FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

4SEG – SEGURANÇA DE REDES
AULA 2

Profa. Maria Cláudia Roenick Guimarães
E-mail: maria.roenick@faeterj-rio.edu.br

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Segurança da Informação

- Definições:
  - É a proteção da informação contra vários tipos de ameaças para garantir a continuidade, minimizar o risco, maximizar o retorno sobre os investimentos e as oportunidades do negócio;
  - Trata-se da proteção, dispensada aos dados e informações, contra ações não autorizadas relativas à divulgação, transferência, modificação ou destruição destes, sejam estas ações intencionais ou acidentais;
  - Condição em que pessoas, instalações, equipamentos, sistemas básicos, sistemas aplicativos, dados, informações e outros recursos significativos encontram-se a salvo de desastres ou ameaças naturais, bem como de desastres ou ameaças causados pelo homem;
  - Sob o prisma legal: Garantir a exatidão, a integridade e a disponibilidade das informações da organização (ex: para o fisco) além de garantir a confidencialidade e a privacidade dos dados mantidos relativos a seus clientes, fornecedores e funcionários (ex: bancos).

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Perigos e Ataques contra a Informação

- Outro ponto relevante na implementação da Segurança da Informação é considerar que todo e qualquer dispositivo de rede pode ser invadido ou infectado por meio:
  - De falhas de configuração;
  - Da ação de códigos maliciosos;
  - Da exploração de vulnerabilidades;
  - De ataques de força bruta.

- Os principais dispositivos que são alvos de ataques são:
  - Roteadores: Ataques de acesso, de negação de serviço e alteração de roteamento;
  - Firewalls: Ataques semelhantes ao de roteador;
  - Switches: Ataques que afetam o fluxo de dados na rede interna;
  - Servidores: Ataques que permitam o comprometimento dos dados e acesso a outros dispositivos da rede.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Mecanismos de Segurança

- Os mecanismos de segurança indicados pelo X.800 da ITU-T são divididos em dois grupos: (1) os implementados em uma camada específica de protocolos, e (2) nos específicos a qualquer protocolo ou serviço de segurança em particular;

Tabela 1.3 Mecanismos de segurança (X.800)

MECANISMOS DE SEGURANÇA ESPECÍFICOS

Podem ser incorporados à camada de protocolo apropriada a fim de oferecer alguns dos serviços de segurança OSI.

Cifragem

O uso de algoritmos matemáticos para transformar os dados em um formato que não seja prontamente decifrável. A transformação e subseqüente recuperação dos dados depende de um algoritmo e zero ou mais chaves de criptografia.

Assinatura digital

Dados anexados a (ou uma transformação criptográfica de) uma unidade de dados que permite que um destinatário da unidade de dados comprove a origem e a integridade da unidade de dados e proteja-se contra falsificação (por exemplo, pelo destinatário).

Controle de acesso

Uma série de mecanismos que impõem direitos de acesso aos recursos.

Integridade de dados

Uma série de mecanismos utilizados para garantir a integridade de uma unidade de dados ou fluxo de unidades de dados.

Troca de informações de autenticação

Um mecanismo com o objetivo de garantir a identificação de uma entidade por meio da troca de informações.

Preenchimento de tráfego

A inserção de bits nas lacunas de um fluxo de dados para frustrar as tentativas de análise de tráfego.

Controle de roteamento

Permite a seleção de determinadas rotas fisicamente seguras para certos dados e permite mudanças de roteamento, especialmente quando existe suspeita de uma brecha de segurança.

Certificação

O uso de uma terceira entidade confiável para garantir certas propriedades de uma troca de dados.

MECANISMOS DE SEGURANÇA PERVASIVOS

Mecanismos que não são específicos a qualquer serviço de segurança OSI ou camada de protocolo específica.

Funcionalidade confiável

Aquela que é considerada como sendo correta em relação a alguns critérios (por exemplo, conforme estabelecido por uma política de segurança).

Rótulo de segurança

A marcação vinculada a um recurso (que pode ser uma unidade de dados) que nomeia ou designa os atributos de segurança desse recurso.

Detecção de evento

Detecção de eventos relevantes à segurança.

Registros de auditoria de segurança

Dados coletados e potencialmente utilizados para facilitar uma auditoria de segurança, que é uma revisão e exame independentes dos registros e atividades do sistema.

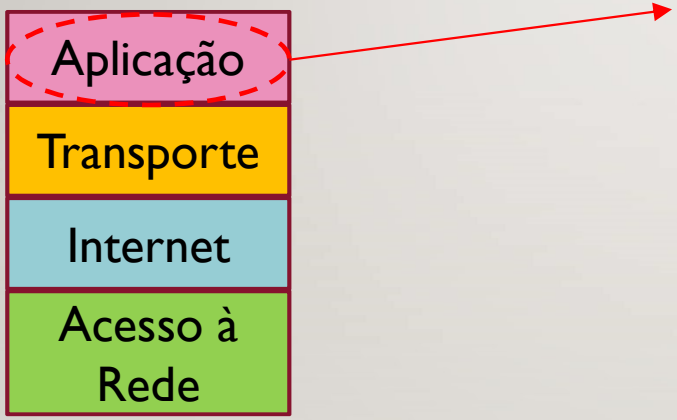
Recuperação de segurança

Lida com solicitações de mecanismos, como funções de tratamento e gerenciamento de eventos, e toma medidas de recuperação.

Fonte: STALLINGS, W. Criptografia e Segurança de Redes, 4ª Ed., São Paulo: Pearson Prentice Hall, 2008

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

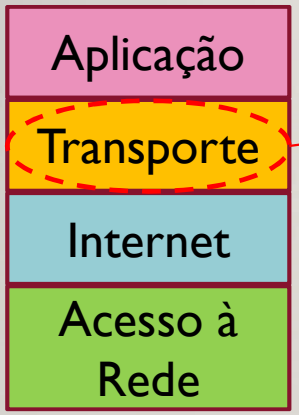
Riscos na Arquitetura TCP/IP



- Plugins para Browsers (ActiveX, Applets Java);
- Senhas enviadas sem criptografia (Telnet, POP);
- Vírus, Worms, Trojans;
- Bugs de software vulnerabilidade;
- Serviços iniciados como root (administrador do sistema);
- Vulnerabilidades em protocolos como SNMP, SSH, FTP, etc;
- Falha na configuração de serviços (FTP, HTTP).

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

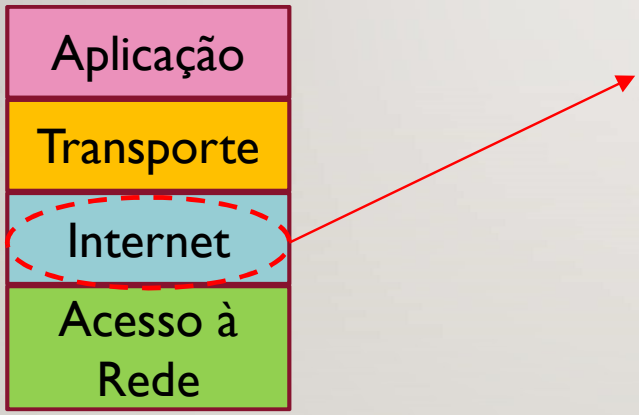
Riscos na Arquitetura TCP/IP



- Aplicações TCP, UDP (varredura de portas);
- Negação de Serviço (DoS / DDoS);

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

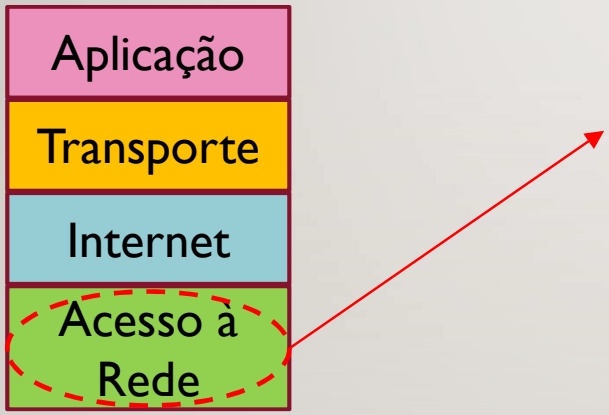
Riscos na Arquitetura TCP/IP



- Vulnerabilidades em roteadores;
  - Senha de administração fraca ou default ou em "branco"(sem senha);
  - Bugs no OS permitem "buffer overflow" (IOs).
- IP – Internet Protocol;
  - IPv4 não oferece confidencialidade;
  - Pacotes atravessam redes públicas ou do ISP.
- Firewalls mal configurados(filtro de pacotes, ACL);
- Vulnerabilidades nos protocolos de roteamento (RIP, BGP, OSPF, etc).

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Riscos na Arquitetura TCP/IP



- Vandalismo;
- Acesso cabos lógicos e de força, disjuntores;
- Acesso a equipamentos e racks distribuído no prédio;
- Manutenção na rede elétrica;
- Interferências.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Princípios de Comunicação Segura em Rede

- Uma mensagem deve ser transferida de uma parte para outra por meio de algum tipo de rede. As duas partes, também conhecidas como entidades principais dessa comunicação, cooperam para que a troca ocorra. Um canal de informação lógico é estabelecido definindo-se uma rota entre a origem e o destino e pela concordância em uso de protocolos comuns entre as partes.

- Os aspectos de segurança entram em cena quando é necessário ou desejável proteger a transmissão de informações de um oponente que pode representar uma ameaça à confidencialidade, autenticidade, etc. Todas as técnicas para oferecer segurança possuem dois componentes: (1) uma transformação relacionada à informação a ser enviada - criptografia da mensagem, autenticação do emissor, entre outras; e (2) uma informação secreta compartilhada pelos elementos principais e, espera-se, desconhecida do oponente - chave de criptografia compartilhada.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Princípios de Comunicação Segura em Rede

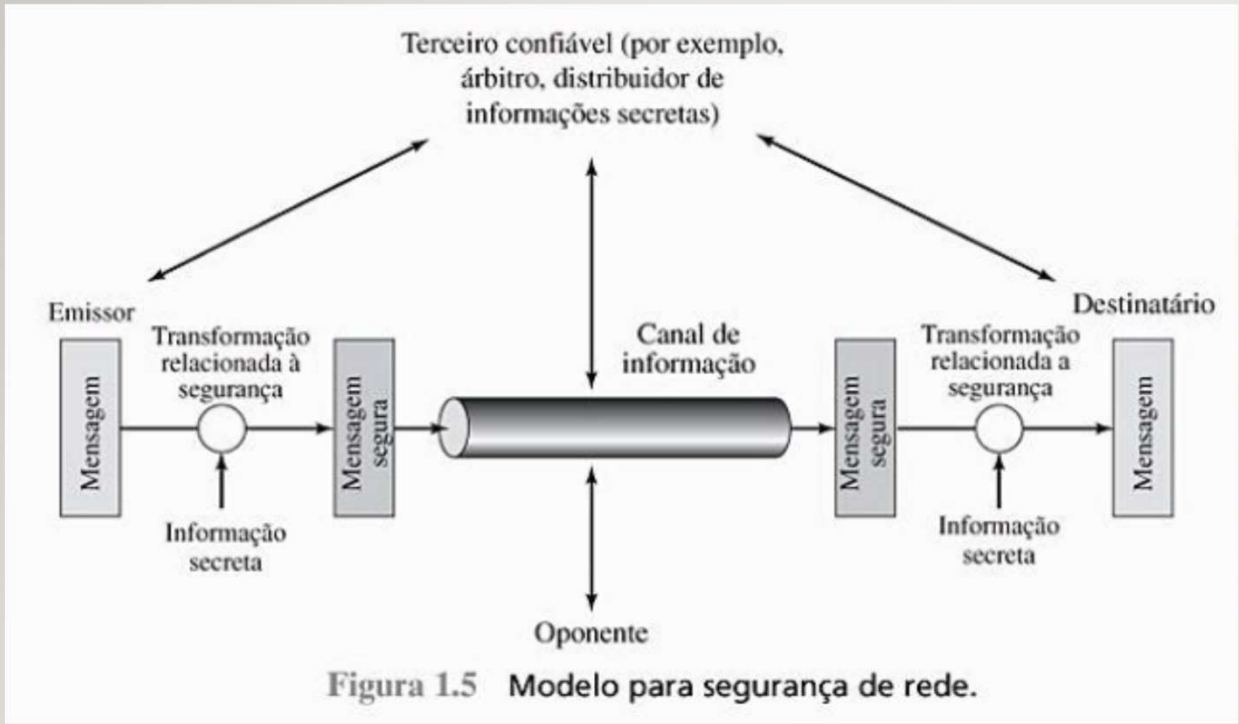


Figura 1.5 Modelo para segurança de rede.

- Um terceiro confiável pode ser necessário para se conseguir uma transmissão segura, como (1) ser responsável pela distribuição da informação secreta aos dois principais enquanto a protege contra qualquer oponente, ou (2) arbitrar disputas entre duas entidades principais em relação à autenticidade de uma transmissão de mensagem.

Fonte: STALLINGS, W. Criptografia e Segurança de Redes, 4ª Ed., São Paulo: Pearson Prentice Hall, 2008

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Noções de Criptografia

- A mensagem original, também conhecida como texto claro, passa por um processo de cifragem ou criptografia, que nada mais é um processo que converte o texto claro em texto cifrado, de forma a dificultar a leitura dos dados por aqueles não participam da comunicação;

- O processo de recuperação da mensagem original a partir do texto criptografado é conhecido como decifragem ou decriptografia;

- A área de estudos dos esquemas utilizados para criptografia chama-se Criptografia. As técnicas utilizadas para decifrar uma mensagem sem qualquer conhecimento dos detalhes de criptografia estão na área de Criptoanálise. As áreas da criptografia e criptoanálise juntas formam a Criptologia;

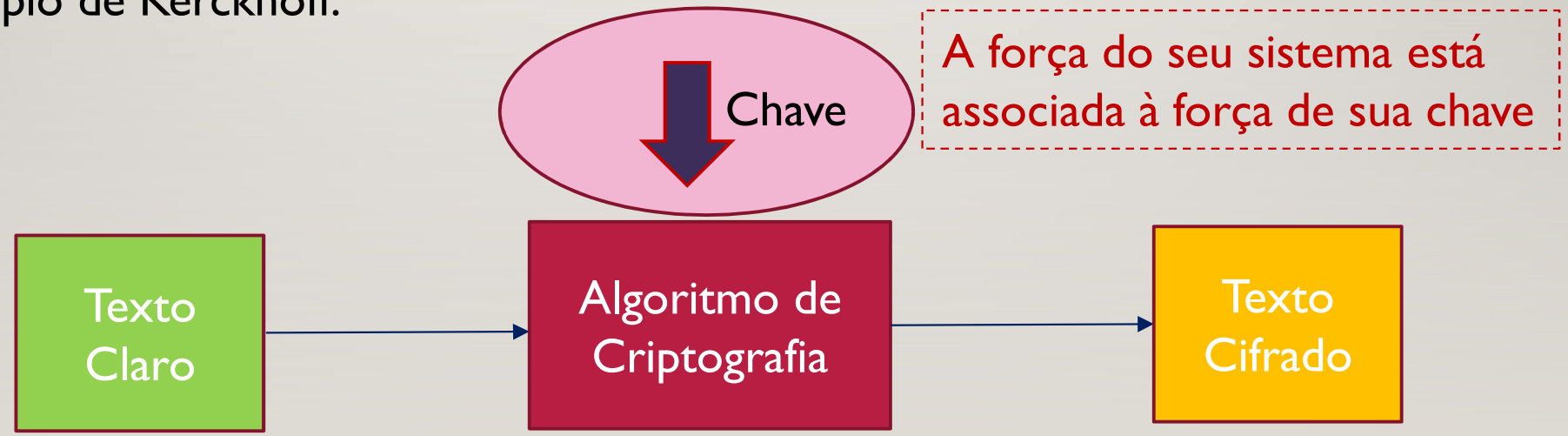
- Esteganografia é a ocultação de uma mensagem dentro de outra.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Noções de Criptografia

- Criptografia convencional ou simétrica: uso de mesma chave para criptografar e decriptografar a mensagem;
- Criptografia por chave pública ou assimétrica: uso de chaves diferentes para as etapas de criptografia e decriptografia da mensagem;

- Princípio de Kerckhoff:



Noções de Criptografia

- O padrão X.800 distingue os mecanismos de criptografia reversíveis e irreversíveis:
  - Um mecanismo de criptografia reversível é simplesmente um algoritmo de criptografia que permite que os dados sejam criptografados e subsequentemente decriptografados;
  - Mecanismos de criptografia irreversíveis incluem algoritmos de hash e códigos de autenticação de mensagem, que são usados em aplicações de assinatura digital e autenticação de mensagens.

- Os sistemas criptográficos são caracterizados por 3 dimensões diferentes:
  - tipo de operações utilizadas para transformar o texto claro em texto cifrado - métodos de substituição e transposição, podendo ser utilizados em vários estágios e combinações (sistemas de produtos);
  - número de chaves utilizadas;
  - modo como o texto claro é processado - cifra de bloco ou cifra de fluxo.

Noções de Criptografia

- A criptografia tem quatro objetivos principais:
  - Confidencialidade da Mensagem: só o destinatário autorizado deve ser capaz de extrair o conteúdo da mensagem da sua forma cifrada. Além disso, a obtenção de informação sobre o conteúdo da mensagem (como uma distribuição estatística de certos caracteres) não deve ser possível, uma vez que, se o for, torna mais fácil a análise criptográfica;
  - Integridade da Mensagem: o destinatário deverá ser capaz de determinar se a mensagem foi alterada durante a transmissão;
  - Autenticação do Remetente: o destinatário deverá ser capaz de identificar o remetente e verificar que foi mesmo ele quem enviou a mensagem;
  - Não-repúdio ou Irretratabilidade do Remetente: não deverá ser possível ao remetente negar o envio da mensagem.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Noções de Criptografia

- A criptografia inclui a utilização de cifras e códigos:
  - Uma cifra é uma transformação de caractere por caractere ou de bit por bit, sem levar em conta a estrutura linguística da mensagem;
  - Em contraste, um código substitui uma palavra por outra palavra ou símbolo. Os códigos não são mais utilizados, embora tenham uma história gloriosa;

- Cifra:
  - A cifra é um ou mais algoritmos que cifram e decifram um texto;
  - A operação do algoritmo costuma ter como parâmetro uma chave. Tal parâmetro costuma ser secreto (conhecido somente pelos comunicantes);
  - Historicamente, os métodos de criptografia têm sido divididos em duas categorias: as cifras de substituição e de transposição;

Noções de Criptografia

- Cifras de Substituição:
  - Em uma cifra de substituição, cada letra ou grupo de letras é substituído por outra letra ou grupo de letras, de modo a criar um "disfarce“;

  - Cifra de César: https://crypto.interactive-maths.com/caesar-shift-cipher.html#act
    - Monoalfabético;
    - Senaível à análise de frequência.

  - Cifra de Vigenere: https://crypto.interactive-maths.com/vigenegravere-cipher.html#act
    - Polialfabético;
    - Imune à análise de frequência;
    - As chaves podem variar por arquivo;
    - Não devem ser pequenas evitando repetição de padrões.

- Cifras de Transposição:
  - As cifras de substituição preservam a ordem dos símbolos no texto simples, mas disfarçam esses símbolos. Por outro lado, as cifras de transposição reordenam as letras, mas não as disfarçam;

  - Cerca de Estrada de Ferro: técnica criada na Guerra Civil, onde as letras alternadas do texto puro formam o texto criptografado.

- Cifras de Transposição:
  - Transposição de Coluna:

5	1	2	6	4	3
S	E	G	U	R	O

V	A	M	O	S	A
P	R	E	N	D	E
R	M	A	I	S	D
E	S	S	E	A	S
S	U	N	T	O	A

Texto Claro:
Vamos aprender mais desse assunto.

Texto Criptografado:
ARMSUMEASNAEDSASDSAOVPRES

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Noções de Criptografia

- Cifras de Transposição:
  - Transposição de Coluna:

5	1	2	6	4	3
S	E	G	U	R	O

V	A	M	O	S	A
P	R	E	N	D	E
R	M	A	I	S	D
E	S	S	E	A	S
S	U	N	T	O	A

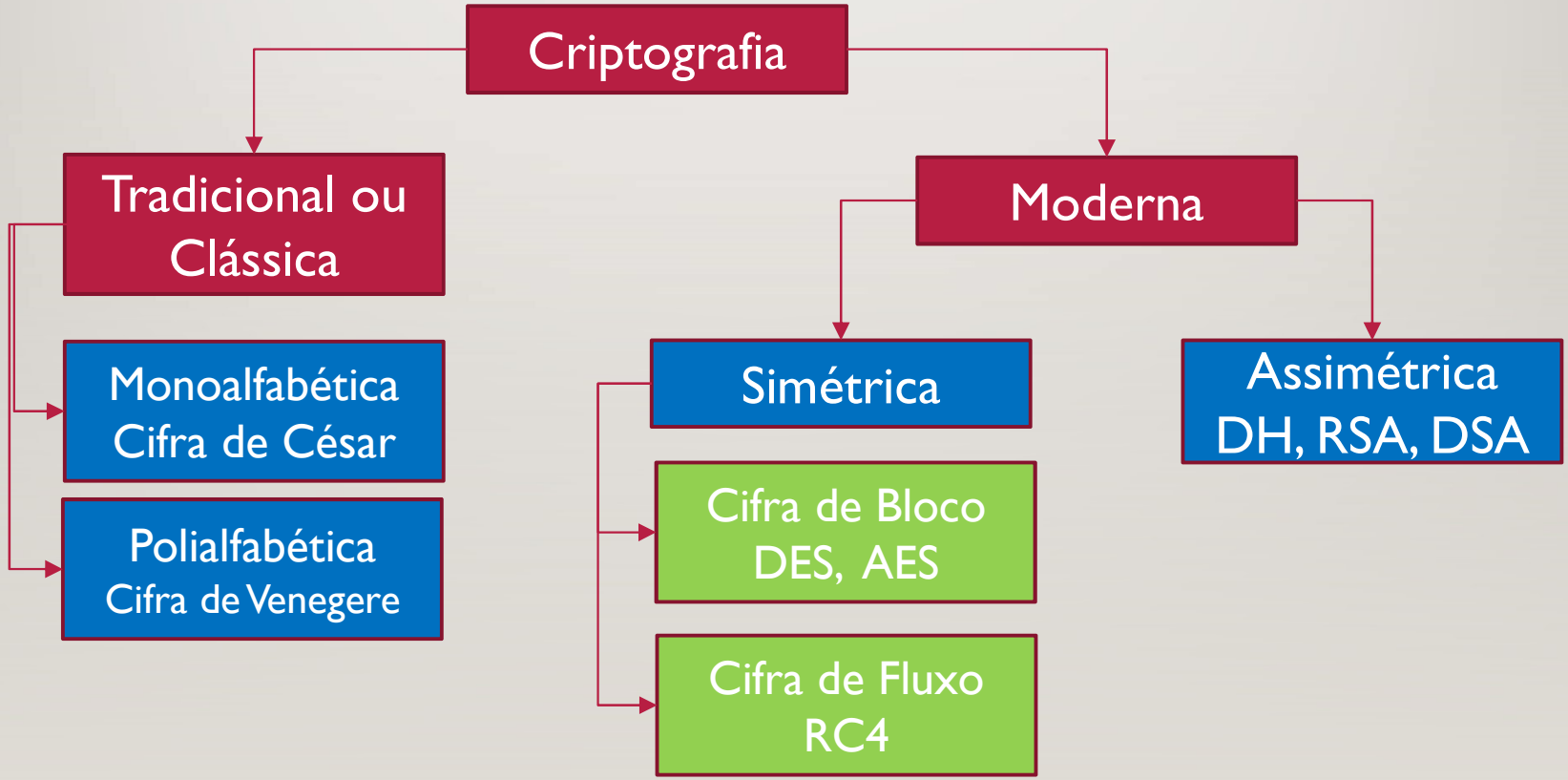
Texto Claro:
Vamos aprender mais desse assunto.

Texto Criptografado:
ARMSU MEASN AEDSA SDSAO VPRES

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Noções de Criptografia

- Organograma da Criptografia:



FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Noções de Criptografia

- Criptografia de Chave Única ou Simétrica:
  - Utiliza um algoritmo e uma chave para cifrar e decifrar;
  - A chave tem que ser mantida em segredo;
  - O conhecimento do algoritmo e de parte do texto cifrado deve ser insuficiente para obtenção da chave;
  - Normalmente utilizam cifra de bloco.

- Criptografia de Chave Pública ou Assimétrica:
  - É um método de criptografia que utiliza um par de chaves: uma chave pública e uma chave privada;
  - A chave pública é distribuída livremente para todos os correspondentes via e-mail ou outras formas;
  - A chave privada deve ser conhecida apenas pelo seu dono;

Noções de Criptografia

- Modo de operação de Criptografia Simétrica:

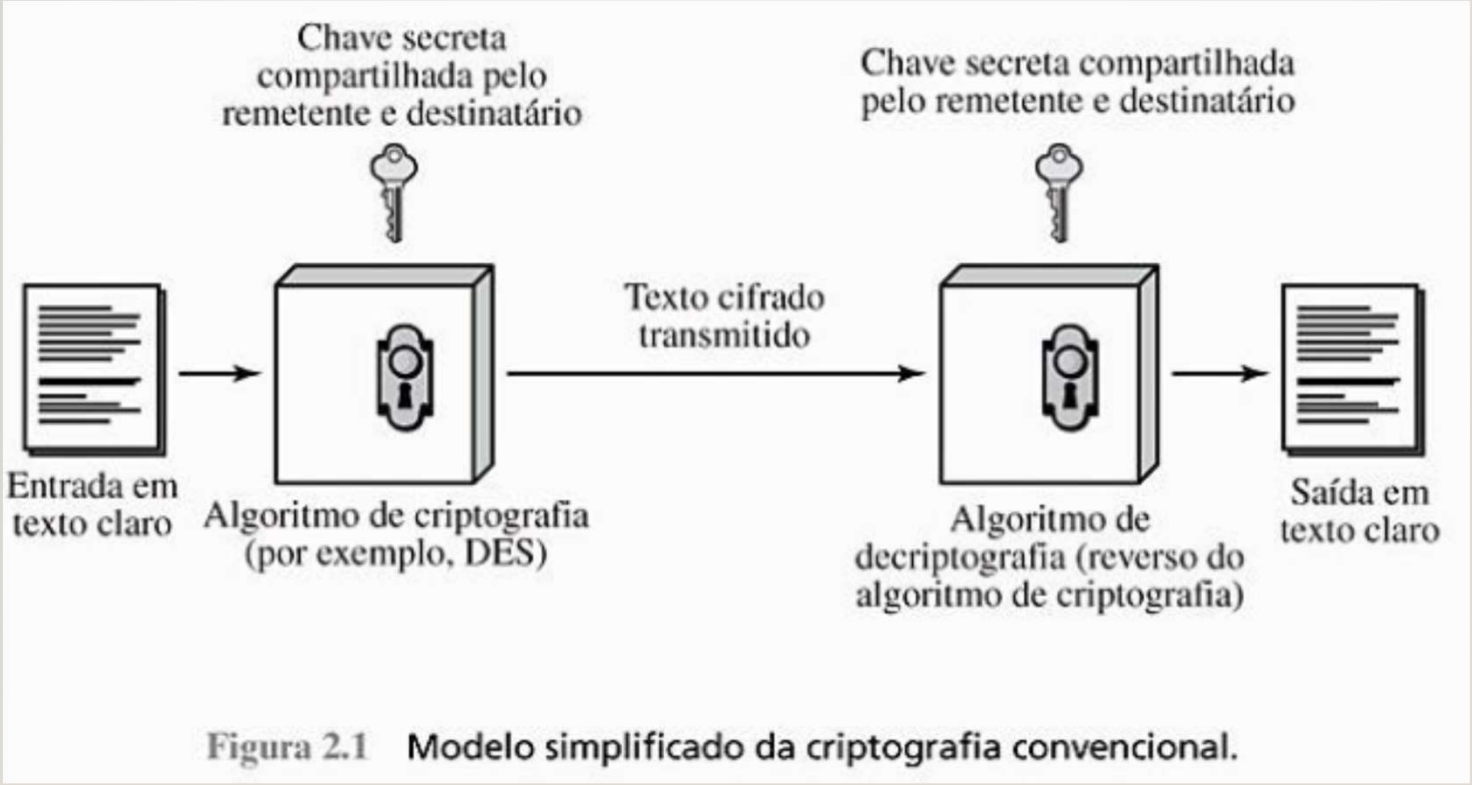
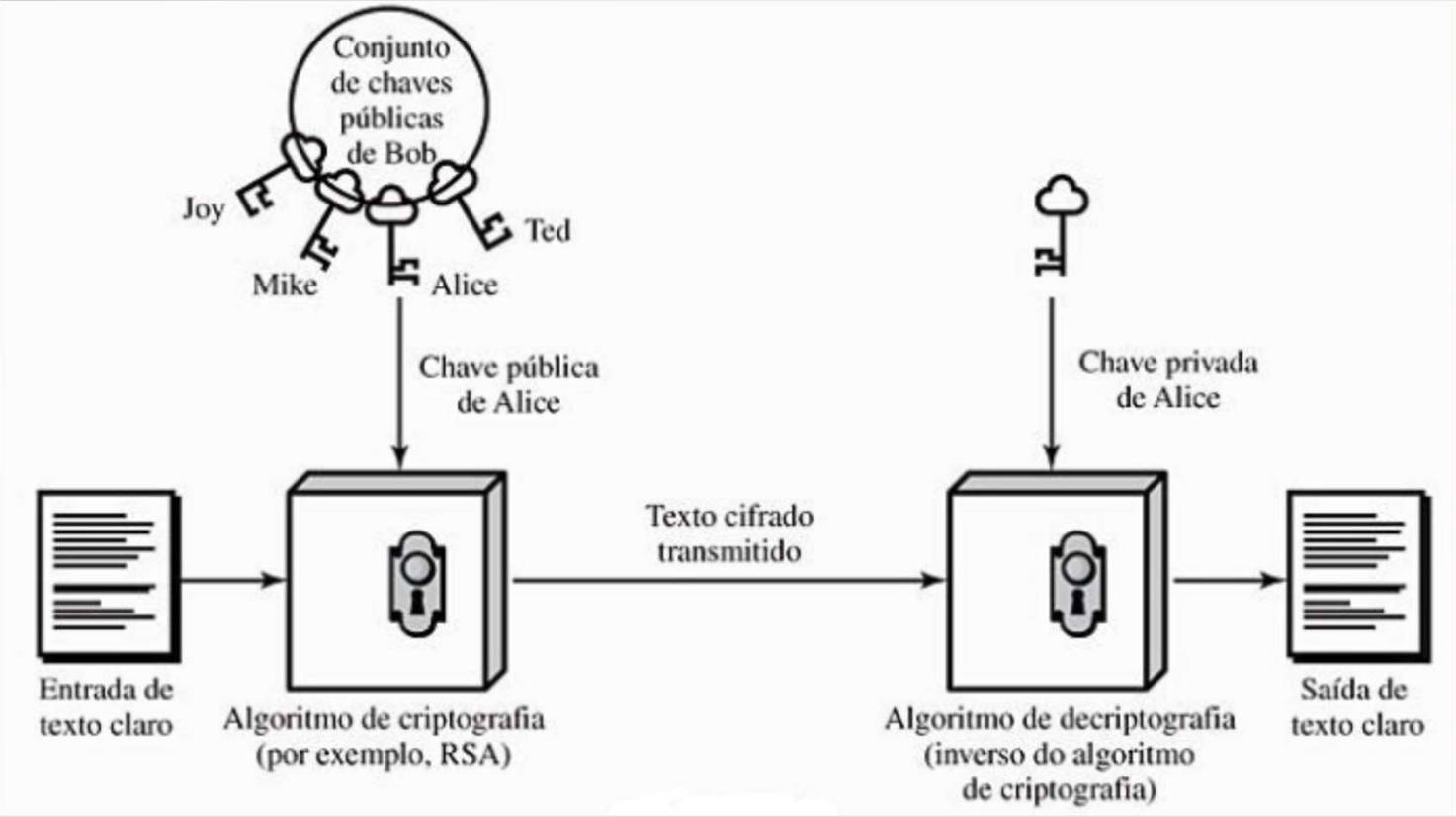


Figura 2.1 Modelo simplificado da criptografia convencional.

Fonte: STALLINGS, W. Criptografia e Segurança de Redes, 4ª Ed., São Paulo: Pearson Prentice Hall, 2008

Noções de Criptografia

- Modo de operação de Criptografia Assimétrica:

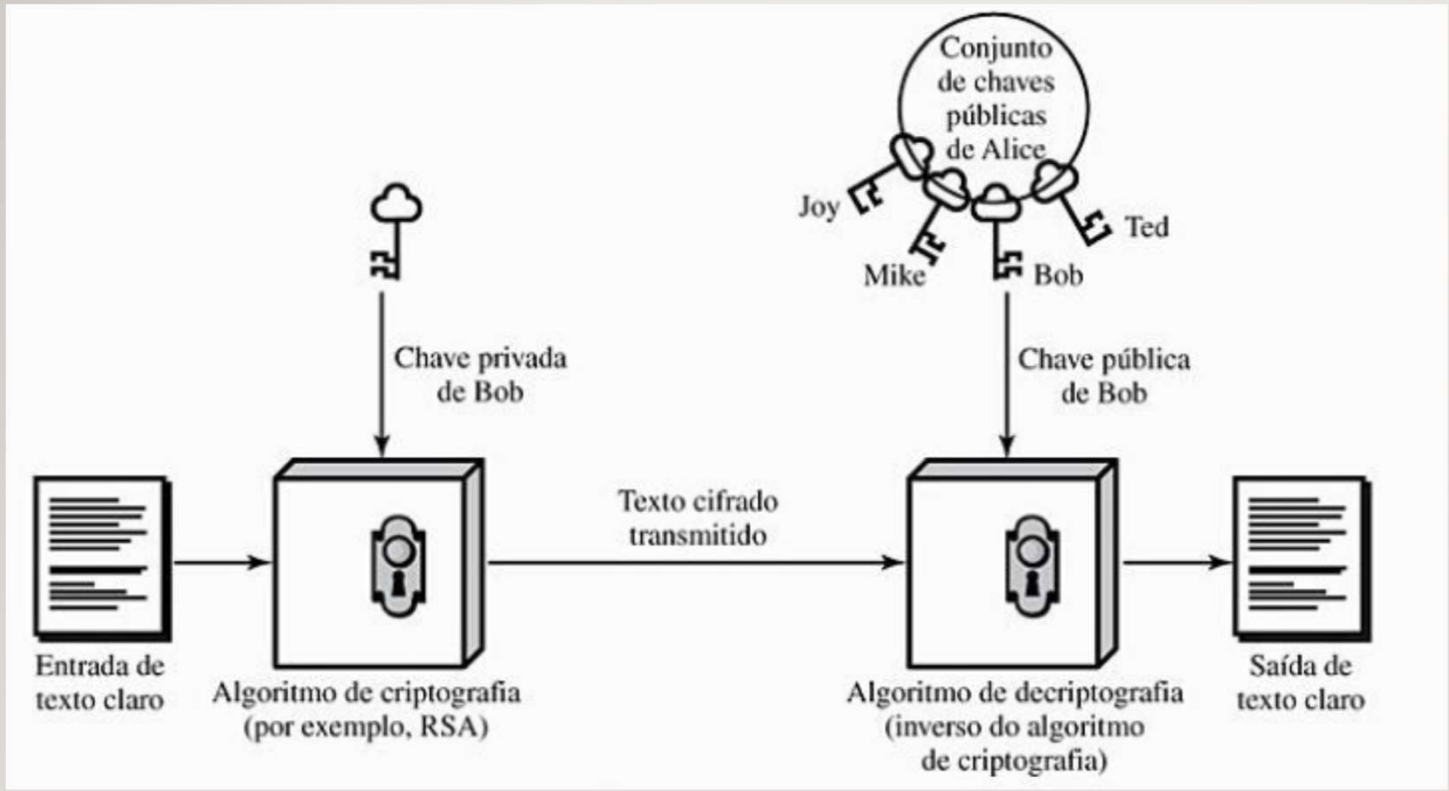


O que se busca conseguir com esse uso das chaves?

Fonte: STALLINGS, W. Criptografia e Segurança de Redes, 4ª Ed., São Paulo: Pearson Prentice Hall, 2008

Noções de Criptografia

- Modo de operação de Criptografia Assimétrica:



O que se busca conseguir com esse uso das chaves?

Fonte: STALLINGS, W. Criptografia e Segurança de Redes, 4ª Ed., São Paulo: Pearson Prentice Hall, 2008

Noções de Criptografia

- Criptografia Simétrica x Criptografia Assimétrica:

Tabela 9.1 Criptografia convencional e de chave pública

Criptografia convencional	Criptografia de chave pública
Necessário para funcionar: 1. O mesmo algoritmo com a mesma chave é usado para criptografia e decriptografia. 2. O emissor e o receptor precisam compartilhar o algoritmo e a chave. **Necessário para a segurança:** 1. A chave precisa permanecer secreta. 2. Deverá ser impossível ou pelo menos impraticável decifrar uma mensagem se nenhuma outra informação estiver disponível. 3. O conhecimento do algoritmo mais amostras do texto cifrado precisam ser insuficientes para determinar a chave.	**Necessário para funcionar:** 1. Um algoritmo é usado para criptografia e decriptografia com um par de chaves, uma para criptografia e outra para decriptografia. 2. O emissor e o receptor precisam ter uma das chaves do par casado de chaves (não a mesma chave). **Necessário para a segurança:** 1. Uma das duas chaves precisa permanecer secreta. 2. Deverá ser impossível ou pelo menos impraticável decifrar uma mensagem se nenhuma outra informação estiver disponível. 3. O conhecimento do algoritmo mais uma das chaves mais amostras do texto cifrado precisam ser insuficientes para determinar a outra chave.

Fonte: STALLINGS, W. Criptografia e Segurança de Redes, 4ª Ed., São Paulo: Pearson Prentice Hall, 2008

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Noções de Criptografia

Pesquisa:

- Algoritmos Simétricos:
  - https://tecnologiadarede.webnode.com.br/news/noticia-aos-visitantes/
- Algoritmos Assimétricos:
  - https://www.lambda3.com.br/2012/12/entendendo-de-verdade-a-criptografia-rsa/
- Comparação entre algoritmos simétricos e assimétricos:
  - https://www.ehow.com.br/vantagens-desvantagens-criptografias-simetrica-assimetrica-info_327051/
  - https://www.binance.vision/pt/security/symmetric-vs-asymmetric-encryption