Introdução à Criptografia

Prof. Msc. Francisco de Assis de Souza Rodrigues



🎯 Objetivos da Aula

- Compreender os fundamentos da criptografia e sua importância.
- Distinguir criptografia simétrica e assimétrica.
- Explicar o papel das funções hash e assinaturas digitais.
- Aplicar exemplos simples com ferramentas ou bibliotecas.

O que é Criptografia?

🕰️ Breve História da Criptografia

A criptografia é uma **técnica** milenar que começou a ser utilizada **para proteger** a **comunicação secreta**, especialmente em tempos de guerra e conflitos. Ela tem uma rica história, com algumas das primeiras formas de codificação de mensagens sendo bastante simples, mas eficazes.

Vamos ver alguns marcos históricos:

- Cifra de César (cerca de 58 a.C.)
- Máquina Enigma (Segunda Guerra Mundial)

Cifra de César (cerca de 58 a.C.)

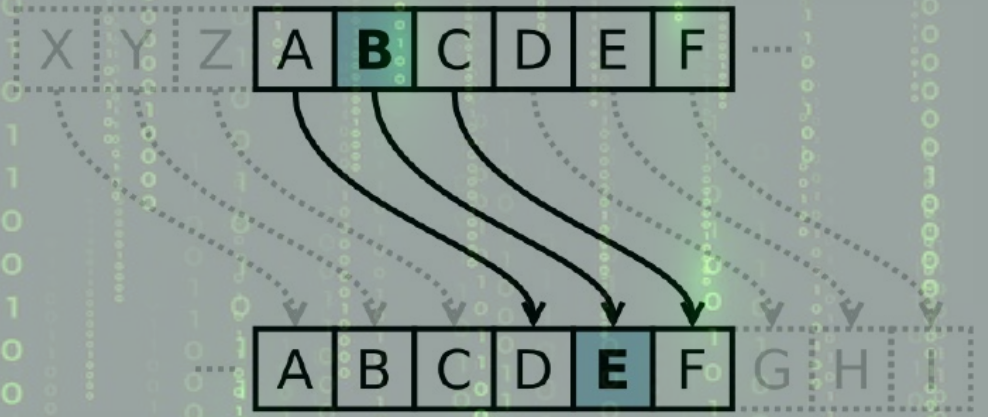
A cifra de César foi uma das primeiras técnicas de criptografia conhecidas. Ela é uma cifra de substituição simples, onde cada letra de uma mensagem é deslocada um número fixo de posições no alfabeto. Por exemplo, se a chave for 3, a letra "A" se torna "D", "B" se torna "E", e assim por diante.

Exemplo:
Mensagem original: **"HELLO"**
Usando uma chave de 3, a mensagem cifrada seria: **"KHOOR"**



Cifra de César (cerca de 58 a.C.)

Texto simples	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifra	D	E	F	G	H	I	J	K	L	M	N	O	P
Texto simples	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifra	Q	R	S	T	U	V	W	X	Y	Z	A	B	C



Máquina Enigma (Segunda Guerra Mundial)

Durante a Segunda Guerra Mundial, os alemães usaram a máquina Enigma para enviar mensagens criptografadas. A máquina usava rotores e um sistema complexo de substituições que dificultavam a quebra da cifra. Ela foi considerada inviolável por muito tempo, até que os aliados, liderados pelo matemático Alan Turing, conseguiram decifrar as mensagens e obter uma vantagem estratégica vital.

Máquina Enigma (Segunda Guerra Mundial)

A quebra da Enigma ilustra como a criptografia pode ser uma questão de segurança crítica em tempos de guerra, e como o avanço da tecnologia pode permitir a quebra de sistemas de criptografia até então considerados seguros.



🧐 Conceito Geral: Proteção da Informação

A criptografia é a prática de proteger a informação através do uso de algoritmos matemáticos, com o objetivo de impedir que pessoas não autorizadas acessem, leiam ou modifiquem dados sensíveis. Ela envolve transformar uma mensagem legível (chamada de texto claro) em uma forma codificada (chamada de texto cifrado), que só pode ser revertida (decifrada) por quem tem a chave correta.

🧐 Conceito Geral: Proteção da Informação

Objetivo da Criptografia:

A criptografia visa garantir que, mesmo que uma mensagem seja interceptada por um atacante, ele não conseguirá entender o seu conteúdo. Ela também é usada para garantir a segurança de transações financeiras, dados pessoais, e comunicação online.

🧐 Conceito Geral: Proteção da Informação

Exemplo do Uso:

- Em uma conexão HTTPS entre um site e um navegador, a criptografia assegura que ninguém, como hackers, possa interceptar e ler a comunicação.
- As senhas armazenadas nos sistemas não ficam em texto simples, mas sim criptografadas, o que impede que quem tenha acesso ao banco de dados veja a senha real do usuário.

⚖️ Três Pilares da Segurança da Informação

A criptografia é uma ferramenta central nos três pilares da segurança da informação, que são fundamentais para garantir que os dados sejam protegidos corretamente.

- Confidencialidade
- Integridade
- Autenticidade

⚖️ Três Pilares da Segurança da Informação

Confidencialidade

- **Definição:** Garante que a informação seja acessada apenas por pessoas ou sistemas autorizados.
- **Exemplo:** Em uma conversa privada via WhatsApp, a criptografia garante que apenas você e a pessoa com quem está conversando possam ler as mensagens. Mesmo se alguém interceptar a comunicação, ela não conseguirá entender o conteúdo sem a chave correta.

⚖️ Três Pilares da Segurança da Informação

Integridade

- **Definição:** Garante que a informação não foi alterada ou corrompida durante a transmissão ou armazenamento.
- **Exemplo:** Ao transferir dinheiro entre contas bancárias, a criptografia garante que o valor da transferência não foi alterado durante o processo. Técnicas como **funções hash** são usadas para verificar se o conteúdo da mensagem foi alterado de alguma forma (ex: adição ou remoção de caracteres).

⚖️ Três Pilares da Segurança da Informação

Autenticidade

- **Definição:** Garante que a origem da informação seja verificada e que a identidade do remetente seja confirmada.
- **Exemplo:** Quando você recebe um e-mail do seu banco, a assinatura digital do e-mail permite que você tenha certeza de que a mensagem realmente veio do banco e não de um impostor. Isso evita ataques como **phishing**, onde um atacante tenta se passar por uma instituição legítima.

Criptografia Simétrica

A criptografia simétrica é um tipo de criptografia onde a mesma chave é usada tanto para cifrar (codificar) quanto para decifrar (desfazer a codificação) a mensagem. A chave secreta deve ser compartilhada entre o remetente e o destinatário de maneira segura antes que eles possam se comunicar de forma confidencial.

Exemplo simples:

Imagine que você e um amigo compartilham uma chave secreta, como uma senha. Para enviar uma mensagem segura, você utiliza essa chave para cifrar a mensagem. Seu amigo, que possui a mesma chave, usada para decifrar a mensagem e entender o conteúdo.

🛡️ Criptografia Simétrica

🔑 Exemplos de Algoritmos Simétricos

AES (Advanced Encryption Standard)

- Um dos algoritmos de criptografia simétrica mais seguros e amplamente utilizados.
- AES pode ter chaves de 128, 192 ou 256 bits.
- Usado em muitas aplicações, incluindo comunicação segura na internet (TLS/SSL), VPNs, e armazenamento seguro de dados.

🛡️ Criptografia Simétrica

🔑 Exemplos de Algoritmos Simétricos

DES (Data Encryption Standard)

- Foi amplamente utilizado em décadas passadas, mas hoje em dia é considerado inseguro devido ao tamanho da chave (56 bits).
- A criptografia com DES é suscetível a ataques de força bruta devido ao número limitado de chaves possíveis.

Criptografia Simétrica

Vantagens da Criptografia Simétrica

- **Eficiência:** A criptografia simétrica é geralmente mais rápida do que a criptografia assimétrica, o que a torna adequada para grandes volumes de dados.
- **Menor sobrecarga computacional:** Como a mesma chave é usada para cifrar e decifrar, o processo é simples e rápido.

Criptografia Simétrica

Desvantagens da Criptografia Simétrica

- **Distribuição da chave:** O maior desafio da criptografia simétrica é como compartilhar a chave secreta de forma segura. Se a chave for interceptada, qualquer pessoa poderá decifrar a mensagem.

- **Escalabilidade:** Em sistemas com muitos usuários, a troca de chaves seguras entre todos os participantes pode se tornar complexa. Para **n** usuários, você precisaria de **n x (n - 1) / 2** chaves únicas.

- **Perda da chave:** Se a chave secreta for perdida ou comprometida, a comunicação segura será perdida, e a integridade da criptografia será comprometida.

🔐 Criptografia Assimétrica

A **criptografia assimétrica** usa **duas chaves diferentes**:

- **Chave pública**: usada para **criptografar** dados.
- **Chave privada**: usada para **descriptografar** os dados.

Essas chaves são matematicamente relacionadas, mas é praticamente impossível descobrir a chave privada a partir da pública.

> **Exemplo de uso**: você quer enviar uma mensagem para Maria. Você criptografa com a *chave pública dela* — e só ela conseguirá ler, porque só ela tem a *chave privada* correspondente.

🔐 Criptografia Assimétrica

🧩 Exemplos de algoritmos

- **RSA** (Rivest-Shamir-Adleman): muito usado na prática, especialmente em assinaturas digitais e troca de chaves.
- **ECC** (Elliptic Curve Cryptography): oferece segurança similar ao RSA, mas com chaves menores (mais rápido e leve, ideal para dispositivos móveis).

🔐 Criptografia Assimétrica

📦 Usos típicos

- **Troca segura de chaves**: usada no início de conexões HTTPS para enviar uma chave simétrica com segurança.
- **Assinatura digital**: o emissor assina uma mensagem com sua chave privada, e qualquer um pode verificar a autenticidade usando sua chave pública.

🔐 Funções Hash

📌 Conceito

Uma **função hash** é um algoritmo que:

- Recebe uma **entrada de qualquer tamanho** (texto, arquivo, senha, etc.)
- Retorna uma **saída de tamanho fixo** (por exemplo, 256 bits no SHA-256)
- É **unidirecional**: não dá para descobrir a entrada a partir do hash gerado
- **Pequenas mudanças na entrada geram resultados totalmente diferentes**

Isso torna as funções hash muito úteis para verificar **integridade**, **autenticar dados** e armazenar senhas com segurança.

🔐 Funções Hash

🧠 Exemplo: SHA-256

SHA-256 é uma das funções hash mais utilizadas, pertencente à família SHA-2, padronizada pela NSA.

- Entrada: qualquer dado (ex: "senha123")
- Saída: um valor de 256 bits (ou 64 caracteres hexadecimais)

🔐 Funções Hash

🔎 Aplicações

1. **Verificação de integridade**
   - Ao baixar arquivos, você pode comparar o hash para confirmar que o conteúdo não foi alterado.

2. **Armazenamento de senhas**
   - Senhas são armazenadas como hash. O sistema compara os hashes (não as senhas em texto).

3. **Blockchain**
   - Cada bloco contém o hash do anterior, garantindo que qualquer alteração corrompe a cadeia.

🔏 Assinatura Digital

📌 Conceito

A **assinatura digital** é uma técnica criptográfica que tem como objetivo:

- **Garantir a integridade** da mensagem (ou seja, que ela não foi alterada);
- **Garantir a autenticidade**, comprovando que a mensagem realmente veio de quem diz ter enviado.

Ela **não serve para manter o conteúdo em sigilo** (isso é papel da criptografia de dados), mas sim para garantir **confiança** na origem e no conteúdo da mensagem.

🔏 Assinatura Digital

🧰 Como funciona o processo

A assinatura digital é composta por duas etapas principais: **geração** e **verificação**.

🔏 Assinatura Digital

✍️ Geração da Assinatura (pelo remetente)

1. **Hash da mensagem**:
   Aplica-se uma função hash (como SHA-256) na mensagem original para obter um resumo fixo (digest).

2. **Criptografa o hash com a chave privada** do remetente:

   - Esse resultado é a **assinatura digital**.

   - Só o remetente tem a chave privada, então só ele pode gerar essa assinatura específica.

🔏 Assinatura Digital

🔍 Verificação da Assinatura (pelo destinatário)

1. **Calcula o hash da mensagem recebida**.

2. **Descriptografa a assinatura digital usando a chave pública do remetente**.
   - Isso revela o hash original gerado por ele.

3. **Compara os dois hashes**:
   - Se forem iguais, a mensagem é **íntegra** e **autêntica**.
   - Se forem diferentes, a mensagem foi alterada ou a assinatura é falsa.

🔏 Assinatura Digital

💡 Por que é confiável?

- A **chave privada** é secreta: só o autor legítimo poderia gerar aquela assinatura.
- A **função hash** é unidirecional e sensível: qualquer pequena mudança no conteúdo muda completamente o hash.

🔏 Assinatura Digital

🧠 Analogia simples

Pense como um **carimbo pessoal**:

- Só você tem o carimbo (chave privada);
- Qualquer pessoa pode verificar sua autenticidade comparando com uma amostra pública (chave pública);
- Se alguém tentar falsificar, o padrão não vai bater.

Google Colab

Experimento:
https://colab.research.google.com/drive/1EipZuduW3J2HpsEc4HfBR33XgnMpwgG6?usp=sharing



📝 Tarefa para a próxima aula

- Pesquisar casos reais de vazamento de dados e como a criptografia poderia ter evitado o problema. Enviar uma análise curta (máx. 1 página).

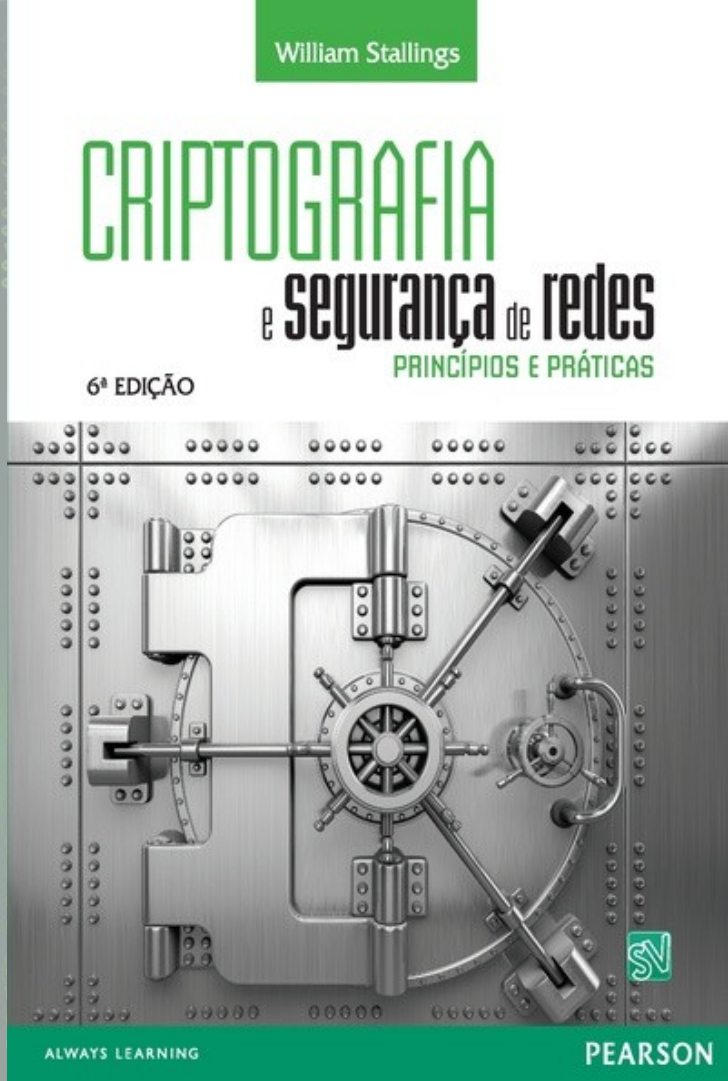
Sugestões de Vídeos





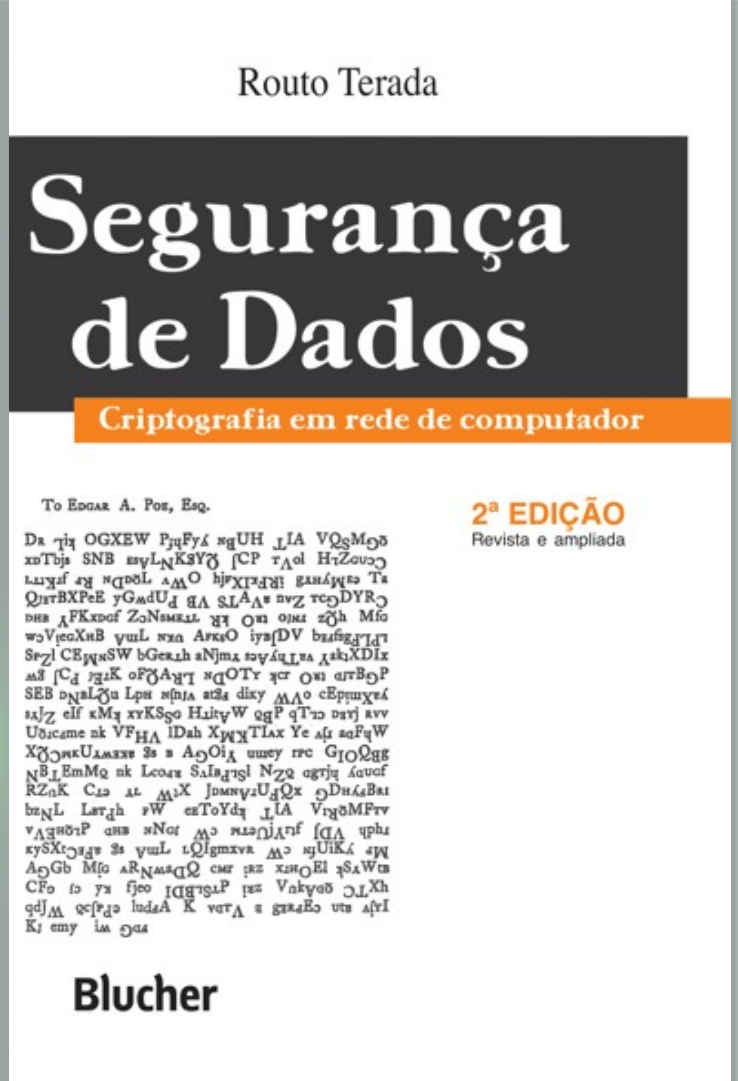
Bibliografia

STALLINGS, William. Criptografia e segurança de redes: princípios e práticas. 6. ed. São Paulo: Pearson, 2015. E-book. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/22446. Acesso em: 02 maio 2025.



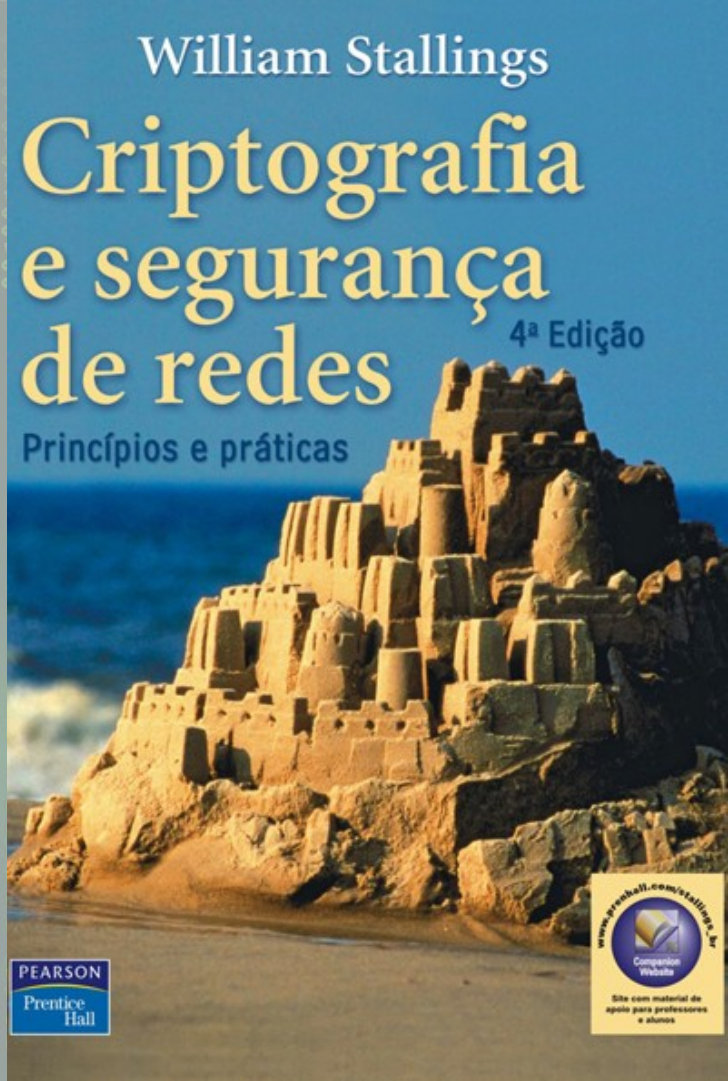
Bibliografia

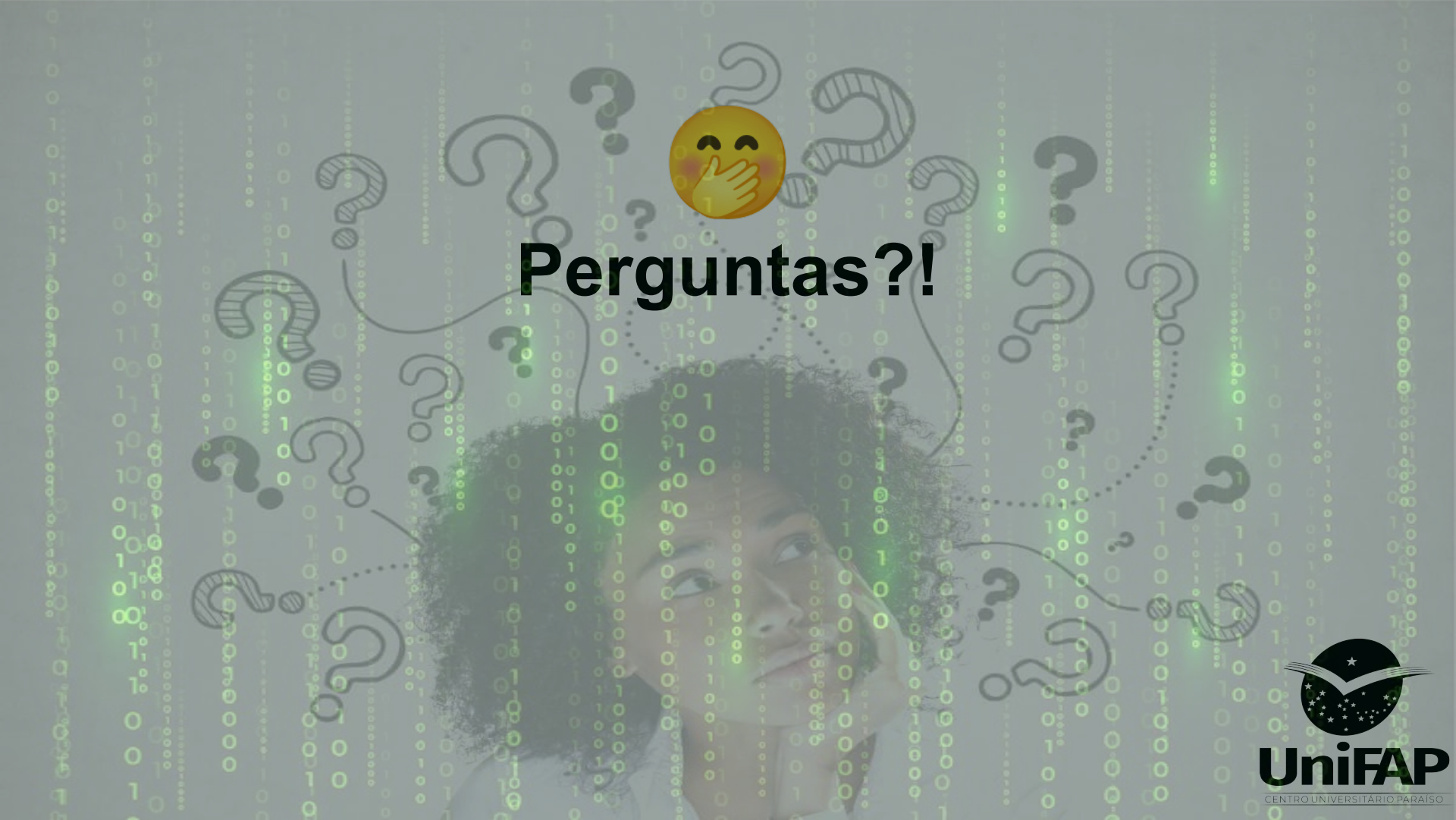
TERADA, Routo. Segurança de dados: criptografia em redes de computador. 2. ed. São Paulo: Blucher, 2008. E-book. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/173353 . Acesso em: 02 maio 2025.



Bibliografia

STALLINGS, William. Criptografia e segurança de redes: princípios e práticas. 4. ed. São Paulo: Pearson, 2008. E-book. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/396. Acesso em: 02 maio 2025.




Perguntas?!
UniFAP
CENTRO UNIVERSITÁRIO PARAÍSO

A tecnologia evolui, mas os desafios humanos permanecem. Use a sabedoria para resolver problemas.

Eclesiastes 1:9 – "Nada há novo debaixo do sol."

UniFAP
CENTRO UNIVERSITÁRIO PARAÍSO



Obrigado!

UniFAP
CENTRO UNIVERSITÁRIO PARAÍSO