



SEGURANÇA EM REDES DE COMPUTADORES

SEGURANÇA EM CONEXÃO FIM A FIM

Autor: Me. Paulo André Zapparoli

Revisor: Rafael Rehm

INICIAR



introdução

Introdução

Nesta unidade aprenderemos o processo de criptografia ou cifragem das informações, os elementos necessários para fazermos o processo de criptografia e a necessidade e formas de gerenciamento das chaves criptográficas que é desses elementos. Compreenderemos os modelos de criptografia simétricos e assimétricos e os algoritmos aplicados a cada um deles.

Estudaremos também a aplicação desses conceitos criptográficos nas comunicações, explorando a segurança em várias camadas da pilha de protocolos TCP/IP. Na camada de transporte veremos a aplicação do SSL, que faz a criptografia nas sessões ou conexões gerenciadas por essa camada. Na camada Internet analisaremos a segurança com a implementação do IPsec, que permite a comunicação segura entre redes, sendo aplicado em acessos remotos entre redes da organização (como escritórios geograficamente distribuídos), diretamente com o cliente remoto (colaboradores em viagem ou *home office*) ou até mesmo com redes locais de parceiros comerciais. Na camada de aplicação, com as assinaturas digitais que implementam autenticidade e não repúdio ou com aplicações que exploram as conexões ou sessões SSL.

Criptografia e Algoritmos Criptográficos

A criptologia é a ciência de criar e violar os códigos secretos. É o modo de armazenar e transmitir dados, de modo que somente o destinatário pretendido possa ler ou processá-los. Bom, antes de iniciar vamos começar com algumas definições.

Uma mensagem original é conhecida como **texto claro** (ou *plaintext*), enquanto a mensagem codificada é chamada de **texto cifrado** (ou *ciphertext*). O processo de converter um texto claro em um texto cifrado é conhecido como **cifração ou encriptação**; restaurar o texto claro a partir do texto cifrado é **decifração ou decriptação**. Os muitos esquemas utilizados para a encriptação constituem a área de estudo conhecida como **criptografia**. Esse esquema é designado **sistema criptográfico ou cifra**. As técnicas empregadas para decifrar uma mensagem sem qualquer conhecimento dos detalhes de encriptação estão na área da **criptoanálise**, que é o que os leigos chamam de “quebrar o código”. As áreas da **criptografia** e criptoanálise, juntas, são chamadas de criptologia (STALLINGS, 2015, p. 21).

A criptografia também precisa de uma **chave**, que desempenha um papel crítico para criptografar e descriptografar uma mensagem. A pessoa que possui a chave pode descriptografar o texto codificado para texto claro. Vamos usar um exemplo histórico de criptografia para melhor compreensão: Acredita-se que Júlio César protegia as mensagens, colocando dois conjuntos do alfabeto lado a lado e, em seguida, trocando um deles por um número específico de casas. **O número de casas na troca atua como chave**. Ele convertia o texto claro em texto cifrado usando essa chave e somente seus generais, que também tinham a chave, sabiam como decifrar as mensagens. Esse método é a cifra de César.

A segurança de um criptossistema normalmente depende do segredo das chaves, não do da cifra. Um criptossistema forte tem uma gama de chaves possíveis, o que inviabiliza testar todas elas em um ataque por força bruta. Além disso, um criptossistema resiste a todo método anteriormente conhecido de quebra de códigos e também deve produzir texto cifrado que pareça aleatório a todo teste estatístico-padrão (KIM; SOLOMON, 2014, p. 214).

Criptografia Simétrica

Existem cinco itens em um esquema de encriptação simétrica (veja figura 3.1):

- **Texto Claro** : informação original, pode ser a entrada do algoritmo de encriptação no caso da criptografia ou sua saída no caso da descriptografia.
- **Algoritmo de Encriptação** : regras para a transformação e substituições no texto claro.
- **Chave Secreta** : sendo a entrada para o algoritmo de encriptação, a chave secreta determina exatamente quais são as substituições e transformações feitas pelo algoritmo. Chaves diferentes produzem saídas diferentes. Deve possuir um valor independente do algoritmo e do texto claro.
- **Texto Cifrado** : é o resultado do processo de criptografia. Um conjunto de dados ininteligível que parece ser aleatório.

- **Algoritmo de Decriptação** : é a execução de modo inverso do algoritmo de encriptação, retornando o texto claro (original) do texto cifrado.

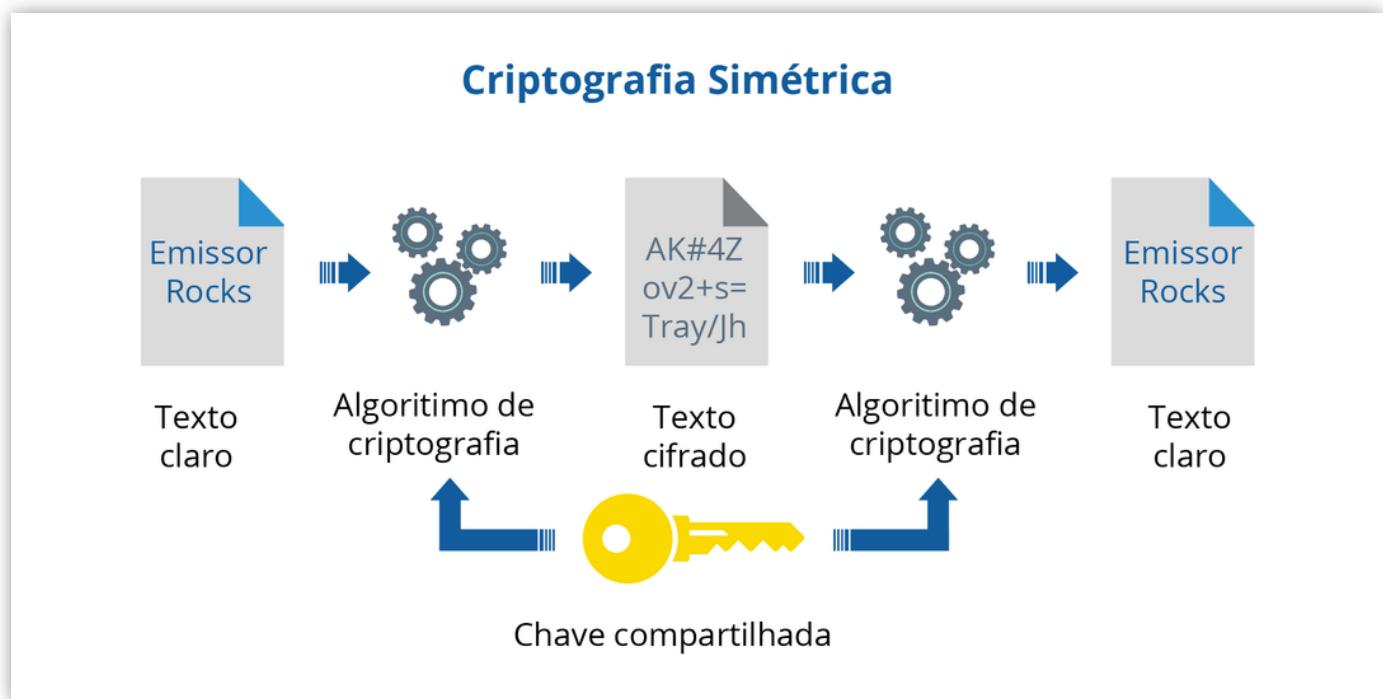


Figura 3.1 - Criptografia Simétrica

Fonte: Munkhzaya Ganbold / Wikimedia Commons.

Para o uso seguro da encriptação simétrica existem dois requisitos que devem ser observados:

1. Precisamos de um algoritmo de encriptação forte. A exigência mínima seria que o algoritmo fosse tal que, mesmo tendo acesso a mensagens cifradas e sabendo qual é o algoritmo o adversário seja incapaz de descobrir a chave ou decifrar o texto.
2. Emissor e receptor devem, de uma forma segura, possuir cópias da chave secreta e mantê-la protegida. Com a descoberta da chave e o algoritmo, toda a comunicação usando essa chave poderá ser lida.

Uma premissa é que mesmo com o texto cifrado e conhecimento do algoritmo de encriptação/decriptação, seja impraticável decriptar a mensagem, ou seja, não precisamos manter o algoritmo secreto, todo o esforço pode ser voltado para que a chave fique secreta. Essa característica torna viável para uso generalizado da encriptação simétrica. Isso tem permitido aos fabricantes desenvolverem implementações de chip de baixo custo, que são encontrados

com facilidade, com algoritmos de encriptação de dados incorporados em diversos produtos. O principal problema de segurança, com o uso da encriptação simétrica, é manter o sigilo da chave.

Algoritmos Simétricos

Vários sistemas de criptografia usam a criptografia simétrica. Alguns dos padrões de criptografia comuns que usam criptografia simétrica incluem o seguinte:

3DES (triplo DES) : *Digital Encryption Standard* (DES) é uma cifra de blocos simétrica de 64 bits, que usa uma chave de 56 bits. Essa cifra usa um bloco de 64 bits de texto claro como entrada e um bloco de 64 bits de texto codificado como saída. Sempre opera em blocos de igual tamanho e usa permutações e substituições no algoritmo. Permutação é uma maneira de organizar todos os elementos de um conjunto.

O Triplo DES criptografa três vezes os dados e usa uma chave diferente para, no mínimo, uma das três passagens, fornecendo um tamanho de chave cumulativa de 112-168 bits. O 3DES é resistente ao ataque, mas é muito mais lento do que o DES.

O ciclo de criptografia do 3DES ocorre da seguinte forma:

1. Dados criptografados pelo primeiro DES.
2. Dados descriptografados pelo segundo DES.
3. Dados criptografados novamente pelo terceiro DES.

O processo inverso descriptografa o texto codificado.

IDEA : Utiliza chave de 128 bits e blocos de 64 bits. A divisão de cada bloco de 64 bits resulta em 16 blocos que são transformados pelo IDEA. Utilizado no PGP (Pretty Good Privacy) substituindo o DES.

AES (Advanced Encryption Standard) : bloco de tamanho fixo de 128 bits, chaves com 128, 192 ou 256 bits de tamanho. Aprovado pelo NIST (Instituto Nacional de Padrões e Tecnologia) em dezembro de 2001. Utilizado para

proteção de informações confidenciais pelo governo americano.

reflita

Reflita

Devido às características da criptografia simétrica ela deve ser empregada em aplicações cuja passagem da chave entre os dois lados da comunicação seja fácil e segura, sob pena de comprometer sua aplicação. Reflita quais são as possíveis aplicações onde você deve encontrar esse tipo de criptografia.

Fonte: Elaborado pelo autor.

O AES é um algoritmo forte que usa chaves de comprimentos maiores. O AES é mais rápido do que DES e 3DES, portanto, oferece uma solução tanto para aplicações de software quanto para uso de hardware em firewalls e roteadores.

Criptografia Assimétrica

Um sistema assimétrico soluciona a vulnerabilidade envolvida no compartilhamento de chaves secretas. A característica de um sistema assimétrico é que as chaves diferentes são usadas para cifrar e decifrar. Os conceitos básicos de um sistema prático e funcional foram concebidos em torno de 1970 por Ron Rivest, Adi Shamir e Len Adleman, e trabalham com base em números primos e aritmética modular. Um exemplo de aritmética modular é o cálculo de tempo com um relógio. Imagine um relógio de 12 horas que indique 9 horas. Adicionar 8 horas resulta no tempo de 5 horas (HINTZBERGEN et al., 2015, p. 94).

A criptografia assimétrica, também chamada de criptografia de chave pública, utiliza uma chave de criptografia para criptografar que é diferente da chave

usada para descriptografar. Um criminoso não pode calcular uma chave de descriptografia baseada no conhecimento da chave de criptografia e vice-versa, em qualquer período de tempo razoável. Vejamos características dos algoritmos assimétricos:

- Utiliza uma chave para criptografar e outra chave para descriptografar;
- Uma chave é pública e outra é privada;
- No sistema de criptografia de chave pública, quando a mensagem é criptografada com a chave pública somente o proprietário da chave privada pode decifrá-la;
- Desnecessário o compartilhamento de chave na troca de mensagens;
- Mais complexos os algoritmos assimétricos consomem mais recursos de máquina o que provoca mais lentidão.

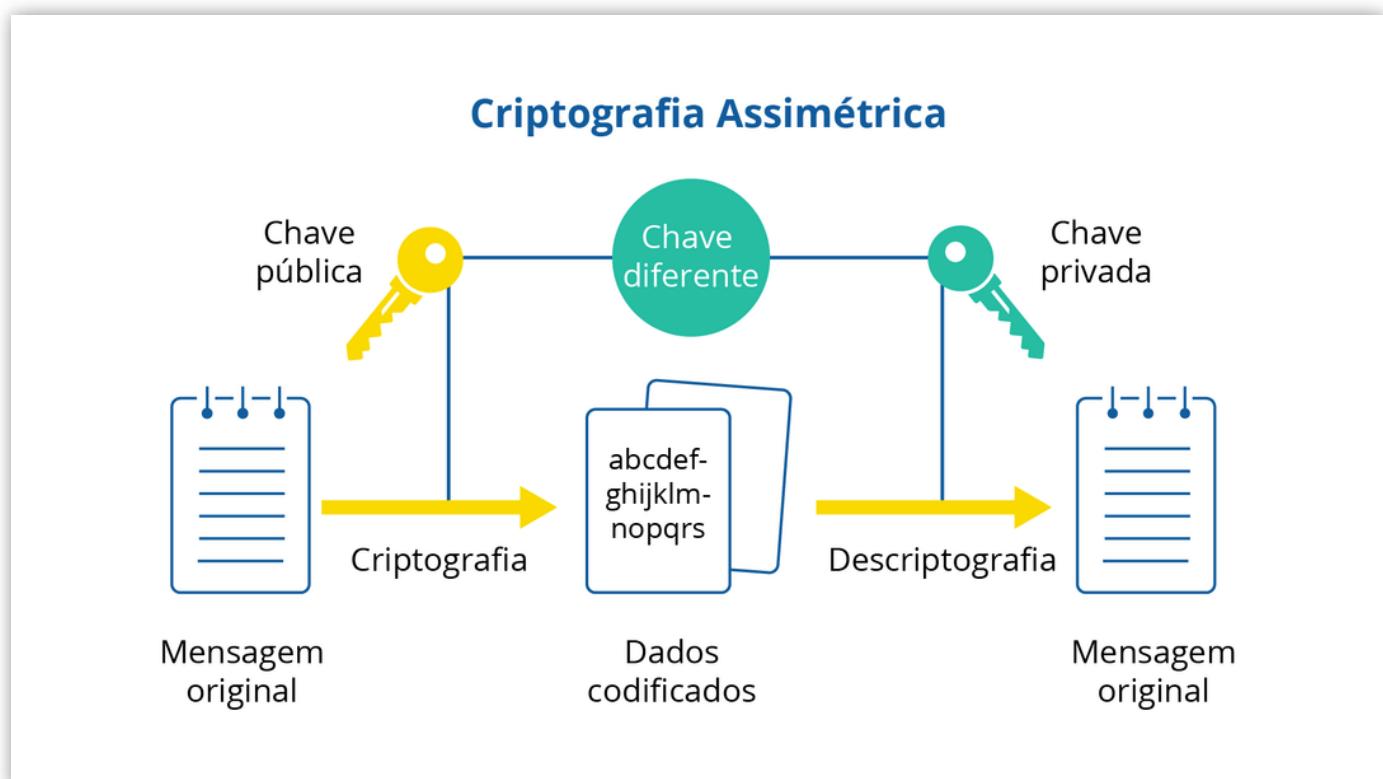


Figura 3.2 - Criptografia Assimétrica

Fonte: Munkhzaya Ganbold / Wikimedia Commons.

Algoritmos Assimétricos

Como é o par de chaves independentes o principal elemento que torna esses

algoritmos seguros, os algoritmos assimétricos usam fórmulas mais simples, que qualquer pessoa pode procurar. São Algoritmos Assimétricos.

RSA (Rivest-Shamir-Adleman) - utiliza o produto de dois números primos muito grandes. Como é comum seu uso no SSL, os navegadores de internet vêm com o RSA preparado para usá-lo em conexões seguras.

Diffie-Hellman - para compartilhar a chave secreta esse algoritmo fornece um método de troca eletrônica. Devido a essas características os protocolos seguros, como *Secure Shell* (SSH), *Internet Protocol Security* (IPsec), *Secure Sockets Layer* (SSL) e *Transport Layer Security* (TLS), utilizam o Diffie-Hellman.

ElGamal - baseia-se na solução de problemas do logaritmo discreto, para assinaturas digitais utiliza o padrão do governo dos EUA. Gratuito.

Criptografia de curva elíptica (ECC - Elliptic Curve Cryptography) - utiliza a estrutura algébrica de curvas elípticas sobre corpos finitos como base do algoritmo. Nos Estados Unidos a ECC para geração de assinatura digital e troca de chave é utilizada pela Agência Nacional de Segurança.

Vamos Praticar

A criptografia é o modo de armazenar e transmitir dados, de forma que somente o destinatário pretendido possa ler ou processá-los. A criptografia moderna usa algoritmos seguros em relação à computação para nos certificar de que criminosos virtuais não possam comprometer facilmente as informações protegidas. A confidencialidade de dados assegura a privacidade para que apenas o destinatário desejado possa ler a mensagem. As partes obtêm a confidencialidade por meio da criptografia. A criptografia é o processo de embaralhamento de dados para impedir

que uma pessoa não autorizada leia os dados com facilidade.

Selecione a alternativa a seguir que indica corretamente o termo usado para descrever a ciência de quebrar códigos secretos.

- a)** Criptografia simétrica.
- b)** Criptologia.
- c)** Criptografia assimétrica.
- d)** Criptoanálise.
- e)** Criptografia.

Segurança na Camada de Transporte

São possíveis diversas técnicas para fornecer segurança na Web. As principais diferenças dessas várias técnicas têm relação com seu escopo de aplicabilidade e local relativo dentro da pilha de protocolos TCP/IP, mas são semelhantes nos serviços oferecidos e, até certo ponto, também nos mecanismos que elas utilizam. Uma solução possível é implementar a segurança logo acima do TCP, conhecida como segurança no nível de transporte, veja o quadro 3.1.

HTTP

FTP

SMTP

SSL ou TLS

TCP

IP

Quadro 3.1 - Segurança no transporte

Fonte: Adaptado de Stallings (2015, p. 412).

Secure Sockets Layer (SSL)

O *Secure Sockets Layer* (SSL) é o serviço de segurança mais usado da Internet.

O SSL é um serviço de uso geral implementado como um conjunto de protocolos que contam com o TCP. Nesse nível, existem duas escolhas de implementação. Para a generalidade total, SSL (ou TLS) poderia ser fornecido como parte do conjunto de protocolos básico e, portanto, ser transparente às aplicações. Como alternativa, SSL pode ser embutido em pacotes específicos. Por exemplo, a maioria dos navegadores vem equipada com SSL, e a maioria dos servidores Web têm implementado o protocolo (STALLINGS, 2015, p. 413).

Arquitetura SSL

Para oferecer um serviço seguro e confiável de ponta a ponta o SSL utiliza duas camadas de protocolo do TCP.

Vários protocolos de camada superior recebem serviços de segurança básicos do protocolo de registro SSL. O HTTP (*Hypertext Transfer Protocol*) em particular, pode operar em cima do SSL oferecendo serviço interativo cliente/servidor WEB. São usados no gerenciamento de trocas e definidos como parte do SSL, três protocolos de camada superior:

- Protocolo de handshake (*Handshake Protocol*);
- Protocolo de especificação de mudança de cifra (*Change Cipher Spec Protocol*); e
- Protocolo de alerta (*Alert Protocol*).

São definidos na especificação dois conceitos importantes do SSL:

Conexão : uma conexão é um transporte que oferece um determinado tipo de serviço. Para SSL, essas conexões são relacionamentos par a par (peer-to-peer). As conexões são transitórias. Cada conexão está associada a uma

sessão.

Sessão : uma sessão SSL é uma associação entre um cliente e um servidor. As sessões são criadas pelo protocolo de handshake. Elas definem um conjunto de parâmetros de segurança criptográficos, que podem ser compartilhados entre múltiplas conexões. As sessões são usadas para evitar a negociação dispendiosa de novos parâmetros de segurança para cada conexão.

Entre qualquer par de partes (aplicações como HTTP no cliente e servidor), pode haver múltiplas conexões seguras. Em teoria, também pode haver múltiplas sessões simultâneas entre as partes, mas esse recurso não é usado na prática.

Existem diversos estados associados a cada sessão. Existe um estado operacional atual para leitura e escrita (ou seja, recepção e envio), quando uma sessão é estabelecida. São criados estados de leitura e escrita pendentes durante o protocolo de handshake. Na conclusão bem-sucedida do protocolo de handshake, os estados pendentes se tornam os atuais.

Um estado de sessão é definido pelos seguintes parâmetros:

Identificador de sessão : uma sequência de byte arbitrária, escolhida pelo servidor para identificar o estado de uma sessão ativa ou retomável.

Certificado do par : um certificado X509.v3 do par. Esse elemento do estado pode ser nulo.

Método de compactação : o algoritmo usado para compactar dados antes da encriptação.

Especificação de cifra : especifica o algoritmo de encriptação de dados em massa (como null, AES etc.) e um algoritmo de hash (como MD5 ou SHA-1) usado para o cálculo do MAC. Ela também define os atributos criptográficos, como hash_size.

Segredo mestre : segredo de 48 bytes compartilhado entre o cliente e o servidor.

É retomável : um flag indicando se a sessão pode ser usada para iniciar novas conexões.

Um estado de conexão é definido pelos parâmetros a seguir.

Aleatórios do servidor e cliente : sequências de bytes que são escolhidas pelo servidor e cliente para cada conexão.

Segredo MAC de escrita do servidor : a chave secreta usada nas operações MAC sobre dados enviados pelo servidor.

Segredo MAC de escrita do cliente : a chave secreta usada em operações MAC sobre dados enviados pelo cliente.

Chave de escrita do servidor : a chave de encriptação secreta para dados encriptados pelo servidor e decriptados pelo cliente.

Chave de escrita do cliente : a chave de encriptação simétrica para dados encriptados pelo cliente e decriptados pelo servidor.

Vetores de inicialização : quando uma cifra em bloco no modo CBC é usada, um vetor de inicialização (IV) é mantido para cada chave. Esse campo é primeiro inicializado pelo protocolo de handshake do SSL. Depois disso, o bloco de texto cifrado final de cada registro é preservado para uso como o IV com o registro seguinte.

Números de sequência : cada parte mantém números de sequência separados para mensagens transmitidas e recebidas para cada conexão. Quando uma parte envia ou recebe uma mensagem de especificação de mudança de cifra o número de sequência apropriado é definido como zero. Números de sequência não podem exceder 264 – 1.

Dois serviços para conexão SSL são oferecidos pelo **protocolo de registro SSL** :

Confidencialidade : Uma chave secreta compartilhada é definida pelo protocolo de handshake, esta chave é usada para encriptação convencional de payloads SSL.

Integridade de mensagem : é usada uma chave secreta compartilhada também definida no protocolo de handshake para formar um código de autenticação de mensagem (MAC, do acrônimo em inglês para *Message Authentication Code*).

Transport Layer Security (TLS)

Uma iniciativa de padronização do IETF, definido como um *Proposed Internet Standard* na RFC 5246, cujo objetivo é produzir uma versão padrão do SSL para Internet. Vamos apresentar algumas diferenças entre os dois.

Conjuntos de cifras - Existem várias diferenças pequenas entre os conjuntos de cifras disponíveis sob SSLv3 e sob TLS:

Troca de chave : o TLS admite a maioria das técnicas de troca de chave do SSLv3.

Algoritmos de criptografia simétrica : o TLS inclui a maioria dos algoritmos de criptografia simétrica encontrados no SSLv3.

Preenchimento - No SSL, o preenchimento acrescentado antes da encriptação de dados do usuário é a quantidade mínima exigida para que o tamanho total dos dados a serem encriptados seja um múltiplo do tamanho de bloco da cifra. No TLS, o preenchimento pode ser qualquer quantidade que resulte em um total que seja um múltiplo do tamanho de bloco da cifra, até um máximo de 255 bytes. Por exemplo, se o texto claro (ou texto compactado, se a compactação for usada) mais MAC mais byte do tamanho do preenchimento tiver 79 bytes de extensão, então o tamanho do preenchimento, em bytes, pode ser 1, 9, 17 e assim por diante, até 249. Um tamanho de preenchimento variável pode ser usado para frustrar ataques com base em uma análise dos tamanhos das mensagens trocadas.

praticar

Vamos Praticar

O *Secure Sockets Layer* (SSL) certamente é o serviço de segurança mais usado da Internet atualmente. Isso se deve à possibilidade de o protocolo HTTP (*Hypertext Transfer Protocol* - Protocolo de Transferência de Hipertexto), protocolo de comunicação utilizado para sistemas de informação de hipermídia, que oferece o serviço de transferência para interação cliente/servidor Web, poder operar em cima do SSL.

Selecione a alternativa a seguir que indica corretamente os parâmetros que definem o estado de sessão SSL.

- a)** Identificador de sessão, Segredo mestre e Vetores de inicialização.
- b)** Números de sequência, Segredo mestre e Especificação de cifra.
- c)** Identificador de sessão, Vetores de inicialização e Números de sequência.
- d)** Identificador de sessão, Segredo mestre e Especificação de cifra.
- e)** Vetores de inicialização, Certificado do par e Números de sequência.



Segurança IP



Em 1994, o Internet Architecture Board (IAB) emitiu um relatório intitulado “Security in the Internet Architecture” — Segurança na Arquitetura da Internet — (RFC 1636). O relatório identificava as principais áreas para mecanismos de segurança. Entre estas estavam a necessidade de proteger a infraestrutura de rede contra monitoração e controle de tráfego da rede sem autorização e a necessidade de proteger o tráfego de usuário final para usuário final usando mecanismos de autenticação e encriptação (STALLINGS, 2015, p. 494).

Uma forma da organização garantir uma rede segura para sua aplicação, incluindo as que ignoram a segurança, é implementando a segurança no nível de IP.

Três áreas funcionais são compreendidas na segurança IP: autenticação, confidencialidade e gerenciamento de chaves. A garantia, pelo mecanismo de autenticação, que um pacote recebido foi transmitido por quem está identificado no pacote, garante também que o pacote não foi alterado em trânsito. As mensagens encriptadas impedem a análise de terceiros

garantindo confidencialidade. A funcionalidade de gerenciamento de chaves trata da troca segura de chaves.

Visando oferecer segurança, o IAB incluiu autenticação e encriptação como recursos de segurança necessários no IPv6. Houve uma preocupação no projeto para que essas capacidades de segurança pudessem ser usadas no IPv4 atual e no IPv6 futuro. Dessa forma muitos fornecedores podem começar a oferecer esses recursos de segurança agora, tendo uma integração com necessidade futura, adicionando a capacidade IPsec em seus produtos. A especificação IPsec agora existe como um conjunto de padrões da Internet.

Aplicações do IPsec

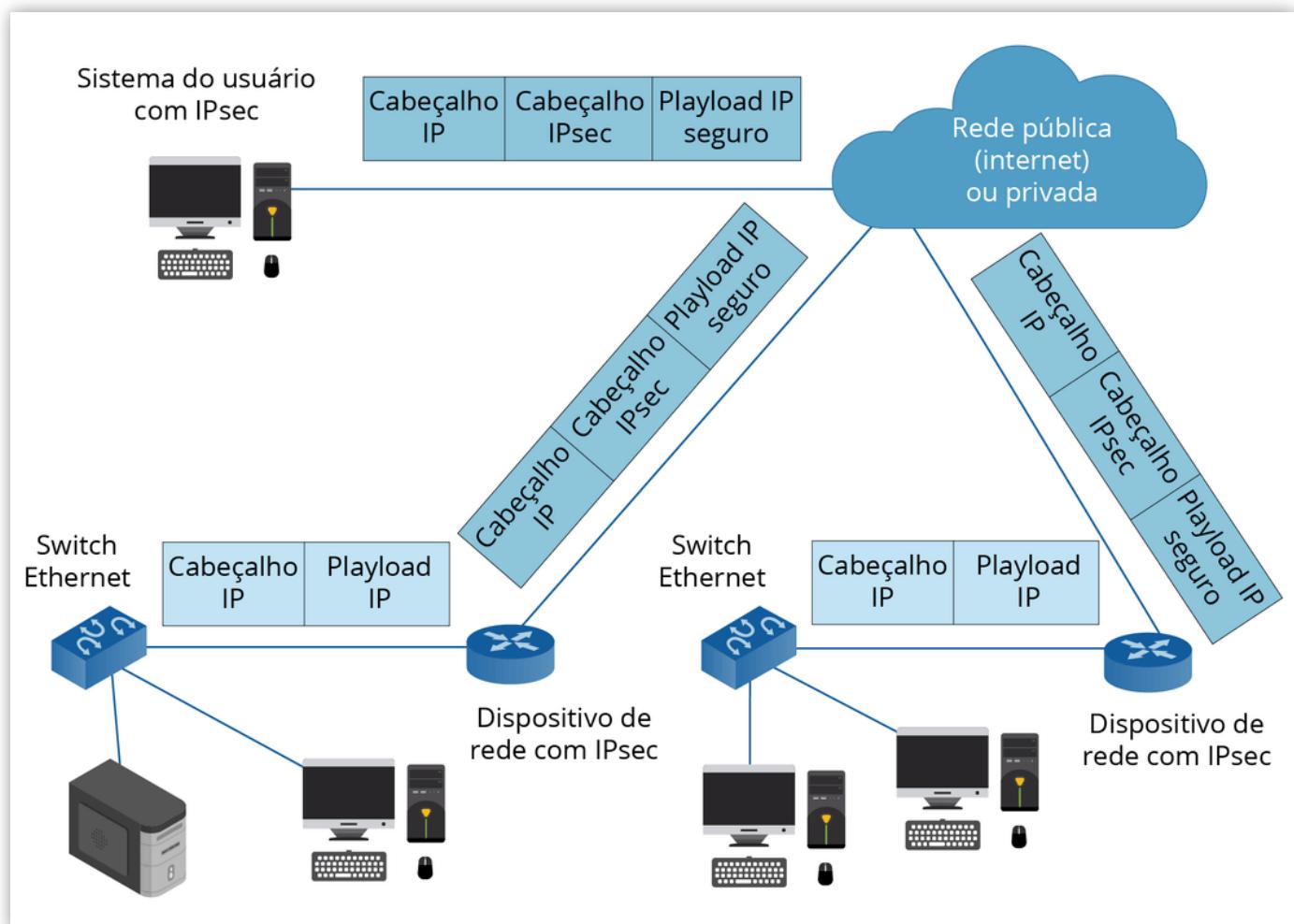
O IPsec foi criado para dar segurança na camada de rede oferecendo a capacidade de proteção em comunicações feitas por uma LAN, por WANs privadas ou públicas e também através da Internet. Vejamos alguns exemplos de uso do IPsec:

- **Conectividade segura do escritório pela Internet** : para uma empresa se conectar a escritórios remotos através da infraestrutura da internet e não mais precisando contratar redes privadas, desta forma economizando custos e overhead de gerenciamento de rede. Para isso basta montar uma VPN (rede privada virtual) segura pela internet ou por uma WAN pública.
- **Acesso remoto seguro pela Internet** : um usuário final cujo sistema é equipado com protocolos IPsec utiliza um acesso à internet qualquer e obtém acesso seguro à rede de uma empresa. Isso facilita a execução dos serviços dos funcionários que trabalham viajando.
- **Estabelecimento de conectividade de extranet e intranet com parceiros** : IPsec pode ser usado para proteger a comunicação com outras organizações, garantindo a autenticação e a confidencialidade, e fornecendo um mecanismo de troca de chave.
- **Melhoria da segurança do comércio eletrônico** : apesar de aplicações de comércio na Web e eletrônico possuírem protocolos de segurança embutidos, o uso do IPsec incrementa mais segurança a comunicação. IPsec acrescenta uma camada de segurança adicional à

que é fornecida na camada de aplicação, garantindo que todo o tráfego designado pelo administrador da rede seja encriptado e autenticado.

-

O IPsec pode encriptar e/ou autenticar todo o tráfego no nível IP, esse recurso permite a ele dar suporte a aplicações variadas. Assim, todas as aplicações distribuídas podem ser protegidas, incluindo logon remoto, cliente/servidor, e-mail, transferência de arquivos, acesso à Web entre outros. A Figura 3.3 apresenta um cenário típico do uso do IPsec.



*Figura 3.3 - Cenário IPsec
Fonte: Stallings (2015, p. 495).*

Benefícios do IPsec

- Quando o IPsec é implementado em um firewall ou roteador, ele

oferece segurança forte, que pode ser aplicada a todo o tráfego cruzando o perímetro. O tráfego dentro de uma empresa ou grupo de trabalho não gera o overhead do processamento relacionado à segurança.

- IPsec em um firewall é resistente ao bypass se todo o tráfego vindo de fora tiver que usar IP, e o firewall é o único meio de entrada da Internet para a organização.
- IPsec está abaixo da camada de transporte (TCP, UDP) e por isso é transparente às aplicações. Não há necessidade de mudar o software em um sistema do usuário ou servidor quando o IPsec é implementado no firewall ou roteador. Mesmo que o IPsec seja implementado nos sistemas finais, o software da camada superior, incluindo as aplicações, não é afetado.
- IPsec pode ser transparente aos usuários finais. Não há necessidade de treinar usuários sobre mecanismos de segurança, emitir material de chave para cada usuário, ou revogar material de chave quando os usuários saem da organização.
- IPsec pode oferecer segurança para usuários individuais, se for necessário. Isso é útil para trabalhadores externos e para configurar uma sub-rede virtual segura dentro de uma organização, para aplicações sensíveis.

Serviços ipsec

O IPsec oferece serviços de segurança na camada IP permitindo que um sistema selecione protocolos de segurança exigidos, determine o(s) algoritmo(s) a usar para o(s) serviço(s) e disponha quaisquer chaves criptográficas exigidas para oferecer os serviços solicitados. Dois protocolos são usados para oferecer segurança: um de autenticação designado pelo cabeçalho do protocolo, *Authentication Header* (AH); e um combinado de encriptação/autenticação, designado pelo formato do pacote para esse protocolo, *Encapsulating Security Payload* (ESP). São serviços do IPsec:

- **Controle de acesso;**
- **Integridade sem conexão;**
- **Autenticação da origem de dados;**

- **Rejeição de pacotes replicados;**
- **Confidencialidade;**
- **Confidencialidade limitada de fluxo de tráfego.**

Saiba mais

Saiba mais

A RFC a seguir descreve a Arquitetura para IPsec, projetado para fornecer serviços de segurança para tráfego na camada IP. Nela estão especificados as definições e o escopo do IPSEC. Também esclarece como o IPsec constrói o túnel de comunicação, indicando os serviços para sua aplicação. Para saber mais, acesse o link disponível.

Fonte: Elaborado pelo autor.

[ACESSAR](#)

O protocolo IPSec fornecido atualmente é o protocolo que melhor atende ao mercado quando imaginamos proteção do tráfego e rede IP. Sua adoção não se restringe à criação dos VPNs, ele está preparado para proteção de todo o ambiente que está exposto.

praticar

Vamos Praticar

O IPsec é a segurança na camada de rede, ele fornece a capacidade de proteger

comunicações feitas pela Internet, por WANs privadas ou públicas e também por uma LAN. O recurso que permite o IPsec dar suporte a aplicações variadas é a possibilidade de encriptar e/ou autenticar todo o tráfego no nível IP. Assim, todas as aplicações distribuídas podem ser protegidas. Selecione a alternativa a seguir que indica corretamente exemplos de aplicações do Ipsec.

- a)** Conectividade segura do escritório pela Internet; Estabelecimento de conectividade de extranet e intranet com parceiros; Autenticação entre domínios.
- b)** Conectividade segura do escritório pela Internet; Controle lógico do enlace; Autenticação entre domínios.
- c)** Autenticação entre domínios; Acesso remoto seguro pela Internet; Estabelecimento de conectividade de extranet e intranet com parceiros.
- d)** Conectividade segura do escritório pela Internet; Acesso remoto seguro pela Internet; Estabelecimento de conectividade de extranet e intranet com parceiros.
- e)** Controle lógico do enlace; Acesso remoto seguro pela Internet; Estabelecimento de conectividade de extranet e intranet com parceiros.



Assinaturas Digitais



A assinatura digital é um dos mais importantes desenvolvimentos a partir do trabalho sobre criptografia de chave pública. O conjunto de capacidades de segurança oferecido pela assinatura digital seria difícil de implementar de qualquer outra maneira.

A Figura 3.4 apresenta o modelo genérico do processo de criação e uso de assinaturas digitais.

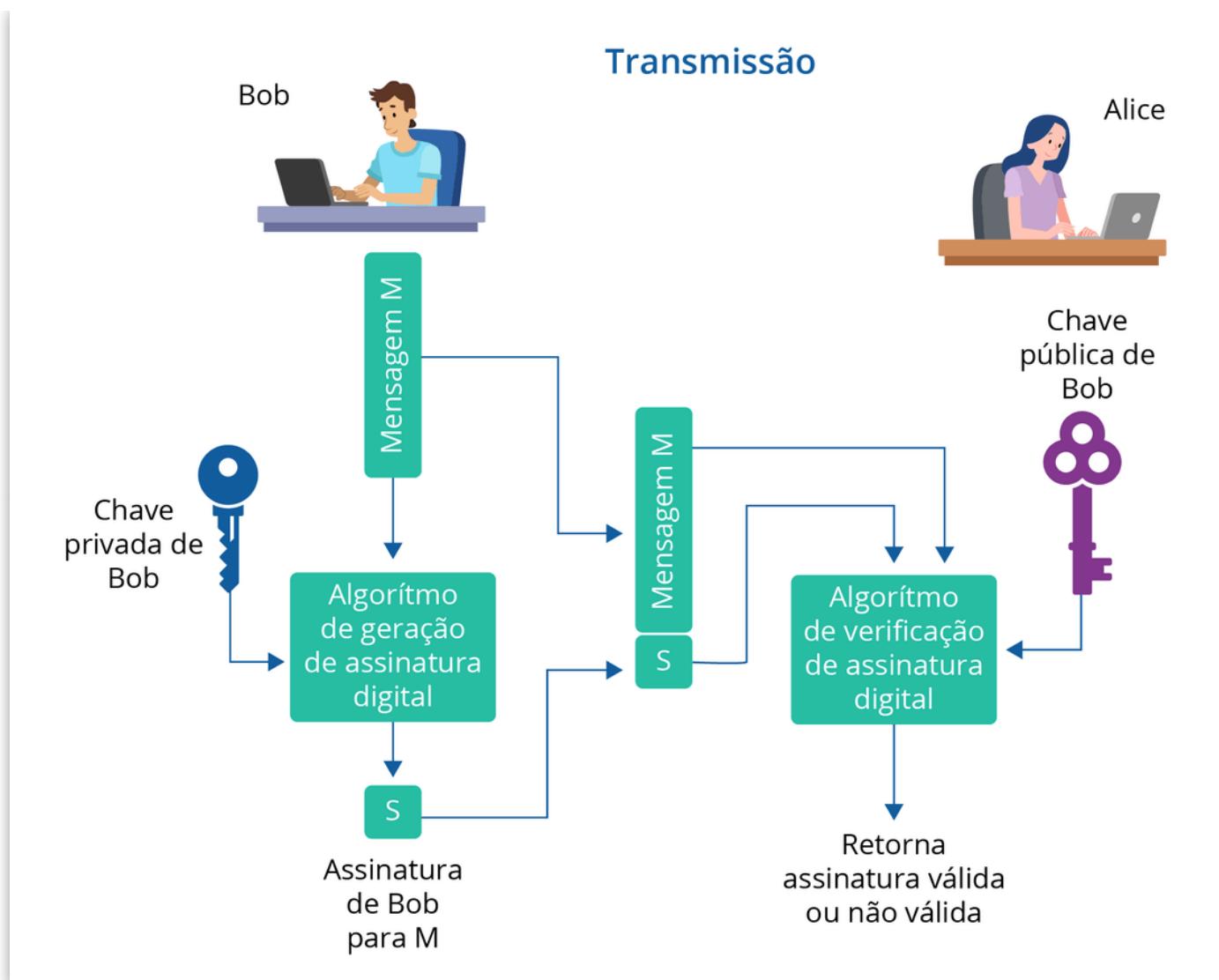


Figura 3.4 - Modelo Genérico de Assinatura Digital

Fonte: Stallings (2015, p. 310).

Propriedades

A autenticação da mensagem protege as duas partes que trocam mensagens contra um terceiro qualquer. Porém, ela não protege as duas partes uma da outra. Várias formas de disputa entre as duas são possíveis.

Por exemplo, suponha que um usuário A envie uma mensagem autenticada ao usuário B. Considere as seguintes disputas que poderiam surgir:

1. Usuário B pode forjar uma mensagem diferente e reivindicar que ela veio de A. Ele simplesmente teria que criar uma mensagem e anexar um código de autenticação usando a chave que eles compartilham.
2. Usuário A pode negar o envio da mensagem. Como é possível que B

falsifique uma mensagem, não há como provar que ele realmente a enviou.

É necessário algo mais do que a autenticação quando não existe confiança completa entre emissor e receptor. A solução para esse problema é a assinatura digital. As seguintes características são necessárias na assinatura digital:

- verificar o autor e a data e hora da assinatura;
- autenticar o conteúdo no momento da assinatura;
- ser verificável por terceiros, para resolver disputas.

Assim, a função de assinatura digital inclui a função de autenticação, veja a Figura 3.5, ela apresenta a essência do mecanismo de assinatura digital em termos simplificados.

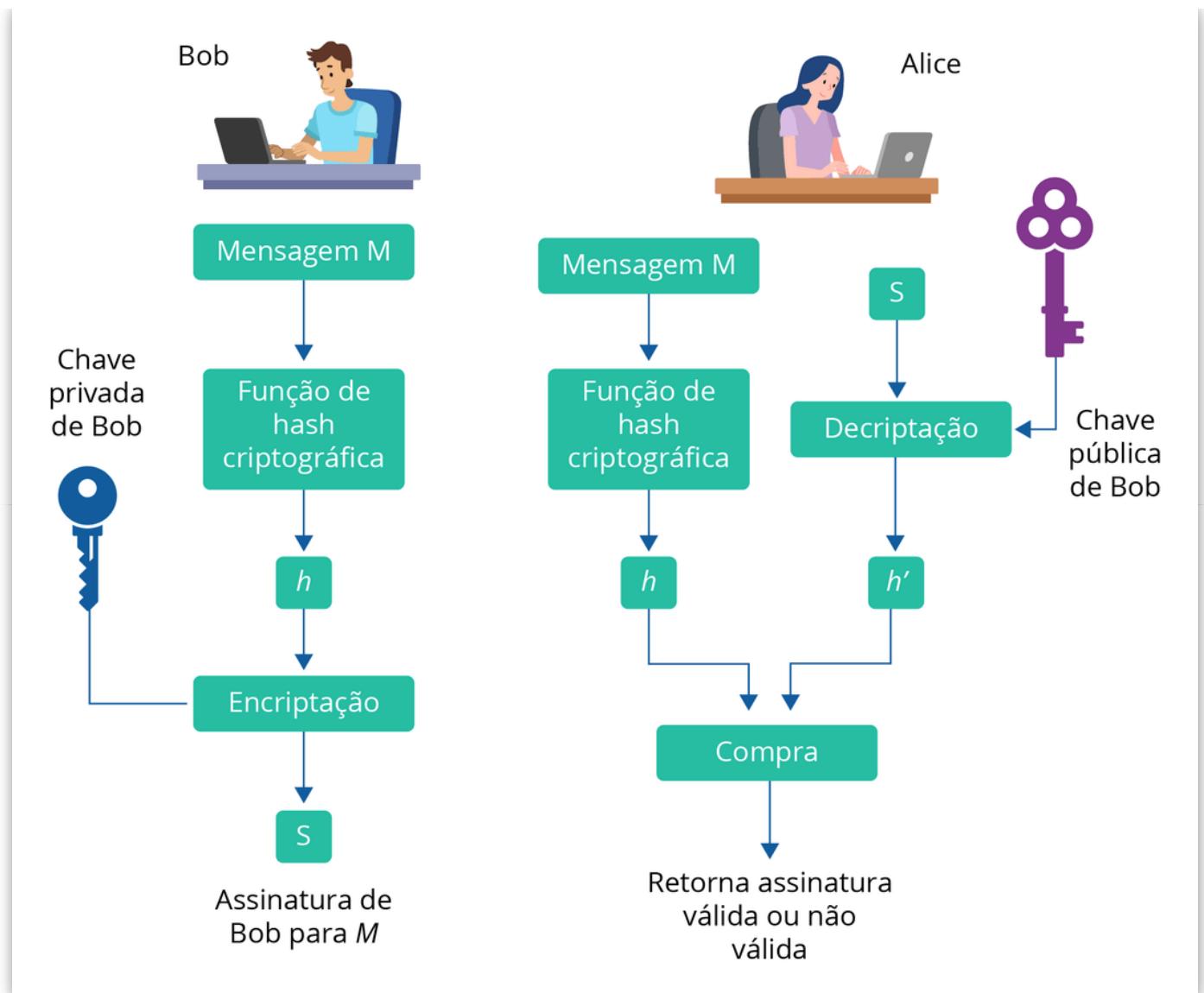


Figura 3.5 - Representação simplificada do processo de assinatura digital
Fonte: Stallings (2015, p. 311).

Ataques e Falsificações

Abaixo está uma lista com tipos de ataques em ordem crescente de severidade, retiradas de Gold (1988 apud STALLINGS, 2015). Onde A indica o usuário cujo método de assinatura está sendo atacado, e C indica o atacante.

- Ataque somente de chave: C só conhece a chave pública de A;
- Ataque de mensagem conhecida: C recebe acesso a um conjunto de mensagens e suas assinaturas;
- Ataque de mensagem escolhida genérica: C escolhe uma lista de mensagens antes de tentar quebrar o esquema de assinatura de A, independente da chave pública de A. C, então, obtém de A

assinaturas válidas para as mensagens escolhidas. O ataque é genérico, pois não depende da chave pública de A; o mesmo ataque é usado contra todos;

- Ataque de mensagem escolhida direcionada: semelhante ao ataque genérico, exceto que a lista de mensagens a serem assinadas é escolhida depois que C conhece a chave pública de A, mas antes que quaisquer assinaturas sejam vistas;
- Ataque de mensagem escolhida adaptativa: C tem permissão para usar A como um “oráculo”. Isso significa que C pode solicitar de A assinaturas de mensagens que dependam de pares mensagem-assinatura previamente obtidos.

Gold (1988 apud STALLINGS, 2015) define então o sucesso na quebra de um esquema de assinatura como resultado em que C pode fazer qualquer uma das seguintes ações, com uma probabilidade não insignificante:

- Quebra total: C determina a chave privada de A;
- Falsificação universal: C encontra um algoritmo de assinatura eficiente que oferece um modo equivalente de construção de assinaturas sobre mensagens arbitrárias;
- Falsificação seletiva: C forja uma assinatura para determinada mensagem escolhida por C;
- Falsificação existencial: C forja uma assinatura para pelo menos uma mensagem. C não tem controle sobre a mensagem. Consequentemente, essa falsificação pode ser somente um pequeno incômodo para A.

Requisitos de assinatura digital

Com base nessas propriedades e ataques discutidos, Stallings (2015) formula os seguintes requisitos para uma assinatura digital:

- A assinatura precisa ser um padrão de bits que depende da mensagem sendo assinada;
- A assinatura precisa usar alguma informação exclusiva do emissor, para impedir falsificação e negação;

- É preciso ser relativamente fácil produzir a assinatura digital;
- É preciso ser relativamente fácil reconhecer e verificar a assinatura digital;
- É preciso ser computacionalmente inviável falsificar uma assinatura digital, seja construindo uma nova mensagem para uma assinatura digital existente ou uma assinatura digital fraudulenta para determinada mensagem;
- É preciso ser prático reter uma cópia da assinatura digital em termos de armazenamento.

Uma função de hash segura, embutida em um esquema como o da Figura 3.5, oferece uma base para satisfazer esses requisitos. Porém, deve-se ter cuidado no projeto dos detalhes do esquema.

praticar

Vamos Praticar

A assinatura digital é um dos mais importantes desenvolvimentos a partir do trabalho sobre criptografia de chave pública. O conjunto de capacidades de segurança oferecido pela assinatura digital seria difícil de implementar de qualquer outra maneira. A autenticação da mensagem protege as duas partes que trocam mensagens contra um terceiro qualquer. Porém, ela não protege as duas partes uma da outra. É necessário algo mais do que a autenticação quando não existe confiança completa entre emissor e receptor. A solução para esse problema é a assinatura digital.

As afirmações abaixo se referem às características necessárias na assinatura digital:

I. verificar o autor e a data e hora da assinatura.

II. controlar acesso.

III. autenticar o conteúdo no momento da assinatura.

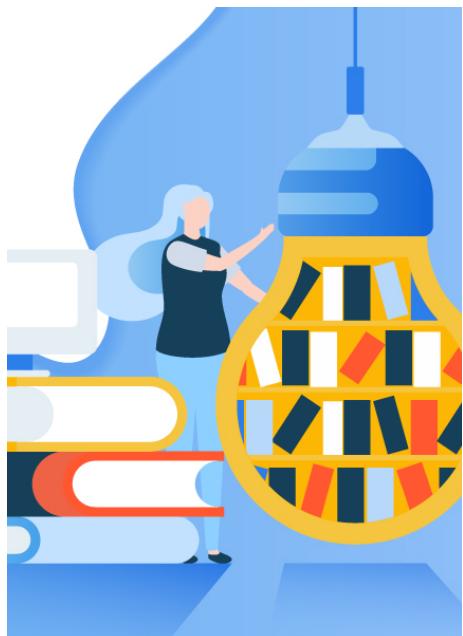
IV. ser verificável por terceiros.

Selecione a alternativa abaixo a que indica corretamente as características necessárias na assinatura digital:

- a)** II, III e IV, apenas.
- b)** I, II e III, apenas.
- c)** I, II e IV, apenas
- d)** I, III e IV, apenas.
- e)** I, II, III e IV.E.

indicações

Material Complementar



LIVRO

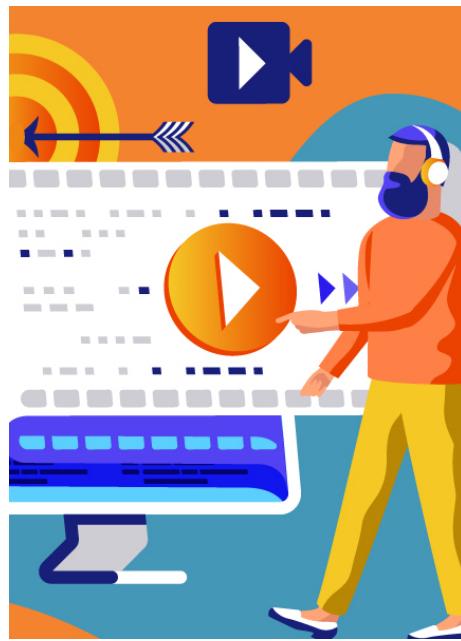
Blockchain para negócios: Promessa, prática e aplicação da nova tecnologia da Internet

William Mougayar

Editora: Alta Books

ISBN: 9788583937890

Comentário: Descreve os possíveis avanços do blockchain no mercado e suas aplicações, descrevendo a importância e aplicação das criptografias no modelo usado pelo blockchain.



FILME

O Jogo da Imitação

Ano: 2015

Comentário: Alan Turing é um matemático apaixonado por criptografia que, durante a segunda guerra, inventa uma máquina para decifrar a criptografia das mensagens alemãs feitas na máquina enigma, até então tida como indecifrável, o que provoca uma mudança no panorama da disputa.

Para conhecer mais sobre o filme, acesse o trailer disponível.

TRAILER

conclusão

Conclusão

Aprendemos nesta unidade quais são os elementos necessários para fazermos o processo de criptografia e a necessidade, a importância das chaves criptográficas e como fazer seu gerenciamento, analisando especificamente os modelos de criptografia simétricos e assimétricos e seus respectivos algoritmos. Entendemos como aplicar esses conceitos criptográficos nas comunicações, aplicando segurança em várias camadas da pilha de protocolos TCP/IP: O SSL aplicado na camada de transporte criptografando as sessões ou conexões. O IPsec implementando segurança na camada Internet, possibilitando a comunicação segura entre redes, sua aplicação em acessos remotos entre redes da organização (como escritórios geograficamente distribuídos), diretamente com o cliente remoto (VPN client para colaboradores em viagem ou *home office*) ou até mesmo um canal seguro com redes locais de parceiros comerciais. Entendemos o processo das assinaturas digitais que implementam autenticidade e não repúdio em documento e mensagens.

referências

Referências

Bibliográficas

KIM, D.; SOLOMON, M. G. **Fundamentos de Segurança de Sistemas de Informação**. Rio de Janeiro: LTC, 2014.

HINTZBERGEN, J. *et al* . **Fundamentos de Segurança da Informação** : com base na ISO 27001 e na ISO 27002. 3. ed. São Paulo: Brasport, 2015.

RFC 4301 - **Security Architecture for the Internet Protocol** . 2005. Disponível em: <https://tools.ietf.org/html/rfc4301>. Acesso em: jan. 2020.

STALLINGS, W. **Criptografia e segurança de redes** : princípios e práticas. 4. ed. São Paulo: Pearson Education do Brasil, 2015.