptografia de chaves simétricas. Eles nunca se encontraram (talvez tenham se conhecido em uma sala se bate-papo on-line) e, assim, não combinaram uma chave secreta. Como é possível, então, que eles combinem uma chave secreta, dado que só podem se comunicar um com o outro pela rede? Uma solução frequentemente adotada na prática é usar uma KDC.

A KDC é um servidor que compartilha uma chave simétrica secreta diferente com cada um dos seus usuários registrados. Essa chave pode ser instalada manualmente co

servidor quando o usuário se registra pela primeira vez. A KDC conhece a chave secreta de cada usuário, e cada um deles pode se comunicar com segurança om a KDC usando essa chave. Vejamos como o conhecimento dessa única chave permite que um usuário obtenha uma chave para se comunicar com qualquer outro registrado. Suponha que Alice e Bob sejam usuários da KDC; eles conhecem apenas suas próprias chaves individuais, $K_{A\text{-}KDC}$ e $K_{B\text{-}KDC}$, respectivamente, para se comunicar com segurança com a KDC. Alice dá o primeiro passo, e eles continuam como ilustrado na Figura a seguir.

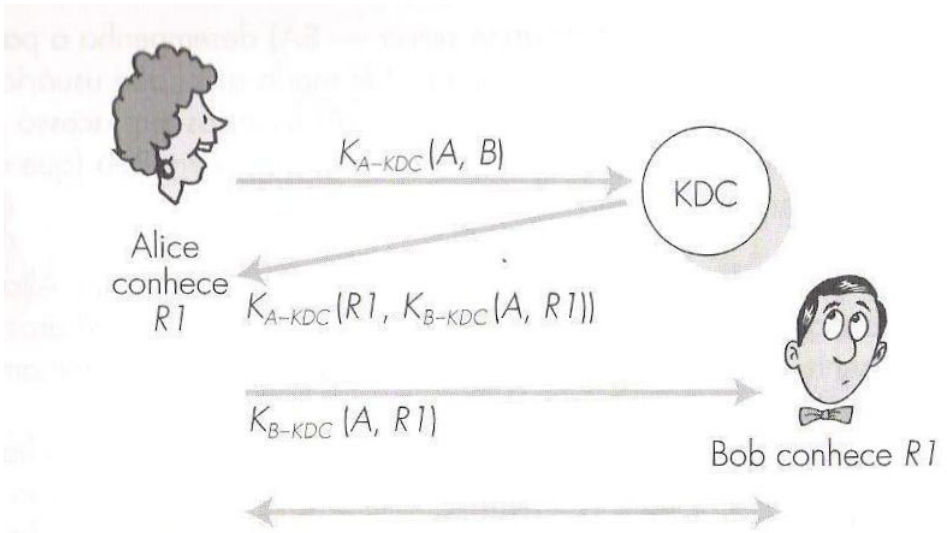

Figura 3 – Estabelecimento de uma chave de sessão única usando uma KDC

1. Usando $K_{A\text{-}KDC}$ para codificar sua comunicação com a KDC, Alice envia uma mensagem à KDC dizendo que ela (A) quer se comunicar com Bob (B). Denominamos essa mensagem de $K_{A\text{-}KDC}$ (A, B).
2. A KDC, como conhece $K_{A\text{-}KDC}$, descriptografa $K_{A\text{-}KDC}$ (A, B). Em seguida, ela gera um número aleatório *R1*. Esse é o valor da chave compartilhada que Al;ice e Bob usarão para realizar criptografia simétrica quando se comunicarem mutuamente. Essa chave é chamada chave de sessão única, pois Alice e Bob a utilizarão apenas durante essa única sessão que estão estabelecendo no momento. A KDC agora precisa informar Alice e Bob do valor de *R1*. Assim, ela devolve a mesma mensagem a Alice, Criptografada usando $K_{A\text{-}KDC}$, contendo o seguinte:

   - *R1*, a chave de sessão única que Alice e Bob vão usar para se comunicarem.

- Um par de valores: *A* e *R1*, criptografados pela KDC usando a chave de Bob, $K_{B\text{-}KDC}$. Chamamos esse valor de (A, R1). É importante notar que a KDC está enviando à Alice não somente o valor de *R1* para seu uso, mas também uma versão criptografada de *R1* e o nome de Alice, criptografados usando a chave de Bob. Alice não pode decifrar esse par de valores da mensagem (ela não conhece a chave criptográfica de Bob), mas na verdade, ela não precisa fazê-lo. Veremos em breve que Alice simplesmente repassa o par de valores criptografados para Bob (que pode decifrá-los).

Esses itens são colocados na mensagem e criptografados usando a chave compartilhada de Alice. A mensagem da KDC para Alice é, portanto, $K_{A\text{-}KDC}(R1, K_{B\text{-}KDC}(R1))$.

3. Alice recebe a mensagem da KDC, extrai *R1* da mensagem e a salva. Ela agora conhece a chave de sessão única, *R1*. Ela também extrai $K_{B\text{-}KDC}(A, R1)$ e a repassa a Bob.
4. Bob decifra a mensagem da KCD, extrai *R1* da mensagem e a salva. Ela agora conhece a chave de sessão única *R1* e sabe quem é a pessoa com a qual está compartilhando essa chave, *A*. É claro que ele toma cuidado de autenticar Alice usando *R1* antes de prosseguir.

3.2. Kerberos

Kerberos (RFC 1510; Neuman, 1994) é um serviço de autenticação desenvolvido no MIT que usa técnicas de criptografia de chaves simétricas e uma central de distribuição de chaves. Embora seja conceitualmente idêntico à KDC genérica descrita acima, o Kerberos tem um vocabulário levemente diferente. Ele contém também diversas variações e extensões interessantes dos mecanismos básicos do KDC. Ele foi projetado para autenticar usuários que acessam servidores de rede e era inicialmente dirigido para o uso de um único domínio administrativo, como um campus ou uma empresa. Assim, ele é estruturado na linguagem de usuários que querem acessar os serviços da rede (servidores) utilizando programas de rede de camada de aplicação, como Telnet (para login remoto) e o NFS (para acesso de arquivos remotos), em vez de

ser estruturado na linguagem de pessoas que querem conversar entre si e precisam se autenticar mutuamente, como nos exemplos apresentados até aqui. Não obstante, a chave (trocadilho proposital) subjacente às duas técnicas continua a mesma.

O servidor de autenticação Kerberos *(authentication server –SA)* desempenha o papel da KDC. Ele é o repositório não apenas das chaves secretas de todos os usuários (de modo que cada usuário pode se comunicar com o SA com segurança), mas também das informações sobre quais usuários têm acesso privilegiado a quais serviços em quais servidores de rede. Quando Alice quer acessar um serviço em Bob (que agora consideramos um servidor), o protocolo segue fielmente o exemplo que demos no tópico acima.

1. Alice contata o SA Kerberos e indica que quer usar Bob. Toda a comunicação entre Alice e o SA é criptografada usando uma chave secreta que é compartilhada entre Alie e o AS. No Kerberos, Alice primeiramente fornece seu nome e senha a seu hospedeiro local. Este e o SA então determinam a chave de sessão única para criptografar a comunicação entre Alice e o SA.
2. O SA autentica Alice, verifica se ela tem acesso privilegiado a Bob e gera uma chave simétrica de sessão única, *R1*, para comunicação entre Bob e Alice. O servidor de autenticação (no jargão do Kerberos, servidor bilheteiro) envia a Alice o valor de *R1* e também um bilhete de entrada para os serviços de Bob. O bilhete contém o nome de Alice, a chave de sessão Alice-Bob, *R1* e o horário de término, tudo criptografado usando a chave secreta de Bob (conhecida apenar por Bob e SA), como na Figura 4 O bilhete de Alice é válido só até o horário de término e será rejeitado por Bob se apresentado após esse horário. Para o Kerberos V4, o tempo máximo de vida útil de um bilhete é de cerca de 21 horas. No Kerberos V5, o tempo de vida útil deve expirara antes do final do ano de 9999, um sério problema para o ano 10000!
3. Alice então envia seu bilhete a Bob. Ela também envia uma marca de tempo criptografada por *R1* que é usada como um nonce. Bob decifra o bilhete usando sua chave secreta, obtém a chave da sessão e decifra a marca de tempo utilizando a chave de sessão que acabou de descobrir. Ele devolve o

nonce a Alice, criptografado por *R1*, mostrando, assim, que ele conhece *R1* e que está 'ao vivo'.

A versão mais recente do Kerberos (V5) fornece suporte para múltiplos servidores de autenticação, delegação de direitos de acesso e bilhetes renováveis (Kaufman, 1995) e (RFC 1510) apresentam mais detalhes sobre o assunto.

3.3. Certificação de Chaves Públicas

Uma das características principais da criptografia de chaves públicas é que é possível que duas entidades troquem mensagens secretas sem ter de trocar chaves secretas. Por exemplo, quando Alice quer enviar uma mensagem secreta a Bob, ela simplesmente criptografa a mensagem com a chave pública de Bob e envia a mensagem criptografada a ele; ela não precisa conhecer a chave secreta (isto é, privada) de Bob nem Bob precisa conhecer a chave secreta de Alice. Assim, a criptografia de chaves públicas evita a necessidade de infra-estrutura de KDC, como o Kerberos.

Evidentemente, com a criptografia de chaves públicas, as entidades comunicantes têm de trocar chaves públicas. Um usuário pode disponibilizar o conhecimento de sua chave pública de muitas maneiras, como, por exemplo, apresentando a chave em sua página Web pessoal, colocando-a em um servidor público de chaves ou enviando-a a um correspondente por e-mail. Um site Web de comércio pode colocar sua chave pública em seu servidor de modo que os browsers descarreguem automaticamente a chave pública ao se conectarem ao site. Roteadores podem colocar sua chave pública em servidores de chaves públicas, permitindo, desse modo, que outras entidades de rede a recuperem.

Há, contudo, um problema sutil, mas importante, com a criptografia de chaves públicas. Para termos uma percepção desse problema, vamos considerar uma transação comercial pela Internet, por exemplo. Suponha que Alice trabalha no ramo de pizzas para entrega e que aceite pedidos pela Internet. Bob, que adora pizza, envia uma mensagem em texto aberto que contém o endereço de sua casa e o tipo de pizza que quer. Nessa mensagem, ele inclui também sua assinatura digital (isto é, um resumo de mensagem criptografado extraído da mensagem original em texto aberto). Alice pode

obter a chave pública de Bob (de sua página Web pessoal, de um servidor de chaves públicas ou de uma mensagem de e-mail) e verificar a assinatura digital. Dessa maneira, ela se certifica de que foi Bob, e não algum adolescente brincalhão, quem fez o pedido.

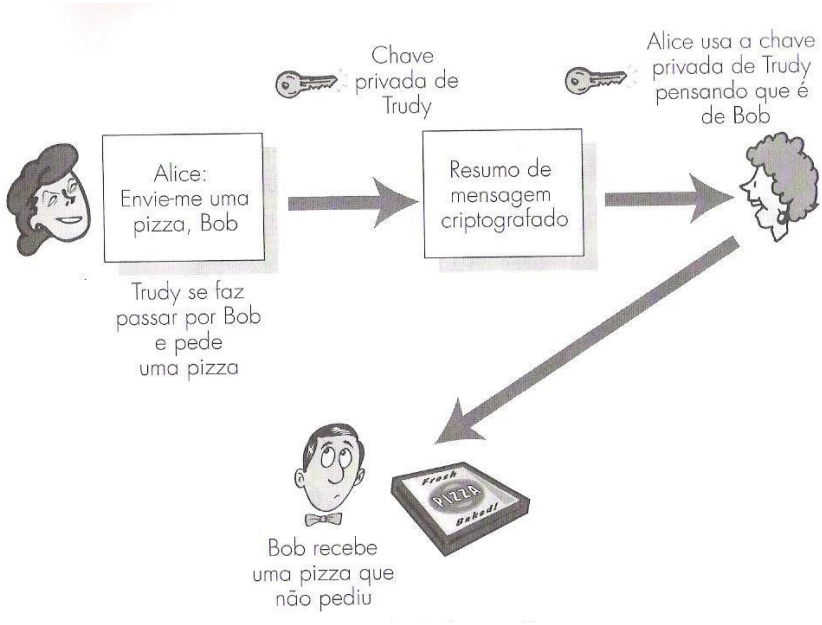

Figura 4 – Trudy se passa por Bob usando a criptografia de chaves Públicas

Tudo parece caminhar bem até que entra em cena a esperta Trudy. Como mostrado na Figura 4, Trudy decide fazer uma travessura. Ela envia uma mensagem a Alice na qual diz que é Bob, fornece o endereço de Bob e pede uma pizza. Ela também anexa uma assinatura digital, mas faz isso assinando o resumo de mensagem com sua chave privada. Ela também de faz passar por Bob enviando a Alice sua chave pública, mas dizendo que a chave pertence a Bob. Nesse exemplo, Alice aplicará a chave pública de Trudy (pensando que é a de Bob) na assinatura digital e concluirá que a mensagem em texto aberto foi, na verdade, criada por Bob. Este ficará muito surpreso quando o entregador aparecer em sua casa com uma pizza, com tudo acertado!

Por esse exemplo, vemos que, para a criptografia de chaves públicas seja útil, as entidades (usuários, browsers, roteadores) precisam ter certeza de quem possuem a chave publica da entidade com a qual estão se comunicando. Por exemplo, quando Alice estiver e comunicando com Bob usando criptografia de chaves públicas, ela precisa saber, com certeza, que a chave pública que supostamente é de Bob, é de fato dele.

A vinculação de uma chave pública a uma entidade particular é feita, tipicamente, por uma autoridade certificadora *(certification authoroty – CA),* cuja tarefa é validar identidades e emitir certificados. A CA tem as seguintes incumbências:

1. A CA verifica se uma entidade (pessoa, roteador e assim por diante) é quem se diz ser. Não há procedimentos obrigatórios quanto ao modo como deve ser feita a certificação. Ao tratarmos com uma CA, devemos confiar que ela tenha realizado uma verificação rigorosa da entidade. Por exemplo, se Trudy conseguisse entrar na autoridade certificadora Fly-by-night, e simplesmente declarasse "Eu sou Alice" e recebesse certificados associados à identidade de 'Alice', então não se deveria dar muita credibilidade às chaves públicas certificadas pela autoridade certificadora Fly-by-night, Por outro lado, se mais sensato (ou não!) estar inclinado a confiar em uma CA que faze parte de uma programa federal, ou estadual, como por exemplo, (Utah, 1999). O grau de confiança que se tem na 'identidade' associado a uma chave pública equivale apenas ao grau de confiança depositado na CA e m suas técnicas de verificação de identidades.
2. Assim que a CA verifica a identidade da entidade, ela cria um certificado que vincula a chave pública da entidade à identidade. O certificado contém a chave pública e a informação exclusiva que identifica mundialmente a chave pública do proprietário (por exemplo, o nome de alguém ou um endereço IP). Esses passos são mostrados na figura abaixo.

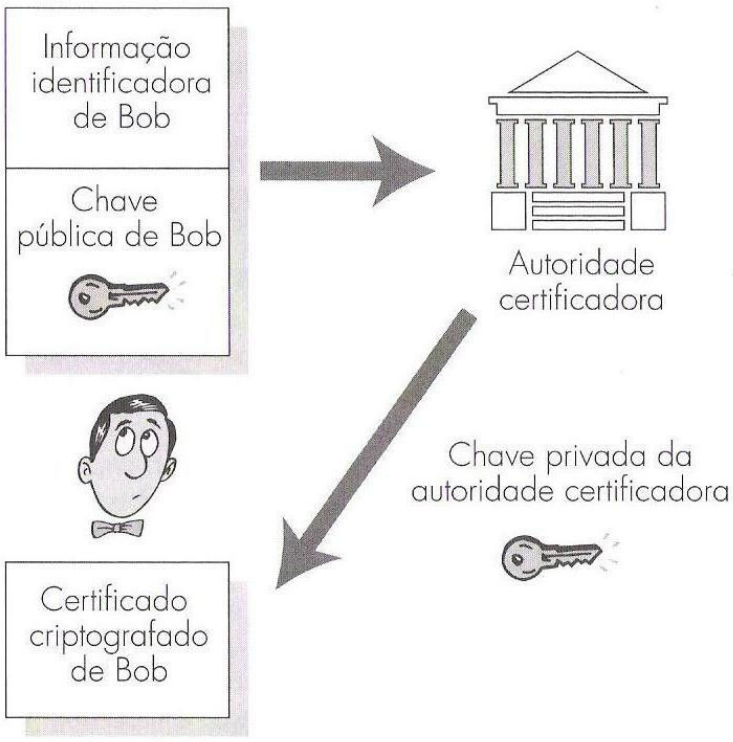

Figura 5 – Bob obtém um certificado de uma CA.

Vejamos, agora, como os certificados podem ser usados para combater os espertinhos das pizzas, como Trudy e outros indesejáveis. Quando Alice recebe o pedido de Bob, ela pega o certificado de Bob, que pode estar na página dele, em uma mensagem de e-mail ou em um servidor de certificados. Alice usa a chave pública da CA para verificar se a chave pública do certificado de Bob, é de fato, de Bob. Supomos qua a chave pública da CA seja conhecida de todos (por exemplo poderia ser divulgada em um local conhecido e de confiança, como no jornal *The New York Times*, de modo que todos a conheçam e que não pode ser falsificada) e que Alice então possa ter certeza de que está realmente tratando com Bob. A Figura 6 ilustra os passos envolvidos na criptografia de chaves públicas mediada por uma CA.

Tanto a International Telecommunication Unio (ITU) quanto a IETF desenvolveram padrões para autoridades certificadoras. Na recomendação ITU X.509 (ITU, 1993), encontraremos especificado um serviço de autenticação, bem como uma sintaxe própria para os certificados. O RFC 1422 descreve um gerenciamento de chaves baseado em CA para uso com o e-mail seguro pela internet. Essa recomendação é compatível com a X.509, mas vai além desta, pois estabelece procedimentos e

convenções para uma arquitetura de gerenciamento de chaves. A tabela abaixo apresenta alguns campos importantes de um certificado.

Nome do Campo	*Descrição*
Versão	Número da versão especificada X.509
Número de Série	Identificador exclusivo emitido pela CA para um certificado
Assinatura	Especifica o algoritmo usado pela CA para 'assinar' esse certificado
Nome do Emissor	Identidade da CA que emitiu o certificado, no formato chamado de nome distinto (DN) especificado na RFC 2253
Período de validade	Inicio e fim do período de validade de um certificado
Nome do sujeito	Identidade da entidade cuja chave pública está associada a esse certificado, em formato DN
Chave pública do sujeito	A chave pública do sujeito bem como a indicação do algoritmo de chave pública (e parâmetros do algoritmo) a ser usado com essa chave.

Campos selecionado de um certificado de chave pública X.509 e RFC 1422

Com o crescimento do comércio eletrônico e a conseqüente necessidade de garantir a segurança das transações, tem havido um interesse crescente em autoridades certificadoras. Dentre as empresas que fornecem serviços de CA destacam-se a Cybertrust (Cybertrust, 1999), a Verisign (Verisign, 1999) e a Netscape (Netscape Certificate, 1999).

4. E-mail seguro

Nessa seção, veremos como as principais ferramentas de segurança em rede está sendo utilizada para garantir a segurança na internet. É interessante o fato de que é possível fornecer serviços de segurança em qualquer uma das 4 camadas superiores da pilha de protocolos da Internet. Quando é fornecida segurança para um protocolo específico de camada de aplicação, a aplicação que usa o protocolo desfruta de um ou mais serviços de segurança, como sigilo, autenticação ou integridade. Quando a segurança é fornecida para um protocolo de camada de transporte, todas as aplicações que usam o protocolo desfrutam dos serviços de segurança do protocolo de transporte. Quando a segurança é fornecida na camada de rede, na base de hospedeiro para hospedeiro, todos os segmentos de camada de transporte desfrutam dos serviços de segurança da camada de rede. Quando a segurança é fornecida com base no enlace, todos os dados de todos os quadros que estão trafegando pelo enlace recebem os serviços de segurança do enlace. A necessidade da segurança nas diversas camadas se dá ao fato de que embora exista na camada de rede um 'cobertor de segurança' com a criptografia dos dados, e autenticação de todos os endereços IP de origem, isso não garante segurança no nível do usuário. Por exemplo, um site comercial não pode confiar na segurança da camada IP para autenticar um cliente que está comprando mercadorias. Assim, existe a necessidade de uma funcionalidade de segurança nas camadas mais altas, bem como um 'cobertor de segurança' nas camadas mais baixas. Em segundo lugar, é geralmente mais fácil disponibilizar novos serviços de Internet, incluindo serviços de segurança nas camadas mais altas da pilha de protocolos. Enquanto aguardamos que a segurança seja disseminada de maneira mais ampla na camada de rede, o que ainda levará alguns anos para acontecer, muitos desenvolvedores de aplicação tomam a iniciativa de fazê-lo mesmo assim e introduzem a funcionalidade em suas aplicações. Um exemplo clássico é o PGP (Pretty Good Privacy), que fornece e-mail seguro. Como exige apenas programas de aplicação cliente e servidor, o PGP foi uma das primeiras tecnologias de segurança a ser usada amplamente na Internet. Examinaremos a seguir a segurança em camada de aplicação, utilizando o E-Mail como estudo de caso.

Para exemplificar criaremos um projeto de alto nível de maneira incremental, introduzindo, a cada estágio, novos serviços de segurança. Ao projetarmos um sistema

de e-mail seguro, vamos manter em mente o exemplo já citado anteriormente onde 2 pessoas se comunicam (Bob e Alice) e uma 3ª pessoa deseja "bisbliotar" a mensagem (Trudy). Primeiramente devemos projetar um sistema de e-mail seguro para Alice e Bob, onde devemos considerar quais as características de segurança mais desejáveis para os dois. A primeira característica a ser considerada, e a mais importante, é o sigilo. A segunda, diz respeito a autenticação do remetente. Isto é, quando Alice manda uma mensagem para Bob, Bob deve ter certeza que a mensagem veio de Alice e não de alguém se passando por Alice. Outra questão, diz respeito a integridade, ou seja, a garantia de que uma mensagem enviada por Alice para Bob, não tenha o seu conteúdo modificado durante o envio da mensagem. Por último, existe a questão da autenticação do receptor, ou seja, Alice quer ter certeza que a mensagem que ela está enviando está indo para Bob e não para alguém se passando por Bob.

Assim vamos começar abordando a primeira preocupação de Alice e Bob, ou seja, o sigilo. A maneira mais direta de consegui-lo é Alice criptografar a mensagem por tecnologia de chaves simétricas e Bob decifrar a mensagem ao recebe-la. Se a chave simétrica for suficientemente longa e se somente Alice e Bob possuírem a chave, então será reduzida consideravelmente a possibilidade de alguém ler a mensagem. Embora essa seja uma abordagem direta, ela apresenta a dificuldade fundamental de que é difícil distribuir chaves simétricas de modo que apenas Bob e Alice tenham copias delas. Assim, a criptografia de chaves públicas é naturalmente uma alternativa. Na abordagem de chave pública, Bob disponibiliza publicamente sua chave pública e Alice criptografa a mensagem utilizando a chave pública de Bob, enviando a mensagem cifrada para o endereço de e-mail de Bob. Quando Bob recebe a mensagem, ele simplesmente a decifra com sua chave privada. Supondo que Alice tenha certeza de que a chave pública que usou é a de Bob, então essa abordagem satisfaz o quesito de sigilo. Porém, existe o problema que a criptografia de chaves públicas é relativamente ineficiente, principalmente para as mensagens longas (que são cada vez mais comuns nos dias de hoje). Para superarmos o problema da eficiência, vamos fazer o uso de uma chave de sessão. Em particular, Alice (1) escolhe uma chave simétrica, K_S aleatoriamente, (2) criptografa sua mensagem *m* com a chave simétrica K_S, (3) criptografa a chave simétrica com a chave pública de Bob, e_B, (4) concatena a mensagem cifrada e a chave simétrica cifrada de modo que formem um 'pacote' e (5) envia o pacote ao endereço de e-mail de Bob. Os passos estão ilustrados na Figura 6 (o sinal '+' representa a concatenação e o sinal '-' representa a desconcatenação). Quando Bob receber o pacote, ele vai (1) usar

sua chave privada d_B para obter a chave simétrica K_S e (2) utilizar a chave simétrica K_S para decifrar a mensagem m.

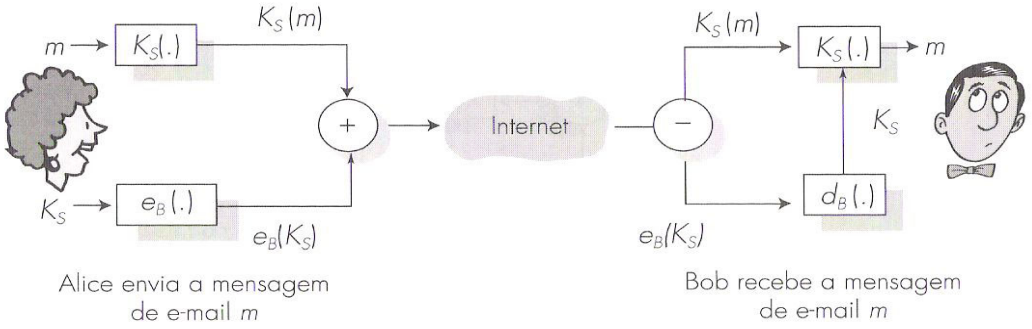

Figura 6 – Passos para criptografia de um email

Agora que projetamos um sistema de e-mail seguro que fornece sigilo, vamos desenvolver um outro sistema que forneça autenticação do remetente e a integridade da mensagem. Vamos supor, no momento, que Alice e Bob não estejam mais preocupados com o sigilo e que estejam somente preocupados com a autenticação do remetente e com a integridade da mensagem. Para realizarmos essa tarefa, faremos uso de assinaturas digitais e resumos de mensagem. Especificamente, Alice (1) aplica uma função de hash H à sua mensagem *m* para obter um resumo de mensagem, (2) criptografa o resultado da função hash com sua chave privada d_A, para criar uma assinatura digital, (3) concatena o original (mensagem não codificada) com a assinatura para criar uma pacote e (4) envia o pacote ao endereço de e-mail de Bob. Quando Bob recebe o pacote, ele (1) aplica a chave pública de Alice, eA, ao resumo de mensagem assinado e (2) compara o resultado dessa operação com o próprio hash H da mensagem. Os passos são ilustrados na Figura 7. Se os dois resultados forem os mesmos, Bob poderá ter certeza de que a mensagem veio de Alice e não foi alterada

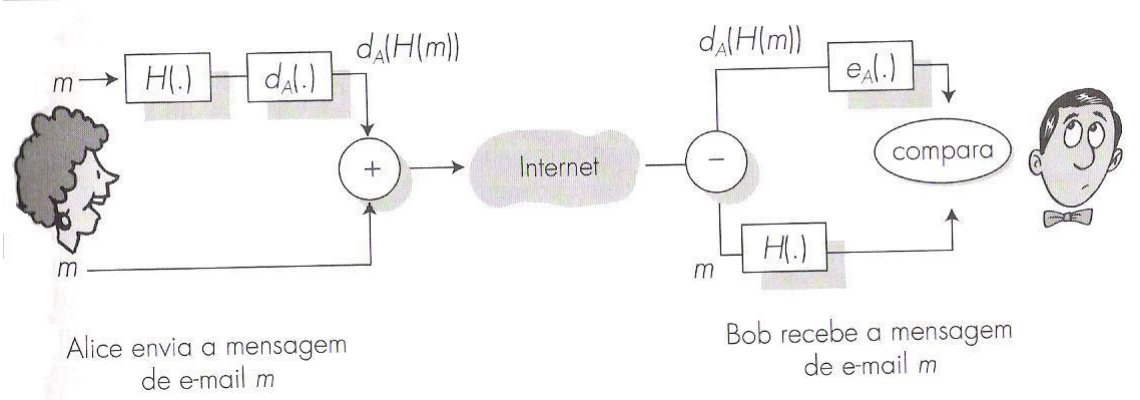

Figura 7 – Uso de funções hash para gerar assinaturas digitais

5. Comércio pela Internet

Para ilustrar a segurança em uma camada inferior, a camada de transporte, usaremos o comércio pela Internet como estudo de caso. Chamamos de comércio pela Internet a compra de 'bens' pela Internet. Nesse contexto, consideraremos o termo 'bens' em um sentido muito mais amplo, que engloba desde livros, CDs, hardwares, softwares, passagens aéreas e assim por diante. Durante a década de 90, muitos sistemas foram projetados para o comércio pela Internet, alguns oferecendo níveis mínimos de segurança e outros fornecendo altos níveis de segurança, acompanhados do anonimato do cliente. No final da década de 90, no entanto, houve uma grande mudança de cenário, pois apenas alguns desses sistemas foram amplamente implementado em browsers e servidores. Dois sistemas se firmaram até o momento; a SSL (Secure Sockets Layer) que é atualmente usada na maioria das transações pela Internet, e a SET (Secure Electronic Transaction Protocol) que deverá competir com a SSL nos próximos anos.

O comércio pela Internet, seja com SSL ou com SET, faz uso extensivo da infra-estrutura de cartões de crédito/débito que os consumidores, comerciantes e instituições financeiras usam há muitos anos. Há três participantes importantes nessa infra-estrutura: o cliente que está comprando o produto, o comerciante que está vendendo o produto e o banco comercial, que autoriza a compra.

CONCLUSÃO

Após uma breve análise, pôde-se avaliar a complexidade e a importância da criptografia. Vimos que os algoritmos de criptografia já são datados desde a época da Roma Antiga, com as cifras de César, e até hoje continuam sendo aprimorados para garantir o sigilo, autenticidade e integridade das informações que trafegam nas redes. Pôde-se observar também a necessidade de elaborar formas de segurança nas diversas camadas de uma rede, uma vez que cada camada tem a sua importância em garantir a confiabilidade das informações.

BIBLIOGRAFIA

Livros:

D. Kahn. **The Codebreakers: The story of secret writing.** The Macmillian Company, 1967

C. Kaufman, R. Perlman e M. Speciner. **Network Security: Pivate communication in a public world.** Englewood Cliffs: Prentice Hall, 1995.

W. Diffie e S. Landau. **Privacy on the line, the politics of wiretapping and encryption.** Cambrige: MIT Press, 1998.

B. Neuman e T. Tso. **Kerberos: An Authentication Service for Computer Networks.** IEEE Communication Magazine, vol. 32, n. 9, 1994, p 33-38

Sites:

J.Kohl e C. Neuman. **The kerberos Network Authentication Service (V5),** RFC 1510 http://www.rfc-editor.org, Acesso em Jun, 2005

S. Kent. **Privacy Enhancement for Internet Eletronic Mail,** RFC 1422 http://www.rfc-editor.org, Acesso em Jun, 2005

Departamento do Comércio do Estado de Utah. **Certification Authority Licensing Program**, http://www.commerce.state.ut.us/digsig/dsmain.htm, Acesso em Jun, 2005

International Telecommunication Unio **(ITU)** http://www.itu.ch/, Acesso em Jun, 2005

Cybertrust Solutions, **Cybertrust Solutions,** http://cybertrust.com, Acesso em Jun, 2005

Verisign, **Verisign,** http://www.verisign.com/, Acesso em Jun, 2005.

Netscape Communication Corp. **Netscape Certificate Server FAQ** http://www.netscape.com/ , Acesso em Jun, 2005.