UNI
METRO
CAMP
wyden

Introdução à Segurança da Informação - ARA0064

Prof. José Luiz Alonso Silva, MsC
E-mail: jose.lsilva@unimetrocamp.edu.br

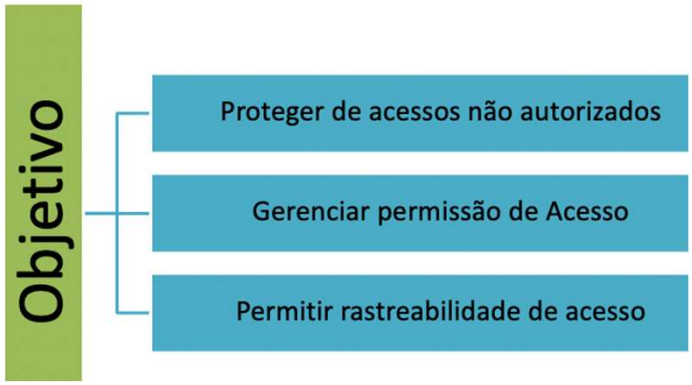
4.3 Criptografia de dados e Certificado Digital

UNI
METRO
CAMP
wyden

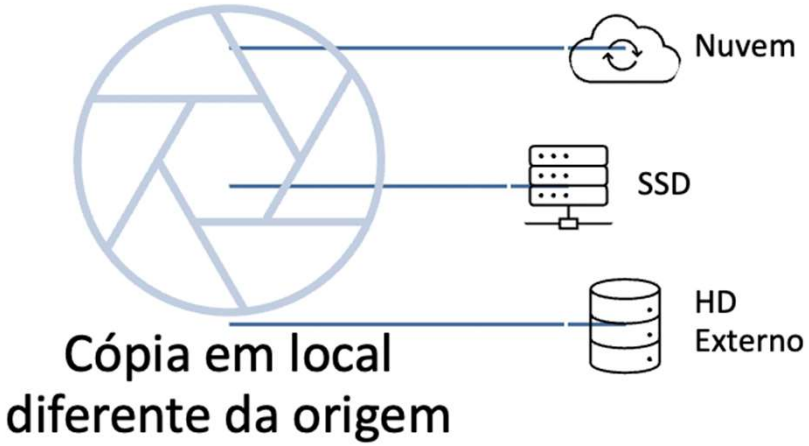
Temas da Aula

- Aspectos Históricos
- Criptografia de Dados
- Chaves de criptografia

Melhores Momentos



Controle de Acesso



Backup e Restore

UNI METRO CAMP wyden

Atividade aula 10

- Ferramentas para Backup

Acronis True Image (2x)
Acronis True Image
BackupAssist
Commvault
CrashPlan
Dropbox (2x)
Google Drive
Google Cloud Backup
Iperius Backup
One drive (2x)
VEEAM BACKUP & REPLICATION

- Respostas no Forms: 13 respostas

Objetivo da Aula

- Identificar os tipos de criptografia de dados e os itens presentes em um certificado digital

Imagem: Autor utilizando Wordart

UNI METRO CAMP wyden

Aspectos Históricos
Evidências

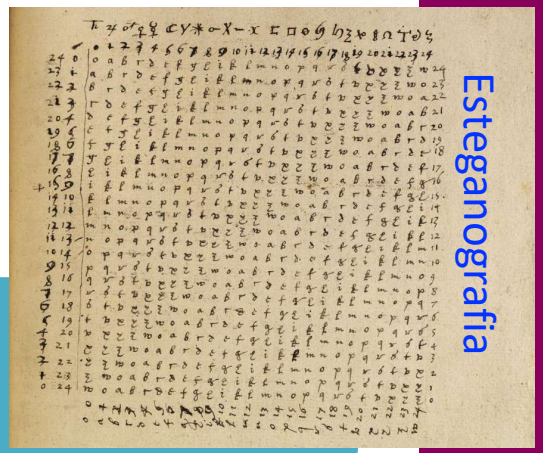
Primeira mensagem criptografa que se tem conhecimento é datada de 1900 A.C. encontrada no Egito

- Hieroglifos irregulares esculpidos em monumentos

Hebreus 500 a 600 A.C. fizeram uso de simples cifras de substituição monoalfabética

- Atbash substituição do alfabeto hebraico
- Substituição do *aleph* (a primeira letra) pela *tav* (a última), *beth* (a segunda) pela *shin* (a penúltima), e assim por diante, invertendo o alfabeto usual
- https://www.hanginghyena.com/solvers/atbash-cipher-decoder

Aspectos Históricos Evidências



Gregos antigos conheciam cifras

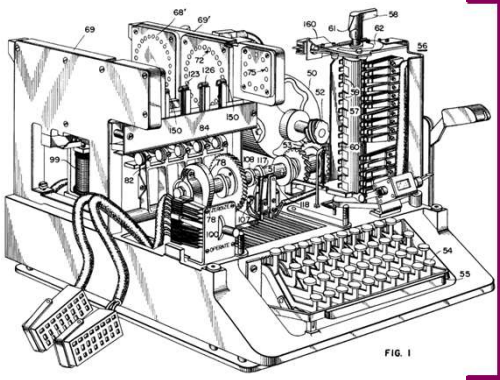
- Exemplo, a cifra de transposição *scytale* utilizada pelos militares de Esparta
- Mensagens secretas escondidas sob a cera em tabletes de madeira
- Tatuagem na cabeça de um escravo oculta pelo cabelo crescido
- Esteganografia (do grego "escrita escondida") uso das técnicas para ocultar a existência de uma mensagem dentro de outra

Ahmad al-Qalqashandi (1355–1418) escreveu o *Subh al-a 'sha*

- Enciclopédia de 14 volumes, que incluía uma seção sobre criptologia

Imagem: http://hdl.handle.net/10107/4396400 - pag. 113

Aspectos Históricos



I Guerra Mundial

SIGABA é descrito na Patente dos EUA 6.175.625, arquivado em 1944 mas somente emitido em 2001

- Sala 40 do Almirantado
- Quebrou os códigos navais alemães e desempenhou um papel importante em vários combates navais

II Guerra Mundial

- Máquinas de codificação mecânica e eletromecânica
- Locais onde essas máquinas eram impraticáveis era utilizado sistemas manuais

Imagem: https://commons.wikimedia.org/w/index.php?curid=1332341

Criptografia Moderna

Claude E Shannon

- Pai da criptografia matemática - Teoria Matemática da Informação
- 1949 publicou *Communication Theory of Secrecy Systems* no *Bell System Technical Journal*
- Livro *The Mathematical Theory of Communication*,

Até anos 1970

- Criptografia desapareceu em parte das comunicações de organizações secretas do governo como a NSA e GCHQ (Britânica) e seus equivalentes no mundo
- Pouco trabalho tornou-se público

Criptografia Moderna

Meados Anos 1970

- 2 grandes avanços públicos (ou seja, não-secreto)

Publicação do projeto DES (*DATA ENCRYPTION STANDARD*)

Chaves Assimétrica

Criptografia Moderna

Publicação do projeto DES (*DATA ENCRYPTION STANDARD*)

- Registo Federal dos EUA em 17 de março de 1975
- Apresentada por grupo de pesquisa da IBM, a convite do NIST
- Esforço para desenvolver instalações seguras de comunicações eletrônicas para as empresas, como bancos e outras grandes organizações financeiras
- Primeira cifra publicamente acessível a ser "abençoada" por uma agência nacional, como a NSA, publicada em 1977 como FIPS (*Federal Information Processing Standards*)

Fonte DES: https://csrc.nist.gov/files/pubs/fips/46-3/final/docs/fips46-3.pdf

Criptografia Moderna

Algoritmos de Chave Assimétrica

- Publicação do artigo New *Directions in Cryptography* (Whitfield Diffie e Martin Hellman)
- Método novo de distribuição de chaves criptográficas
- Solução de um dos problemas fundamentais da criptografia, distribuição de chaves
- O artigo também estimulou o desenvolvimento público quase que imediato de uma nova classe de algoritmos de cifragem

Fonte https://ee.stanford.edu/~hellman/publications/24.pdf

Criptografia de Dados

- Criptografia palavra de origem grega, significa "escrita secreta"
- Termo para nos referirmos Ciência e arte de transformar mensagens de modo a torná-las seguras e imunes a ataques

Técnica visa garantir o sigilo e/ou a autenticidade da informação

Criptografia de Dados

Codificação que permite proteger documentos contra acessos e/ou alterações indevidas

"Criptografia é baseada sempre em um mecanismo de conversão (o algoritmo de cifragem) que converte informações de texto claro para texto cifrado usando uma chave de cifragem conhecida somente pelo emitente e do receptor"

Caruso e Steffen (1999, p. 155)

Fonte: CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. Segurança em informática e de informações. 2. ed. rev. e ampl. São Paulo: Editora SENAC São Paulo, 1999.

Criptografia de Dados

- Conversão de dados de um formato legível em um formato codificado

Dados criptografados só podem ser lidos ou processados depois de serem descriptografados

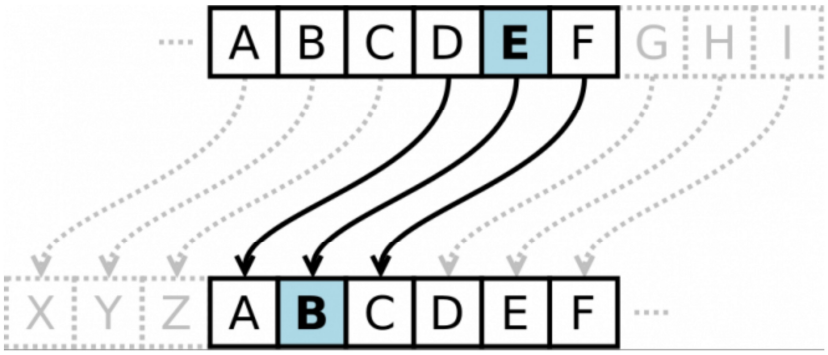
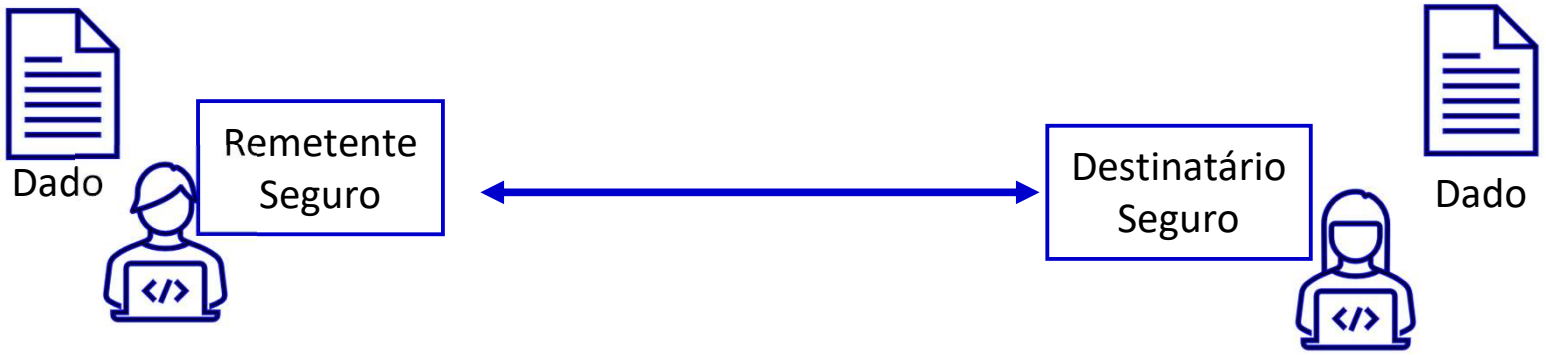


Imagem: https://images.app.goo.gl/Awb1EpKxYXF7bGMM8

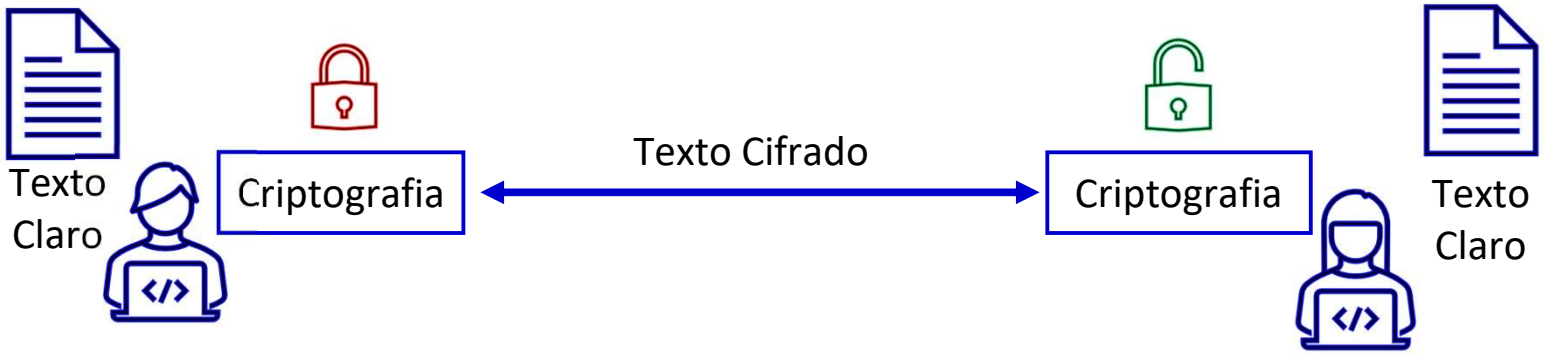
Criptografia de Dados



O destinatário, deve estar habilitado a recuperar os dados originais a partir dos dados "disfarçados"

Imagem: Autor

Criptografia de Dados

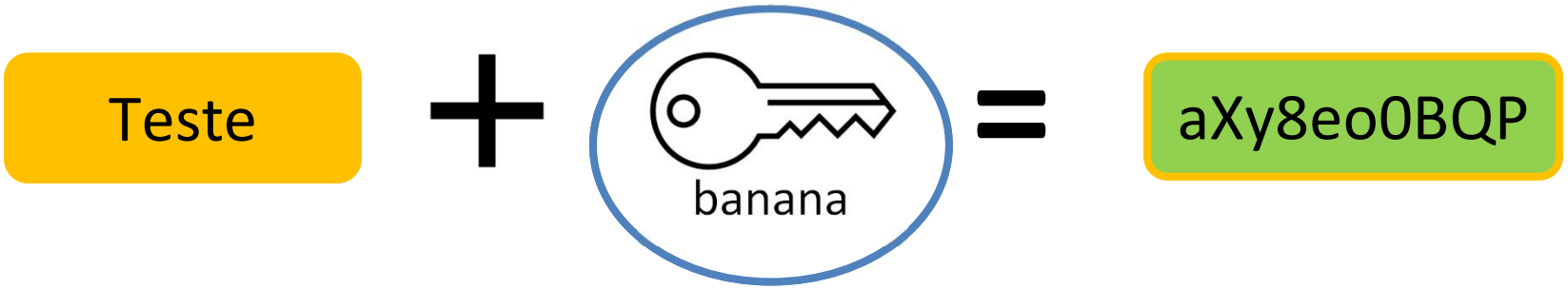


- A mensagem original, é chamada Texto Claro
- Após transformada, é denominada simplesmente Texto Cifrado
- Algoritmo de criptografia (cifra) transforma o Texto Claro em Texto Cifrado
- Algoritmo de descriptografia transforma o Texto Cifrado de volta para Texto Claro

Imagem: Autor

Chave Criptográfica

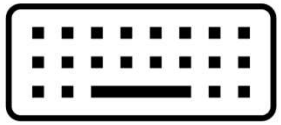
- Um grupo de caracteres aleatórios em uma ordem específica
- Os protocolos de criptografia usam uma chave para alterar os dados de forma que sejam embaralhados e que ninguém sem a chave possa decodificar as informações



UNI METRO CAMP wyden

Chave Criptográfica

- Atualmente, os algoritmos criptográficos são divulgados à comunidade e o sigilo das informações é garantido apenas pela chave



Quanto maior a chave, mais dificuldade para um ataque por força bruta

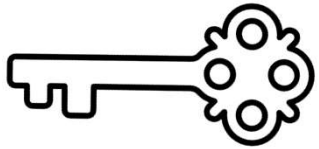


Imagem: autor

Chave Criptográfica

- Quanto tempo leva para decifrar uma mensagem?

  - Depende do tamanho da chave de do algoritmo
  - Algoritmo fraco não importa o tamanho da chave
  - Depende da capacidade de processamento

Chave Criptográfica

A quebra da criptografia utilizando força bruta (todas as chaves possíveis)

- Praticamente inviável para chaves acima de 128 bits

Chaves de 64 bits:

- Utilizando o computador gerando 90 bilhões de chaves por segundo para testar

Chave de 128 bits:

- utilizando um computador bem melhor (gerando 1 trilhão de chaves por segundo) temos o tempo de 10 milhões de trilhões de anos para testarmos todas as chaves

10 bits 2^{10} chaves possíveis de 1024 chaves

Pesquise: EFF DES cracker (apelidado de "Deep Crack“) máquina utilizada para ataque de força bruta
https://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/

Chave Criptográfica

- Porque utilizar chaves e não algoritmo que não precise de chave?

  - Mais fácil guardar em segredo uma uma chave ou algoritmo?
  - É possível diversas chaves para proteger os dados, se uma for descoberta outros dados continuaram protegidos, e se quebrar algoritmo?

Criptografia de Dados

Simétrica – Chave única ou Chave Privada

- **M**odelo utiliza apenas um conjunto de algoritmos responsáveis tanto pela cifragem de determinada operação, assim como a sua decifragem.
- Confiabilidade entre os interlocutores deve ser total, visto que ambos partilham de uma única chave de criptografia, tanto para codificar como para descodificar uma mensagem, por exemplo.

Assimétrica - criptografia de chave pública

- Sistema de protocolos criptográficos que requer a formação de duas chaves
- P**rivada** (usada para descodificar)
- P**ública** (utilizada para codificar e autenticar assinaturas digitais)

Criptografia de Dados Simétrica

- Simétrica – Chave única ou chave privada

Imagem: https://images.app.goo.gl/mJxYRcZEcLr6YU419

UNI METRO CAMP wyden

Criptografia de Dados
Chave Assimétrica

- Conhecida como criptografia de chave pública
- Utiliza duas chaves diferentes, mas matematicamente associadas
  - Chave Pública – faz a criptografia, disponível para todos
  - Chave Privada – faz a descriptografia, somente o detentor decodifica

Criptografia de Dados
Chave Assimétrica

Emissor e receptor das informações geram pares de chaves assimétricas

Pública e Privada

Ambos enviam a chave pública para o outro

Chave criptográfica pública do receptor

O emissor criptografa os dados e os envia ao destinatário

Chave privada (Recebida)

Destinatário decodifica os dados criptografados transmitidos e assim revela as informações.

Caso o receptor queira enviar os dados de volta ao emissor

Criptografa as informações através da chave pública do emissor original

Criptografia de Dados

- Assimétrica - criptografia de chave pública

Imagem: https://images.app.goo.gl/mJxYRcZEcLr6YU419

Criptografia de Dados
Exemplos de algoritmos simétricos

AES - *Advanced Encryption Standard* ou nome original Rijndael

- Especificação para a criptografia de dados eletrônicos estabelecida pelo NIST em 2001

Serpent

- Método de cifragem em bloco de chave simétrica que foi um finalista no "AES process", segundo lugar, criado por Ross Anderson, Eli Biham, e Lars Knudsen

CAST5

- Cifragem em bloco usada em um número de produtos, é a cifragem padrão em algumas versões do GPG e PGP. Criado em 1996 por Carlisle Adams e Stafford Tavares

Criptografia de Dados
Exemplos de algoritmos simétricos

RC4

- Algoritmo simétrico de criptografia de fluxo mais usado no software e era utilizado nos protocolos mais conhecidos, como *Secure Socket Layers* (SSL, hoje conhecido como TLS) (para proteger o tráfego Internet) e WEP (para a segurança de redes sem fios, obsoleto, hoje se usa o WPA).

IDEA - *International Data Encryption Algorithm*

- Criado em 1991 por James Massey e Xuejia Lai, algoritmo de cifra de bloco que faz uso de chaves de 128 bits

Criptografia de Dados
HTTPS

HTTPS

- Protocolo de criptografia para criptografar as comunicações
- Chave pública e privada

Protocolos de Criptografia

- *TLS - Transport Layer Security*, antigo SSL *Secure Sockets Layer*

Especificado por RFC 2818 05/2000

- https://datatracker.ietf.org/doc/rfc2818/

Utiliza a porta 443

- Porta 443 padrão em vez da porta 80 do HTTP

Criptografia de Dados
HTTPS

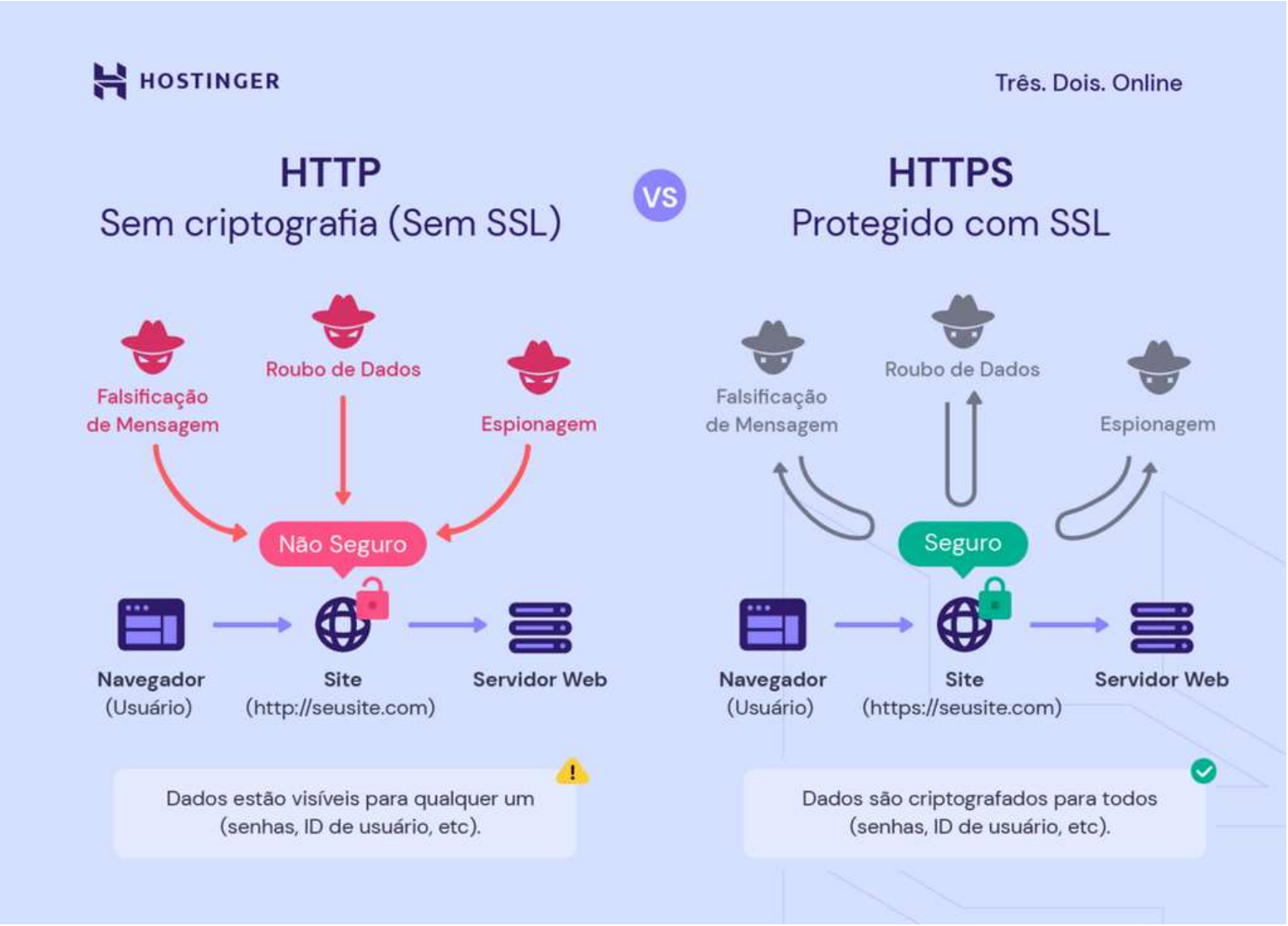


Imagem: https://www.hostinger.com.br/tutoriais/o-que-e-criptografia

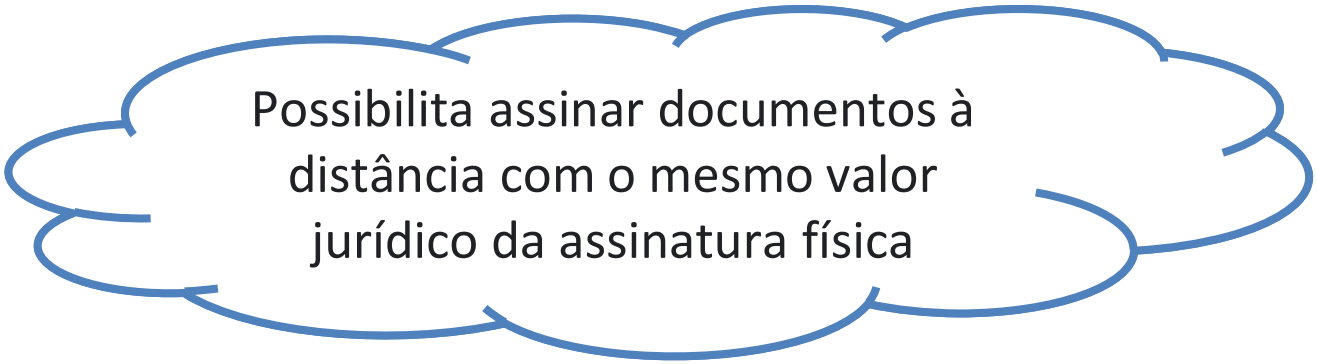
UNI METRO CAMP wyden

Certificado Digital

- Informação textual que identifica uma entidade

Identidade eletrônica de uma pessoa ou empresa

Carteira de Identificação Virtual



UNI METRO CAMP wyden

Certificado Digital

- Aceito legalmente
- Tipos
  - e-CPF é utilizado por pessoas físicas
  - e-CNPJ é ideal para empresas, corporações e instituições
  - NF-e permite a emissão de notas sem a preocupação de utilizar o certificado para tarefas ilegais ou sem autorização

Certificado

Certificado A1

- Validade de 1 ano
- Um arquivo
- Pode ser instalado facilmente em vários computadores mediante cópia de segurança (backup) do arquivo

Certificado A3

- Validade de até 5 anos
- Usado geralmente por meio de mídia criptográfica (token ou cartão USB)
- Precisa estar conectada em computador para cada uso
- Caso de perda da mídia, perde-se também o certificado digital

Duvidas, considerações ...

Imagem Ícones MS-Power Point

UNI METRO CAMP wyden

Referências

- BAARS, Hans. Fundamentos de **Segurança da Informação: com base na ISO 27001 e na ISO 27002.** Rio de Janeiro ? RJ ? Editora Brasport, 2018. Capitulo 3. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/160044
- GALVÃO, Michele da Costa, Agnaldo Aragon. **Fundamentos em Segurança da Informação.** Rio de Janeiro ? RJ: Editora Pearson, 2015. Capitulo 3. Disponível em: <https://plataforma.bvirtual.com.br/Acervo/Publicacao/26525>

Referências

- Governo Federal do Brasil. **Obter Certificado Digital.** Disponível em: <https://www.gov.br/pt-br/servicos/obter-certificacao-digital>. Acesso em 12/05/2024
- Otto Carlos Muniz Bandeira Duarte. **Assinatura Digital.** Disponível em: <https://www.gta.ufrj.br/grad/07_1/ass-dig/index.html>. Acesso em 12/05/2024
- C. E. SHANNON ***Communication Theory of Secrecy Systems***. Disponível em: <https://pages.cs.wisc.edu/~rist/642-spring-2014/shannon-secrecy.pdf>. Acesso em 12/05/2024

Referências

- IBM. ***Encryption methods***. Disponível em: <https://www.ibm.com/docs/en/was-zos/9.0.5?topic=apis-encryption-methods>. Acesso em 12/05/2024
- Google. **Google Pay para pagamentos Web**. Disponível em: <https://developers.google.com/pay/api/web/overview?hl=pt-br>. Acesso em 12/05/2024
- SSL.com. **SSL/TLS Aperto de mão: garantindo interações online seguras**. Disponível em: <https://www.ssl.com/pt/article/ssl-tls-handshake-ensuring-secure-online-interactions/>. Acesso em 12/05/2024

Atividade Aula 10
Criptografia

- Utilizar um aplicativo ou página web que criptografe uma frase utilizando chave
- **Objetivo**: Consolidar conhecimento do uso de chave criptográfica
- Realizar em Dupla

- Responder no Teams
- https://forms.office.com/r/YGmCwcd3j3

UNI METRO CAMP wyden

Para Próxima Aula
Assista aos vídeos

- Segurança da Informação Confidencialidade, Integridade e Disponibilidade: https://www.youtube.com/watch?v=3vhz3IFjl7M
- INFORMÁTICA Princípios da SEGURANÇA DA INFORMAÇÃO | REVISÃO rápida com Mapa Mental Explicado: https://www.youtube.com/watch?v=T3CkJMZCrL8
- Não repúdio Segurança da Informação Dicionário de Informática: https://www.youtube.com/watch?v=Nzb_qGPj

UNI METRO CAMP

wyden