

# Criptografia - aplicações

**Segurança da Informação**

**Curso Técnico em Redes de Computadores**

**ETER – FAETEC - Rio de Janeiro - RJ**

# Criptografia aplicada.

- Segundo a norma ISO 27001, os princípios da **confidencialidade**, **integridade** e **disponibilidade** são princípios básicos; **autenticidade** e o **não repúdio** (ou irrevocabilidade) são princípios secundários.
- Algumas questões pertinentes são:
  - Quais princípios são garantidos, e por qual tipo de criptografia;
  - Em que ordem cada um deve ser usado, e por quê;
  - Entre outras questões.

# Criptografia x Confidencialidade

- **Confidencialidade** é garantida quando a informação só pode ser vista por quem pode ter *acesso legítimo* à mesma, o que pode ser fornecido pelas criptografias, tanto simétrica quanto a assimétrica.
- Na criptografia assimétrica, a cifragem é feita pela chave pública e a decifragem, pela chave privada.
- A criptografia simétrica é mais rápida (uma chave apenas para cifrar e decifrar), mas a segurança depende de como a chave é compartilhada.

# Criptografia x Integridade.

- **Integridade** é garantida quando a informação *não é alterada* entre a origem e o destino, o que pode ser garantido pelas funções de hash, que é tido como o mais eficaz e eficiente.
- As funções de hash geram os hashes e os enviam juntamente com a mensagem. O receptor deve calcular o hash com a mesma função e comparar os resultados: Se estiver igual, a informação é íntegra. Se não, a integridade foi comprometida.
- Mas um atacante pode comprometer a mensagem e o hash. Logo, é comum cifrarem o hash com criptografia.

# Criptografia x Disponibilidade.

- **Disponibilidade** é acessibilidade da informação para os seus usuários, sempre sempre que ela for necessária.
- Este é o único princípio que a criptografia não traz garantias, visto que ela depende de fatores como hardware, software, processos e pessoas, não só mitigar ataques a ativos.

# Criptografia x Autenticidade e não repúdio.

- **Autenticidade** é a garantia de que a informação pertence ao emissor legítimo.
- O **não repúdio** (irretratabilidade) é consequência direta da autenticidade, visto que quem gerou esta informação, não pode ter como negá-la.
- Logo, ambas estão ligadas, sob perspectivas diferentes.

# Criptografia x Autenticidade e não repúdio.

- Logo, é possível garantir a autenticidade com criptografia. Apesar de exemplos usando criptografia simétrica, é muito mais comum usando criptografia assimétrica.

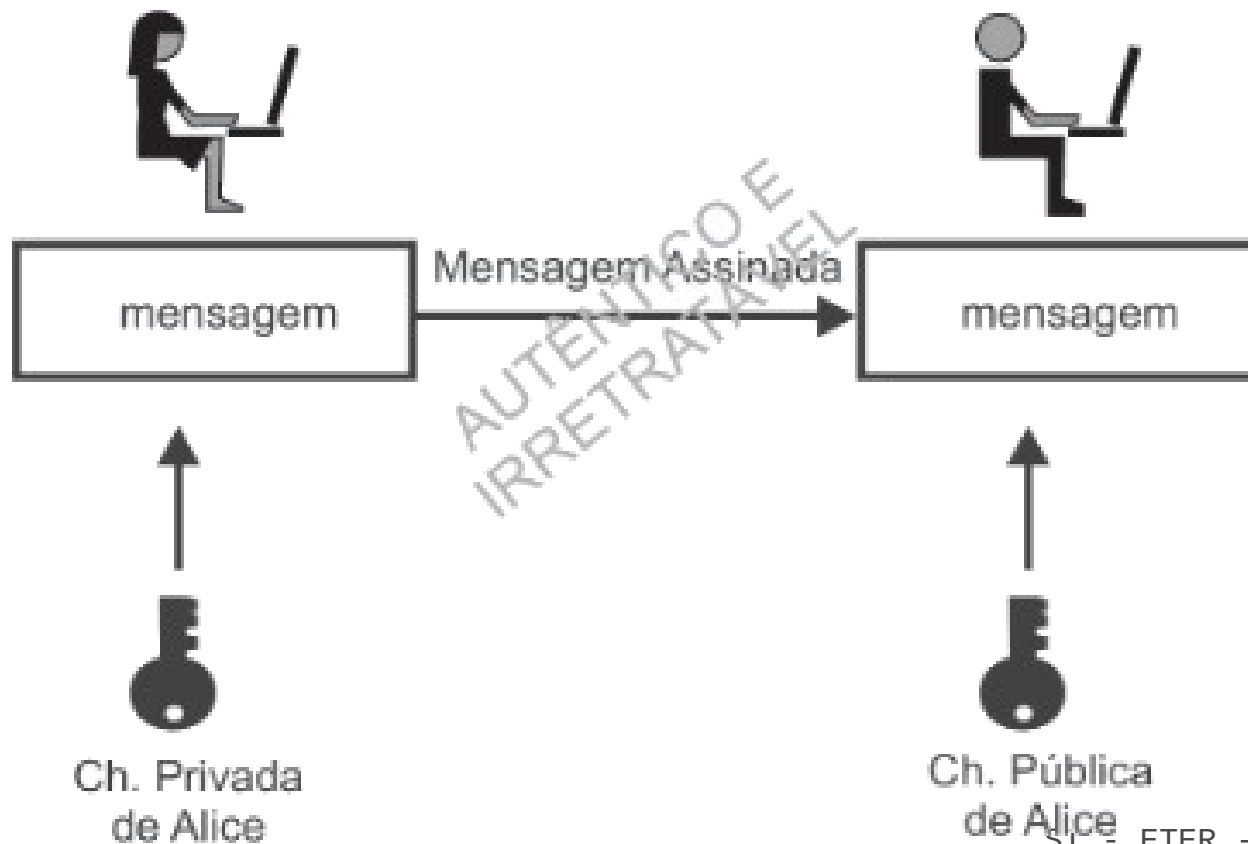
# Assinaturas e cartórios.

- Assinar um documento consiste em validar as informações contidas nesse documento.
- No mundo real, assinaturas podem ser falsificadas, assim como o inteiro teor dos documentos. Para evitar isto, existem os sistemas de cartórios, que dão fé pública, autenticando documentos, reconhecendo firmas, etc.

# Assinatura digital.

- No meio digital, não é possível distinguir uma cópia do seu original, e nem vamos falar de NFTs... Afinal, para o computador, tanto o original quanto a cópia são duas sequências de bytes idênticas.
- **Assinatura digital**, então, no conceito da criptografia assimétrica, consiste em usar a chave privada do remetente para cifrar a mensagem.
- Dessa forma, a *autenticidade* é garantida (foi usada a chave privada para cifrar), assim como o *não repúdio* (não é possível negar a sua autoria).

# Assinatura digital.



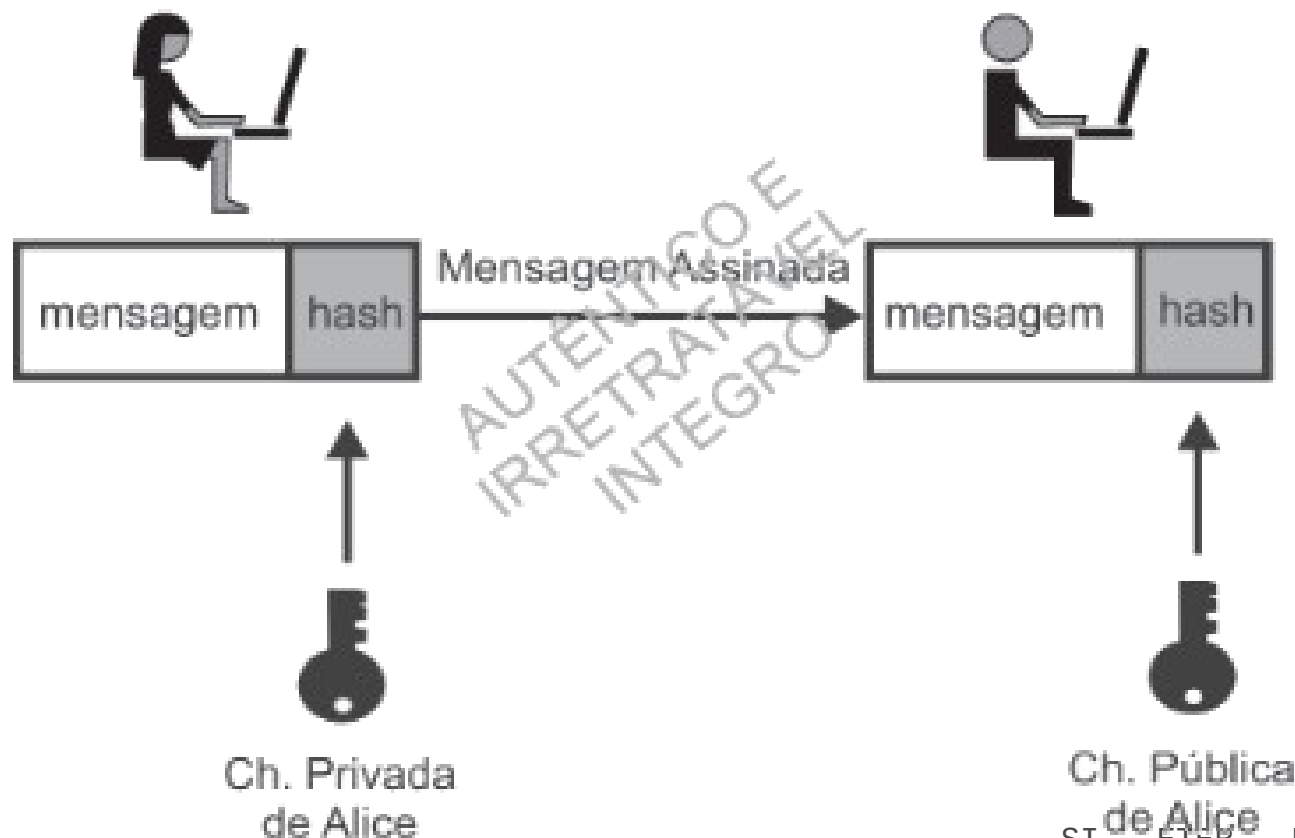
# Assinatura digital.

- Na prática, para “ganhar tempo”, as aplicações não assinam digitalmente **toda** a informação – afinal, criptografia assimétrica é mais lenta.
- O que as aplicações fazem é calcular o hash da informação e usar a chave privada do remetente para cifrar o hash.

# Vantagens e desvantagens.

- Feito desta forma, é um processo mais rápido, além de garantir autenticidade, o não repúdio e a integridade do documento.
- Mas ainda assim, a confidencialidade do documento não está garantida: Se apenas estes procedimentos forem feitos, qualquer um pode ler a mensagem.

# Como funciona a assinatura digital?

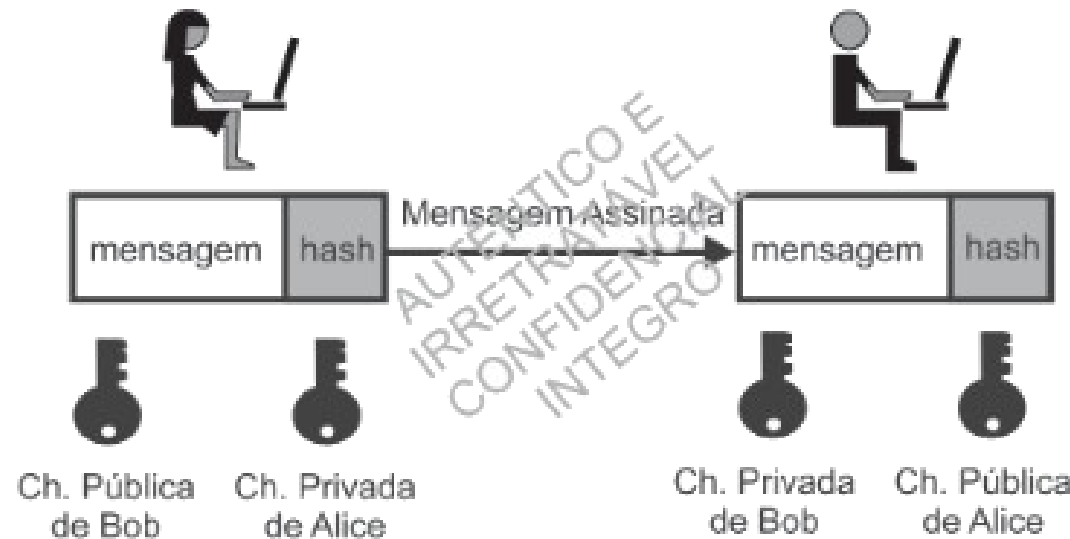


# Sessões de criptografia.

- Como garantir confidencialidade, integridade, não repúdio e autenticidade simultaneamente?
- Isto é obtido com sistemas que fazem uso de funções hash, criptografias simétrica e assimétrica, tudo ao mesmo tempo.
- Veremos aqui alguns exemplos, que são na prática, a base para aplicações comerciais que usam criptografia.

# Confidencialidade com criptografia assimétrica.

- Uma maneira de garantir a confidencialidade é cifrar a mensagem a ser enviada com a chave pública do receptor, e o hash com a chave privada do transmissor.
- Vale lembrar que criptografia assimétrica é mais lenta, o que pode causar uma perda de eficiência.



# Confidencialidade com criptografia assimétrica.

- Sequência de passos feitos pelo **remetente** são:
  - 1) Calcular o hash da mensagem;
  - 2) Usar sua chave privada para cifrar o hash;
  - 3) Usar a chave pública do receptor para cifrar a mensagem.
- Sequência de passos feitos pelo **destinatário** são:
  - 1) Usar sua chave privada para decifrar a mensagem;
  - 2) Usar a chave pública do remetente para decifrar o hash;
  - 3) Calcular o hash da mensagem;
  - 4) Comparar o hash calculado com o hash que foi recebido.

# Confidencialidade com criptografia simétrica.

- O uso de criptografia simétrica para garantir confidencialidade é criptografia assimétrica para garantir autenticidade e não repúdio.
- É uma solução mais eficiente, mas aqui volta o problema de compartilhar a chave secreta usada pelos algoritmos simétricos.
- Um modo seria o remetente gerar a chave simétrica e enviá-la para o destinatário de uma forma segura, como por exemplo, usando criptografia assimétrica.

# E-mail seguro (PGP).

- O Pretty Good Privacy, ou PGP (em português: *privacidade muito boa*), é um software de criptografia que fornece autenticação e privacidade criptográfica para comunicação de dados.
- É muito usado para assinar, cifrar e decifrar textos, e-mails, arquivos, diretórios e partições inteiras de disco e para incrementar a segurança de comunicações via e-mail. Foi desenvolvido por Phil Zimmermann em 1991.



# E-mail seguro (PGP).

- O PGP é um software livre, e foi distribuído via Internet. Isto deu origem a uma batalha judicial travada entre o governo dos EUA e Phil Zimmerman que durou três anos.
- Nos anos 1990, algoritmos de criptografia com chaves acima de um certo tamanho de chave eram considerados **armas de guerra**, e Phil Zimmerman foi investigado sobre uma possível violação do direito à exportação de software de criptografia nos Estados Unidos.
- Hoje o PGP deu origem ao OpenPGP, que está documentado na RFC 4880.

# PGP.

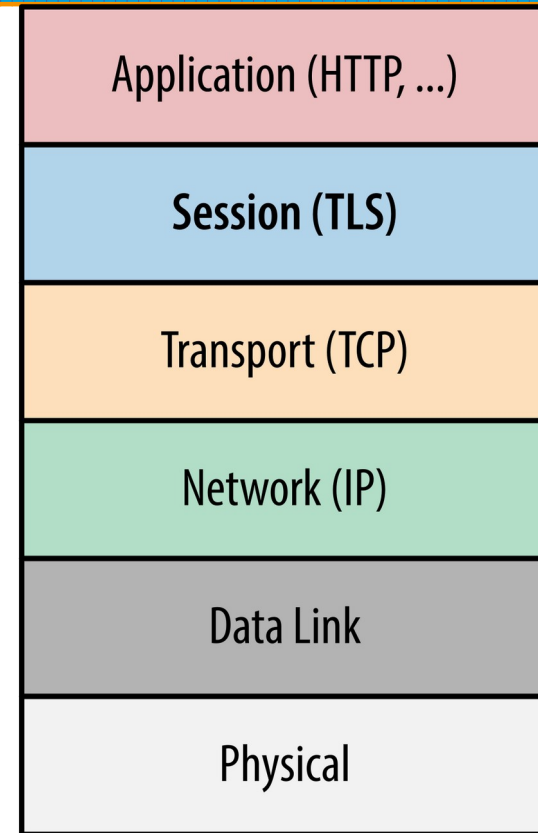
- O PGP usava o protocolo IDEA, para criptografia simétrica; RSA como protocolo de criptografia assimétrica; MD5 como função de hash.
- Ele trabalhava na seguinte forma:
  - 1) Cálculo do hash da mensagem;
  - 2) Mensagem seria assinada com a chave privada do remetente.
  - 3) Assinatura concatenada à mensagem.
  - 4) A mensagem e o hash assinado eram compactados.
  - 5) A criptografia simétrica era usada para cifrar o texto da mensagem e seu hash.
- Isso garantia confidencialidade e eficiência.

# S/MIME.

- MIME (Multipurpose Internet Mail Extensions) é um padrão de formatação de mensagens de correio eletrônico. A maior parte das mensagens são enviadas usando o protocolo SMTP e usando o MIME para formatar a mensagem.
- O formato S/MIME (Secure MIME) é uma extensão, que permite o uso de criptografia. Ele foi criado pela RSA Data Security, e tornado padrão em 1999. Sua especificação está descrita nos RFCs 2632 e 2633.
- Graças a esse padrão, o cliente de e-mail pode gerenciar chaves e protocolos, escolhendo tamanho de chaves, funções hash, protocolos de criptografia, entre outros.

# SSL.

- O Secure Socket Layer (SSL) é um conjunto de diretrizes que especificam uma camada adicional na arquitetura TCP/IP, localizada entre as camadas de transporte e aplicação. É a **camada de sessão**, exibida ao lado.
- Dessa forma, várias aplicações podem se beneficiar do uso de criptografia sem precisar fazer mudanças nos protocolos, como navegação segura através de navegadores, transferência de arquivos, leitura de e-mails, etc.



# TLS.

- A 1<sup>a</sup> versão do SSL foi feita pela Netscape em 1994, e a 3<sup>a</sup> versão já saiu em 1996.
- O Transport Layer Security (TLS) é um protocolo feito a partir do SSL e aprovado por instituições financeiras de todo o mundo. A versão atual é a 1.1, documentada na RFC 4346, de 2006.
- Na prática, há poucas diferenças entre o TLS e o SSL.

# Etapas do SSL.

- São 4 fases, para estabelecer a conexão segura.
  - Fase 1: O cliente envia uma mensagem inicial, e o servidor responde. Esta mensagem inicia a negociação (*handshake*, ou aperto de mãos), e carregam informações que mais tarde serão usadas para gerar uma chave de sessão.

# Etapas do SSL (fase 2).

- Fase 2: O servidor se anuncia ao cliente, enviando um certificado com a sua chave pública. O cliente deve validar o certificado, verificando se a sua assinatura digital veio de uma autoridade certificadora na qual ele confia.
- Logo, se o cliente não tiver a chave para decifrar o hash da assinatura, ele considera o certificado inválido e alerta o usuário a respeito da invalidade desse certificado.

# Exemplo de uma mensagem de alerta.



## Esta conexão não é confiável

Você solicitou que o Firefox conecte-se de forma segura a: [redacted]. Porém, não foi possível confirmar a segurança da sua conexão.

Normalmente, quando você tenta conecta-se de forma segura, os sites apresentarão uma identificação confiável para comprovar que você está indo ao lugar certo. Entretanto, a identidade deste site não pôde ser atestada.

### O que devo fazer?

Se você habitualmente conecta-se sem problemas a este site, este erro pode significar que alguém está tentando se passar por ele. Você não deve continuar.

Me tire daqui!

### ► Detalhes técnicos

### ▼ Entendo os riscos

Se você entender o que está acontecendo, pode instruir o Firefox a confiar na identificação deste site. **Mesmo que você confie neste site, este erro pode significar que alguém está interceptando sua conexão.**

Não adicione uma exceção a menos que você saiba que exista uma boa razão para este site não usar uma identificação confiável.

Adicionar exceção...

# Etapas do SSL (fase 3).

- Fase 3: Agora, o cliente envia o seu certificado para o servidor, para que seja validado. Esta configuração é feita diretamente no servidor Web (Apache, nginx, etc).
- Obs: Há situações que não faz sentido solicitar o certificado do cliente. Afinal, dessa forma certos sites só seriam acessíveis por pessoas cujos navegadores usassem certificados digitais. Isto inviabilizaria o acesso da maioria das pessoas, quando o que se quer – normalmente – é que muita gente acesse seu site.

# Etapas do SSL (fase 4).

- Fase 4: Aqui a negociação se encerra, com ambas as partes (cliente e servidor) chegando a um acordo com relação aos parâmetros que serão usados na sessão: protocolos, algoritmos, tamanhos de chave, etc.
- O cliente envia as suas capacidades através de mensagens de especificação de criptografia. O servidor determina as especificações da sessão escolhendo, dentre as que forem suportadas pelo cliente, as que são mais seguras.
- Por exemplo, se o cliente informa que consegue trabalhar com DES-64, DES-128, 3DES-128, AES-128 e AES-256, o servidor responde escolhendo AES-256.

# Conclusão.

- A criptografia é uma aliada para resolver problemas crônicos de segurança na Internet.
- É importante que o administrador da rede conheça as técnicas de criptografia empregadas, pois são usadas em conjunto com as aplicações.
- Tudo gira em torno do mesmo modo operacional: *criptografia assimétrica para assinatura, criptografia simétrica para esconder e funções de hash para assinar*. Se olharmos o PGP (1991) e o TLS (2006), usado nas sessões SSL, verá que é basicamente isto.

# Resumo.

- Integridade é garantida com hash; confidencialidade, com criptografia simétrica; autenticidade e não repúdio, com criptografia assimétrica.
- A criptografia simétrica é mais rápida que a assimétrica.
- Assinatura digital é o processo pelo qual uma chave privada é aplicada a um conteúdo qualquer: normalmente ela é usada para assinar hashes.
- Geralmente uma sessão de criptografia típica utiliza um protocolo de criptografia assimétrica (RSA etc.), um de criptografia simétrica (AES, 3DES etc.), uma função de hash, uma chave de sessão, certificados digitais etc.
- O PGP foi a primeira solução de e-mail seguro mundialmente conhecida. Inventado por Philip Zimmermann em 1991, gerou polêmica e deu origem a boas iniciativas na área.
- O S/MIME permite que os clientes de correio eletrônico utilizem criptografia.
- O SSL permite que aplicações TCP/IP utilizem criptografia.