Marisangila Alves, MSc
marisangila.alves@udesc.br
marisangila.com.br

UDESC
UNIVERSIDADE DO ESTADO DE SANTA CATARINA
JOINVILLE
CENTRO DE CIÊNCIAS TECNOLÓGICAS

UDESC
Universidade do Estado de Santa Catarina

2025/2

Segurança da Informação

Funções Hash e Assinatura Digital

Sumário

Funções Hash

- A **cifração** protege contra **ataques passivos** (como escutas).
- Mas não protege de **ataques ativos** como falsificação de dados ou mensagens.
- Uma mensagem é **autêntica** quando é genuína e veio da fonte declarada.
- A **autenticação de dados** permite verificar:
  - Se o conteúdo não foi alterado;
  - Se a origem é verdadeira;
  - Se a mensagem foi transmitida no tempo e sequência corretos.
- Essas garantias fazem parte do serviço de **integridade da triáde CID**.

> *(Stallings, 2020) Uma função de hash aceita uma mensagem de tamanho variável M como entrada e produz um valor de hash de tamanho fixo h = H(M).*

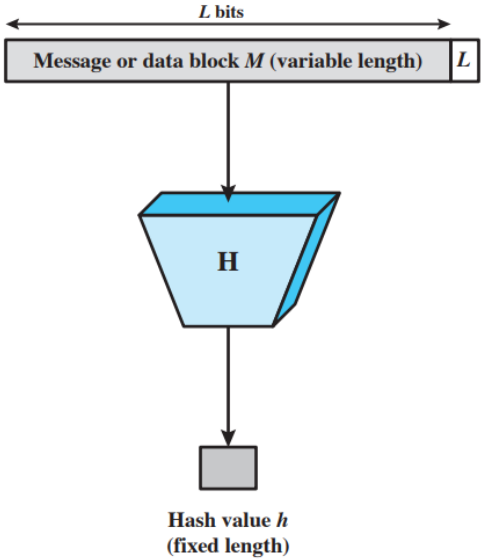
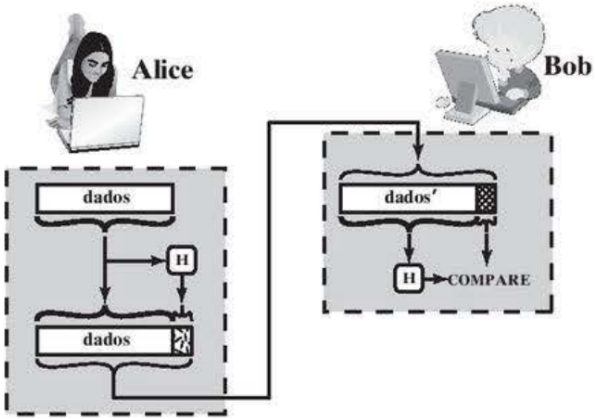


Figura: Função hash (STALLINGS; BROWN, 2015)



(a) Uso da função de hash para verificar integridade de dados

Figura: Hash Integridade.(Stallings, 2020).

1. A essência do uso de uma função de hash para autenticação de mensagem é a seguinte: o emissor calcula um valor de hash como uma função dos bits da mensagem e transmite o valor do hash juntamente com a mensagem.
2. O receptor realiza o mesmo cálculo de hash sobre os bits da mensagem e compara esse valor com o valor de hash recebido.
3. Se houver divergência, o receptor saberá que a mensagem (ou possivelmente o valor de hash) foi alterada.

Exemplos de Funções Hash

- **MD5** — 128 bits (obsoleto, vulnerável a colisões).
- **SHA-1** — 160 bits (em desuso).
- **SHA-256** / **SHA-512** — padrão atual de integridade (hrefhttps://www.youtube.com/watch?v=orIgy2MjqrAClique aqui).
- **SHA-3**, ainda não é padrão.

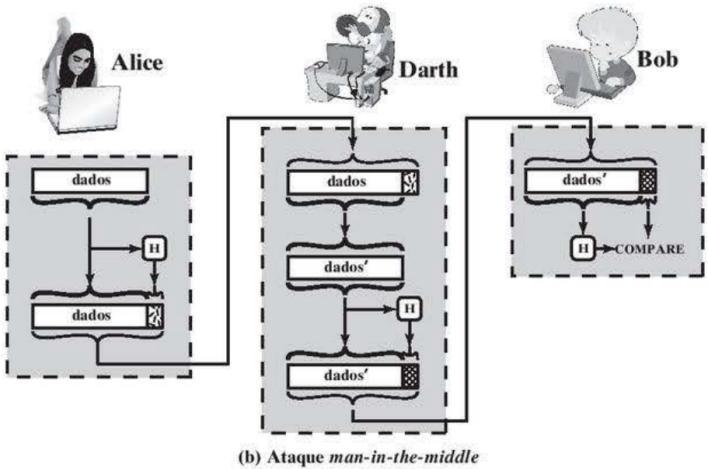


Figura: Ataque man-in-the-middle.(Stallings, 2020).

Problema: Autenticidade II

1. A função de hash precisa ser transmitida de forma segura. Ou seja, deve ser protegida de modo que, se um adversário alterar ou substituir a mensagem, não seja viável para ele alterar também o valor de hash para enganar o receptor.
2. Esse tipo de ataque é mostrado na Figura 11.2b. Neste exemplo, Alice transmite um bloco de dados e anexa um valor de hash.
3. Darth intercepta a mensagem, altera ou substitui o bloco de dados, calcula e anexa um novo valor de hash.
4. Bob recebe os dados alterados com o novo valor de hash e não detecta a mudança.
5. Para impedir esse ataque, o valor de hash gerado por Alice precisa ser protegido.

Autenticação

Uso de Hash para Autenticação I

- A mensagem mais o código de hash concatenado são encriptados usando a encriptação simétrica. Como somente A e B compartilham a chave secreta, a mensagem deverá ter vindo de A e sem alteração. O código de hash oferece a estrutura ou redundância exigida para conseguir a autenticação. Como a encriptação é aplicada à mensagem inteira mais o código de hash, a confidencialidade também é fornecida.

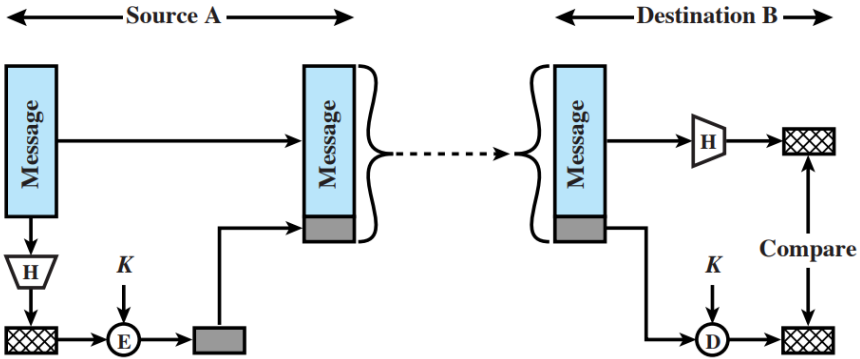


Figura: Criptografar hash e mensagem (STALLINGS; BROWN, 2015).

- A mensagem mais o código de hash concatenado são encriptados usando a encriptação simétrica. Como somente A e B compartilham a chave secreta, a mensagem deverá ter vindo de A e sem alteração. O código de hash oferece a estrutura ou redundância exigida para conseguir a autenticação. Como a encriptação é aplicada à mensagem inteira mais o código de hash, a confidencialidade também é fornecida.

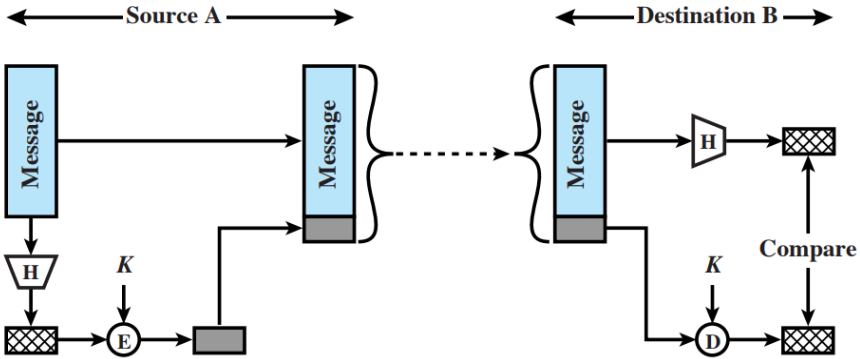


Figura: Criptografia simétrica do hash e mensagem (STALLINGS; BROWN, 2015).

- Somente o código de hash é encriptado, usando a encriptação simétrica. Isso reduz o peso do processamento para as aplicações que não exigem confidencialidade.

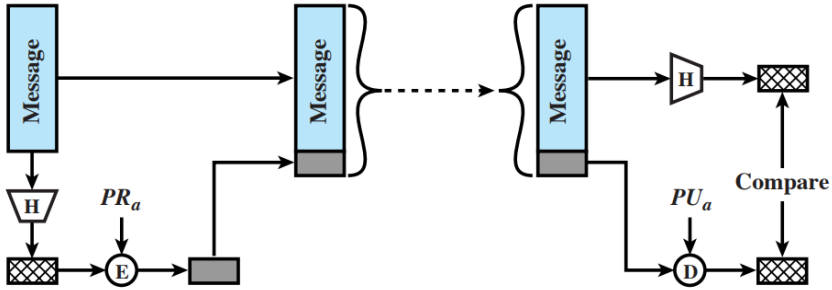


Figura: Criptografia assimétrica do hash (STALLINGS; BROWN, 2015).

- É possível usar uma função de hash, mas não a encriptação para autenticação de mensagem. A técnica considera que as duas partes se comunicando compartilham um valor secreto comum. A calcula o valor de hash sobre a concatenação de M e S, e anexa o valor de hash resultante a M. Como B possui S, ele pode recalcular o valor de hash para verificar. Como o valor secreto em si não é enviado, um oponente não pode modificar uma mensagem interceptada e não pode gerar uma mensagem falsa.

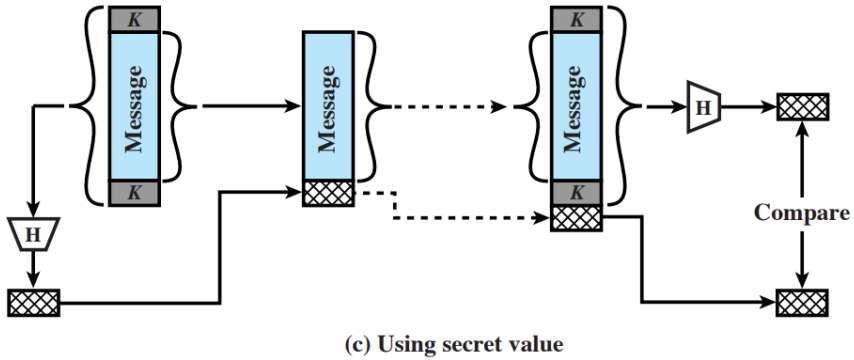


Figura: Criptografia simétrica de hash e valor secreto (STALLINGS; BROWN, 2015).

- A confidencialidade pode ser acrescentada à abordagem do método (c) encriptando a mensagem inteira mais o código de hash.

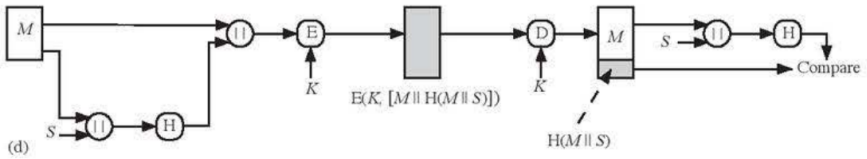


Figura: Criptografia simétrica de hash, valor secreto e mensagem (Stallings, 2020).

- A autenticação de mensagem é normalmente alcançada usando um código de autenticação de mensagem (MAC), também conhecido como função de hash chaveada.
- MACs são usados entre duas partes que compartilham uma chave secreta para autenticar informações trocadas entre elas.
- Uma função MAC recebe como entrada:
  - uma chave secreta, e
  - um bloco de dados,

  e produz um valor de hash conhecido como MAC, que é associado à mensagem protegida.
- Para verificar a integridade da mensagem:
  - aplica-se novamente a função MAC à mensagem, e
  - compara-se o resultado com o MAC associado.
- Um invasor não pode alterar a mensagem e o valor MAC sem conhecer a chave secreta.

- A parte que verifica também sabe quem é a emissora, pois somente quem conhece a chave secreta pode produzir o MAC válido.
- A combinação de hashing e encriptação pode resultar em uma função geral que, na prática, é um MAC, conforme a expressão:

$$E(K, H(M))$$

onde:

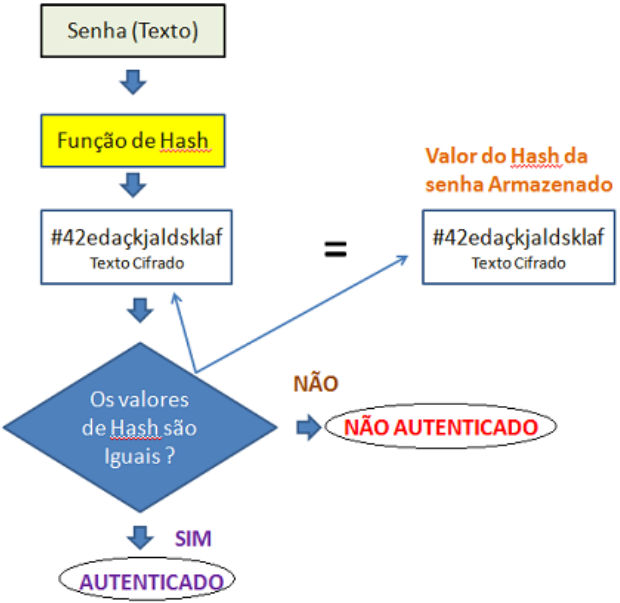
  - M = mensagem de tamanho variável,
  - K = chave secreta,
  - saída = valor de tamanho fixo protegido contra adversários.

- Na prática, algoritmos MAC específicos são criados, geralmente mais eficientes do que algoritmos de encriptação tradicionais.

Outras Aplicações de Hash I

- **Senhas**:
  - Armazena-se o hash da senha, não a senha real.
  - O sistema compara o hash da senha digitada com o hash armazenado.
  - Protege contra vazamento direto de credenciais.
- **Detecção de intrusão**:
  - Armazena-se H(F) para cada arquivo, em local seguro.
  - Posteriormente, recalcula-se H(F) para verificar alterações.
  - Um intruso teria que alterar F sem alterar H(F).
- **Bases de dados de malware**: empresas de antivírus mantêm bancos de dados de hashes de arquivos maliciosos conhecidos (malware signatures).

Outras Aplicações de Hash II



Assinatura Digital

- É uma aplicação de hash + criptografia assimétrica.
- Garante:
  - **Autenticidade**: confirma o autor;
  - **Integridade**: assegura que o conteúdo não foi alterado;
  - **Não repúdio**: o autor não pode negar a autoria.

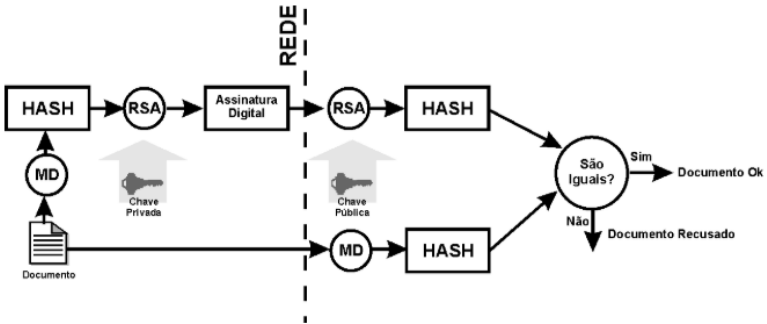


Figura: Fluxo de assinatura digital (Schneier, 2015).

Assinatura Digital III

- A criptografia de chave pública pode ser usada para autenticação. Suponha que Bob queira enviar uma mensagem a Alice.
- Embora não seja importante mantê-la em segredo, Bob quer que Alice tenha certeza de que a mensagem vem realmente dele.
- Para isso, Bob:
  - usa uma função de hash segura (ex.: SHA-512) para gerar um valor de hash da mensagem;
  - cifra o código de hash com sua chave privada, criando uma assinatura digital;
  - envia a mensagem com a assinatura anexada.
- Quando Alice recebe a mensagem e a assinatura, ela realiza:
  1. Calcula um valor de hash da mensagem.
  2. Decifra a assinatura usando a chave pública de Bob.
  3. Compara o valor de hash calculado com o valor de hash decifrado.

- Se os valores de hash forem iguais:
  - Alice tem certeza de que a mensagem foi assinada por Bob,
  - Ninguém mais possui a chave privada de Bob,
  - Ninguém mais poderia ter criado um texto cifrado que se decifra com a chave pública de Bob,
  - A mensagem está protegida contra alterações sem acesso à chave privada.
- A assinatura digital **não fornece confidencialidade**:

Certificados

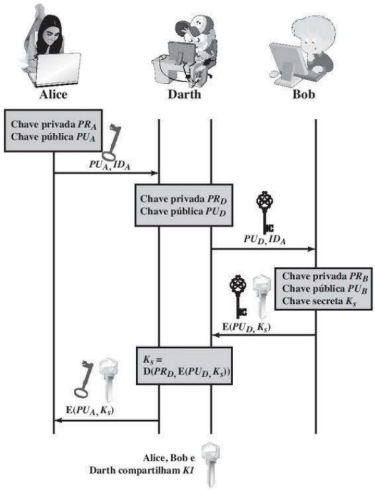


Figura: Ataque MITM na transmissão de chave públicas.

1. A gera um par de chaves pública/privada $[PU_A, PR_A]$ e transmite uma mensagem destinada a B consistindo em PU_A e um identificador de A, ID_A.
2. D intercepta a mensagem, cria seu próprio par de chaves pública/privada $[PU_D, PR_D]$ e transmite PU_D, ID_A para B.
3. B gera uma chave secreta K_s e transmite $E(PU_D, K_s)$.
4. D intercepta a mensagem e descobre K_s, calculando $D(PR_D, E(PU_D, K_s))$.
5. D transmite $E(PU_A, K_s)$ para A.

> *A força de qualquer sistema criptográfico está na técnica de distribuição de chave, um termo que se refere aos meios de entregar uma chave a duas partes que querem trocar dados, sem permitir que outros vejam a chave.*
>
> (Stallings, 2020)

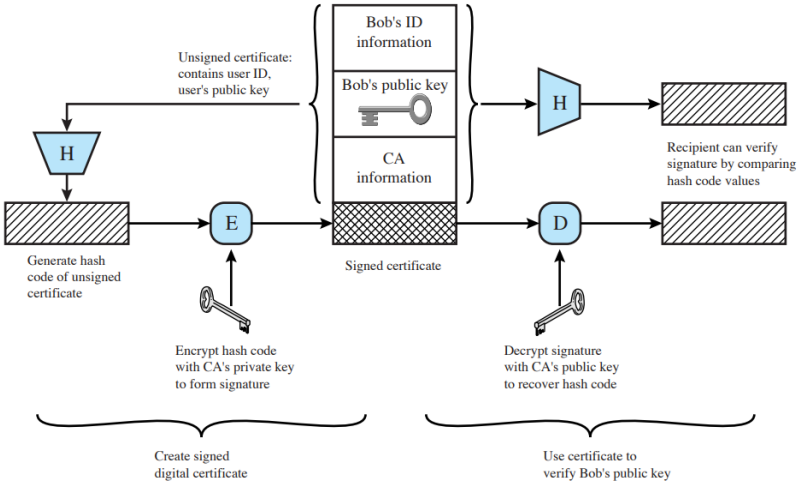


Figura: Certificado Digital (Schneier, 2015).

Certificados III

- O padrão X.509 é o formato amplamente aceito para certificados de chave pública.
- Certificados X.509 são utilizados na maioria das aplicações de segurança de rede.
- Entre as principais tecnologias que usam X.509 estão:
  - IP Security (IPsec),
  - Transport Layer Security (TLS),
  - Secure Shell (SSH),
  - Secure/Multipurpose Internet Mail Extension (S/MIME).

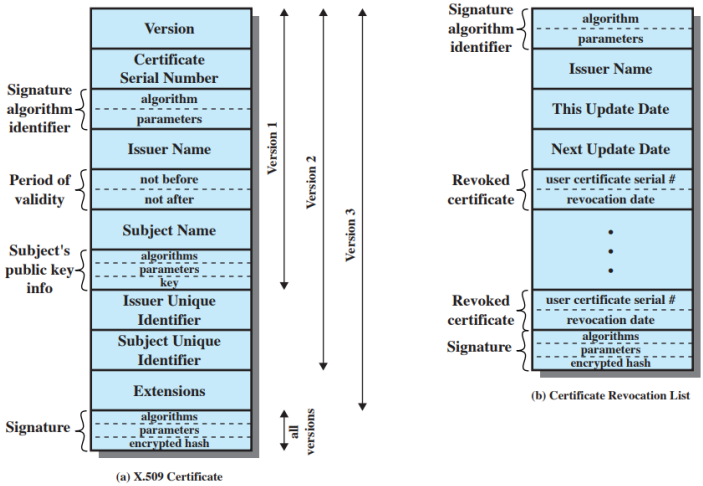


Figura: Padrão de certificados X.509.

Certificados V

1. Qualquer usuário com acesso à chave pública da CA pode verificar a chave pública do usuário, que foi certificada.
2. Nenhuma parte além da autoridade certificadora pode modificar o certificado sem que isso seja detectado.

```
# /etc/ssl/certs/
# /usr/share/ca-certificates/
# /etc/ssl/certs/ca-certificates.crt
```

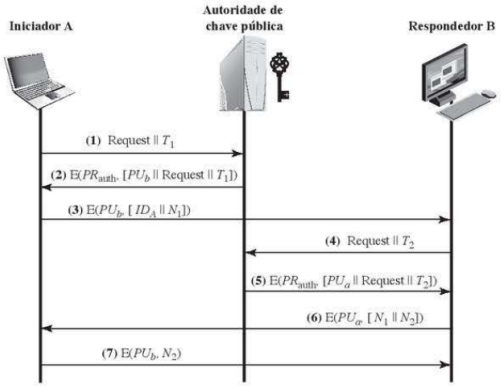


Figura: Distribuição de Chave Pública (**schneier2020**).

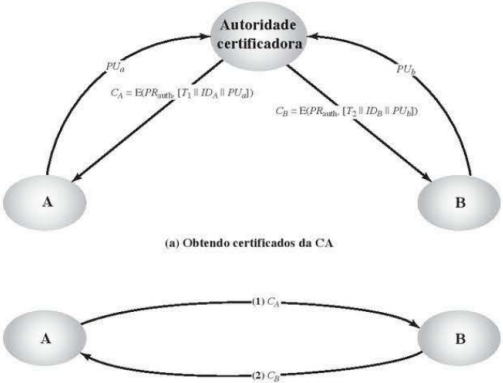


Figura: Troca de Certificados (**schneier2020**).

Atenção

O próprio servidor de diretório não é responsável pela criação das chaves públicas ou pela função de certificação; ele simplesmente oferece um local de fácil acesso para os usuários obterem certificado (Stallings, 2020).

Em Resumo:

- A particularidade da criptografia de chave pública é que a chave pública é, de fato, pública.
- Com um algoritmo amplamente aceito, como RSA:
  - qualquer participante pode enviar sua chave pública a outros,
  - ou divulgá-la amplamente à comunidade.

Autoridades Certificadoras (CAs) V

- Embora conveniente, isso apresenta uma fraqueza importante:
  - qualquer pessoa pode forjar um anúncio público de chave,
  - alguém pode fingir ser Bob e enviar uma chave pública falsa,
  - ou divulgar amplamente uma chave pública fraudulenta,
  - permitindo ao atacante:
    - ler mensagens cifradas enviadas a "Bob",
    - usar chaves falsificadas para autenticação,
    - explorar o golpe até que Bob descubra o problema e alerte os demais.
- A solução é o **certificado de chave pública**

Autoridades Certificadoras (CAs) VI

- Um certificado consiste em:
  - uma chave pública,
  - um ID de usuário do proprietário da chave,
  - o bloco inteiro assinado por uma terceira entidade confiável.
- O certificado também contém:
  - informações sobre a terceira entidade confiável,
  - e o período de validade do certificado.

Autoridades Certificadoras (CAs) VII

- A terceira entidade normalmente é uma **Autoridade Certificadora (CA)** confiada pela comunidade:
  - agência governamental,
  - instituição financeira,
  - ou outra entidade amplamente confiável.
- O processo funciona assim:
  - o usuário apresenta sua chave pública à CA de forma segura,
  - obtém um certificado assinado,
  - publica o certificado para uso geral.
- Quem precisar da chave pública do usuário:
  - obtém o certificado publicado,
  - verifica sua validade por meio da assinatura da CA,
  - garantindo autenticidade e proteção contra fraude.

PKI

A RFC 4949 (*Internet Security Glossary*) define a infraestrutura de chave pública (PKI, do acrônimo em inglês para *Public-Key Infrastructure*) como o conjunto de hardware, software, pessoas, políticas e procedimentos necessários para criar, gerenciar, armazenar, distribuir e revogar certificados digitais com base na criptografia assimétrica.

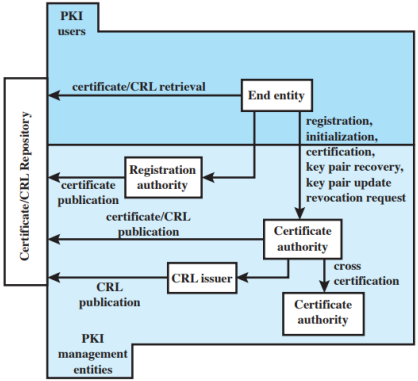


Figura: Infraestrutura de Chaves Públicas - PKI.

- Validam a identidade de usuários e entidades.
- Emitem certificados digitais baseados no padrão X.509.
- No Brasil, fazem parte da **ICP-Brasil**.

ICP BRASIL

CLIQUE AQUI.

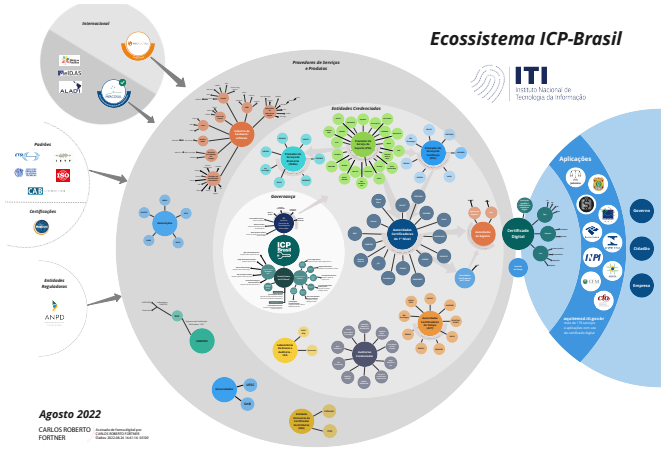


Figura: Infraestrutura de Chaves Públicas do Brasil (ICP Brasil).

Protocolos

Kerberos é um sistema de autenticação baseado em um servidor centralizado e seguro.

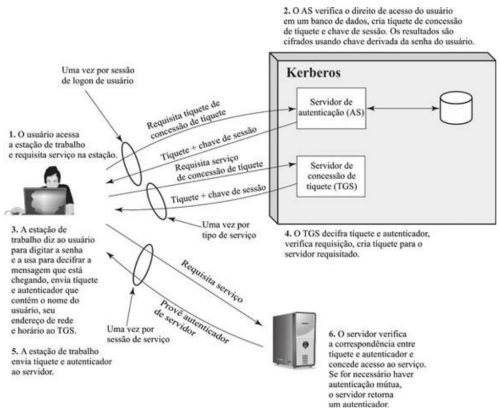


Figura: Autenticação Kerberos (Stallings, 2020).

- **MIME**: Extensão do padrão de e-mail que permite enviar anexos, imagens, áudio, vídeo e conteúdo em diferentes formatos além de texto simples.
- **S/MIME**: Padrão que usa criptografia e assinatura digital para garantir confidencialidade, autenticidade e integridade em e-mails.
- **DKIM**: Mecanismo que usa assinatura digital baseada em DNS para verificar se o e-mail realmente veio do domínio que afirma enviá-lo e que não foi alterado.

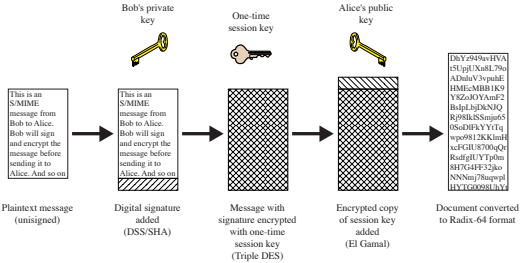


Figure 21.6 Typical S/MIME Process

Figura: S/MIME (STALLINGS; BROWN, 2015).

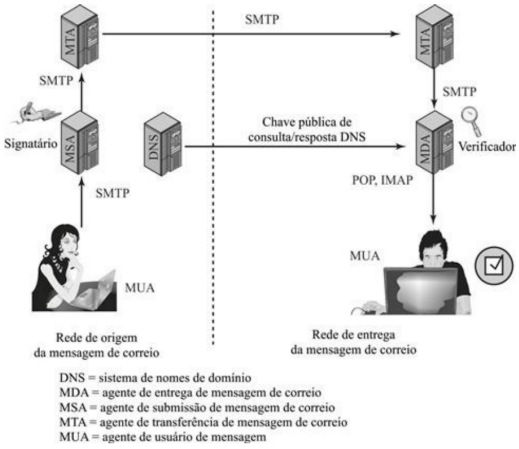


Figura: DKIM (STALLINGS; BROWN, 2015).

- **Active Directory (AD)** É uma solução da Microsoft que provê serviços de diretório para redes — inclui autenticação, autorização, armazenamento de usuários, grupos e políticas. AD é o serviço global na rede corporativa: "quem são os usuários", "quem pode fazer o quê", políticas de grupo etc. Ele suporta protocolos como Kerberos e LDAP.
- **Kerberos** Focado estritamente em autenticação: garante que o usuário é quem ele diz ser, utilizando tickets emitidos e validados.
- **LDAP** Voltado para acesso ao diretório: recuperar informações de usuários e grupos, buscar "quem está em qual grupo", verificar atributos e, em alguns casos, autenticar via *bind*.

Atenção!

O SSL não é um protocolo único, mas sim duas camadas de protocolos.

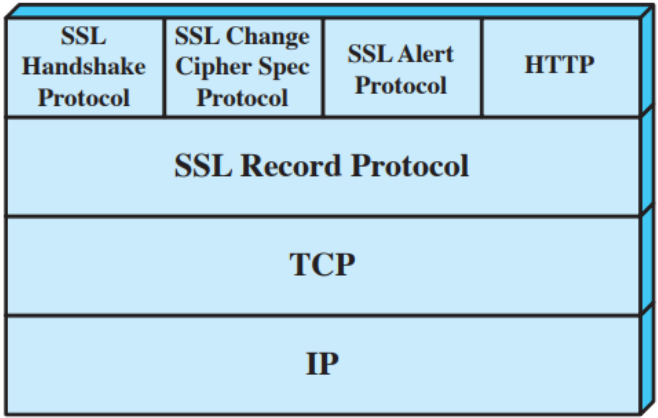


Figura: Cabeçalho SSL (STALLINGS; BROWN, 2015).

Protocolo / Conceito	Função Resumida
SSL Record Protocol	Camada base do SSL; provê **confidencialidade** (cifração simétrica) e **integridade** (MAC); fragmenta, comprime (opcional) e encapsula dados.
Handshake Protocol	Realiza **autenticação**, **negociação de algoritmos** e **estabelecimento de chaves**; cria a **sessão SSL**.
Change Cipher Spec Protocol	Envia mensagem única (valor 1) para ativar a **CipherSpec** negociada, movendo o estado pendente para o atual.
Alert Protocol	Envia alertas de erro ou evento: **warning** ou **fatal**; alertas fatais encerram a conexão.
Sessão SSL	Associação segura contendo **parâmetros criptográficos** compartilhados; pode ser reutilizada, evitando renegociação.
Conexão SSL	Canal temporário e seguro; usa parâmetros da sessão; uma sessão pode ter **múltiplas conexões**.

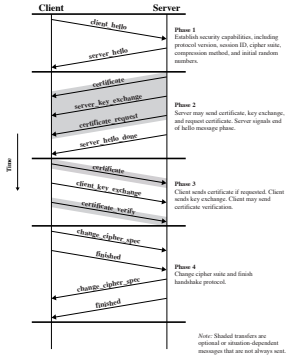


Figure 21.3 Handshake Protocol Action

Figura: Procolo de Apresentação (STALLINGS; BROWN, 2015).

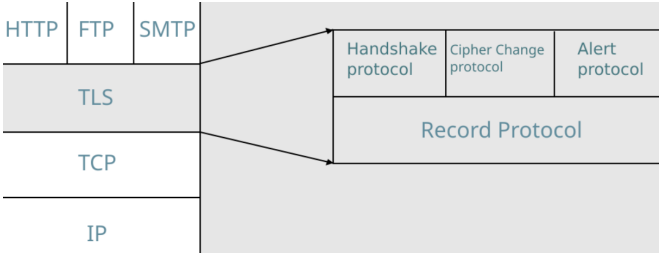


Figura: TLS

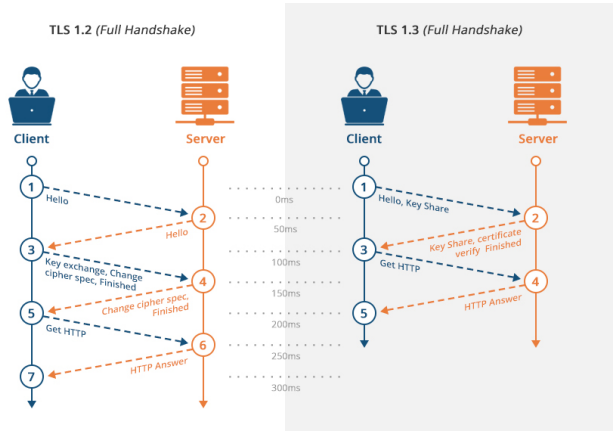


Figura: TLS 1.2 vs TLS 1.3

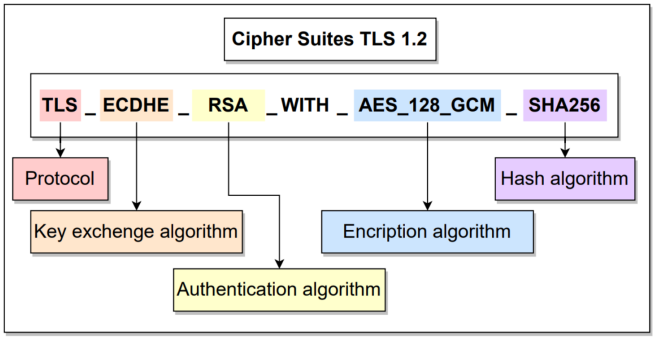
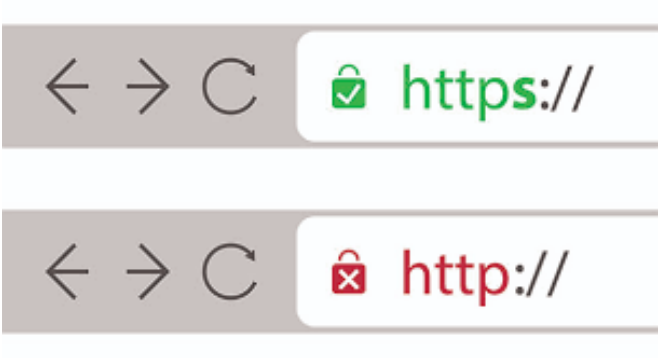
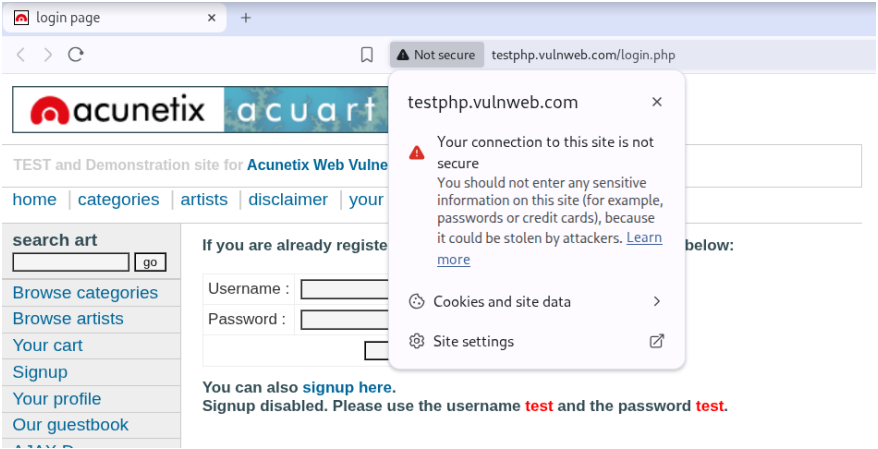


Figura: Cipher Suite

- O HTTPS é a combinação do protocolo HTTP com o SSL/TLS para criar uma conexão segura entre navegador e servidor Web.
- Todos os navegadores modernos suportam HTTPS, mas isso depende de o servidor Web também oferecer suporte ao protocolo seguro.
- Para o usuário, a principal diferença visível é que o endereço começa com `https://` em vez de `http://`.
- Conexões HTTP usam a porta 80, enquanto conexões HTTPS utilizam a porta 443, que ativa o SSL/TLS.

- Quando o HTTPS é utilizado, são cifrados:
  - a URL do documento requisitado;
  - o conteúdo do documento;
  - os dados enviados por formulários;
  - os cookies enviados entre navegador e servidor;
  - o conteúdo dos cabeçalhos HTTP.
- O HTTPS é definido na RFC 2818 (HTTP Over TLS) e funciona igualmente tanto com SSL quanto com TLS.

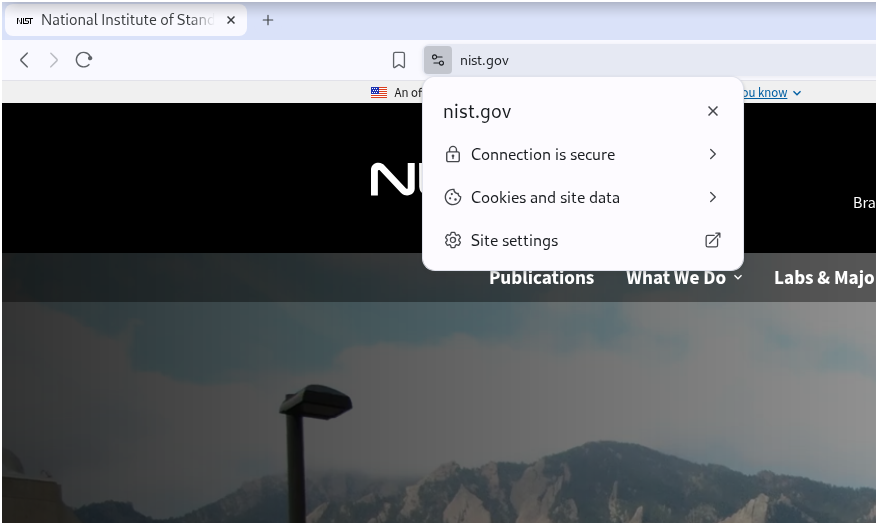


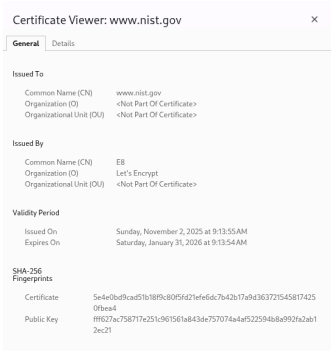


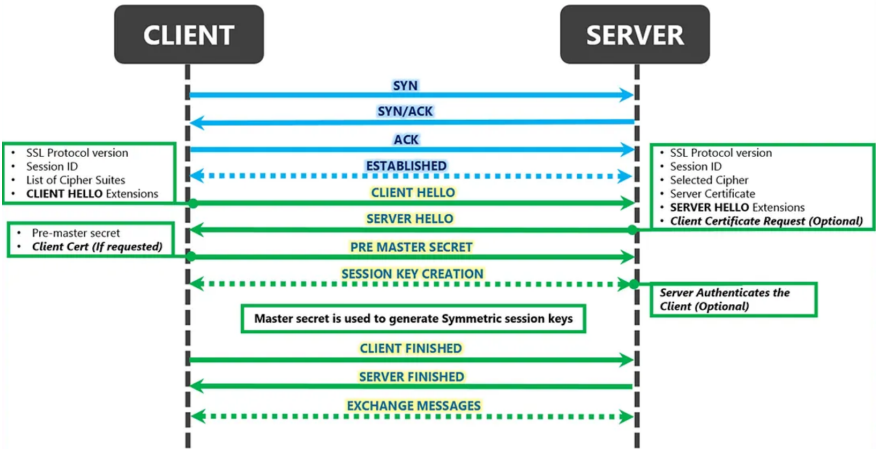
SITE HTTP!

CLIQUE AQUI.

Use o Wireshark para visualizar os pacotes HTTP e HTTPS.







- O IPSec provê comunicações seguras em redes locais (LAN), WANs privadas e públicas, além da própria Internet.
- Exemplos de uso:
  - Conectividade segura entre escritórios e filiais de uma empresa.
  - Acesso remoto seguro pela Internet.

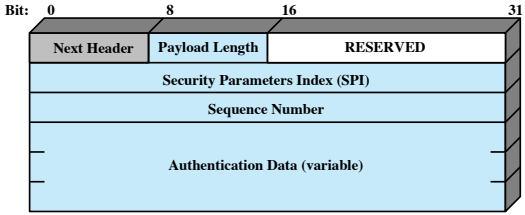


Figure 21.4 IPSec Authentication Header

Figura: Cabeçalho IP Sec (STALLINGS; BROWN, 2015).

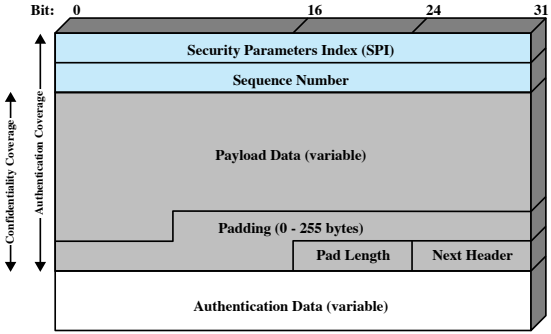


Figure 21.5 IPSec ESP Format

Figura: Cabeçalho ESP (STALLINGS; BROWN, 2015).

BISHOP, Matt. **Computer Security: Art and Science**. 2. ed. Boston, MA: Addison-Wesley, 2018.

STALLINGS, William. **Cryptography and Network Security: Principles and Practice**. 8. ed. [*S. l.*]: Pearson, 2020.

STALLINGS, William; BROWN, Lawrie. **Computer security: principles and practice**. 1. ed. São Paulo: Pearson Prentice Hall, 2015. p. 492. ISBN 9788576051190.

Licença