

Módulo 21: Criptografia



CyberOps Associate v1.0

Prof. Clemilson Oliveira

clemilson.oliveira@edu.sc.senai.br



Objetivos do módulo

Título do módulo: criptografia de chave pública

Objetivo do módulo: Explicar como a infraestrutura de chave pública (PKI) oferece suporte à segurança de rede.

Título do Tópico	Objetivo do Tópico
Integridade e Autenticidade	Explique a função da criptografia para garantir a integridade e autenticidade dos dados.
Confidencialidade	Explicar como as abordagens criptográficas aumentam a confidencialidade dos dados.
Criptografia de chave pública	Explicar a criptografia de chave pública.
Autoridades e o Sistema de Confiança PKI	Explicar como funciona a infraestrutura de chave pública.
Aplicações e impactos da criptografia	Explicar como o uso da criptografia afeta as operações de segurança cibernética.

21.1 Integridade e autenticidade

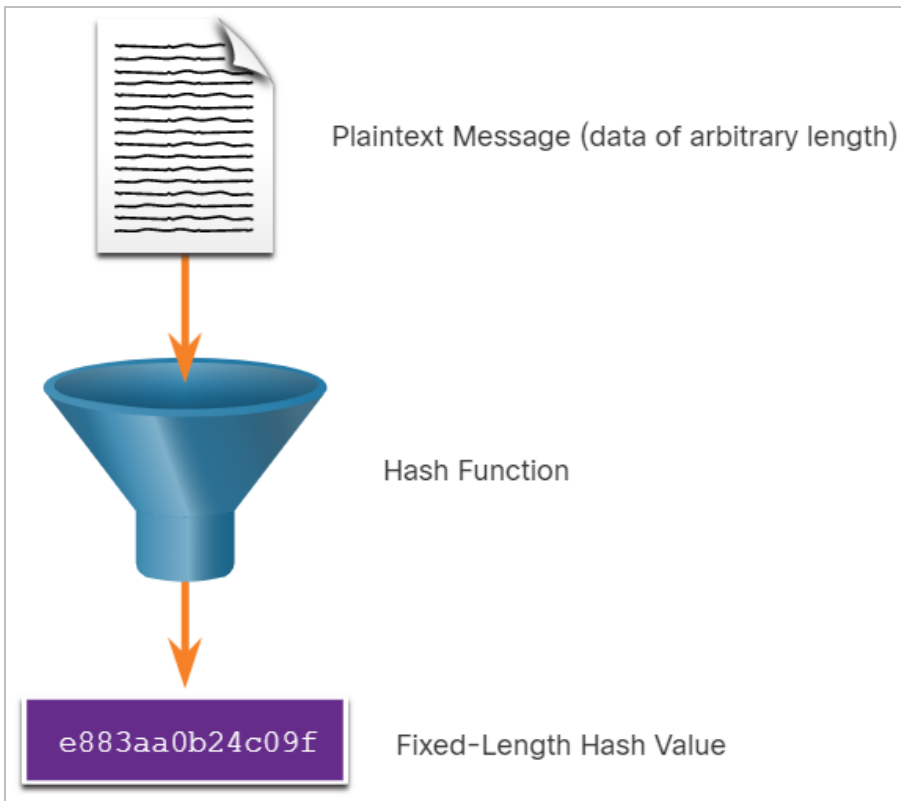
Protegendo Comunicações

Estes são os quatro elementos das comunicações seguras:

- **Integridade dos dados** - Garante que a mensagem não foi alterada. Quaisquer alterações nos dados em trânsito serão detectadas. A integridade é garantida pela implementação de um dos algoritmos Secure Hash (SHA-2 ou SHA-3). O algoritmo MD5 message digest ainda está em uso, mas deve ser evitado, pois é inseguro e cria vulnerabilidades em uma rede.
- **Autenticação de origem** - garante que a mensagem não é uma falsificação e realmente vem de quem é declarada.. Muitas redes modernas garantem autenticação com algoritmos como código de autenticação de mensagem baseado em hash (HMAC).
- **Confidencialidade dos dados** - Garante que apenas usuários autorizados possam ler a mensagem. Se a mensagem for interceptada, ela não poderá ser decifrada dentro de um razoável período de tempo. A confidencialidade dos dados é implementada usando algoritmos de criptografia simétrica e assimétrica.
- **Dados não repudiáveis** - Garante que o remetente não possa repudiar ou refutar a validade de uma mensagem enviada. O não repúdio depende do fato de que apenas o remetente possui as características ou a assinatura exclusivas de como essa mensagem é tratada.

Funções criptográficas de hash de criptografia

- Hashes são usados para verificar e garantir a integridade dos dados.
- O hash é baseado em uma função matemática unilateral que é relativamente fácil de calcular, mas significativamente mais difícil de reverter.
- Como mostrado na figura, uma função hash leva um bloco variável de dados binários, chamado de mensagem, e produz uma representação condensada de comprimento fixo, chamado hash.
- O hash resultante também é às vezes chamado de mensagem digest, digest ou impressão digital.

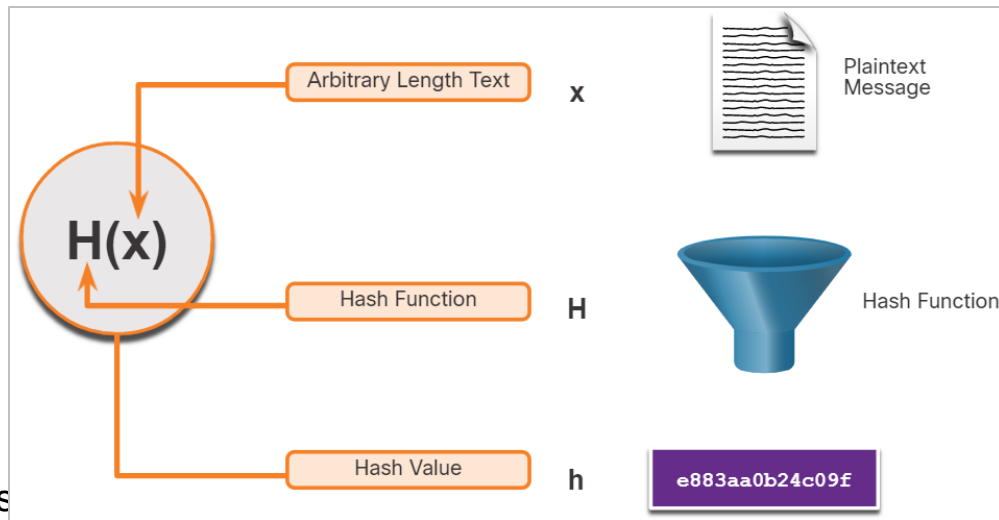


Criptografia Criptográfica Hash Funções (Cont.)

- Com funções hash, é computacionalmente inviável que dois conjuntos diferentes de dados apresentem a mesma saída hash.
- Cada vez que os dados são modificados ou alterados, o valor de hash também muda. Por isso, muitas vezes os valores criptográficos de hash são chamados de impressões digitais.
- Eles podem ser usados para detectar arquivos de dados duplicados, alterações de versão de arquivo e aplicativos semelhantes.
- Esses valores são usados para proteger contra uma alteração acidental ou intencional dos dados ou corrupção acidental dos dados.
- A função hash criptográfico é aplicada em muitas situações diferentes para autenticação de entidade, integridade de dados e fins de autenticidade de dados.

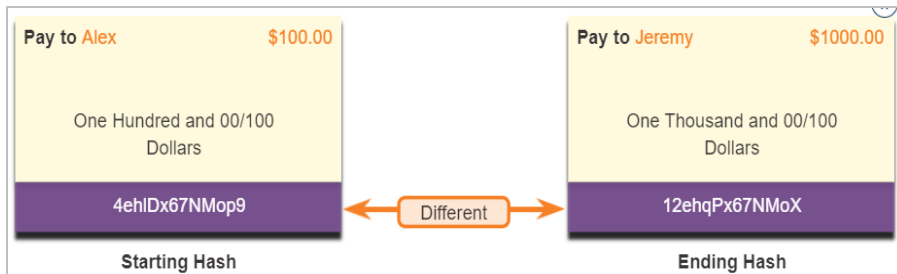
Criptográfica Operação Hash

- Matematicamente, a equação $h=H(x)$ é usada para explicar como um algoritmo de hash opera.
- Como mostrado na figura, uma função hash H leva uma entrada x e retorna um valor hash string de tamanho fixo h .
- Uma função hash criptográfica deve ter as seguintes propriedades:
 - A entrada pode ser de qualquer comprimento.
 - A saída tem um comprimento fixo.
 - $H(x)$ é relativamente fácil de calcular para determinado x .
 - $H(x)$ é um caminho e não reversível.
 - $H(x)$ é livre de colisões, o que significa que dois valores de entrada diferentes resultarão em valores de hash diferentes.
- Se uma função hash é difícil de inverter, ela é considerada um hash unidirecional. Difícil de inverter significa que, dado um valor de hash de h , é computacionalmente inviável encontrar uma entrada para x tal que $H(x)=h$.



MD5 e SHA

- As funções de hash são usadas para garantir a integridade de uma mensagem accidental ou intencionalmente.
- Na figura, o remetente está enviando uma transferência de dinheiro de US \$ 100 para Alex. O remetente deseja garantir que a mensagem não seja alterada no caminho para o destinatário.
- O remetente insere a mensagem em um algoritmo de hash e calcula seu hash de comprimento fixo.
- Esse hash é anexado à mensagem e enviado ao destinatário. A mensagem e o hash estão em texto sem formatação.
- O receptor remove o hash da mensagem e insere a mensagem no mesmo algoritmo de hash. Se este hash for igual ao anexado à mensagem, a mensagem não foi alterada em trânsito. Se os hashes não forem iguais a integridade da mensagem não será mais confiável.



MD5 e SHA (Condd.)

Existem quatro funções hash bem conhecidas:

- **MD5 com resumo de 128 bits**- Desenvolvido por Ron Rivest e usado em muitos aplicativos da Internet, MD5 é uma função unilateral que produz uma mensagem hash de 128 bits. MD5 é um algoritmo legado e usado somente quando nenhuma alternativa melhor está disponível. Recomenda-se que SHA-2 ou SHA-3 sejam usados em vez disso.
- **SHA-1** - Desenvolvido pela Agência de Segurança Nacional dos EUA (NSA) em 1995. É muito semelhante às funções hash MD5. O SHA-1 cria uma mensagem de 160 bits e é um pouco mais lento que o MD5. O SHA-1 possui falhas conhecidas e é um algoritmo antigo.
- **SHA-2** - Desenvolvido pela NSA. Ele inclui SHA-224, SHA-256, SHA-384 e SHA-512. Se estiver usando SHA-2, os algoritmos SHA-256, SHA-384 e SHA-512 devem ser usados.
- **SHA-3** - SHA-3 é o mais novo algoritmo de hash e foi introduzido pelo NIST como uma alternativa para a família SHA-2 de algoritmos de hash. O SHA-3 inclui SHA3-224, SHA3-256, SHA3-384 e SHA3-512. A família SHA-3 são algoritmos de última geração e devem ser usados sempre que possível.

MD5 e SHA (Condd.)

- Embora o hashing possa ser usado para detectar alterações acidentais, ele não pode ser usado para proteger contra alterações deliberadas feitas por um agente de ameaça.
- Não há informações de identificação única do remetente no procedimento de hash.
- Isso significa que qualquer pessoa pode processar um hash para quaisquer dados, desde que tenha a função hash correta.
- Portanto, hash é vulnerável a ataques man in the middle e não oferece segurança aos dados transmitidos. Para fornecer autenticação de integridade e origem, é necessário algo mais.

Observação: Os algoritmos de hash protegem somente contra alterações acidentais e não protegem os dados contra alterações feitas deliberadamente por um ator de ameaça.

Autenticação de origem de criptografia

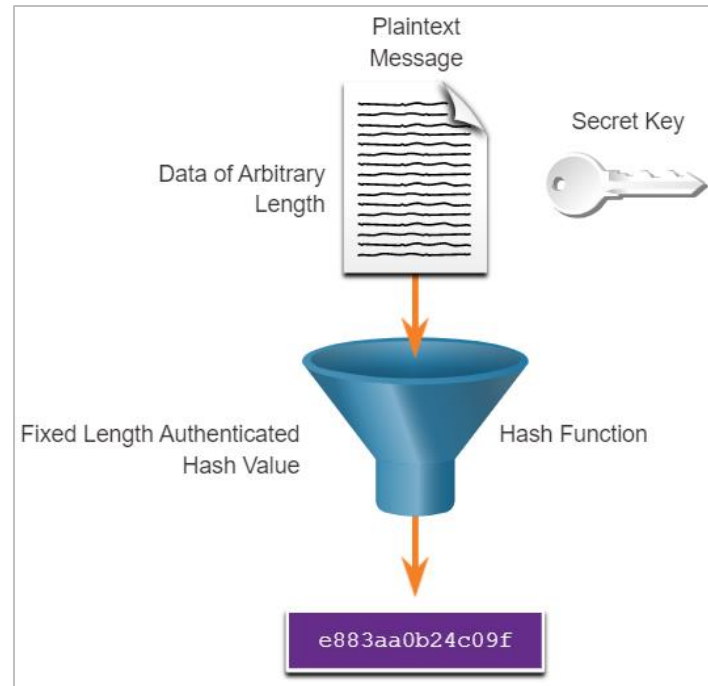
- Para adicionar autenticação de origem e garantia de integridade, use um código de autenticação de mensagem hash com chave (HMAC).
- HMACs usam uma chave secreta adicional como entrada à função hash.

Observação: Outros métodos MAC (Message Authentication Code) também são usados. No entanto, o HMAC é usado em muitos sistemas, incluindo SSL, IPsec e SSH.

Autenticação de origem de criptografia (cont.)

Algoritmo de hash HMAC

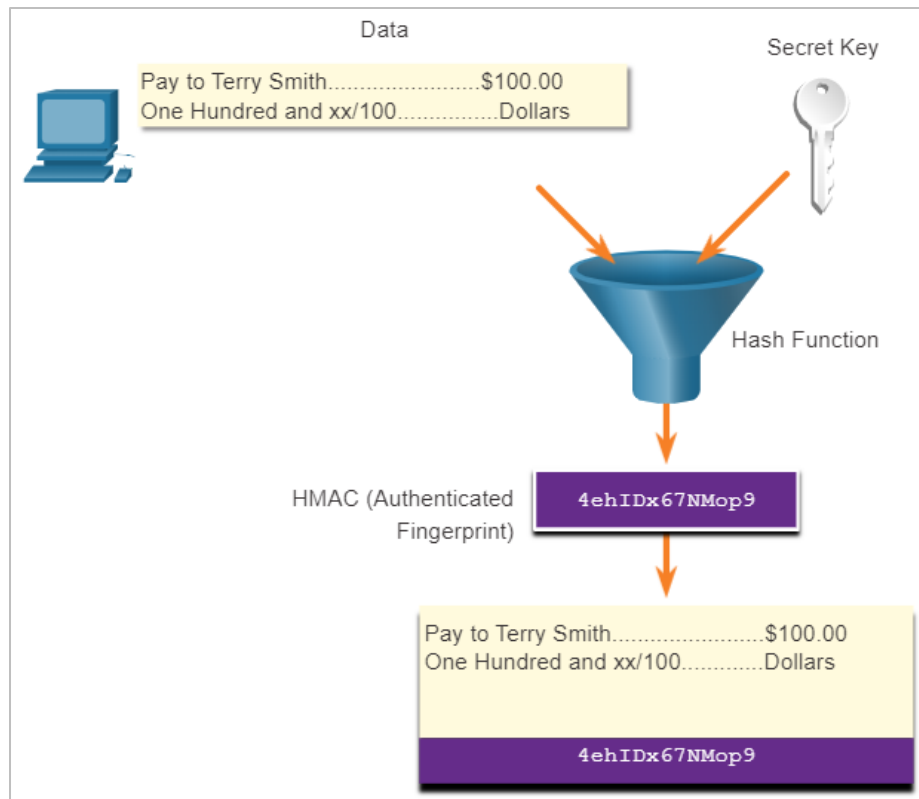
- Conforme mostrado na figura, um HMAC é calculado usando qualquer algoritmo criptográfico que combina uma função hash criptográfica com uma chave secreta. As funções de hash são a base do mecanismo de proteção dos HMACs.
- Apenas o remetente e o receptor conhecem a chave secreta, e a saída da função hash depende dos dados de entrada e da chave secreta. Isso derrota os ataques man-in-the-middle e fornece autenticação da origem dos dados.
- Se duas partes compartilharem uma chave secreta e usarem as funções HMAC para autenticação, uma mensagem HMAC adequadamente construída, a parte recebeu indica que a outra parte foi a originadora da mensagem. Isso ocorre porque a outra parte possui a chave secreta.



Autenticação de origem de criptografia (cont.)

Criação do valor de HMAC

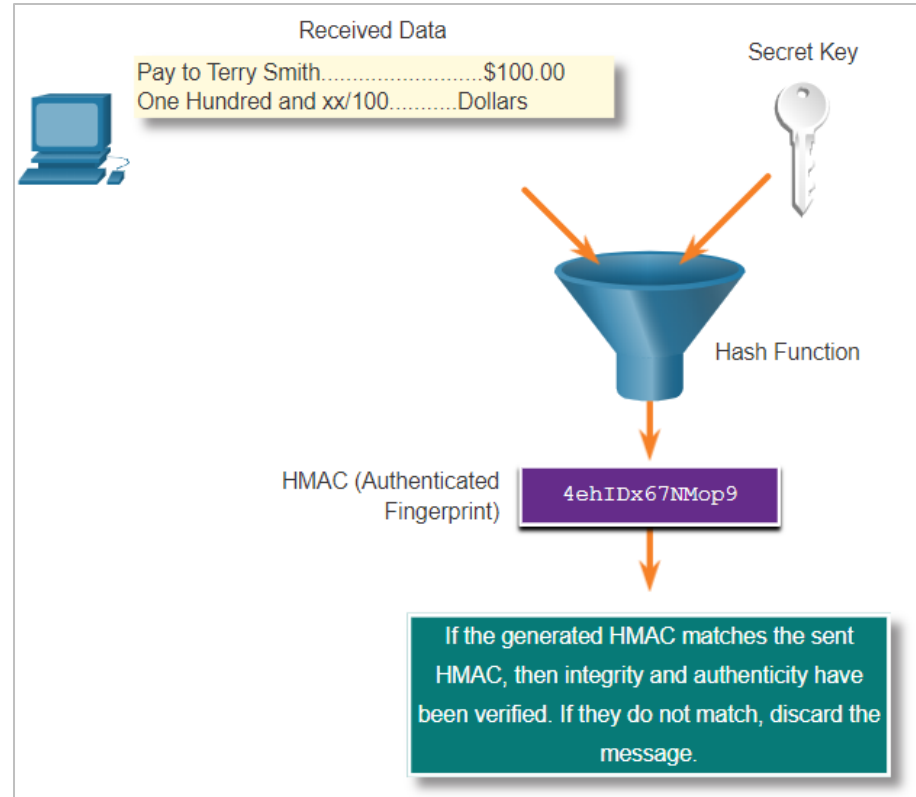
- Conforme mostrado na figura, o dispositivo de envio insere dados no algoritmo de hashing e calcula o resumo HMAC de comprimento fixo.
- Esse Digest autenticado é anexado à mensagem e enviado ao destinatário.



Autenticação de origem de criptografia (cont.)

Verificação do valor de HMAC

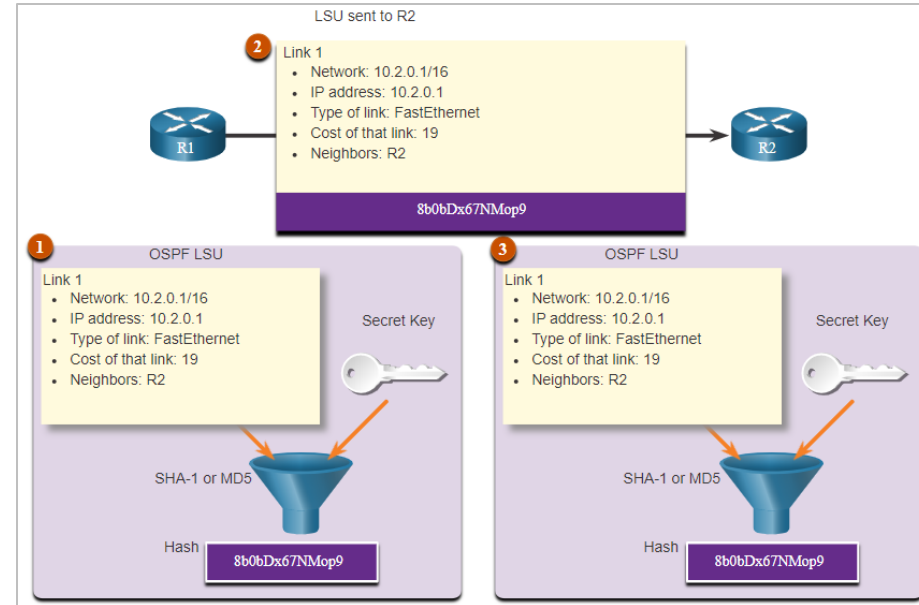
- Na figura, o dispositivo receptor remove o Digest da mensagem e usa a mensagem de texto sem formatação com sua chave secreta como entrada na mesma função de hash.
- Se o Digest calculado pelo dispositivo receptor for igual ao resumo enviado, a mensagem não foi alterada.
- Adicionalmente, a origem da mensagem é autenticada porque apenas o remetente possui uma cópia da chave secreta compartilhada. A função HMAC garantiu a autenticidade da mensagem.



Autenticação de origem de criptografia (cont.)

Exemplo Cisco Router HMAC

- Na figura, os HMACs são usados por roteadores Cisco configurados para usar a autenticação de roteamento Open Shortest Path First (OSPF).
- R1 está enviando uma atualização de estado do link (LSU) referente a uma rota para a rede 10.2.0.0/16:
- R1 calcula o valor do hash usando a mensagem LSU e a chave secreta.
- O valor do hash resultante é enviado com o LSU para o R2.
- R2 calcula o valor do hash usando o LSU e sua chave secreta. R2 aceita a atualização se os valores de hash corresponderem. Se eles não corresponderem, o R2 descartará a atualização.



Laboratório de Criptografia — Hashing Things Out

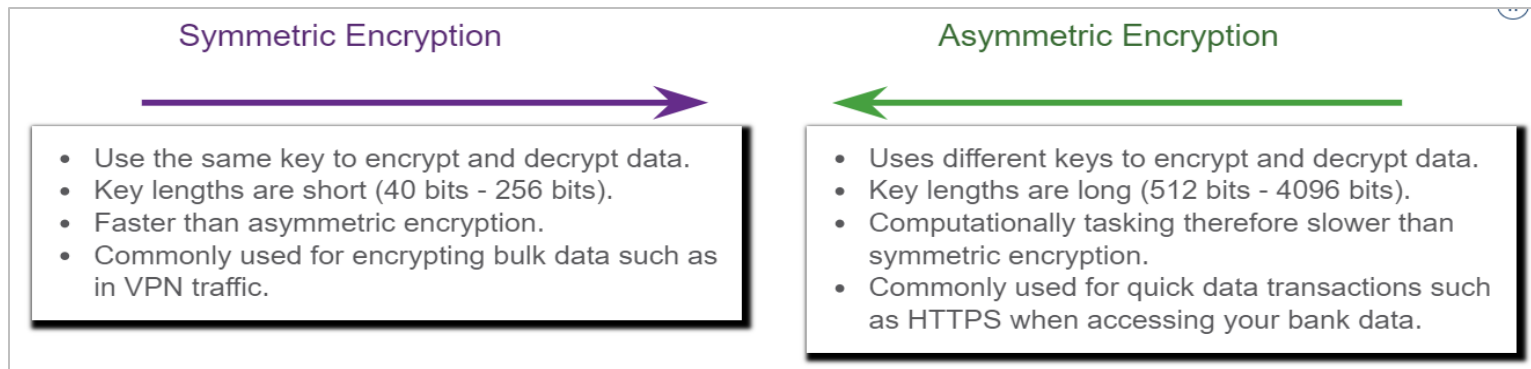
Neste laboratório, você completará os seguintes objetivos:

- Criando hashes com OpenSSL
- Verificando Hashhes

21.2 Confidencialidade

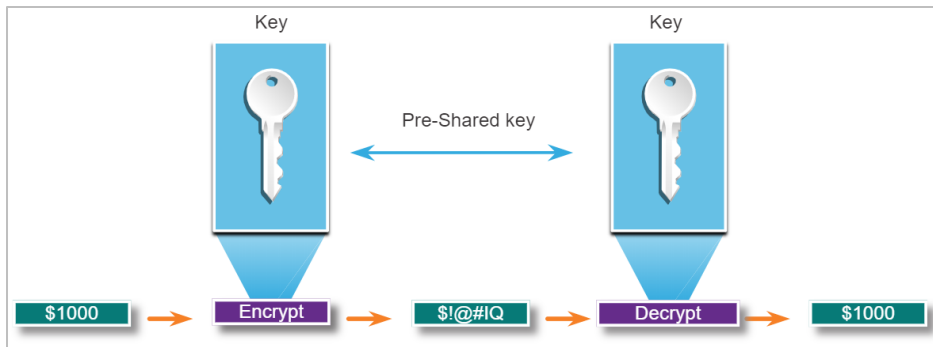
Confidencialidade dos dados

- Existem duas classes de criptografia usadas para fornecer confidencialidade de dados; assimétrico e simétrico. Essas duas classes diferem na maneira como usam as chaves.
- Algoritmos de criptografia simétrica, como Data Encryption Standard (DES), 3DES e Advanced Encryption Standard (AES), baseiam-se na premissa de que cada parte que se comunica conhece a chave pré-compartilhada.
- A confidencialidade dos dados também pode ser garantida usando algoritmos assimétricos, incluindo Rivest, Shamir e Adleman (RSA) e a infraestrutura de chave pública (PKI).
- A figura destaca algumas diferenças entre criptografia simétrica e assimétrica.



Criptografia simétrica de confidencialidade

- Os algoritmos simétricos usam a mesma chave pré-compartilhada para criptografar e descriptografar dados.
- Uma chave pré-compartilhada, também chamada de chave secreta, é conhecida pelo remetente e pelo receptor antes que qualquer comunicação criptografada possa ocorrer.
- Considere um exemplo de criptografia simétrica em que Alice e Bob desejam trocar mensagens secretas um com o outro por meio do sistema de correio.
- Na figura, Alice e Bob têm chaves idênticas e pré-compartilhadas. Alice escreve uma mensagem secreta e a coloca em uma pequena caixa e a tranca usando sua chave. Ela manda a caixa para Bob. Quando Bob recebe a caixa, ele usa sua chave para desbloquear e recuperar a mensagem. Bob pode usar a mesma caixa e chave para enviar uma resposta secreta de volta para Alice.



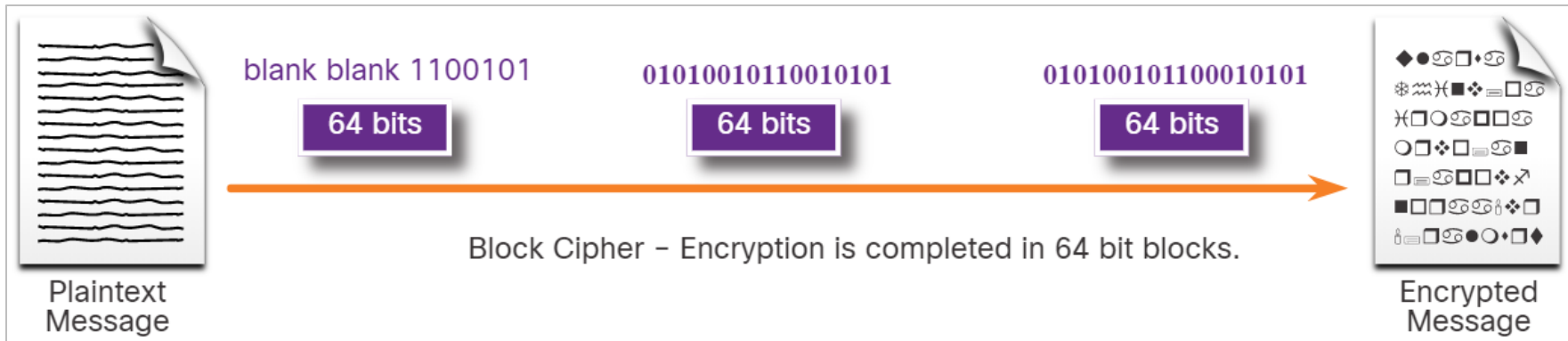
Criptografia simétrica de confidencialidade (Condd.)

- Os algoritmos de criptografia simétricos são comumente usados com tráfego VPN.
- Isso ocorre porque os algoritmos simétricos usam menos recursos da CPU do que os algoritmos de criptografia assimétrica.
- Isso permite que a criptografia e a descriptografia de dados sejam rápidas ao usar uma VPN.
- Ao usar algoritmos de criptografia simétrica, quanto maior a chave, mais tempo levará para alguém descobrir a chave. A maioria das chaves de criptografia tem entre 112 e 256 bits.
- Para garantir que a criptografia é segura, um comprimento mínimo de chave de 128 bits deve ser usado. Use uma chave mais longa para comunicações mais seguras.
- Algoritmos de criptografia simétrica às vezes são classificados como uma cifra de bloco ou uma cifra de fluxo.

Criptografiasimétrica de confidencialidade (Cont.)

Cifras de blocos

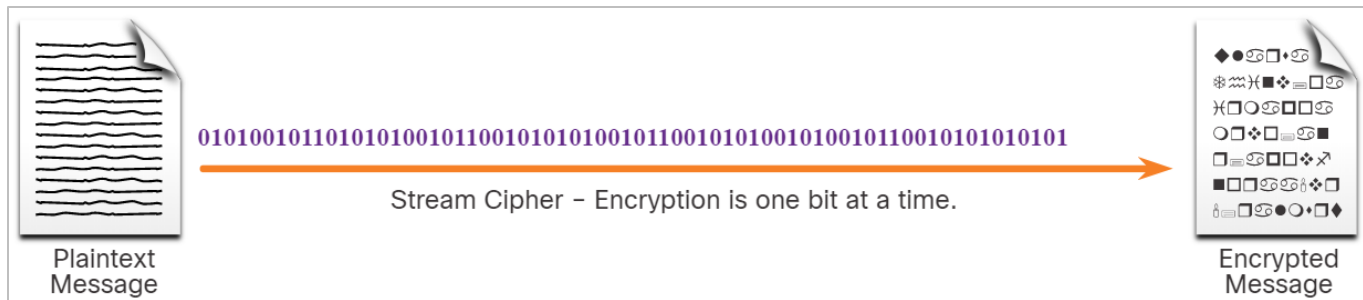
- Bloco cifragem transforma um bloco de texto simples de comprimento fixo em um bloco comum de texto cifrado de 64 ou 128 bits.
- As cifras de bloco comuns incluem DES com um tamanho de bloco de 64 bits e AES com um tamanho de bloco de 128 bits.



Criptografiasimétrica de confidencialidade (Cont.)

Cifras de fluxo

- Transmite cifra e criptografa o texto simples um byte ou um bit de cada vez.
- As cifras de fluxo são basicamente uma cifra de bloco com um tamanho de bloco de um byte ou bit.
- As cifras de fluxo geralmente são mais rápidas do que as cifras de bloco porque os dados são criptografados continuamente.
- Exemplos de cifras de fluxo incluem RC4 e A5, que é usado para criptografar comunicações de telefone celular GSM.



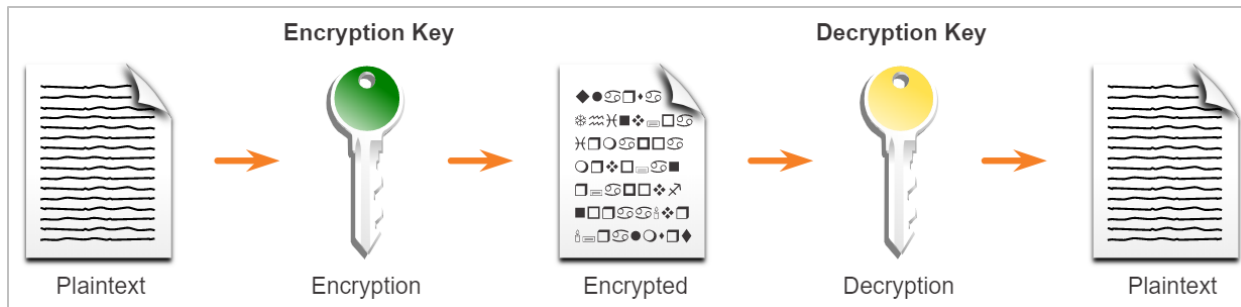
Criptografiasimétrica de confidencialidade (Cont.)

Algoritmos de criptografia simétrica mais conhecidos são descritos na tabela.

Algoritmos de criptografia simétrica	Descrição
Padrão de criptografia de dados (DES)	Este é um algoritmo legado. Ele usa um comprimento de chave curto que o torna inseguro.
3DES (Triple DES)	Este é o substituto para DES e repete o algoritmo DES três vezes. Deve ser evitado, pois está programado para ser aposentado em 2023. Se implementado, use durações de chave muito curtas.
AES (Advanced Encryption Standard)	Este é um algoritmo de criptografia simétrica popular e recomendado. Ele oferece combinações de chaves de 128, 192 ou 256 bits para criptografar blocos de dados de 128, 192 ou 256 bits.
Software-Optimized Encryption Algorithm (SEAL)	Este é um algoritmo alternativo mais rápido para AES. É uma cifra de fluxo que usa uma chave de criptografia de 160 bits e tem um impacto menor na CPU em comparação com outros algoritmos baseados em software.
Algoritmos da série Rivest ciphers (RC)	Este algoritmo foi desenvolvido por Ron Rivest. RC4 é uma cifra de fluxo usada para proteger o tráfego da web. Verificou-se que tem múltiplas vulnerabilidades que o tornaram inseguro. O RC4 não deve ser utilizado.

Confidencialidade Criptografia Assimétrica

- Os algoritmos assimétricos, também chamados de algoritmos de chave pública, são projetados de forma que a chave usada para criptografia seja diferente da chave usada para descryptografia, conforme mostrado na figura.
- Algoritmos assimétricos usam uma chave pública e uma chave privada. Ambas as chaves são capazes do processo de criptografia, mas a chave emparelhada complementar é necessária para descryptografia.
- O processo também é reversível. Os dados criptografados com a chave pública requerem a chave privada para descryptografar. Algoritmos assimétricos alcançam confidencialidade e autenticidade usando este processo.



Criptografia assimétrica de confidencialidade (Condd.)

- A criptografia assimétrica pode usar comprimentos de chave entre 512 e 4.096 bits.
- Comprimentos de chave maiores ou iguais a 2.048 bits podem ser confiáveis, enquanto comprimentos de chave de 1.024 ou menores são considerados insuficientes.
- Exemplos de protocolos que usam algoritmos de chave assimétrica incluem:
 - **Internet Key Exchange (IKE)** - é um componente fundamental das redes virtuais privadas IPsec (VPNs).
 - **Secure Socket Layer (SSL)** - Agora isso é implementado como TLS (Transport Layer Security) padrão da IETF.
 - **Secure Shell (SSH)** - Este protocolo fornece uma conexão segura de acesso remoto a dispositivos de rede.
 - **Pretty Good Privacy (PGP)** - Este programa de computador fornece privacidade e autenticação criptográficas. É frequentemente usado para aumentar a segurança das comunicações por email.
- Os algoritmos assimétricos são substancialmente mais lentos que os algoritmos simétricos.

Criptografia assimétrica de confidencialidade (Condd.)

Exemplos comuns de algoritmos de criptografia assimétrica são descritos na tabela.

Algoritmos de criptografia assimétrica	comprimento da chave	Descrição
Diffie-Hellman (DH)	512, 1024, 2048, 3072, 4096	Este algoritmo permite que duas partes concordem sobre uma chave que podem usar para criptografar as mensagens que desejam enviar uma para a outra. A segurança depende da suposição de que é fácil elevar um número a uma determinada potência, mas difícil calcular qual potência foi usada, dados o número e o resultado.
Padrão de Assinatura Digital (DSS) e Algoritmo de Assinatura Digital (DSA)	512 – 1024	Ele especifica DSA como o algoritmo para assinaturas digitais. DSA é um algoritmo de chave pública baseado no esquema de assinatura ElGamal. A velocidade de criação da assinatura é semelhante ao RSA, mas é 10 a 40 vezes mais lenta para verificação.
Algoritmos de criptografia Rivest, Shamir e Adleman (RSA)	512 até 2048	É para criptografia de chave pública com base na dificuldade atual de fatorar números muito grandes. É o primeiro algoritmo adequado para assinatura e criptografia. É usado em protocolos de comércio eletrônico e é considerado seguro devido a chaves suficientemente longas e ao uso de implementações atualizadas.

Criptografia assimétrica de confidencialidade (Cont.)

Algoritmos de criptografia assimétrica	comprimento da chave	Descrição
EIGamal	512 – 1024	Um algoritmo de criptografia de chave assimétrica para criptografia de chave pública que se baseia no contrato de chave Diffie-Hellman. Uma desvantagem do sistema EIGamal é que a mensagem criptografada se torna muito grande, aproximadamente o dobro do tamanho da mensagem original e, por esse motivo, é usada apenas para mensagens pequenas, como chaves secretas.
Técnicas de curva elíptica	224 ou superior	A criptografia de curva elíptica pode ser usada para adaptar muitos algoritmos criptográficos, como Diffie-Hellman ou EIGamal. A principal vantagem da criptografia de curva elíptica é que as chaves podem ser muito menores.

Confidencialidade Criptografia Assimétrica - Confidencialidade

- Algoritmos assimétricos são usados para fornecer confidencialidade sem pré-compartilhar uma senha.
- O objetivo de confidencialidade dos algoritmos assimétricos é iniciado quando o processo de criptografia é iniciado com a chave pública.
- O processo pode ser resumido usando a fórmula:

Chave pública (criptografar) + chave privada (descriptografar) = confidencialidade

- Quando a chave pública é usada para criptografar os dados, a chave privada deve ser usada para descriptografar os dados.
- Apenas um host tem a chave privada; portanto, a confidencialidade é alcançada.
- Se a chave privada estiver comprometida, outro par de chaves deve ser gerado para substituir a chave comprometida.

Confidencialidade Criptografia Assimétrica - Confidencialidade (Cond.)

Vamos ver como as chaves privadas e públicas podem ser usadas para fornecer confidencialidade para a troca de dados entre Bob e Alice.

Alice adquire a chave pública de Bob

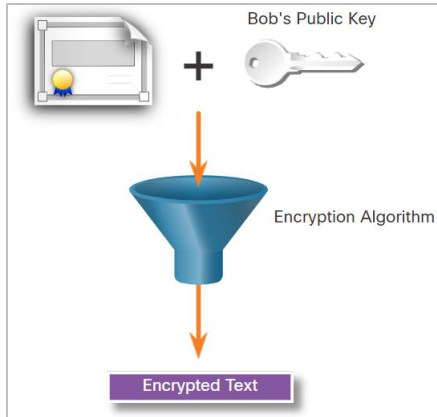
Alice solicita e obtém a chave pública de Bob



Confidencialidade Criptografia Assimétrica - Confidencialidade (Cont.)

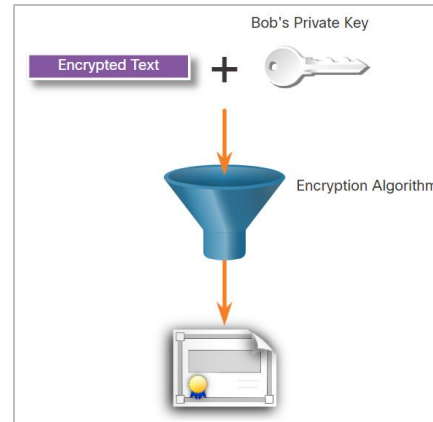
Alice usa a chave pública

Alice usa a chave pública de Bob para criptografar uma mensagem usando um algoritmo acordado. Alice envia a mensagem criptografada para Bob.



Bob descriptografa mensagem com chave privada

Bob então usa sua chave privada para descriptografar a mensagem. Como Bob é o único com a chave privada, a mensagem de Alice só pode ser descriptografada por Bob e, portanto, a confidencialidade é alcançada.



Confidencialidade Criptografia assimétrica - Autenticação

- O objetivo de autenticação de algoritmos assimétricos é iniciado quando o processo de criptografia é iniciado com a chave privada.
- O processo pode ser resumido usando a fórmula:

Chave privada (criptografar) + chave pública (descriptografar) = autenticação

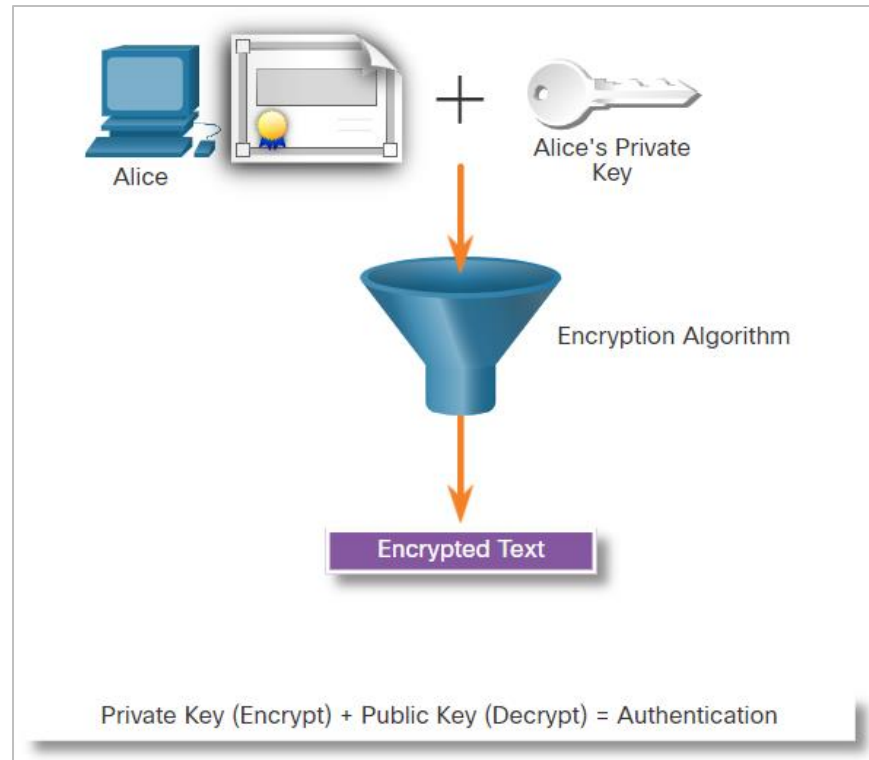
- Quando a chave privada é usada para criptografar os dados, a chave pública correspondente deve ser usada para descriptografar os dados.
- Como apenas um host tem a chave privada, somente esse host poderia ter criptografado a mensagem, fornecendo autenticação do remetente.
- Normalmente, nenhuma tentativa é feita para preservar o sigilo da chave pública, portanto, qualquer número de hosts pode descriptografar a mensagem.
- Quando um host descriptografa uma mensagem com êxito usando uma chave pública, é confiável que a chave privada criptografou a mensagem, o que verifica quem é o remetente. Esta é uma forma de autenticação.

Criptografia assimétrica de confidencialidade - Autenticação (Cont.)

Vamos ver como as chaves privadas e públicas podem ser usadas para fornecer autenticação para a troca de dados entre Bob e Alice.

Alice usa sua chave privada

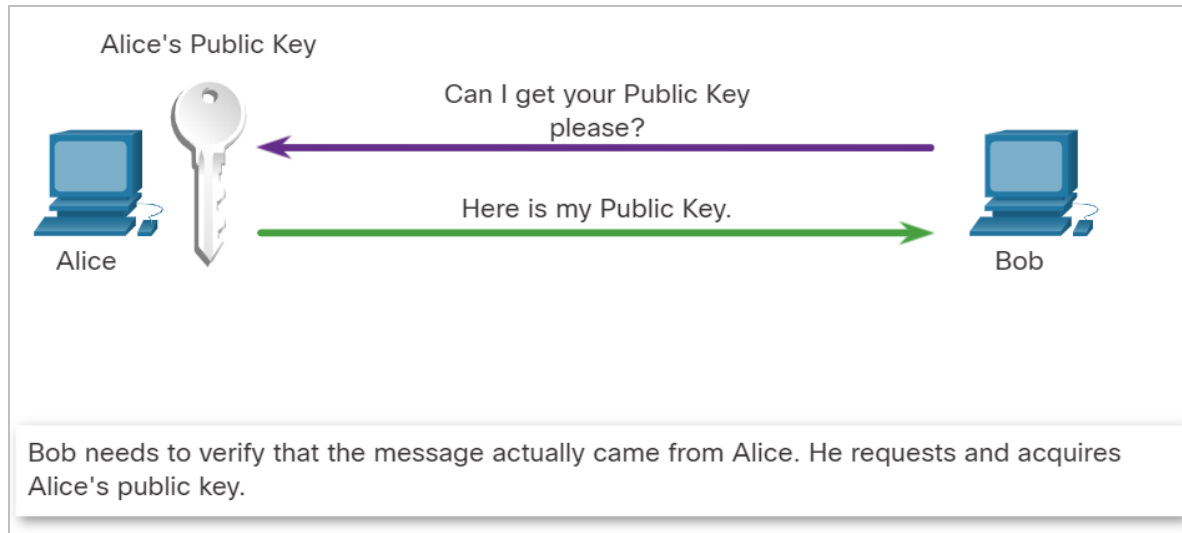
- Alice criptografa uma mensagem usando sua chave privada.
- Alice envia a mensagem criptografada para Bob.
- Bob precisa autenticar que a mensagem realmente veio de Alice.



Criptografia assimétrica de confidencialidade - Autenticação (Cont.)

Bob solicita a chave pública

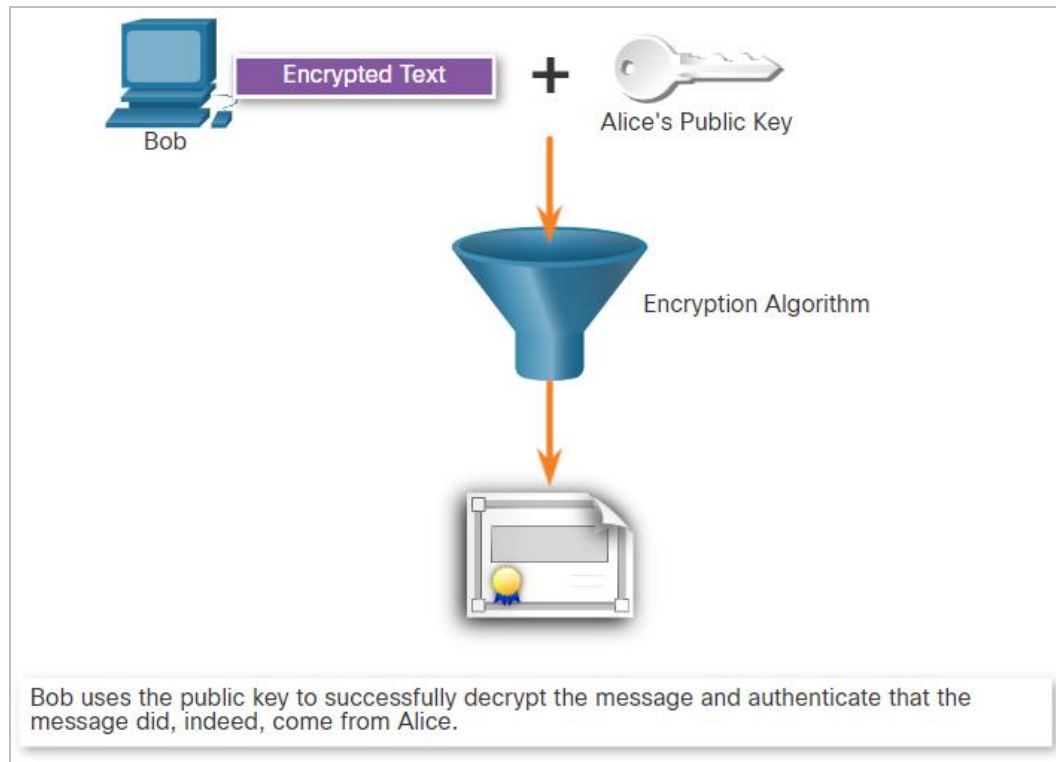
Para autenticar a mensagem, Bob solicita a chave pública de Alice.



Criptografia assimétrica de confidencialidade - Autenticação (Cont.)

Bob descriptografa usando a chave pública

Bob usa a chave pública de Alice para descriptografar a mensagem.



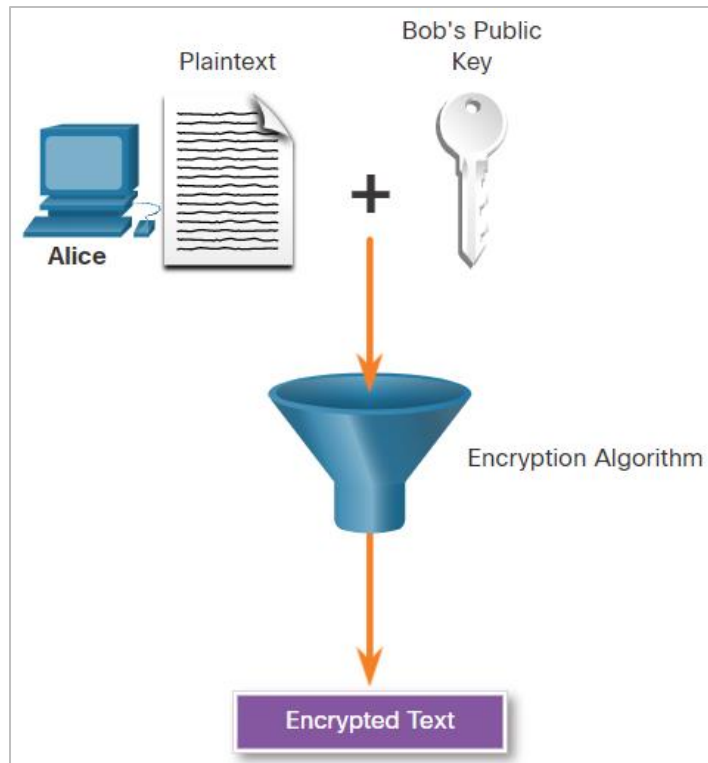
Criptografia assimétrica de confidencialidade - Integridade

Combinar os dois processos de criptografia assimétrica fornece confidencialidade, autenticação e integridade da mensagem.

Neste exemplo, uma mensagem será cifrada usando a chave pública de Bob e um hash cifrado será criptografado usando a chave privada de Alice para fornecer confidencialidade, autenticidade e integridade.

Alice usa a chave pública de Bob

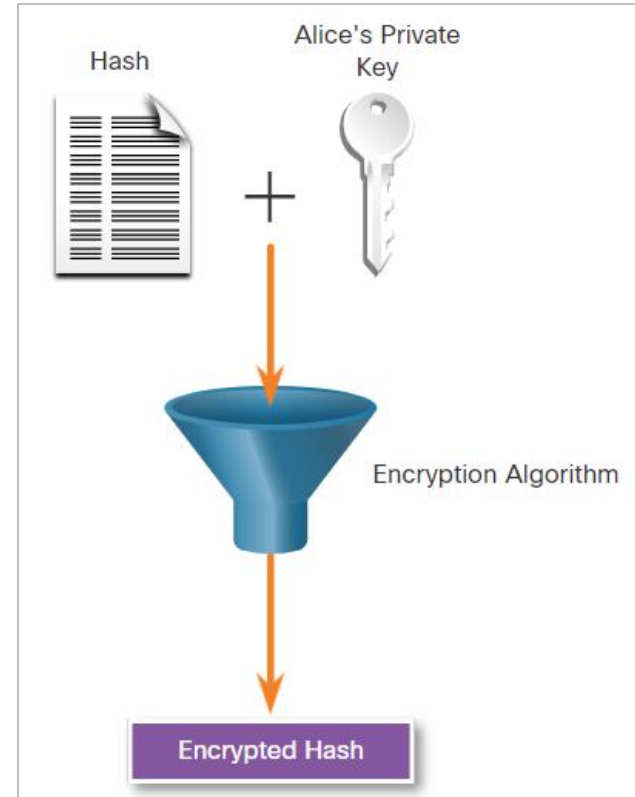
Alice quer enviar uma mensagem para Bob assegurando que só Bob pode ler o documento. Alice quer garantir a confidencialidade da mensagem. Alice usa a chave pública de Bob para cifrar a mensagem. Só Bob será capaz de decifrá-lo usando sua chave privada.



Criptografiaassimétrica de confidencialidade - Integridade (Cont.)

Alice criptografa um hash usando sua chave privada

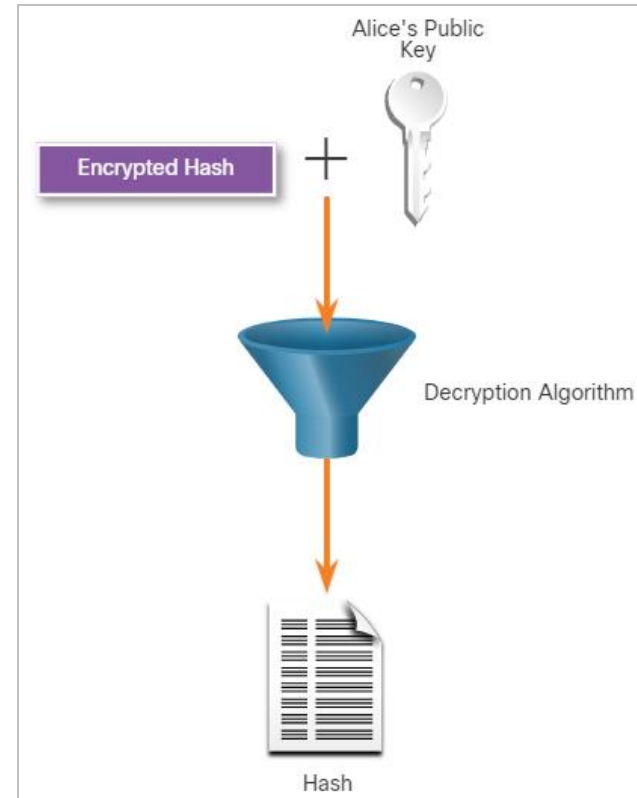
- Alice também quer garantir a autenticação e integridade da mensagem.
- A autenticação garante ao Bob que o documento foi enviado por Alice, e a integridade garante que ele não foi modificado.
- Alice usa sua chave privada para cifrar um hash da mensagem.
- Alice envia a mensagem criptografada com seu hash criptografado para Bob.



Criptografiaassimétrica de confidencialidade - Integridade (Cont.)

Bob usa a chave pública de Alice para descriptografar o hash

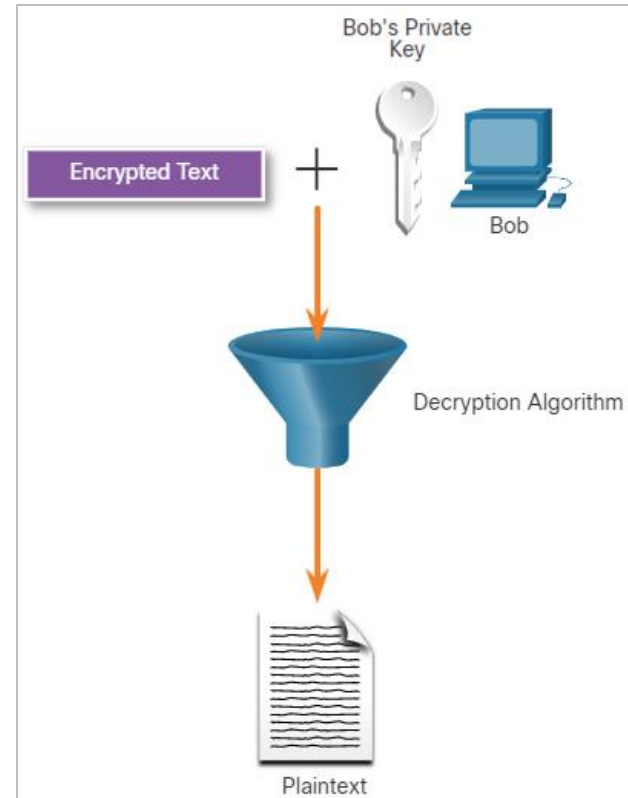
- Bob usa a chave pública de Alice para verificar se a mensagem não foi modificada.
- O hash recebido é igual ao hash determinado localmente com base na chave pública de Alice.
- Além disso, isso verifica se Alice é definitivamente o remetente da mensagem porque ninguém mais tem a chave privada de Alice.



Criptografia assimétrica de confidencialidade - Integridade (Cont.)

Bob usa sua chave privada para descriptografar a mensagem

Bob usa sua chave privada para decifrar a mensagem.

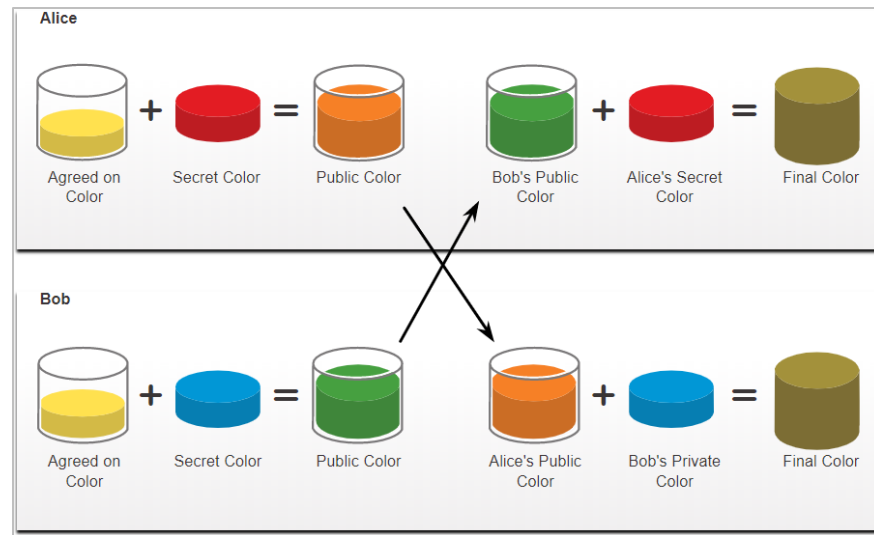


Diffie-Hellman

- Diffie-Hellman (DH) é um algoritmo matemático assimétrico que permite que dois computadores gerem um segredo compartilhado idêntico sem terem se comunicado antes.
- A nova chave compartilhada nunca é realmente trocada entre o remetente e o destinatário.
- A chave pode ser usada por um algoritmo de criptografia para criptografar o tráfego entre os dois sistemas como ambas as partes o conhecem.
- Aqui estão dois exemplos de casos em que DH é comumente usado:
 - Os dados são trocados usando uma VPN IPsec
 - Dados SSH são trocados

Diffie-Hellman (Condd.)

- A figura mostra como o DH opera. As cores são usadas em vez de números longos complexos para simplificar o processo de acordo de chave DH.
- A troca de chaves DH começa com Alice e Bob concordando em uma cor que é amarelo aqui.
- Em seguida, Alice e Bob selecionarão uma cor secreta. Alice escolheu vermelho enquanto Bob escolheu azul.
- Alice e Bob agora misturam a cor compartilhada (amarelo) com suas respectivas cores secretas para produzir uma cor pública.
- Alice envia sua cor pública (laranja) para Bob e Bob envia sua cor pública (verde) para Alice.
- Alice e Bob misturam a cor que receberam com sua própria cor secreta original. O resultado é uma mistura final de cor marrom que é idêntica a ambas. A cor marrom representa a chave secreta compartilhada resultante entre Bob e Alice.



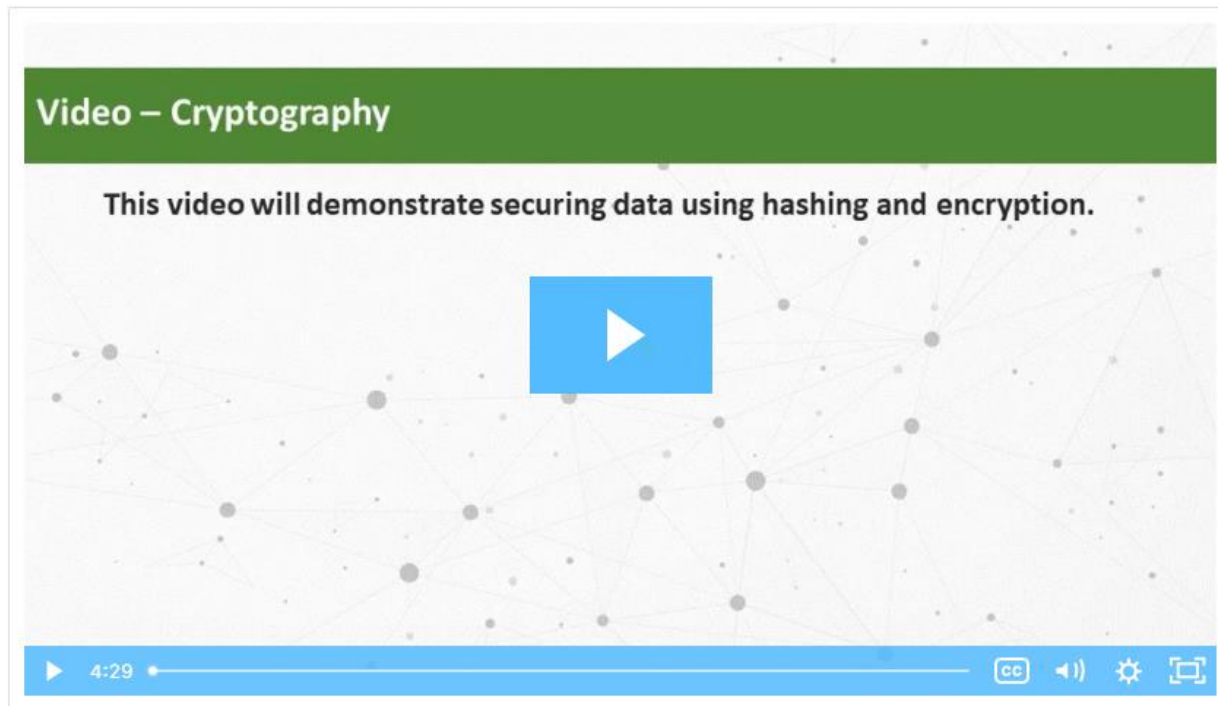
Diffie-Hellman (Condd.)

- A segurança do DH baseia-se no fato de que ele usa números muito grandes em seus cálculos.
- Diffie-Hellman usa diferentes grupos DH para determinar a força da chave que é usada no processo de acordo de chave. Os números de grupo mais altos são mais seguros, mas exigem tempo adicional para calcular a chave.
- O seguinte identifica os grupos DH suportados pelo Cisco IOS Software e seu valor de número primo associado:
 - Grupo DH 1:768 bits
 - Grupo DH 2:1024 bits
 - Grupo DH 5:1536 bits
 - Grupo DH 14:2048 bits
 - Grupo DH 15:3072 bits
 - Grupo DH 16:4096 bits

Nota: Um acordo de chave DH também pode ser baseado em criptografia de curva elíptica. Os grupos DH 19, 20 e 24 são suportados pelo Cisco IOS Software.

Vídeo de confidencialidade - criptografia

Assista ao vídeo para aprender sobre Criptografia.



Laboratório de confidencialidade - Criptografando e descriptografando dados usando OpenSSL

Neste laboratório, você completará os seguintes objetivos:

- Criptografando mensagens com OpenSSL
- Descriptografando mensagens com OpenSSL

Laboratório de confidencialidade - Criptografando e descriptografando dados usando uma ferramenta de hacker

Neste laboratório, você completará os seguintes objetivos:

- Cenário de configuração
- Criar e Criptografar Arquivos
- Recuperar senhas criptografadas de arquivos

Laboratório de Confidencialidade - Examinando Telnet e SSH no Wireshark

Neste laboratório, você completará os seguintes objetivos:

- Examinar uma Sessão Telnet com o Wireshark
- Examinar uma Sessão SSH com o Wireshark

21.3 Criptografia de chave pública

usando assinaturas digitais

- As assinaturas digitais são uma técnica matemática usada para fornecer autenticidade, integridade e não repúdio.
- As assinaturas digitais têm propriedades específicas que permitem autenticação de entidade e integridade de dados. Além disso, as assinaturas digitais fornecem não repúdio da transação.
- Em outras palavras, a assinatura digital serve como prova legal de que o intercâmbio de dados ocorreu. As assinaturas digitais usam criptografia assimétrica.
- As propriedades das assinaturas digitais são as seguintes:
 - **Autêntico** - A assinatura não pode ser forjada e fornece prova de que o signatário, e ninguém mais, assinou o documento.
 - **Imutável** - Depois que um documento é assinado, ele não pode ser alterado.
 - **Não reutilizável** - A assinatura do documento não pode ser transferida para outro documento.
 - **Não repudiado** - O documento assinado é considerado o mesmo que um documento físico. A assinatura é a prova de que o documento foi assinado pela pessoa real.

usando assinaturas digitais (Cont.)

- As assinaturas digitais são comumente usadas nas duas situações a seguir:
 - **Assinatura de código** - Isso é usado para fins de integridade de dados e autenticação. A assinatura de código é usada para verificar a integridade dos arquivos executáveis baixados do site de um fornecedor. Ele também usa certificados digitais assinados para autenticar e verificar a identidade do site que é a origem dos arquivos.
 - **Certificados digitais** - são semelhantes a um cartão de identificação virtual e usados para autenticar a identidade do sistema com o site de um fornecedor e estabelecer uma conexão criptografada para trocar dados confidenciais.

usando assinaturas digitais (Cont.)

- Existem três algoritmos DSS (Digital Signature Standard) que são usados para gerar e verificar assinaturas digitais:
 - **Algoritmo de Assinatura Digital (DSA)** - DSA é o padrão original para gerar pares de chaves públicas e privadas e para gerar e verificar assinaturas digitais.
 - **Rivest-Shamir Adelman Algoritmo (RSA)**- RSA é um algoritmo assimétrico que é comumente usado para gerar e verificar assinaturas digitais.
 - **Elliptic Curve Digital Signature Algoritmo (ECDSA)**- O ECDSA é uma variante mais recente do DSA e fornece autenticação de assinatura digital e não repúdio com os benefícios adicionais da eficiência computacional, tamanhos de assinatura pequenos e largura de banda mínima.
- Na década de 1990, a RSE Security Inc. começou a publicar padrões de criptografia de chave pública (PKCS). Havia 15 PKCS, embora 1 tenha sido retirado a partir do momento em que esta escrita foi escrita.

digitais de criptografia de chave pública para assinatura de código

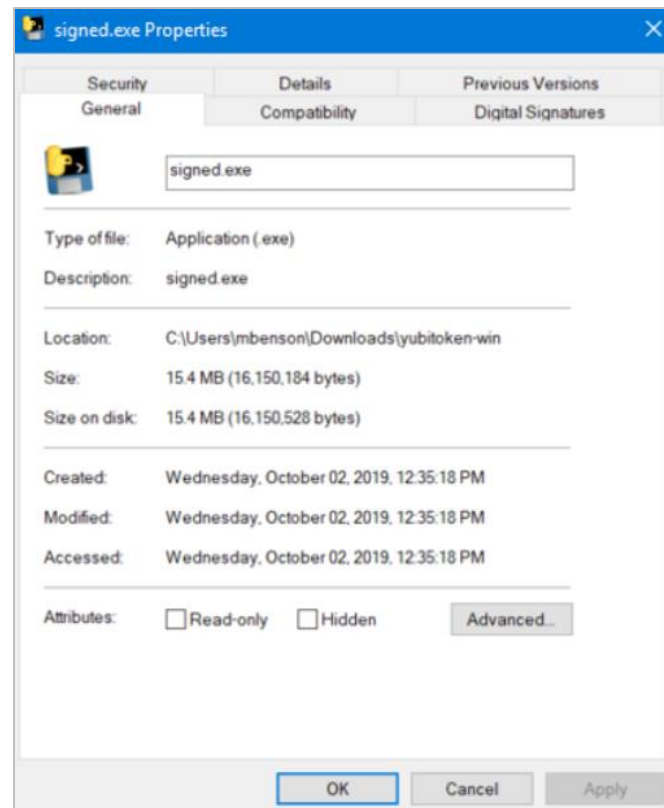
- As assinaturas digitais são comumente usadas para garantir a autenticidade e integridade do código de software.
- Os arquivos executáveis são empacotados em um envelope assinado digitalmente, o que permite ao usuário final verificar a assinatura antes de instalar o software.
- Assinar digitalmente o código fornece várias garantias sobre o código:
 - O código é autêntico e é realmente originado pela editora.
 - O código não foi modificado desde que saiu do editor do software.
 - A editora publicou inegavelmente o código. Isso fornece não repúdio do ato de publicação.
- O objetivo do software assinado digitalmente é garantir que o software não foi adulterado e que ele foi originado da fonte confiável, conforme reivindicado.
- As assinaturas digitais servem como verificação de que o código não foi adulterado por agentes da ameaça e o código malicioso não foi inserido no arquivo por terceiros.

Assinaturas digitais de criptografia de chave pública para assinatura de código (Cont.)

As propriedades de um arquivo que tem um certificado assinado digitalmente são as seguintes:

Propriedades do arquivo

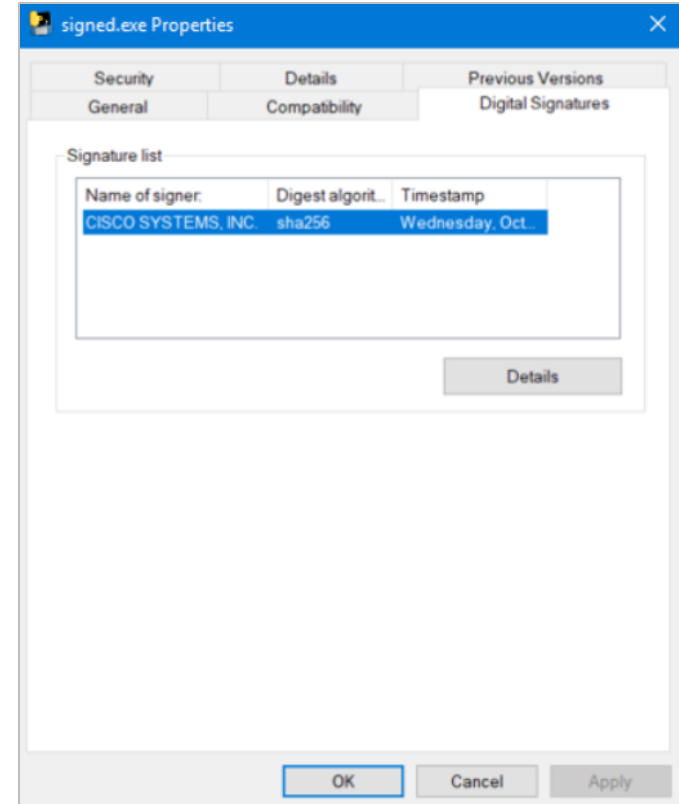
Este arquivo executável foi baixado da Internet. O arquivo contém uma ferramenta de software da Cisco Systems.



Assinaturas digitais de criptografia de chave pública para assinatura de código (Cont.)

Assinaturas digitais

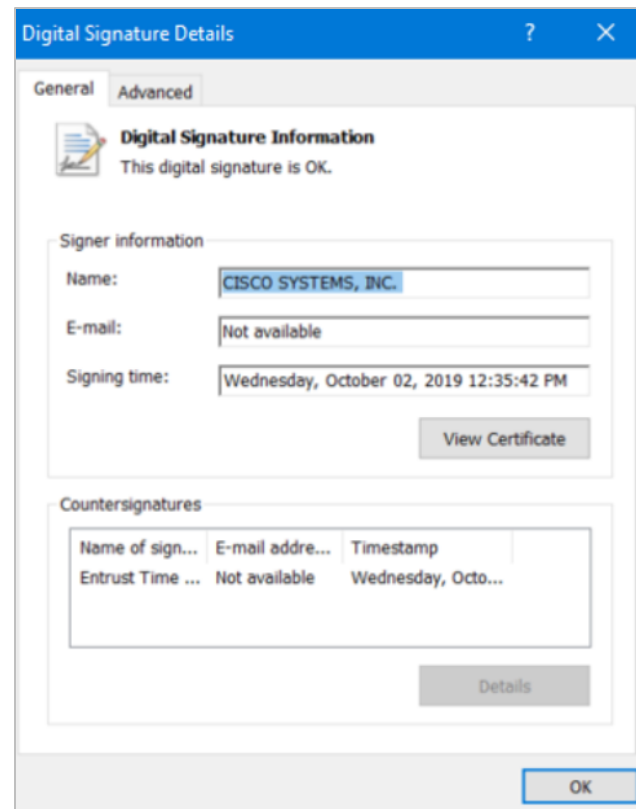
- Clicar na guia **Assinaturas Digitais** revela que o arquivo é de uma organização confiável, a Cisco Systems Inc. A compilação de arquivos foi criada com o algoritmo sha256.
- A data em que o arquivo foi assinado também é fornecida.
- Clicar em **Detalhes** abre a janela Detalhes das Assinaturas Digitais.



Assinaturas digitais de criptografia de chave pública para assinatura de código (Cont.)

Detalhes de assinaturas digitais

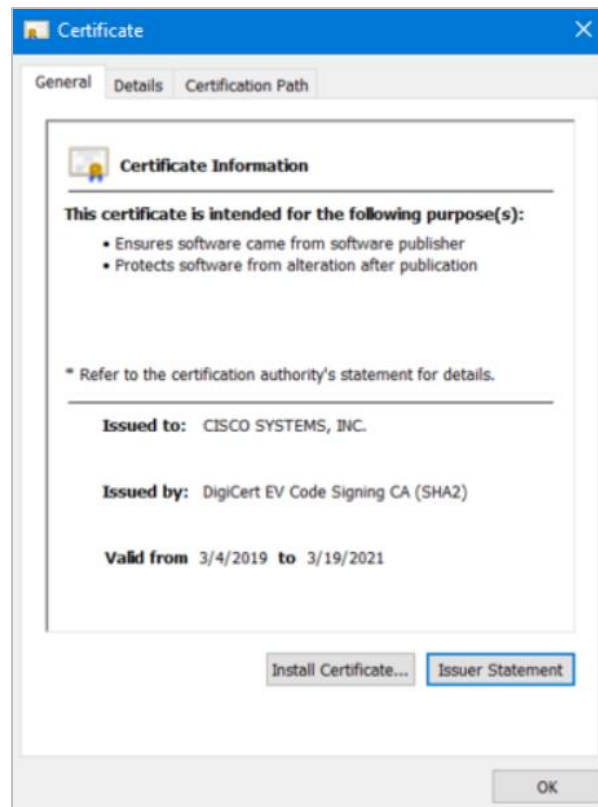
- A janela Detalhes da assinatura digital revela que o arquivo foi assinado pela Cisco Systems, Inc em outubro de 2019.
- Isso foi verificado pela contrassinatura fornecida pela Entrust Time Stamping Authority no mesmo dia em que foi assinado pela Cisco.
- Clique em **Exibir Certificado** para ver os detalhes do próprio certificado.



Assinaturas digitais de criptografia de chave pública para assinatura de código (Cont.)

Informações do certificado

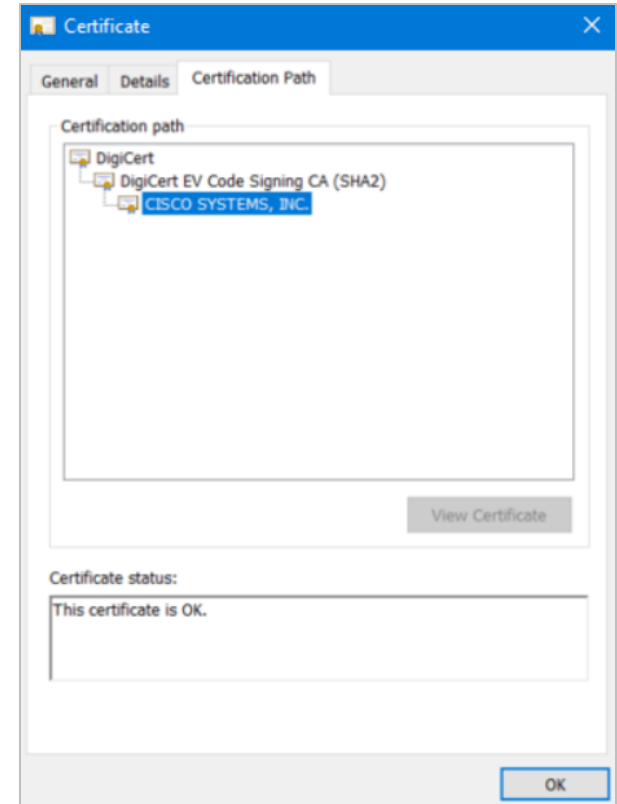
- A guia **Geral** fornece as finalidades do certificado, para quem o certificado foi emitido e quem emitiu o certificado.
- Ele também exibe o período para o qual o certificado é válido. Certificados inválidos podem impedir que o arquivo seja executado.



Assinaturas digitais de criptografia de chave pública para assinatura de código (Cont.)

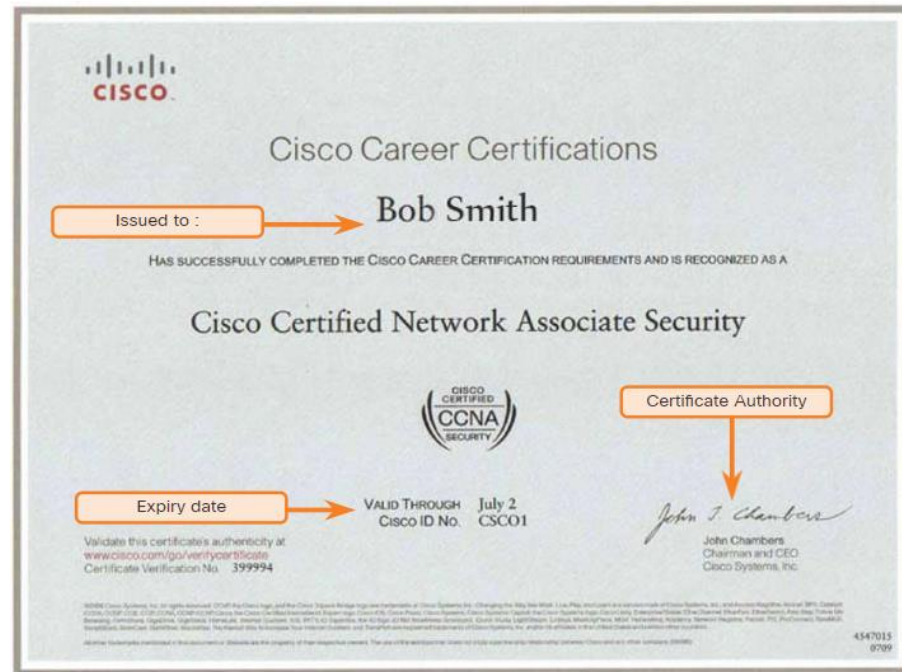
Caminho do Certificado

- Clique na guia **Caminho de Certificação** para ver se o arquivo foi assinado pela Cisco Systems, conforme verificado para a DigiCert.
- Em alguns casos, uma entidade adicional pode verificar independentemente o certificado.



Assinaturas digitais de criptografia de chave pública para certificados digitais

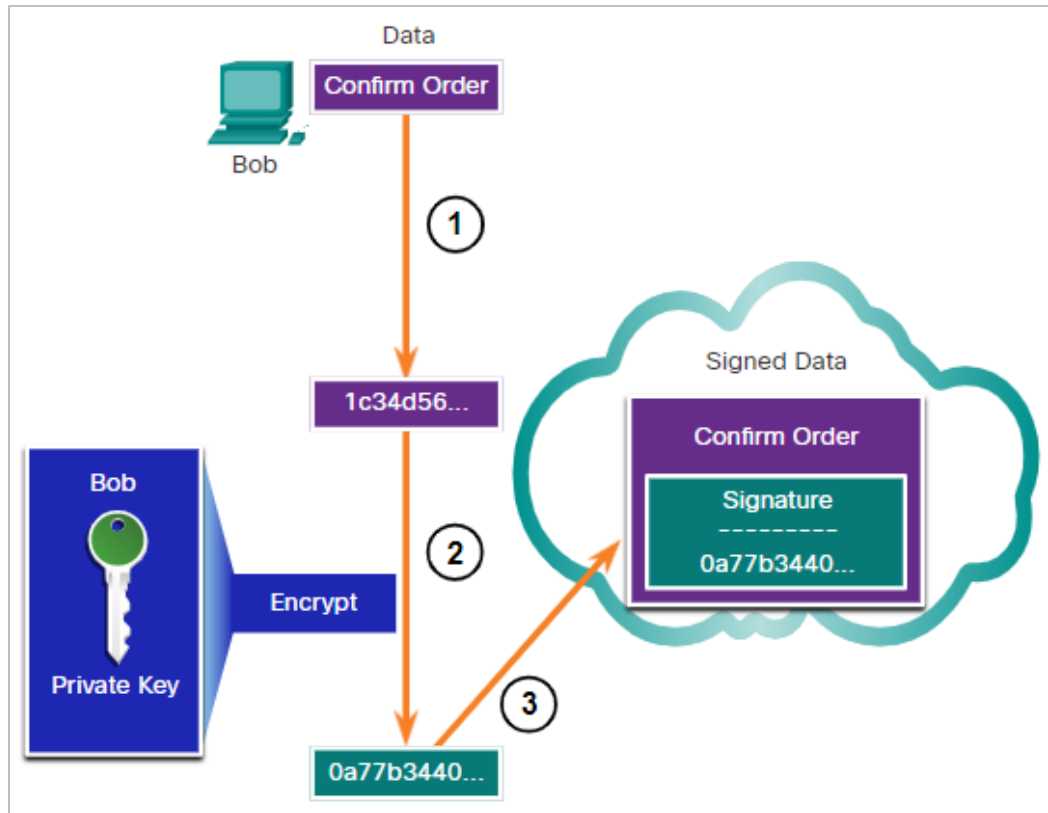
- Um certificado digital é usado para autenticar e verificar se um usuário que está enviando uma mensagem é quem afirma ser.
- Os certificados digitais também podem ser usados para fornecer confidencialidade ao receptor com os meios de criptografar uma resposta.
- Os certificados digitais são semelhantes aos certificados físicos, conforme mostrado na figura.
- O certificado digital verifica de forma independente uma identidade.
- Um certificado verifica a identidade, uma assinatura verifica se algo vem dessa identidade.



Assinaturas digitais de criptografia de chave pública para certificados digitais (Cont.)

Esse cenário ajudará você a entender como uma assinatura digital é usada.

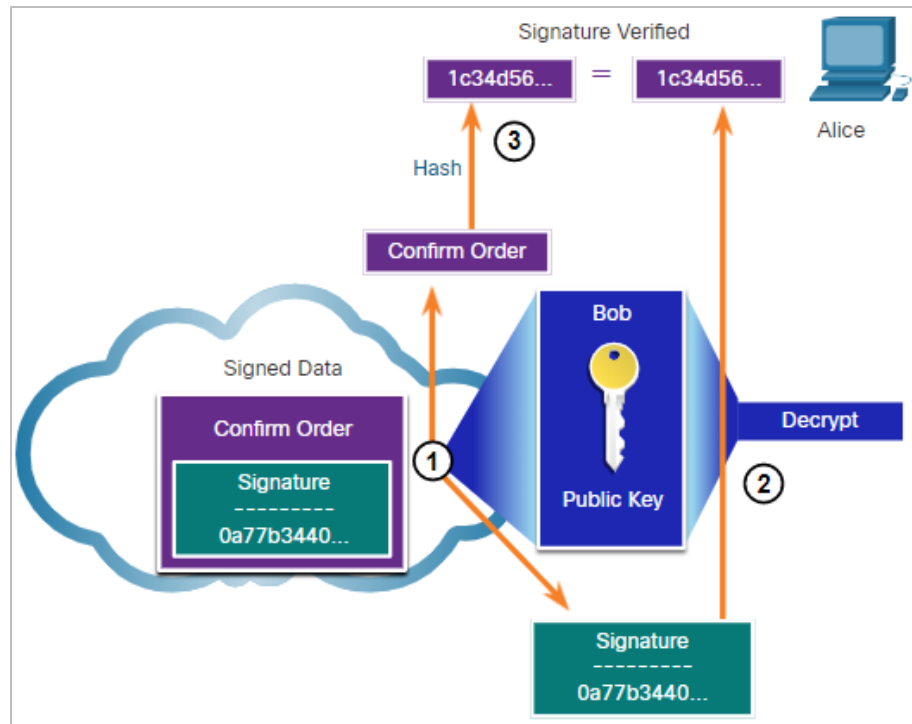
- Bob está confirmando um pedido com Alice. Alice está encomendando do site do Bob.
- Bob confirma a ordem e seu computador cria um hash da confirmação.
- O computador criptografa o hash com a chave privada do Bob.
- O hash criptografado, que é a assinatura digital, é adicionado ao documento.
- A confirmação do pedido é então enviada para Alice através da internet.



Assinaturas digitais de criptografia de chave pública para certificados digitais (Cont.)

Quando Alice recebe a assinatura digital, ocorre o seguinte processo:

- O receptor de Alice aceita a confirmação do pedido com a assinatura digital e obtém a chave pública de Bob.
- O computador de Alice, em seguida, descriptografa a assinatura usando a chave pública de Bob, que revela o valor de hash assumido do dispositivo de envio.
- O computador de Alice cria um hash do documento recebido, sem sua assinatura, e compara esse hash com o hash descriptografado.
- Se os hashes corresponderem, o documento é autêntico. Isso significa que a confirmação foi enviada por Bob e não mudou desde que foi assinada.



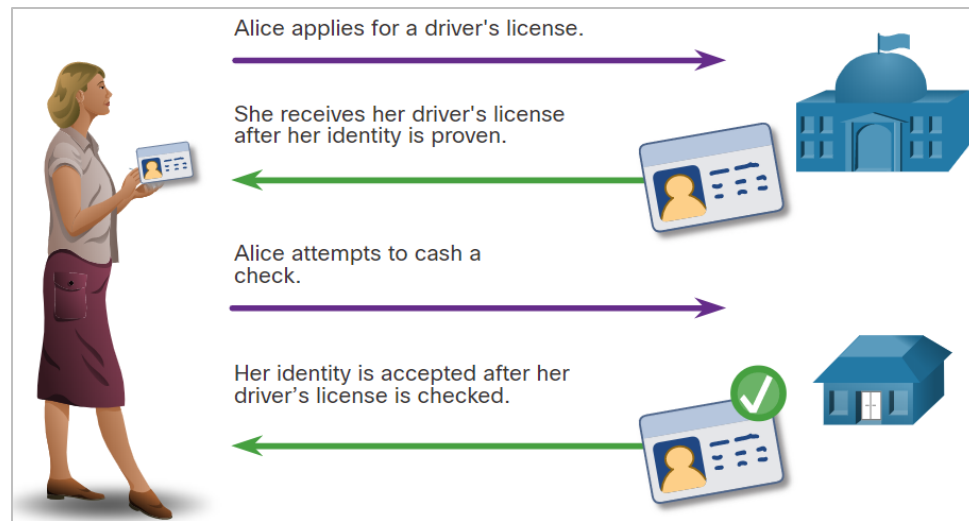
21.4 Autoridades e o sistema de confiança de PKI

Autoridades e Gerenciamento de Chave Pública do Sistema de Confiança PKI

- O tráfego da Internet consiste no tráfego entre duas partes. Ao estabelecer uma conexão assimétrica entre dois hosts, os hosts trocarão suas informações de chave pública.
- Um certificado SSL é um certificado digital que confirma a identidade de um domínio de site.
- Para implementar SSL em um site, o usuário compra um certificado SSL para o domínio de um provedor de Certificado SSL.
- O terceiro de confiança faz uma avaliação antes da emissão das credenciais. Após essa investigação aprofundada, o terceiro emite credenciais que são difíceis de falsificar.
- Quando os computadores tentam se conectar a um site via HTTPS, o navegador verifica o certificado de segurança do site e verifica se ele é válido e originado com uma autoridade de certificação confiável.
- Isso valida que a identificação do site é verdadeira. O certificado é salvo localmente pelo navegador da Web e, em seguida, é usado em transações subsequentes. A chave pública do site está incluída no certificado e é usada para verificar futuras comunicações entre o site e o cliente.

Autoridades e o Gerenciamento de Chave Pública do Sistema de Confiança PKI (Cont.)

- Esses terceiros confiáveis fornecem serviços semelhantes aos escritórios de licenciamento governamentais.
- A figura ilustra como uma carteira de motorista é análoga a um certificado digital.
- A Infraestrutura de Chave Pública (PKI) consiste em especificações, sistemas e ferramentas que são usados para criar, gerenciar, distribuir, usar, armazenar e revogar certificados digitais.
- A autoridade de certificação (CA) é uma organização que cria certificados digitais vinculando uma chave pública a uma identificação confirmada, como um site ou indivíduo.
- O PKI é um sistema complexo projetado para proteger identidades digitais contra hacking por atores de ameaças ou estados-nação.

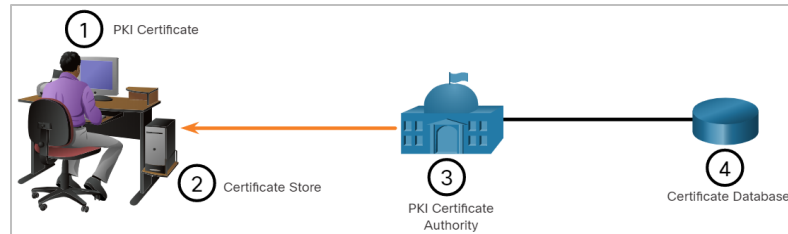


A infra-estrutura de chave pública

- A PKI é necessária para oferecer suporte à distribuição em larga escala e à identificação de chaves de criptografia públicas.
- A estrutura PKI facilita uma relação de confiança altamente escalável.
- Consiste em hardware, software, pessoas, políticas e procedimentos necessários para criar, gerenciar, armazenar, distribuir e revogar certificados digitais.

A Infraestrutura de Chave Pública (Cont.)

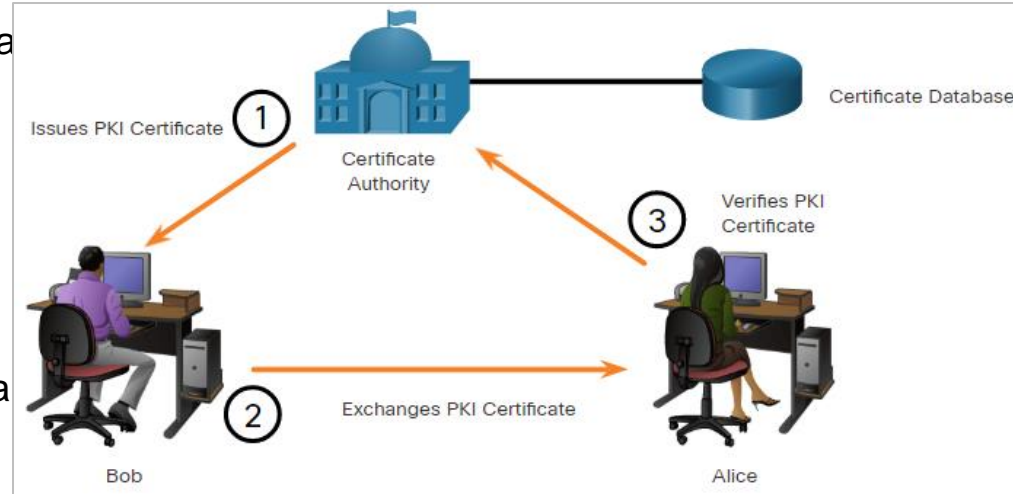
- A figura mostra os principais elementos da PKI.
- Os certificados PKI contêm a chave pública de uma entidade, a sua finalidade, a autoridade de certificação (AC) que validou e emitiu o certificado, o intervalo de datas em que o certificado é válido e o algoritmo usado para criar a assinatura.
- O armazenamento de certificados reside em um computador local e armazena certificados emitidos e chaves privadas.
- O Certificado de Autoridade PKI (CA) é um terceiro confiável que emite certificados PKI para entidades e indivíduos após verificar sua identidade. Ele assina esses certificados usando sua chave privada.
- O banco de dados de certificados armazena todos os certificados aprovados pela autoridade de certificação.



A Infraestrutura de Chave Pública (Cont.)

A figura mostra como os elementos da PKI interoperam:

- Emissões Certificado PKI: Bob inicialmente solicita um certificado da autoridade de certificação. A autoridade de certificação autentica Bob e armazena o certificado PKI de Bob no banco de dados de certificados.
- Trocas Certificado PKI: Bob se comunica com Alice usando seu certificado PKI.
- Verifica o certificado PKI: Alice se comunica com a autoridade de certificação confiável usando a chave pública da CA. A AC refere-se ao banco de dados de certificados para validar o certificado PKI de Bob.



Observação: nem todos os certificados PKI são recebidos diretamente de uma autoridade de certificação. Uma autoridade de registro (RA) é uma autoridade de certificação subordinada e é certificada por uma autoridade de certificação raiz para emitir certificados para usos específicos.

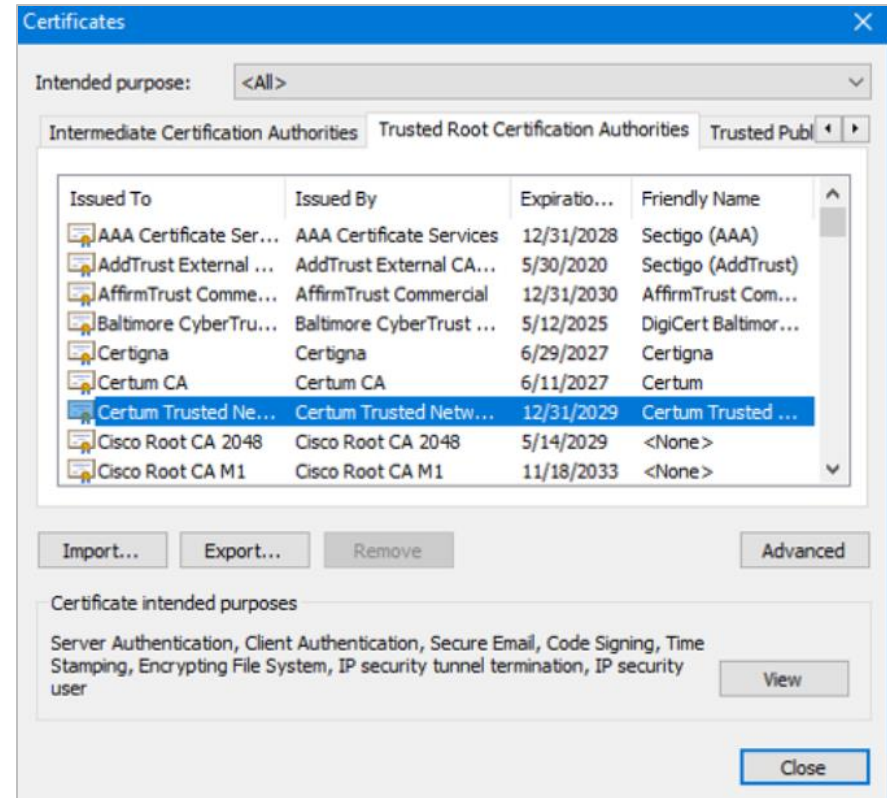
O Sistema de Autoridades PKI

- Muitos fornecedores fornecem servidores da CA como um serviço gerenciado ou como um produto de usuário final. Alguns desses fornecedores incluem Symantec Group, Comodo, Go Daddy Group, GlobalSign e assim por diante.
- As organizações também podem implementar PKIs privadas usando o Microsoft Server ou Open SSL.
- As autoridades de certificação, especialmente aquelas que são terceirizadas, emitem certificados baseados em classes que determinam a confiabilidade de um certificado.
- A tabela fornece uma descrição das classes. Quanto maior o número da classe, mais confiável será o certificado. Um certificado de classe 5 é confiável muito mais do que um certificado de classe inferior.

Classe	Descrição
0	Usado para testes em situações em que não foram realizadas verificações.
1	Usado por indivíduos que exigem verificação de e-mail.
2	Usado por organizações para as quais a prova de identidade é necessária.
3	Usado para servidores e assinatura de software.
4	Usado para transações comerciais on-line entre empresas.
5	Usado para organizações privadas ou segurança do governo.

Autoridades e o Sistema de Confiança PKIO Sistema de Autoridades PKI (Cont.)

- Algumas chaves públicas da CA são pré-carregadas, como as listadas em navegadores da Web.
- A figura exhibe vários certificados VeriSign contidos no armazenamento de certificados no host.
- Quaisquer certificados assinados por qualquer uma das autoridades de certificação na lista serão vistos pelo navegador como legítimos e serão confiáveis automaticamente.

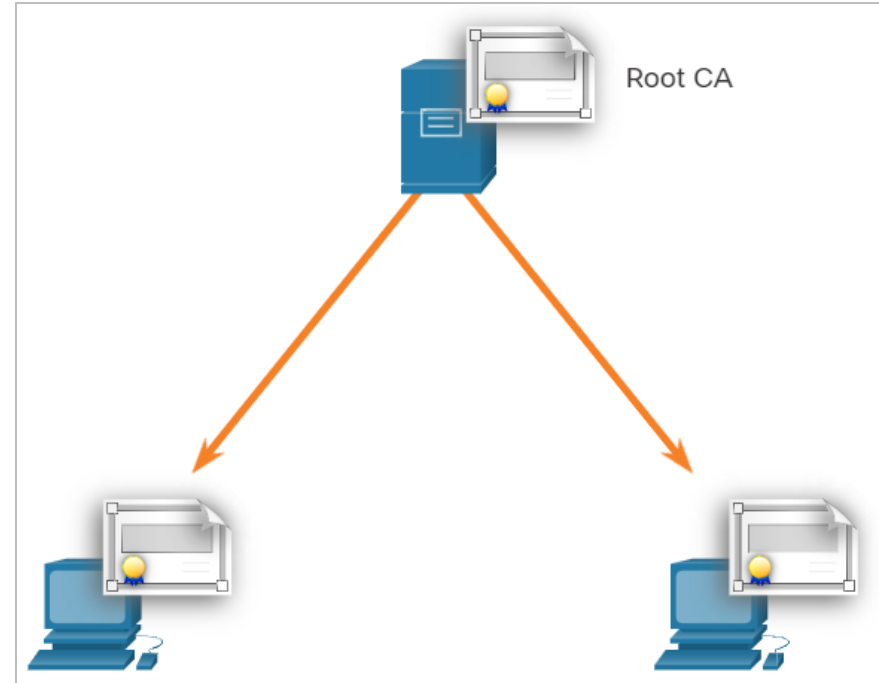


O sistema de confiança PKI

PKIs podem formar diferentes topologias de confiança que são as seguintes:

Topologia PKI de raiz única

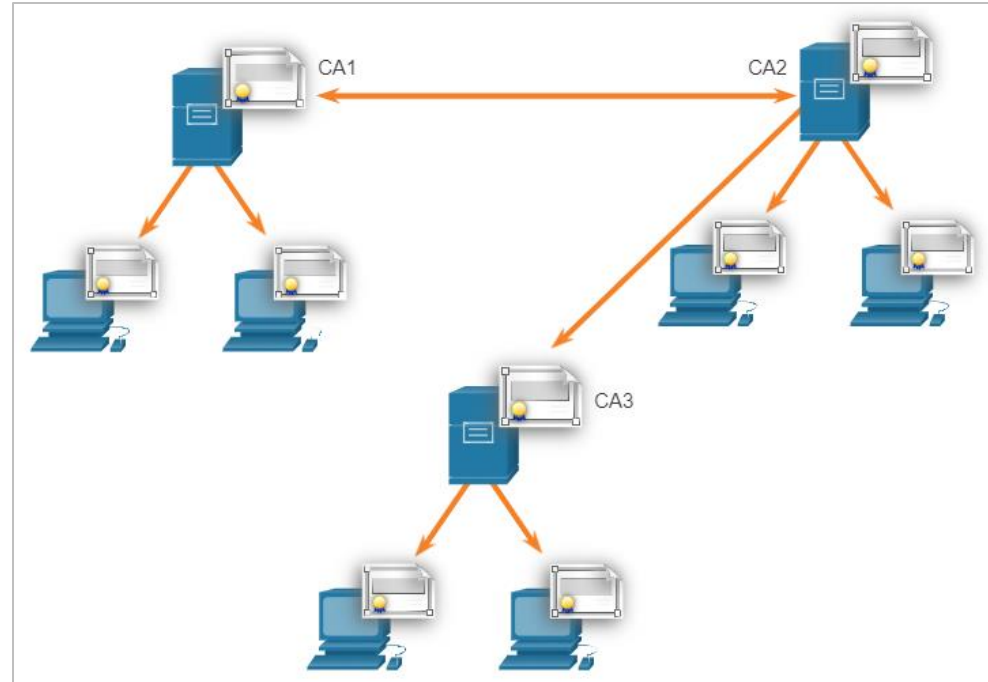
- Uma única AC, chamada de AC raiz, emite todos os certificados para os utilizadores finais dentro da mesma organização.
- O benefício da abordagem é a sua simplicidade.
- É difícil dimensionar para um ambiente grande, pois requer uma administração estritamente centralizada, o que cria um único ponto de falha.



Autoridades e o Sistema de Confiança PKIO Sistema de Confiança PKI (Cond.)

Topologias de CA certificadas entre

- Este é um modelo ponto a ponto no qual as ACs individuais estabelecem relações de confiança com outras ACs através da certificação cruzada de certificados de AC.
- Os usuários em ambos os domínios da CA também têm a certeza de que podem confiar uns nos outros.
- Isso fornece redundância e elimina o ponto único de falha.

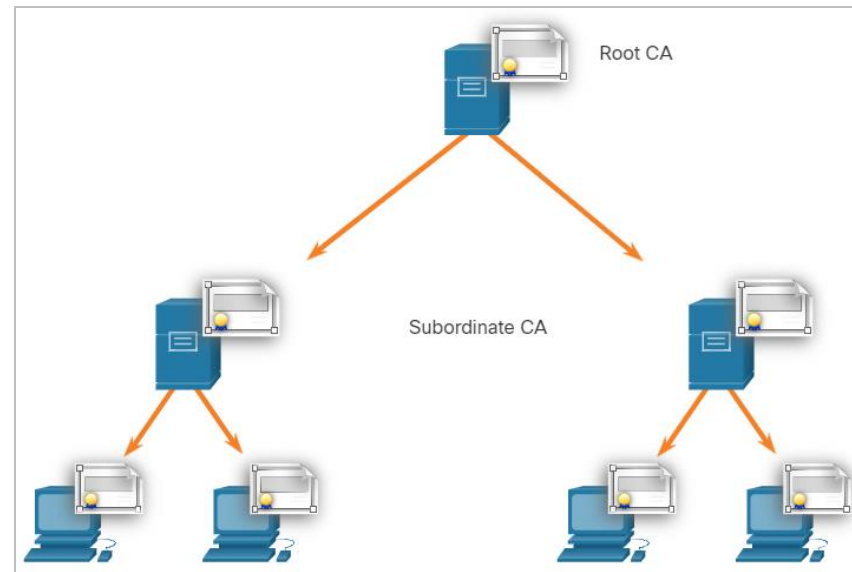


Autoridades e o Sistema de Confiança PKIO Sistema de Confiança PKI

(Cont.)

Topologias hierárquicas de CA

- A AC de nível mais alto é a AC raiz que emite certificados para utilizadores finais e para uma AC subordinada.
- As subCAs podem ser criadas para suportar várias unidades de negócios, domínios ou comunidades de confiança.
- A autoridade de certificação raiz mantém a “comunidade de confiança” estabelecida garantindo que cada entidade na hierarquia confirme um conjunto mínimo de práticas.
- Os benefícios da topologia incluem maior escalabilidade e capacidade de gerenciamento.
- Uma topologia hierárquica e de certificação cruzada pode ser combinada para criar uma infraestrutura híbrida.



interoperabilidade do sistema de confiança PKI de diferentes fornecedores de PKI

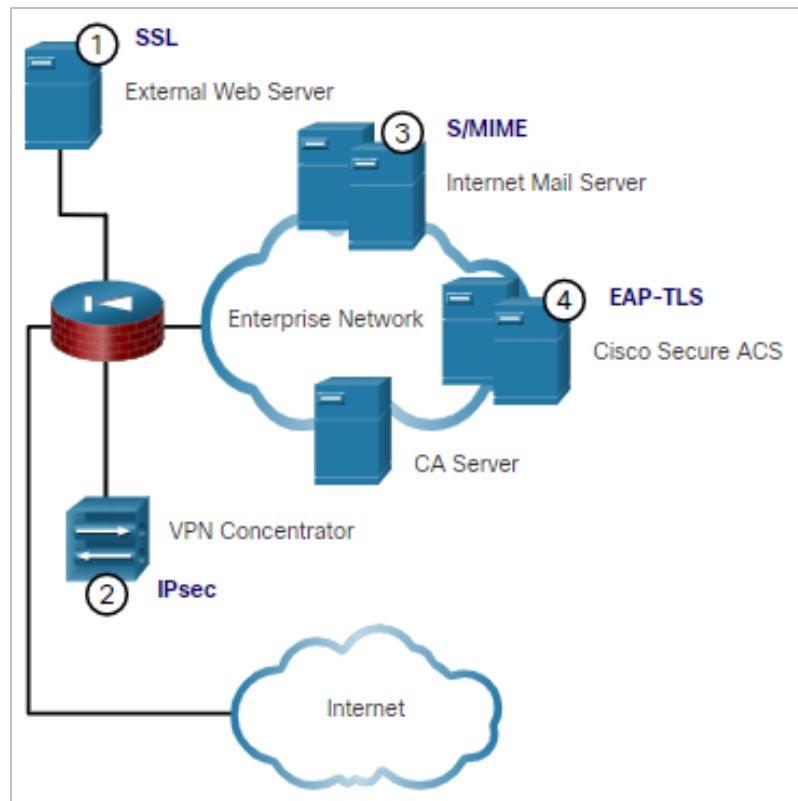
- A interoperabilidade entre uma PKI e seus serviços de suporte, como o Lightweight Directory Access Protocol (LDAP) e diretórios X.500, é uma preocupação porque muitos fornecedores de CA propuseram e implementaram soluções proprietárias.
- Para resolver esse problema de interoperabilidade, o IETF publicou o Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527).
- O padrão X.509 versão 3 (X.509 v3) define o formato de um certificado digital.

Observação: *LDAP e X.500 são protocolos usados para consultar um serviço de diretório, como o Microsoft Active Directory, para verificar um nome de usuário e senha.*

Autoridades e a interoperabilidade do sistema de confiança PKI de diferentes fornecedores de PKI (Cont.)

Aplicações x.509v3

- **SSL:** Servidores Web seguros usam X.509 v3 para autenticação de sites nos protocolos SSL e TLS, enquanto os navegadores da Web usam X.509 v3 para implementar certificados de cliente HTTPS.
- **IPsec:** VPNs IPsec usam X.509 quando certificados podem ser usados como um mecanismo de distribuição de chave pública para autenticação baseada em RSA de troca de chaves de Internet (IKE).
- **S/MIME:** agentes de correio do utilizador que suportam a proteção de correio com o protocolo S/MIME utilizam certificados X.509.
- **EAP-TLS:** Os switches podem usar certificados para autenticar dispositivos finais que podem ser fornecidos a um ACS central por meio do protocolo de autenticação extensível com TLS (EAP-TLS).



Autoridades e o Registro, Autenticação e Revogação de Certificados do Sistema Confiável PKI

- A primeira etapa no procedimento de autenticação da autoridade de certificação é obter com segurança uma cópia da chave pública da autoridade de certificação.
- Todos os sistemas que utilizam a PKI devem ter a chave pública da autoridade de certificação, que é chamada de certificado autoassinado.
- A chave pública da autoridade de certificação verifica todos os certificados emitidos pela autoridade de certificação e é vital para o bom funcionamento da PKI.
- Para muitos sistemas, como navegadores da Web, a distribuição de certificados de CA é processada automaticamente. O navegador da Web vem pré-instalado com um conjunto de certificados raiz de CA públicos.
- O processo de registro de certificado é usado por um sistema host para se inscrever com uma PKI. Para fazer isso, os certificados de CA são recuperados em banda através de uma rede e a autenticação é feita fora de banda (OOB) usando o telefone.

Observação: somente uma autoridade de certificação raiz pode emitir um certificado autoassinado reconhecido ou verificado por outras autoridades de certificação dentro da

Autoridades e o Registro, Autenticação e Revogação de Certificados do Sistema de Confiança PKI (Cont.)

- O registro do sistema com a PKI entra em contato com uma autoridade de certificação para solicitar e obter um certificado de identidade digital para si mesmo e para obter o certificado autoassinado da autoridade de certificação.
- O estágio final verifica se o certificado da autoridade de certificação foi autêntico e é executado usando um método fora de banda, como o POTS, para obter a impressão digital do certificado de identidade da autoridade de certificação válido.
- A autenticação não requer mais a presença do servidor da autoridade de certificação e cada usuário troca seus certificados contendo chaves públicas.
- Os certificados devem, por vezes, ser revogados. Aqui estão dois métodos mais comuns de revogação:
 - **Lista de revogação de certificados (CRL)**- Uma lista de números de série de certificados revogados que foram invalidados porque expiraram. As entidades PKI pesquisam regularmente o repositório CRL para receber a CRL atual.
 - **Protocolo de Status de Certificado Online (OCSP)**- Um protocolo de Internet usado para consultar um servidor OCSP para o status de revogação de um certificado digital X.509. As informações de revogação são imediatamente enviadas para um banco de dados on-line.

Laboratório de Sistemas de Confiança PKI — Armazenamentos de Autoridade

Neste laboratório, você completará os seguintes objetivos:

- Certificados Confiáveis pelo Seu Navegador
- Verificando o Man-In-Mi

21.5 Aplicações e impactos da criptografia

PKI de criptografia

O seguinte fornece uma pequena lista de usos comuns de PKIs:

- Autenticação de peer baseada em certificado SSL/TLS
- Proteja o tráfego de rede usando VPNs IPsec
- Tráfego da web HTTPS
- Controle o acesso à rede usando a autenticação 802.1x
- E-mail seguro usando o protocolo S/MIME
- Mensagens instantâneas seguras
- Aprovar e autorizar aplicativos com assinatura de código
- Proteja os dados do usuário com o sistema de arquivos de criptografia (EFS)
- Implementar autenticação de dois fatores com cartões inteligentes
- Protegendo dispositivos de armazenamento USB

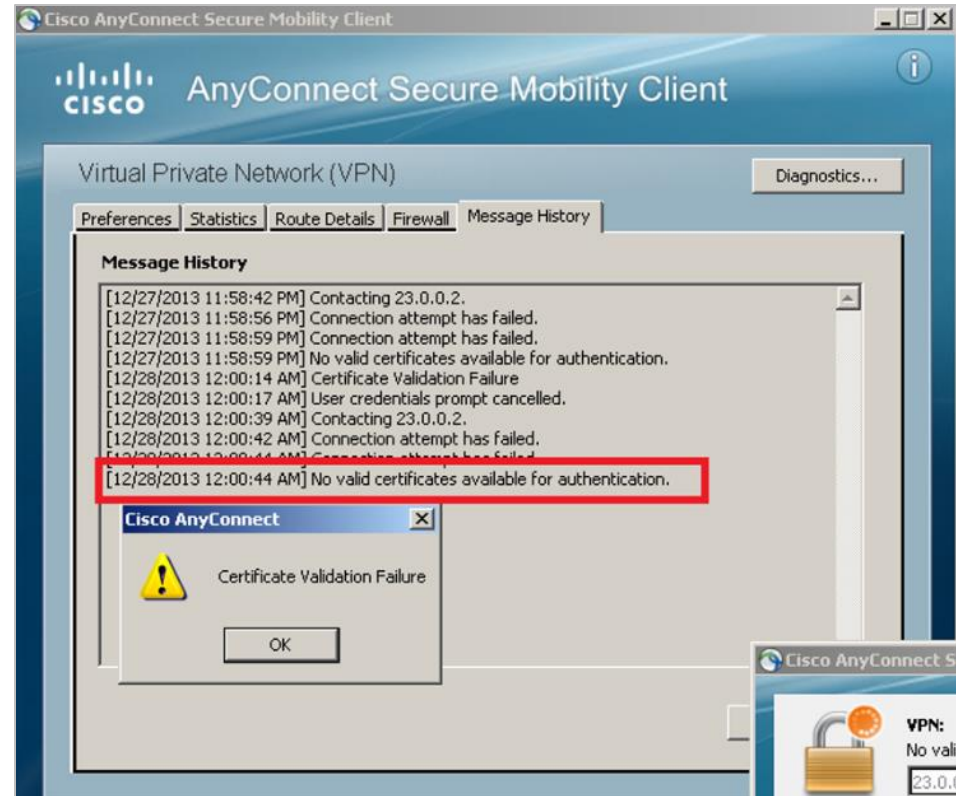
Aplicações e Impactos de Transações de Rede Criptografada

- Um analista de segurança deve ser capaz de reconhecer e resolver possíveis problemas relacionados à permissão de soluções relacionadas à PKI na rede corporativa.
- O aumento do tráfego SSL/TLS representa um grande risco de segurança para as empresas, uma vez que o tráfego é criptografado e não pode ser interceptado e monitorado por meios normais. Os usuários podem introduzir malware ou vazam informações confidenciais através de uma conexão SSL/TLS.
- Outros problemas relacionados a SSL/TLS podem estar associados à validação do certificado de um servidor Web. Quando isso ocorre, os navegadores da Web exibirão um aviso de segurança. Os problemas relacionados à PKI associados a avisos de segurança incluem:
 - **Faixa de datas de validade**- Os certificados X.509v3 especificam datas “não antes” e “não depois”. Se a data atual estiver fora do intervalo, o navegador da Web exibirá uma mensagem.
 - **Erro de validação de assinatura**- Se um navegador não puder validar a assinatura no certificado, não há garantia de que a chave pública no certificado seja autêntica. A validação de assinatura falhará se o certificado raiz da hierarquia da autoridade de certificação não estiver disponível no armazenamento de certificados do navegador.

Aplicações e Impactos de Transações de Rede Criptografada de Criptografia (Cont.)

Erro de validação de assinatura

- Alguns desses problemas podem ser evitados, pois os protocolos SSL/TLS são extensíveis e modulares. Isto é conhecido como um conjunto de cifras.
- Os principais componentes do conjunto de cifras são o MAC (Message Authentication Code Algoritmo), o algoritmo de criptografia, o algoritmo de troca de chaves e o algoritmo de autenticação.
- À medida que a criptoanálise continua a revelar falhas nesses algoritmos, o conjunto de cifras pode ser atualizado para corrigir essas falhas. Quando as versões de protocolo dentro do conjunto de cifras mudam, o número de versão do SSL/TLS também muda.



Criptografia e Monitoramento de Segurança

- O monitoramento de rede torna-se mais desafiador quando os pacotes são criptografados.
- Os analistas de segurança devem estar cientes desses desafios e enfrentá-los da melhor forma possível.
- Por exemplo, quando VPNs site a site são usadas, o IPS deve ser posicionado para que ele possa monitorar o tráfego não criptografado. No entanto, o aumento do uso de HTTPS na rede empresarial introduz novos desafios.
- Os analistas de segurança devem saber como contornar e resolver esses problemas. Aqui está uma lista de algumas das coisas que um analista de segurança pode fazer:
 - Configure regras para distinguir entre tráfego SSL e não-SSL, tráfego SSL HTTPS e não-HTTPS.
 - Melhore a segurança através da validação de certificados de servidor utilizando CRLs e OCSP.
 - Implemente proteção antimalware e filtragem de URL de conteúdo HTTPS.
 - Implante um Cisco SSL Appliance para descriptografar o tráfego SSL e enviá-lo para dispositivos IPS (Intrusion Prevention System, sistema de prevenção de intrusões) para identificar riscos normalmente ocultos pelo SSL.

Criptografia e Monitoramento de Segurança (Condd.)

- A criptografia é dinâmica e está sempre mudando. Um analista de segurança deve manter um bom entendimento de algoritmos criptográficos e operações para ser capaz de investigar incidentes de segurança relacionados à criptografia.
- Há duas maneiras principais em que a criptografia afeta as investigações de segurança.
- Primeiro, os ataques podem ser direcionados especificamente para os próprios algoritmos de criptografia.
- Após o algoritmo ter sido rachado e o invasor obter as chaves, todos os dados criptografados que foram capturados podem ser descriptografados pelo invasor e lidos, expondo assim dados privados.
- Em segundo lugar, a investigação de segurança também é afetada porque os dados podem ser escondidos à vista, encriptando-os.

21.6 Resumo de criptografia de chave pública

O que aprendi neste módulo?

- Os quatro elementos das comunicações seguras: integridade de dados, autenticação de origem, confidencialidade de dados e não repúdio de dados.
- Uma função hash leva um bloco variável de dados binários, chamado de mensagem, e produz uma representação condensada de comprimento fixo, chamado de hash.
- Existem duas classes de criptografia que são usadas para fornecer confidencialidade de dados: assimétrica e simétrica.
- Algoritmos de criptografia simétricos, como DES, 3DES e AES são baseados na premissa de que cada parte que se comunica conhece a chave pré-compartilhada. Os algoritmos assimétricos (algoritmos de chave pública) são projetados de forma que a chave usada para criptografia seja diferente da chave usada para criptografia.
- A confidencialidade dos dados também pode ser garantida usando algoritmos assimétricos, incluindo Rivest, Shamir e Aldeman (RSA) e PKI. O processo é resumido usando esta fórmula: Chave pública (Criptografar) + Chave Privada (Decrypt) = Confidencialidade.

O que aprendi neste módulo? (Continuação)

- O objetivo de autenticação de um algoritmo assimétrico é iniciado quando o processo de criptografia é iniciado com a chave privada. O processo pode ser resumido com esta fórmula: Chave Privada (Criptografar) + Chave Pública (Decrypt) = Autenticação.
- Diffie-Hellman (DH) é um algoritmo de equação matemática assimétrica que permite que dois computadores gerem uma chave secreta compartilhada idêntica sem se comunicar antes.
- As assinaturas digitais são uma técnica matemática usada para fornecer três serviços básicos de segurança: autenticidade, integridade e não-repúdio. As assinaturas digitais são comumente usadas em assinatura de código e certificados digitais.
- A Infraestrutura de Chave Pública (PKI) consiste em especificações, sistemas e ferramentas que são usados para criar, gerenciar, distribuir, usar, armazenar e revogar certificados digitais.
- Há muitos usos comuns de PKIs, incluindo alguns listados aqui: autenticação de ponto baseada em certificado SSL/TLS, tráfego da Web HTTPS, mensagens instantâneas seguras e proteção de dispositivos de armazenamento USB.
- Um analista de segurança deve ser capaz de reconhecer e resolver possíveis problemas relacionados à permissão de soluções relacionadas à PI na rede empresarial.

