Introdução à Segurança da Informação

Criptografia e Hash

Prof. Dr. Daniel Caetano

2021 - 1

Compreendendo o problema

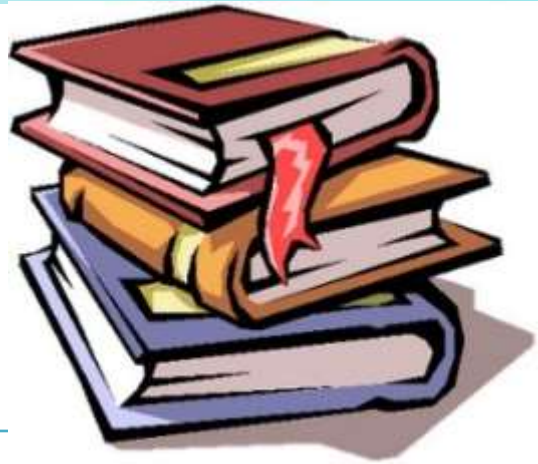
- **Situação:** Secretária pega 8 anos de prisão por tentar vender segredos da Coca-Cola à concorrente Pepsi. Foi descoberta porque a Coca-Cola foi alertada por funcionários da Pepsi

Como evitar esse tipo de problema no caso de um ataque?

Objetivos

- Compreender a necessidade de cifrar dados
- Conceituar criptografia e hash e exemplificar alguns tipos
- Tomar contato prático com a criptografia

Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	http://www.caetano.eng.br/ (Segurança da Informação – Aula 8)
Biblioteca Virtual	Segurança da Informação: caminhos e ideias para a proteção de dados. Págs 86 a 98. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002, Cap. 10. Criptografia eSegurança de Redes: princípios e práticas. Cap. 2.

A Vulnerabilidade dos Dados Armazenados e Transmitidos

Mecanismos de Segurança

- Os dados estão sempre vulneráveis?
- Mesmo que o dado não saia do computador
  - Pessoa com acesso físico...

Mecanismos de Segurança

- Mas... E na transmissão pela internet?
  - Internet é pública e os dados são abertos
  - Isso, em si, é uma vulnerabilidade

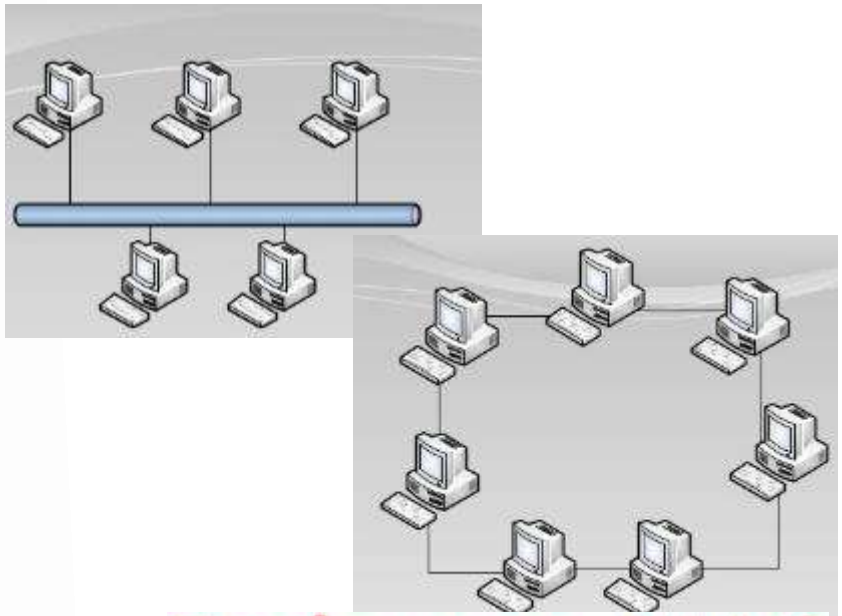
Vamos entender como isso funciona!

Resumão:

O que é a Internet?

Origens

- Redes locais x Inter-net



Endereço MAC

Endereço IP

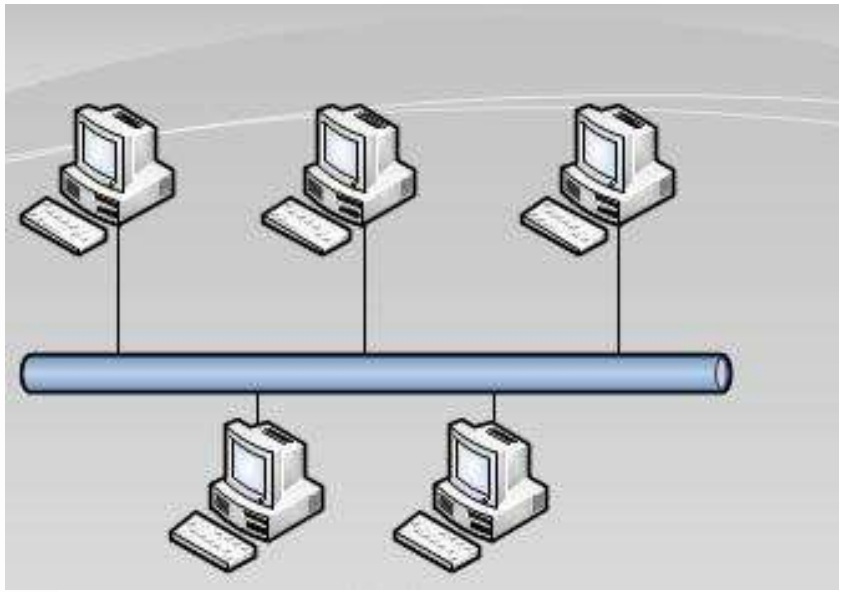
- Diferença importante:
  - Organização do tráfego de dados

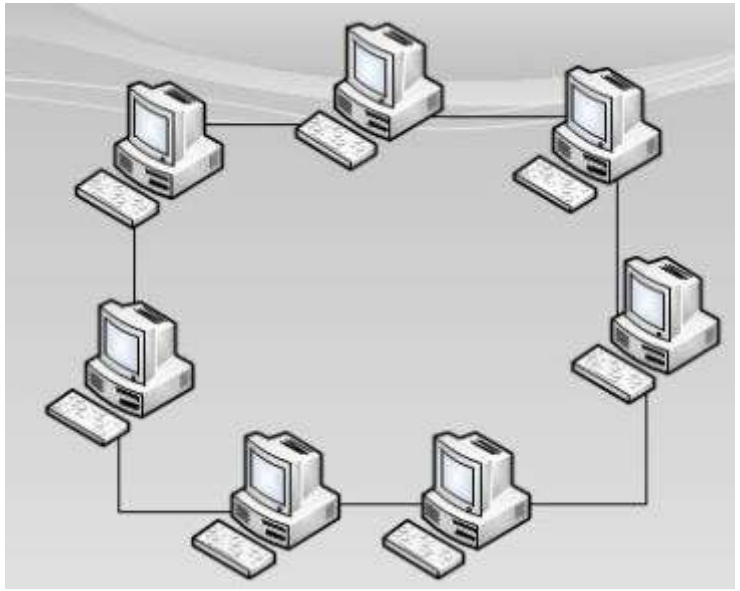
Origens

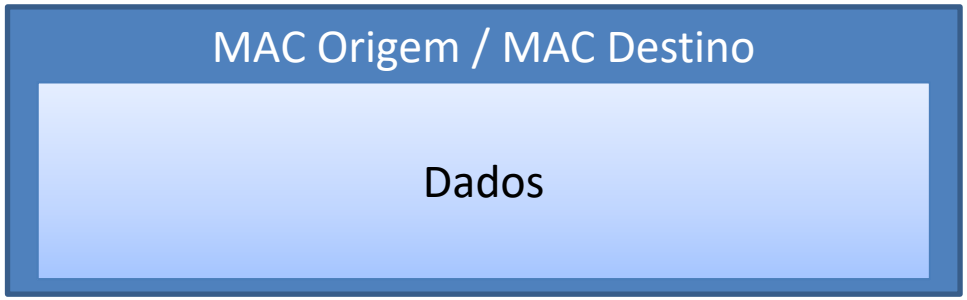
- Diferença importante:
  - Organização do tráfego de dados

Rede Local: Comunicação Direta

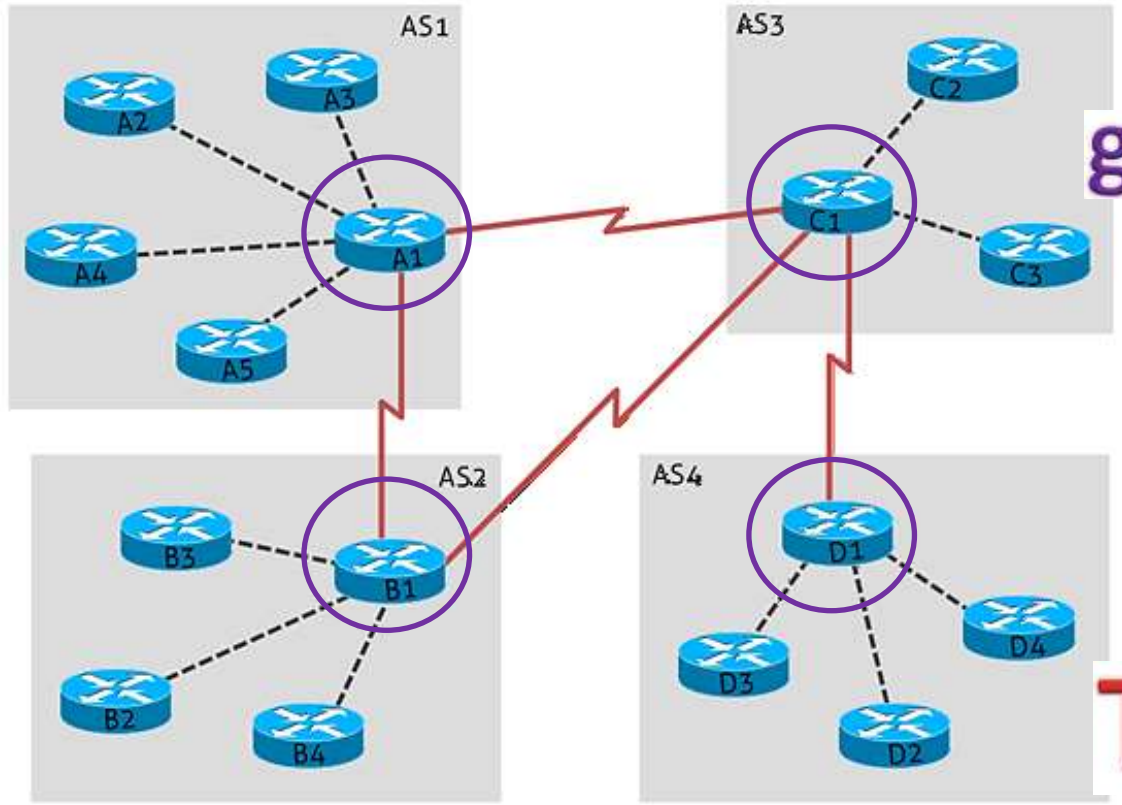
- Pacote com dado e endereço MAC







Internet: Comunicação Hierárquica



gateways

IP

TCP/IP

MAC Origem / MAC Destino

IP Origem / IP Destino

Dados

MAC Origem / MAC Destino

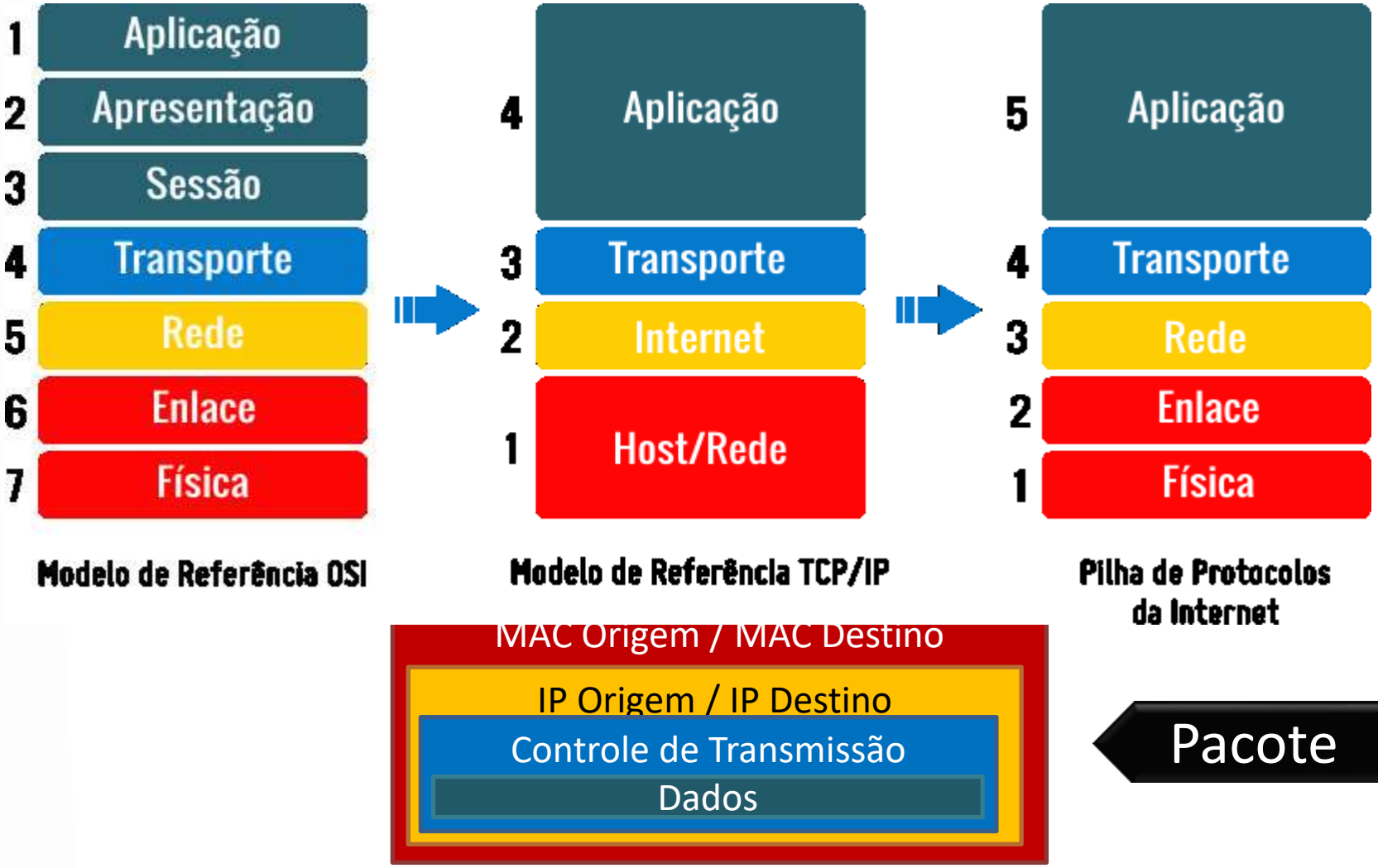
IP Origem / IP Destino

Controle de Transmissão

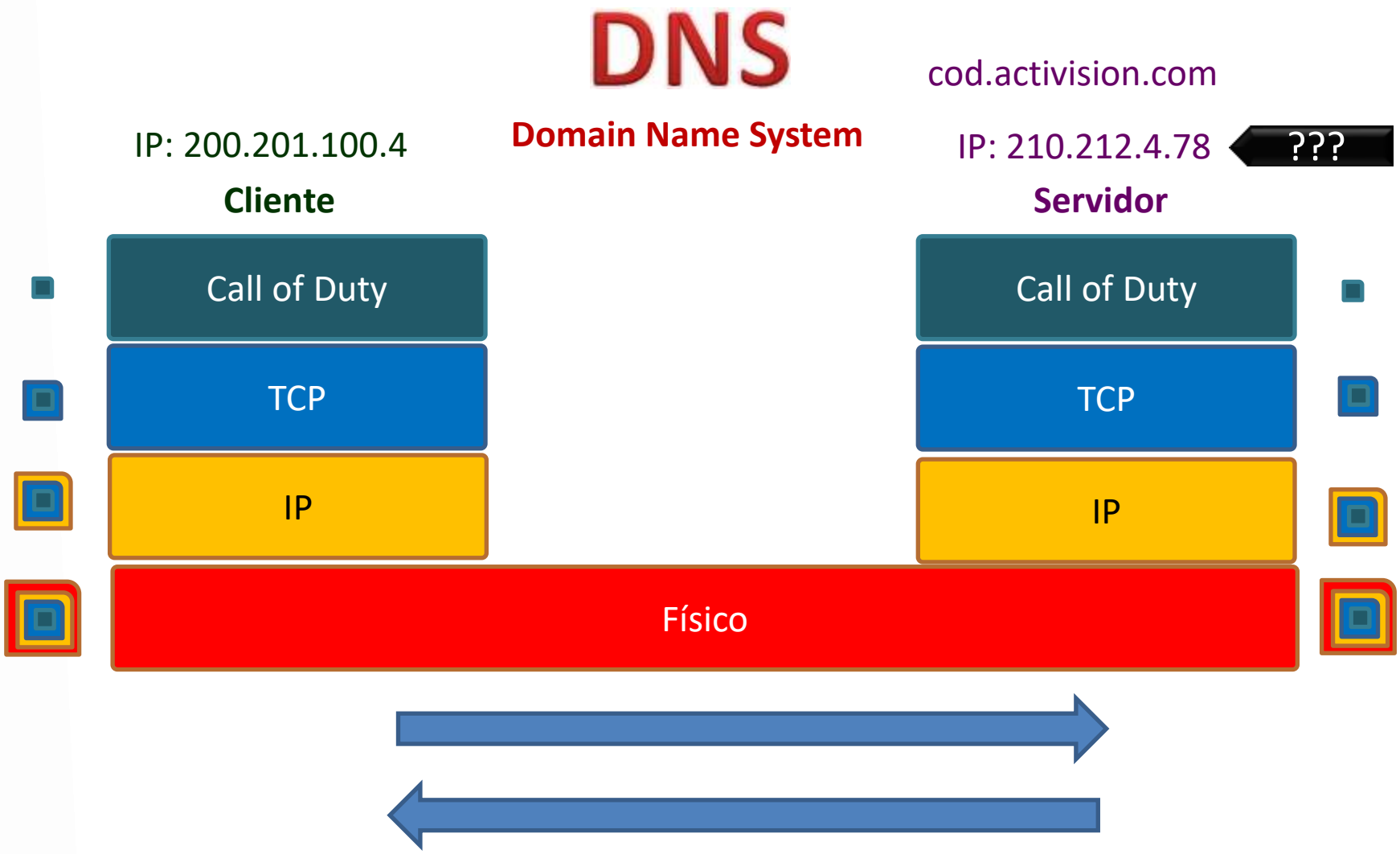
Dados

Protocolos

- Comunicação padronizada

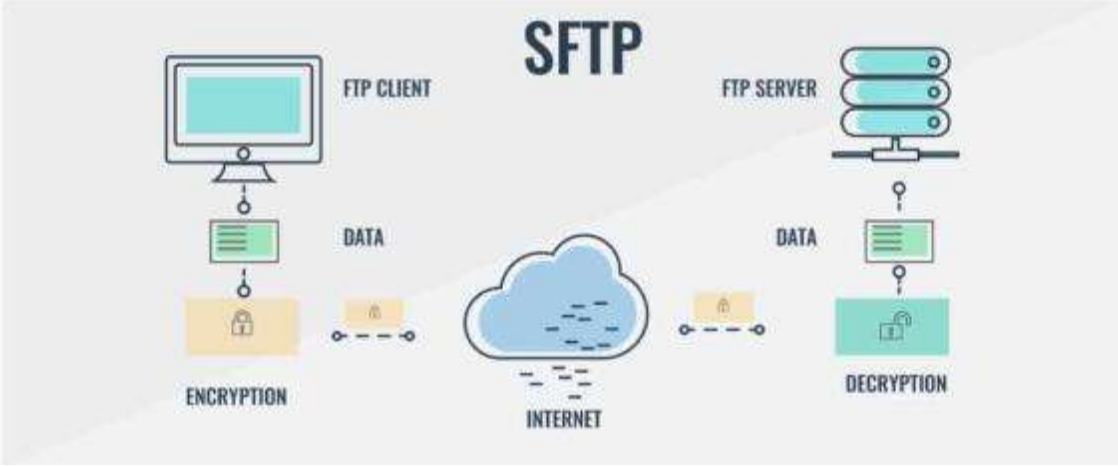


Protocolos: Caminho dos Dados



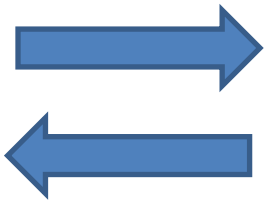
Protocolos de Aplicações Internet

- Aplicações também usam protocolos
  - Transmissão de arquivos: FTP e SFTP
  - Web: HTTP e HTTPS
  - E-mail: SMTP, POP, IMAP
  - Comunicação (Signal/Telegram): MTProto
  - Dentre muitos outros!



O que é a World Wide Web?

- Chrome, Firefox, Edge, Safari, Opera...
  - São Navegadores
- Eles acessam conteúdo de um servidor
  - Apache, Nginx, IIS...



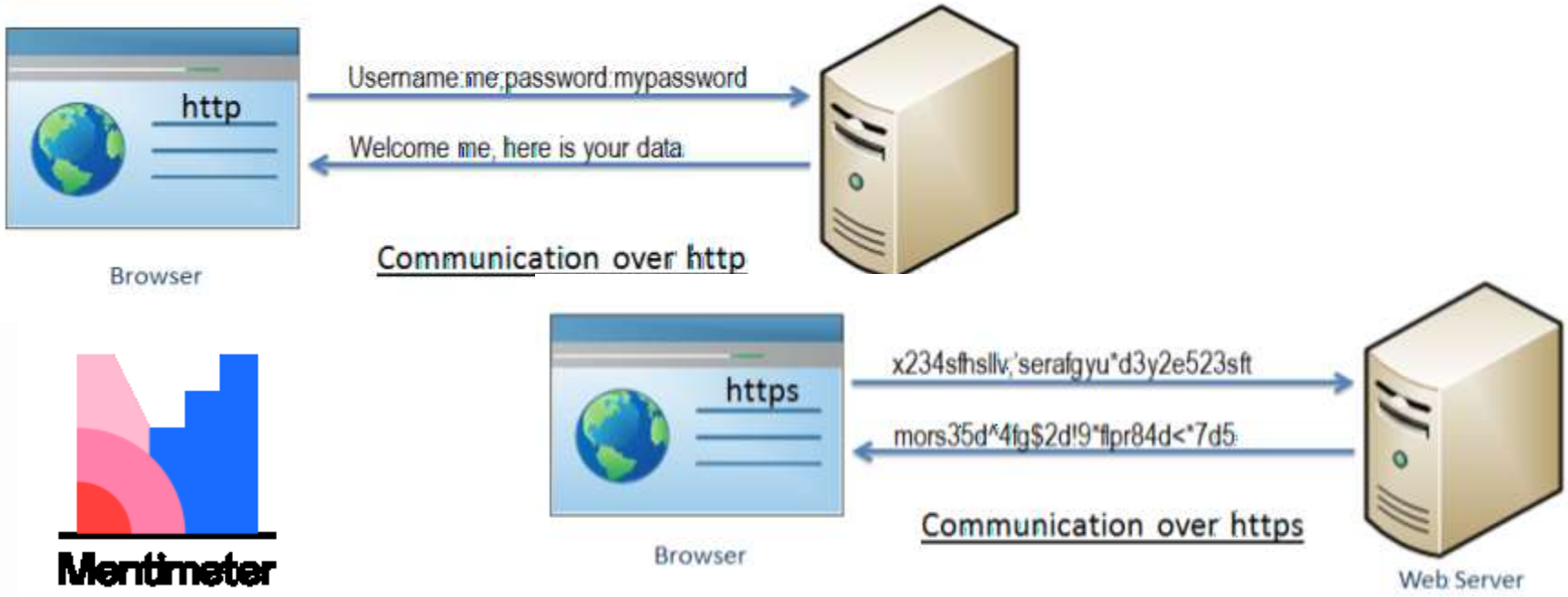
Web Server x Navegador

- Comunicação por meio do HTTP
- HTTP significa: HyperText Transfer Protocol
  - Especificado por Tim Berners-Lee em 1990
  - Transmitir documentos hipertexto

http://www.meuservidor.com/index.html

Navegação Segura

- Comunicação por meio do HTTPS
- HTTP + SSL (Secure Socket Layer)
  - Criptografa as informações ponto-a-ponto
  - HTTPS, por si só, não significa segurança



Mecanismos de Segurança para os Dados

Vídeo: O Jogo da Imitação

- Criptografia e computação: tudo a ver

https://youtu.be/YIkKbMcJL_4

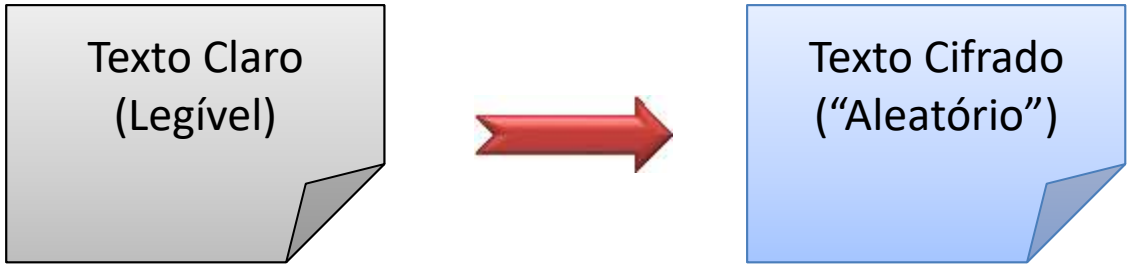
Mecanismos de Segurança

- Os mecanismos mais clássicos são:
  - Criptografia dos dados
  - Assinatura digital dos dados
    - **Aula que vem!**

- Focam em garantir
  - Sigilo: só quem pode acessar, acessará
  - Integridade: conferir se dado permanece “original”
  - Autenticação: de usuário, remetente, destinatário
  - Atualidade: a mensagem é nova, não um reenvio.

Criptografia

- Codificação dos dados
- Processo que transforma

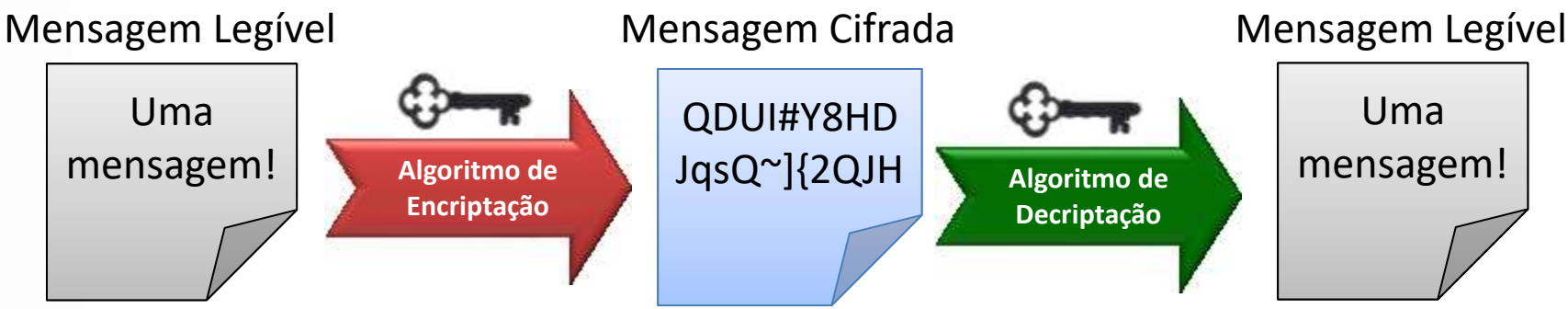


- Algoritmo de criptografia
  - Cifragem: tornar o texto claro em cifrado
    - “Criptografar” ou “Encriptar”
  - Decifragem: tornar o texto cifrado em claro
    - “Decriptografar” ou “Decriptar”

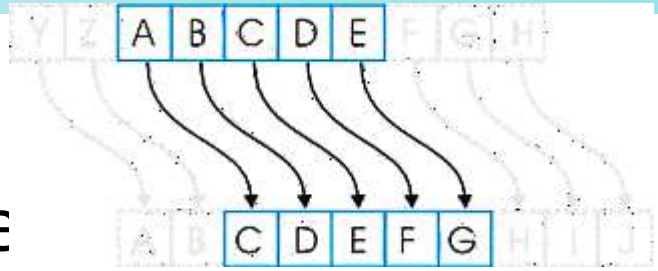
Criptologia

Chave Criptográfica

- Porta: basta ela existir?
  - Precisa haver uma chave
- Chave permite “trancar” e “destrancar”
  - É o “segredo” de um criptografia
  - Similar a uma “senha”
- Tradicionalmente, remetente e destinatário...
  - Precisam ter uma cópia da chave



Exemplo: Substituição



- Codificar: “somar 2” a cada le

A B A C A X I

+2 +2 +2 +2 +2 +2 +2

C D C E C Z K

Algoritmo: somar o valor da chave à letra

Chave: 2

Tamanho da Chave?

- Decodificar: “subtrair 2” de cada letra

C D C E C Z K

-2 -2 -2 -2 -2 -2 -2

A B A C A X I

Algoritmo: subtrair o valor da chave da letra

Chave: 2

Criptografia Simétrica ou de Chave Secreta

Criptografia de Chave Pública

- Codificar: “somar 2” a cada letra

Algoritmo: somar o valor da chave “α” à letra
Chave: 2 **Chave Privada**

- Decodificar: “somar 24” a cada letra

Algoritmo: somar o valor da chave “β” à letra
Chave: 24 **Chave Pública**

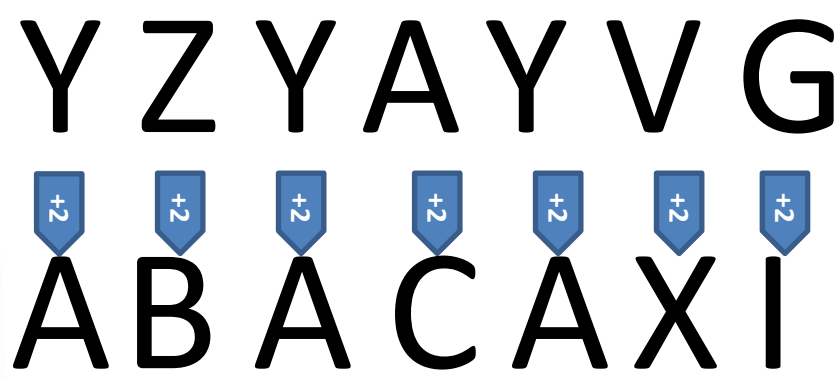
Criptografia Assimétrica ou de Chave Pública

Criptografia de Chave Pública

- E se codificar com a chave pública (Ex. 24)?

Algoritmo: somar o valor da chave pública
Chave: 24 **Chave Pública**

- Decodificar: "somar 2" a cada letra

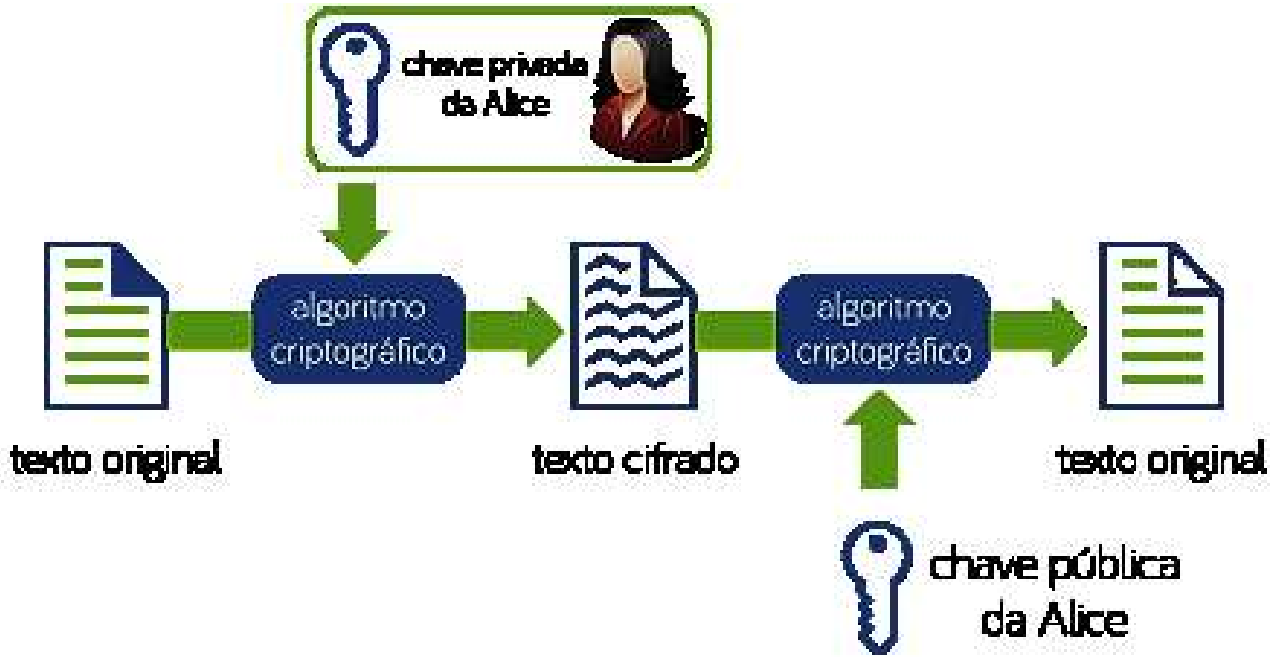


Algoritmo: somar o valor da chave privada
Chave: 2 **Chave Privada**

Funciona nas duas direções!

Criptografia de Chave Pública

- Se eu codifico com minha chave privada
  - As pessoas podem decifrar com minha chave pública e verificar que a mensagem é minha



Criptografia de Chave Pública

- Se alguém codifica com minha chave pública
  - Apenas eu posso decifrar com minha chave privada

Criptografia de Chave Pública

- Se eu quero mandar uma mensagem secreta
  - Eu codifico essa mensagem com a chave pública do receptor e só ele poderá abrir

Criptografia de Chave Pública

- Se receber uma mensagem codificada com a chave privada de alguém
  - Eu me certifico do autor decodificando com a chave pública dessa pessoa***

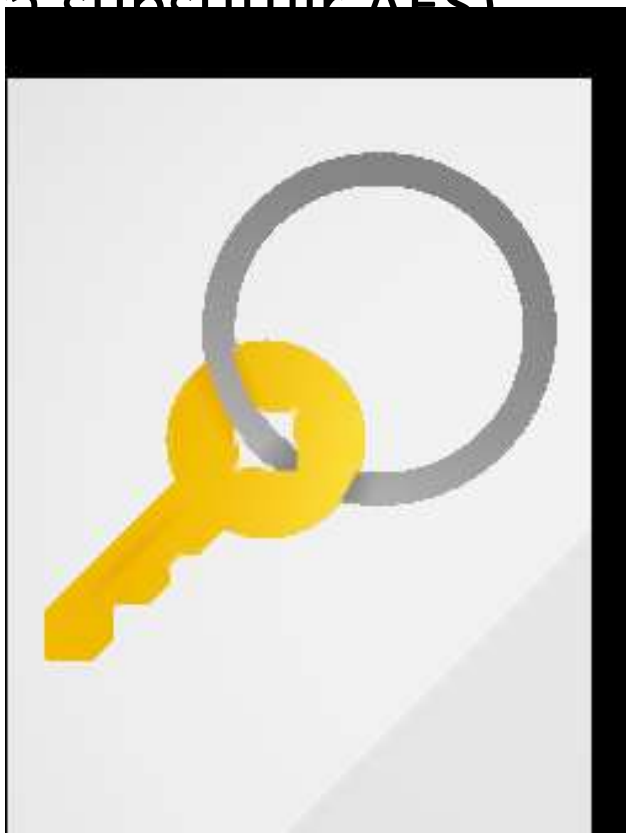
Uso da Criptografia

- Assim, dados criptografados...
  - Armazenados ou transmitidos
  - Só serão legíveis por quem tiver a chave

Estarão mais seguros!

Algoritmos Comuns

- Criptografia de chave simétrica (128, 256...)
  - AES - Rijndael
  - Blowfish
  - Twofish, Serpent (concurso para substituir AES)
  - CAST5 (GPG)
  - RC4 (Não é mais recomendado
  - 3DES (Mais lento que outros)
  - IDEA (PGP)



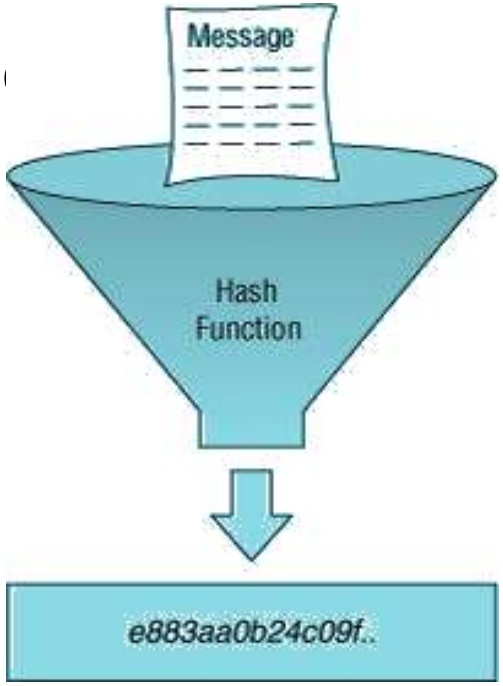
Algoritmos Comuns

- Criptografia de chave assimétrica (1024...)
  - RSA (problemas com as chaves)
  - Diffie-Hellman
  - ECC (Preferido para substituir o RSA, atualmente)
  - ElGamal (quase não é mais usado)
  - DSA (Substituto do ElGamal,

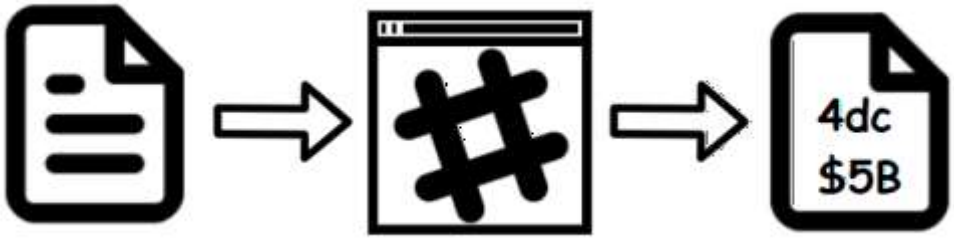
HASH CRIPTOGRÁFICO

Hash ou Número Resumo

- Analisar arquivo ou mensagem:
  - Certificar-se de que não foi alterad
- Criptografia: “ida” e “volta”
  - Se eu codifiquei, eu decodifico
- Hash: só “ida”
  - Só codifico, nunca decodifico
  - Deve ser único para uma mensagem legível



Hash ou Número Resumo



- Exemplo: pegar apenas as letras de posições pares, somando 1 se a anterior for vogal

T R A B A L H O

+0 +1 +1 +0

R C M O

Hash ou Número Resumo

- Algoritmos Comuns
  - MD5 (Message Digest)
    - Muitas “colisões” – não usado em criptografia
  - SHA-1 (Secure Hash Algorithm)
    - 160 bits... Não é mais considerado seguro
  - SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512)
    - Considerados relativamente seguros para criptografia
  - SHA-3
    - Vencedor de competição em 2015

https://www.convertstring.com/pt_BR/Hash

Hash ou Número Resumo

- Usado, por exemplo, para armazenar senha

- Quando for ocorrer um *login*?
  - Usuário digita a senha
  - Geramos o hash da senha
  - Comparamos com o banco de dados
- Vantagem?
  - Se roubarem o BD, não terão as senhas!

GINCANA CRIPTOGRÁFICA

Gincana de Criptografia

- Abra o PDF na área de Tarefas do Teams
- Acompanhe a explicação do professor
- Siga os passos do documento!

- Quando acabar, não esqueça de postar as resposta no formulário indicado no próprio texto!

ENCERRAMENTO

Resumo e Próximos Passos

- Vulnerabilidade da Informação
  - Sempre que estiver “exposta”!
- Mecanismos para proteger a informação
  - Criptografia e hash
  - Principais algoritmos
- **Pós Aula**: Aprenda Mais, Pós Aula e Desafio!
  - No padlet: https://padlet.com/djcaetano/seguranca

- Certificados digitais e assinaturas digitais
  - Para que servem? Como funcionam?

PERGUNTAS?