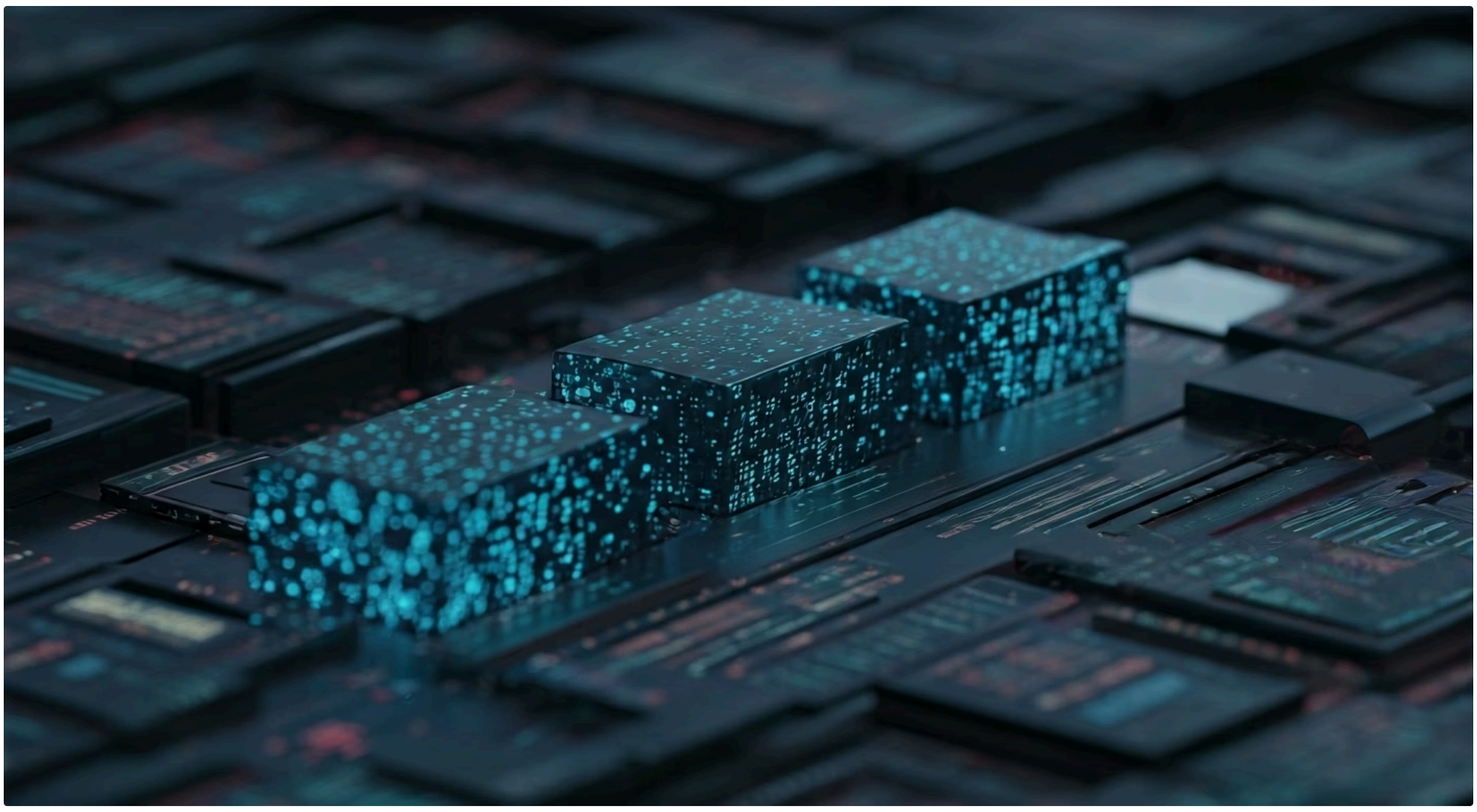
Aula 6 – Algoritmos de Criptografia Simétrica: Parte 1

Imagine que você precisa enviar uma mensagem secreta para um amigo, mas sabe que há espiões tentando interceptá-la. Como garantir que apenas seu amigo consiga ler o conteúdo, mesmo que a mensagem caia em mãos erradas? Essa é a essência da criptografia, uma arte milenar que se tornou a espinha dorsal da segurança digital em nosso mundo conectado.

Nesta aula, mergulharemos no fascinante universo dos algoritmos de criptografia simétrica. Eles são como cadeados e chaves que, embora invisíveis, protegem nossos dados mais sensíveis, desde transações bancárias até conversas pessoais. Compreender como funcionam é crucial não apenas para quem busca aprimorar seus conhecimentos em segurança da informação, mas também para qualquer profissional que lide com dados, dada a crescente importância de leis como a LGPD e a GDPR.

Nosso objetivo é desvendar os mistérios por trás das cifras de bloco, entender como o DES, um padrão histórico, funcionava e por que foi superado, e finalmente, conhecer o poderoso AES, o algoritmo que hoje protege grande parte da nossa comunicação digital. Ao final, você será capaz de identificar os principais algoritmos simétricos, compreender seus modos de operação e reconhecer a importância de cada um no cenário da segurança de dados. Prepare-se para desvendar os segredos que mantêm o mundo digital seguro.

Cifras de Bloco: O Alicerce da Criptografia Moderna



No dia a dia, quando pensamos em criptografia, muitas vezes imaginamos um texto sendo transformado em uma sequência ilegível de caracteres. Mas como essa transformação acontece de forma segura e eficiente? As cifras de bloco são um dos pilares dessa magia, atuando como verdadeiras "máquinas de embaralhar" que operam sobre pedaços fixos de dados.

Pense em uma cifra de bloco como uma máquina de moer carne, mas ao invés de carne, ela processa blocos de informações. Você alimenta a máquina com um pedaço de carne (um bloco de dados de tamanho fixo) e, usando uma receita secreta (a chave criptográfica), ela o transforma em algo completamente diferente (o bloco cifrado). O segredo é que, com a mesma receita e a máquina funcionando ao contrário, você pode obter a carne original de volta. Essa é a beleza da criptografia simétrica: a mesma chave é usada para cifrar e decifrar.

A grande sacada das cifras de bloco é que elas não trabalham com um caractere por vez, mas sim com blocos inteiros de dados. Isso as torna muito eficientes para lidar com grandes volumes de informação. Por exemplo, o AES, que veremos mais adiante, opera com blocos de 128 bits. Isso significa que, a cada operação, 128 bits de dados são transformados em outros 128 bits, garantindo que pequenas mudanças no texto original resultem em grandes mudanças no texto cifrado, dificultando enormemente qualquer tentativa de adivinhação ou quebra.

Modos de Operação: Como as Cifras de Bloco Ganham Flexibilidade

Flexibilidade

Diferentes "programas" para processar dados de qualquer tamanho

Segurança

Escolha do modo correto é crucial para proteção robusta

Adaptação

Cada modo atende diferentes cenários e necessidades

Uma cifra de bloco, por si só, é uma ferramenta poderosa, mas um tanto rígida. Ela só consegue processar blocos de um tamanho específico. E se sua mensagem for maior ou menor que esse bloco? Ou se você precisar de mais segurança em certas situações? É aí que entram os **modos de operação**. Eles são como diferentes "programas" ou "configurações" para a sua máquina de moer carne, permitindo que ela lide com diferentes cenários e necessidades de segurança.

Os modos de operação definem como uma cifra de bloco é aplicada repetidamente para cifrar dados de qualquer tamanho, e como ela interage com o texto puro e o texto cifrado. Eles são cruciais para a segurança, pois um modo de operação mal escolhido pode comprometer a robustez de um algoritmo criptográfico, mesmo que o algoritmo em si seja forte. Vamos explorar os mais comuns.

Modo ECB (Electronic Codebook): Simples, mas Perigoso

O modo de operação mais direto e, ironicamente, um dos mais perigosos para a maioria das aplicações, é o **Electronic Codebook (ECB)**. Sua simplicidade é tentadora: cada bloco de texto puro é cifrado independentemente dos outros, usando a mesma chave.

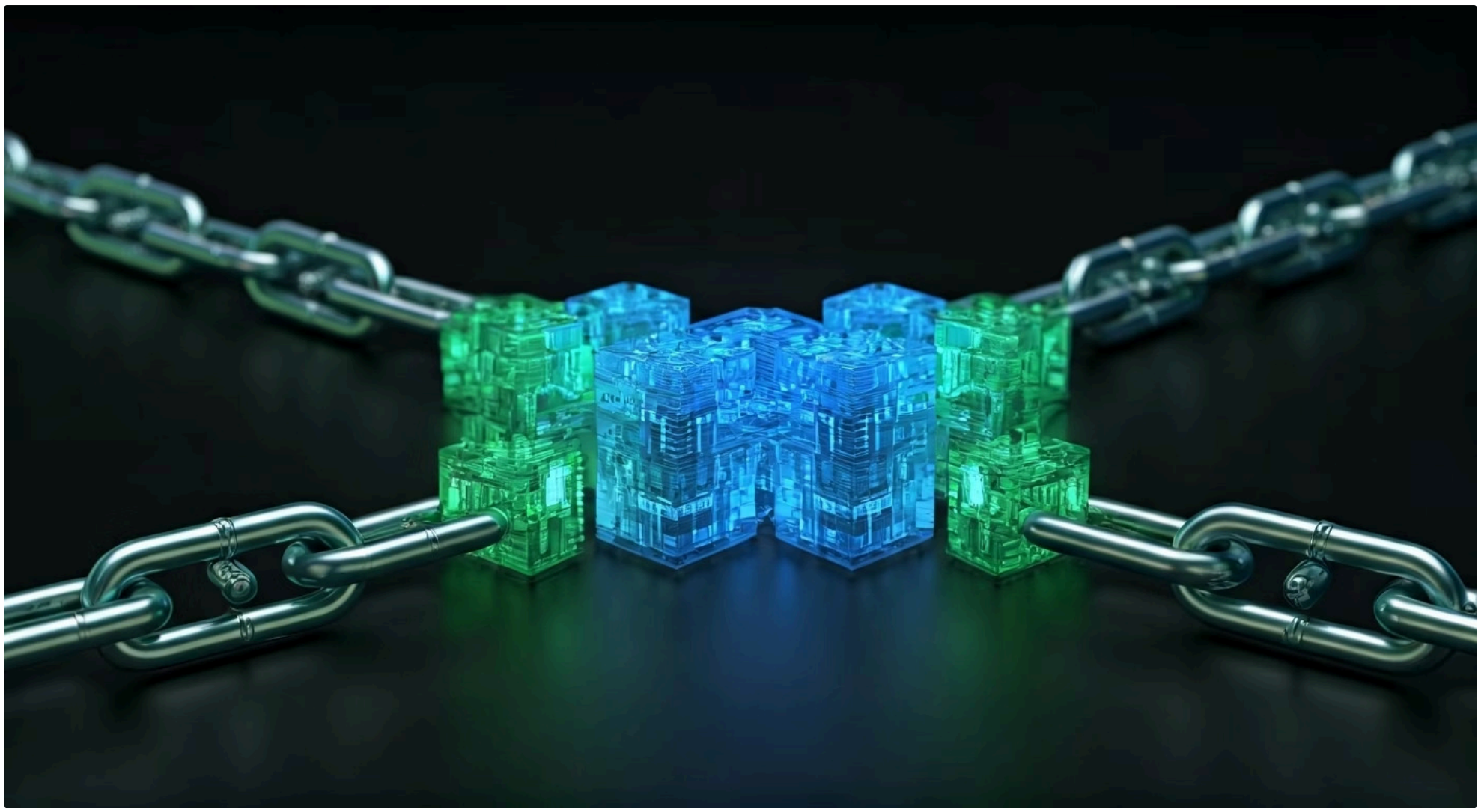
Imagine que você tem um livro de códigos secreto, onde cada palavra comum (bloco de texto puro) tem uma palavra cifrada correspondente. Se você encontrar a palavra "ataque" no livro, ela sempre será cifrada como "XyZ123". No modo ECB, é exatamente isso que acontece: se dois blocos de texto puro forem idênticos, seus blocos cifrados também serão idênticos. Isso pode parecer inofensivo, mas as implicações de segurança são enormes.

> ⚠️ **Vulnerabilidade Crítica**
>
> A grande vulnerabilidade do ECB reside na sua falta de "aleatoriedade". Como blocos idênticos geram cifrados idênticos, padrões no texto original podem ser facilmente identificados no texto cifrado.

Pense em uma imagem digital, que é composta por muitos blocos de pixels. Se você cifrar essa imagem com ECB, a estrutura e as cores gerais da imagem original ainda serão visíveis no resultado cifrado, pois blocos de pixels com a mesma cor ou padrão serão cifrados para o mesmo valor. Isso é inaceitável para a privacidade e segurança de dados.

Por essa razão, o ECB é raramente recomendado para cifrar dados que contenham qualquer tipo de padrão repetitivo, como imagens, áudios ou grandes volumes de texto. Sua aplicação é restrita a cenários muito específicos, como a cifragem de chaves criptográficas únicas, onde cada chave é um bloco diferente e não há repetição de padrões.

Modo CBC (Cipher Block Chaining): Encadeando a Segurança



Para superar as deficiências do ECB, foi desenvolvido o modo **Cipher Block Chaining (CBC)**. Este modo introduz uma dependência entre os blocos cifrados, tornando o processo muito mais seguro e resistente à análise de padrões.

Pense no CBC como uma linha de montagem onde cada peça (bloco de dados) que entra é influenciada pela peça anterior. Antes de ser cifrado, cada bloco de texto puro é combinado (usando uma operação XOR) com o bloco cifrado *anterior*. O resultado dessa combinação é então cifrado. Para o primeiro bloco, como não há um bloco cifrado anterior, usa-se um valor inicial aleatório e único, chamado **Vetor de Inicialização (IV)**.

01

Combinação XOR

Bloco de texto puro é combinado com bloco cifrado anterior

02

Cifragem

Resultado da combinação é cifrado com a chave

03

Encadeamento

Bloco cifrado alimenta o próximo bloco na cadeia

04

IV Inicial

Vetor de Inicialização único inicia a cadeia

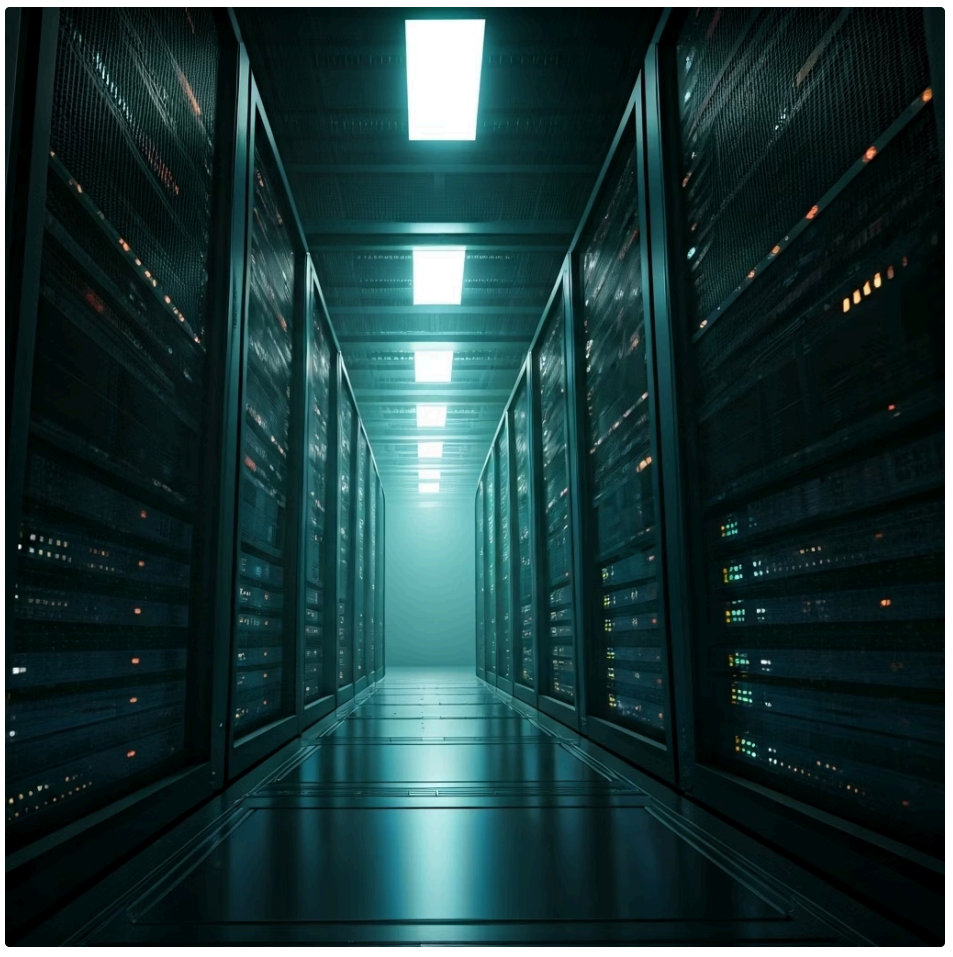
Essa "cadeia" de dependências garante que, mesmo que dois blocos de texto puro sejam idênticos, seus blocos cifrados serão completamente diferentes, pois eles foram combinados com blocos cifrados anteriores distintos. O IV, que deve ser imprevisível e único para cada operação de cifragem, é crucial para a segurança do CBC, pois ele "semeia" a aleatoriedade no início da cadeia.

O CBC é amplamente utilizado em diversas aplicações, como a proteção de dados em disco e a comunicação segura em protocolos como o SSL/TLS (embora versões mais modernas prefiram outros modos). Sua capacidade de ocultar padrões e fornecer uma forte integridade de dados o torna uma escolha robusta para a maioria das necessidades de criptografia de dados em massa.

Modo CTR (Counter): A Flexibilidade do Contador

Outro modo de operação muito popular e versátil é o **Counter (CTR)**. Diferente do CBC, que encadeia blocos, o CTR transforma a cifra de bloco em uma cifra de fluxo, oferecendo vantagens significativas em termos de desempenho e paralelização.

Imagine que, em vez de cifrar os dados diretamente, você está gerando uma sequência de "máscaras" aleatórias. Cada máscara é criada cifrando um contador que é incrementado a cada bloco. Essa máscara é então combinada (via XOR) com o bloco de texto puro para produzir o bloco cifrado. Para decifrar, o processo é o mesmo: o contador é incrementado, a máscara é gerada e combinada com o bloco cifrado para revelar o texto puro.



⚡ Paralelização

Blocos podem ser processados simultaneamente, ideal para multi-core

🚀 Alta Performance

Excelente para servidores e sistemas que exigem velocidade

📦 Sem Padding

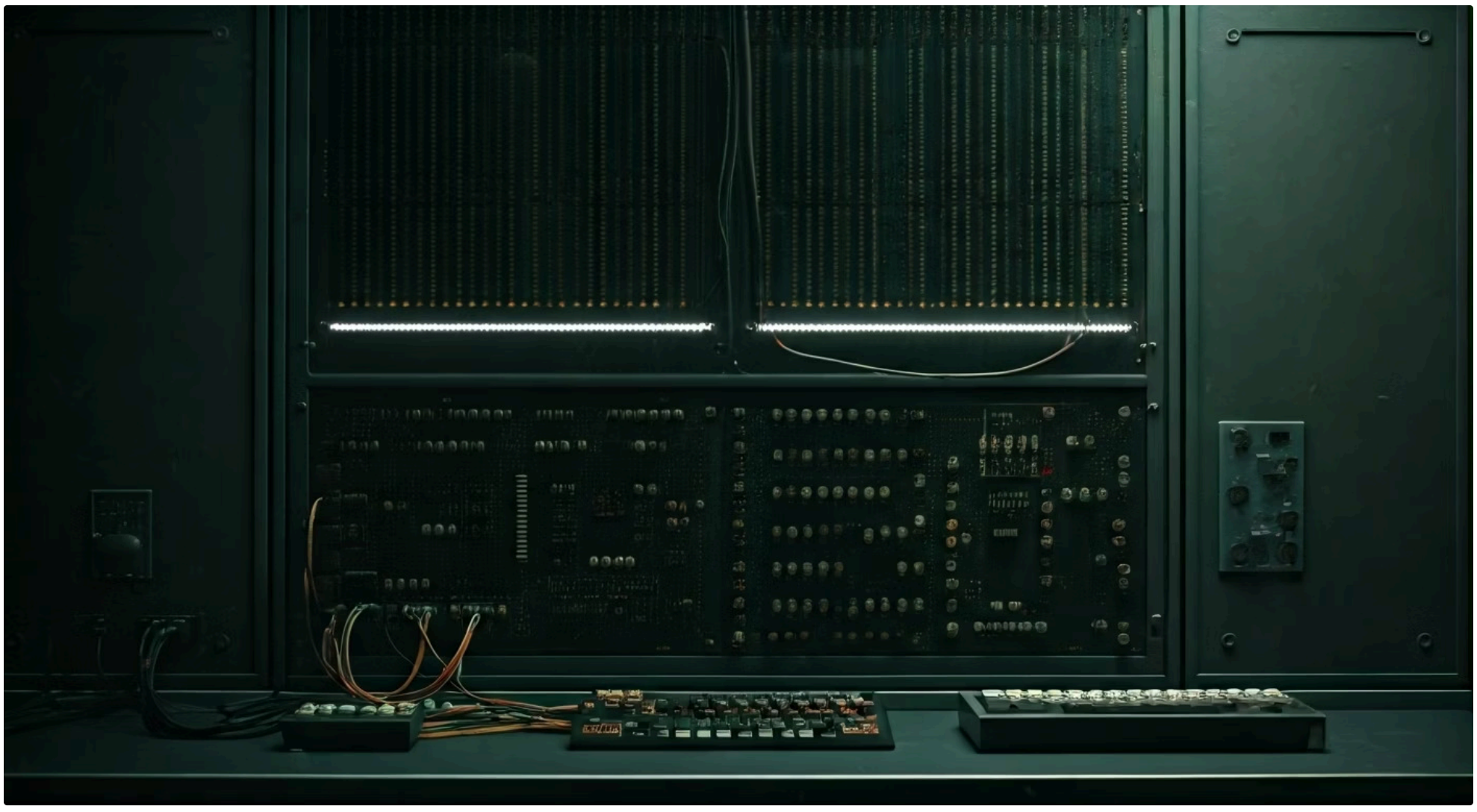
Não requer preenchimento para o último bloco

A grande vantagem do CTR é que cada bloco pode ser cifrado ou decifrado independentemente dos outros, desde que o contador seja sincronizado. Isso permite que as operações de cifragem e decifragem sejam realizadas em paralelo, o que é excelente para sistemas que precisam de alta performance, como servidores de dados ou processadores multi-core. Além disso, o CTR não requer preenchimento (padding) para o último bloco, o que simplifica o manuseio de dados de tamanhos variados.

O CTR é amplamente utilizado em protocolos de rede e sistemas de armazenamento de dados, especialmente onde a velocidade e a capacidade de processamento paralelo são críticas. Sua natureza de cifra de fluxo também o torna ideal para aplicações onde a perda de pacotes é comum, pois um erro em um bloco não afeta a decifragem dos blocos subsequentes.

Conceito	Âmbito/Aplicação	Base/Origem	Exemplo de Uso
ECB	Cifragem de chaves únicas	Cifra de bloco direta	Cifragem de chaves mestras
CBC	Cifragem de dados em massa	Encadeamento de blocos	Proteção de arquivos em disco
CTR	Cifragem de fluxo, alta performance	Contador incrementado	Protocolos de rede (TLS 1.3)

O Padrão DES (Data Encryption Standard): Um Gigante do Passado



Agora que entendemos os modos de operação, vamos voltar no tempo para conhecer um dos algoritmos mais influentes da história da criptografia: o **Data Encryption Standard (DES)**. Desenvolvido pela IBM e adotado como padrão federal nos EUA em 1977, o DES foi, por décadas, o algoritmo simétrico mais utilizado no mundo, protegendo desde transações financeiras até comunicações governamentais.

Pense no DES como o "Fusca" da criptografia. Foi um carro revolucionário para sua época, confiável e amplamente adotado. Ele introduziu muitos conceitos que ainda são relevantes hoje, como a estrutura de Feistel, que permite que a cifragem e a decifragem usem a mesma lógica, apenas invertendo a ordem das chaves. Sua arquitetura era complexa e bem pensada para os recursos computacionais da época, mas o tempo e o avanço tecnológico revelaram suas limitações.

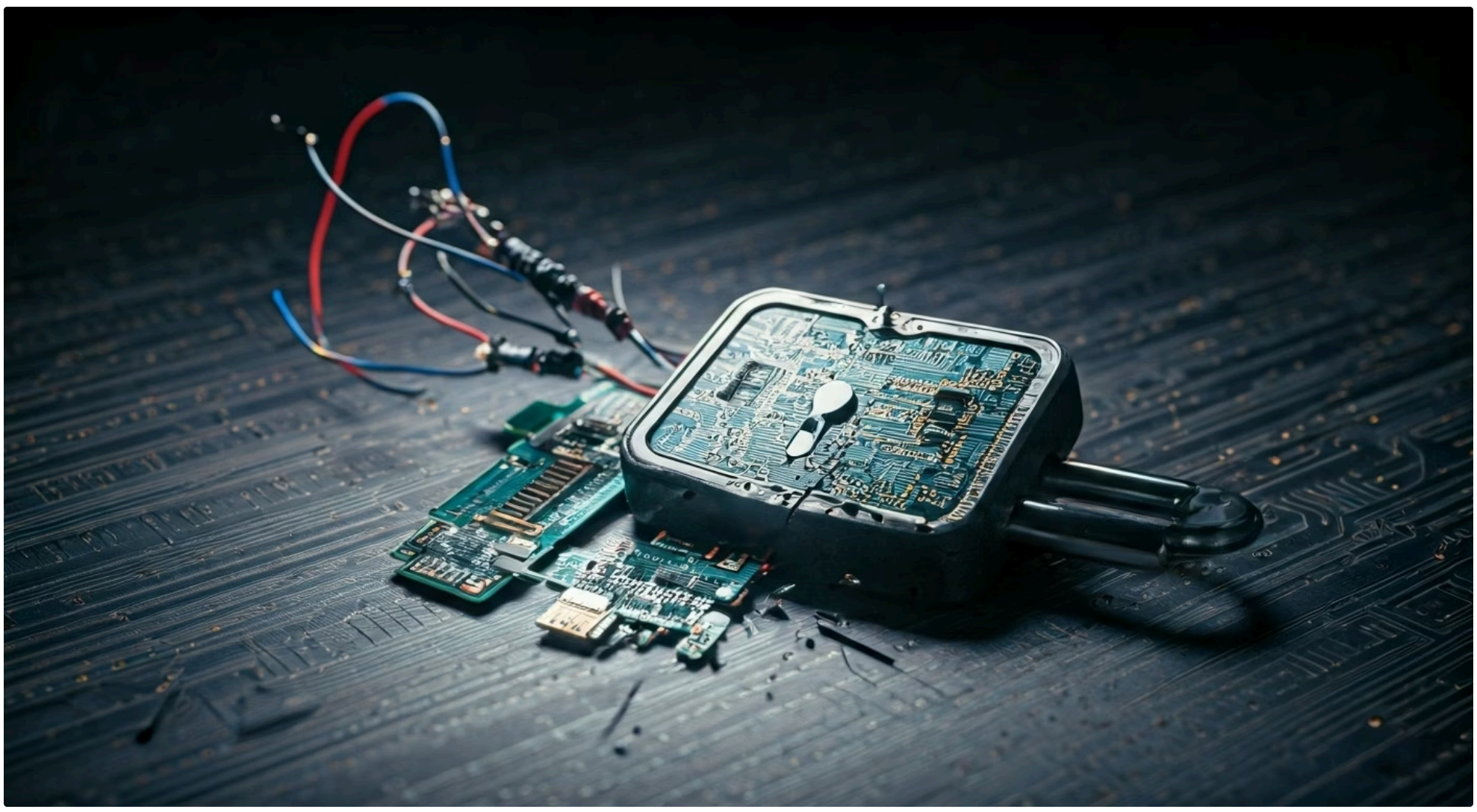
🔧 Arquitetura Técnica

A arquitetura do DES é baseada em uma **cifra de Feistel**, que divide o bloco de dados em duas metades e aplica uma série de operações de substituição e permutação (S-boxes e P-boxes) em 16 rodadas. A cada rodada, uma subchave diferente, derivada da chave principal, é utilizada. Essa estrutura garante que, mesmo com uma chave relativamente curta, o processo de cifragem seja complexo o suficiente para resistir a ataques por um bom tempo.

Vulnerabilidades do DES: O Calcanhar de Aquiles

Apesar de sua importância histórica e robustez inicial, o DES começou a mostrar sinais de fraqueza à medida que a tecnologia avançava. Sua principal vulnerabilidade não estava em sua arquitetura interna, que era bastante sólida, mas sim no tamanho de sua chave.

O DES utilizava uma chave de 56 bits. Em 1977, essa chave era considerada segura o suficiente para resistir a ataques de força bruta (tentar todas as combinações possíveis). No entanto, com o exponencial aumento do poder computacional, especialmente a partir dos anos 90, essa chave de 56 bits tornou-se cada vez mais fácil de ser quebrada. Pense em uma fechadura com 56 pinos: para um ladrão com poucas ferramentas, é impossível. Mas para um especialista com um arsenal de equipamentos, torna-se uma questão de tempo.



Em 1998, o projeto DES-Challange II, organizado pela Electronic Frontier Foundation (EFF), conseguiu quebrar uma chave DES em menos de três dias usando um hardware customizado de US$ 250.000. Pouco tempo depois, o mesmo grupo quebrou uma chave em menos de 23 horas. Isso demonstrou de forma inequívoca que o DES não era mais adequado para proteger informações sensíveis. A capacidade de processamento dos computadores havia superado a segurança oferecida pela chave de 56 bits, tornando o algoritmo obsoleto para a maioria das aplicações.

> **Lição crucial:** A segurança de um algoritmo não depende apenas de sua complexidade matemática, mas também do tamanho da chave e do poder computacional disponível para os atacantes. O que é seguro hoje pode não ser amanhã, exigindo uma constante evolução e substituição de padrões.

O Triple DES (3DES): Uma Solução Temporária e Necessária

Diante da crescente vulnerabilidade do DES, a comunidade de segurança precisava de uma solução rápida. Desenvolver um algoritmo completamente novo e testá-lo rigorosamente levaria tempo. A resposta veio na forma do **Triple DES (3DES ou TDES)**, uma adaptação engenhosa que estendia a vida útil do DES.

Imagine que, para tornar sua fechadura de 56 pinos mais segura, você não a substitui, mas sim a instala três vezes, em sequência, com chaves diferentes. É exatamente isso que o 3DES faz. Ele aplica o algoritmo DES três vezes consecutivas a cada bloco de dados, usando duas ou três chaves distintas. A operação mais comum é Cifrar-Decifrar-Cifrar (EDE), onde o texto puro é cifrado com a Chave 1 (K1), o resultado é decifrado com a Chave 2 (K2) e, finalmente, cifrado novamente com a Chave 1 (K1) ou uma terceira Chave 3 (K3).

Cifrar (K1)

Primeira camada de cifragem

Decifrar (K2)

Operação intermediária

Cifrar (K3)

Camada final de proteção

A principal vantagem do 3DES era que ele aumentava efetivamente o tamanho da chave, elevando a segurança para um nível aceitável para a época. Com três chaves de 56 bits, a segurança efetiva era de aproximadamente 112 bits (no caso de K1, K2, K3 distintas) ou 168 bits (no caso de K1, K2, K3 distintas), tornando-o muito mais resistente a ataques de força bruta do que o DES original. Isso permitiu que sistemas existentes que dependiam do DES pudessem ser atualizados com relativa facilidade, sem a necessidade de uma reengenharia completa.

⚠️ Limitações do 3DES

No entanto, o 3DES era uma solução paliativa. Sua principal desvantagem era o desempenho. Realizar três operações DES para cada bloco de dados tornava-o significativamente mais lento do que o DES original e, mais tarde, do que o AES. Além disso, embora mais seguro que o DES, ele ainda era suscetível a certos ataques criptográficos e não oferecia a mesma margem de segurança que algoritmos mais modernos. Por isso, o 3DES foi gradualmente descontinuado, com o NIST (National Institute of Standards and Technology) recomendando sua transição para o AES.

Introdução ao AES (Advanced Encryption Standard): O Padrão Atual

Com as limitações do DES e 3DES evidentes, a necessidade de um novo padrão criptográfico se tornou urgente. Em 1997, o NIST lançou um concurso público para encontrar um substituto, e em 2001, o algoritmo **Rijndael** foi selecionado, tornando-se o **Advanced Encryption Standard (AES)**. Hoje, o AES é o algoritmo de criptografia simétrica mais amplamente utilizado e reconhecido globalmente, protegendo desde dados em nuvem até comunicações militares.

Velocidade

Extremamente rápido e eficiente em software e hardware

Segurança

Robusto contra ataques de força bruta por décadas

Flexibilidade

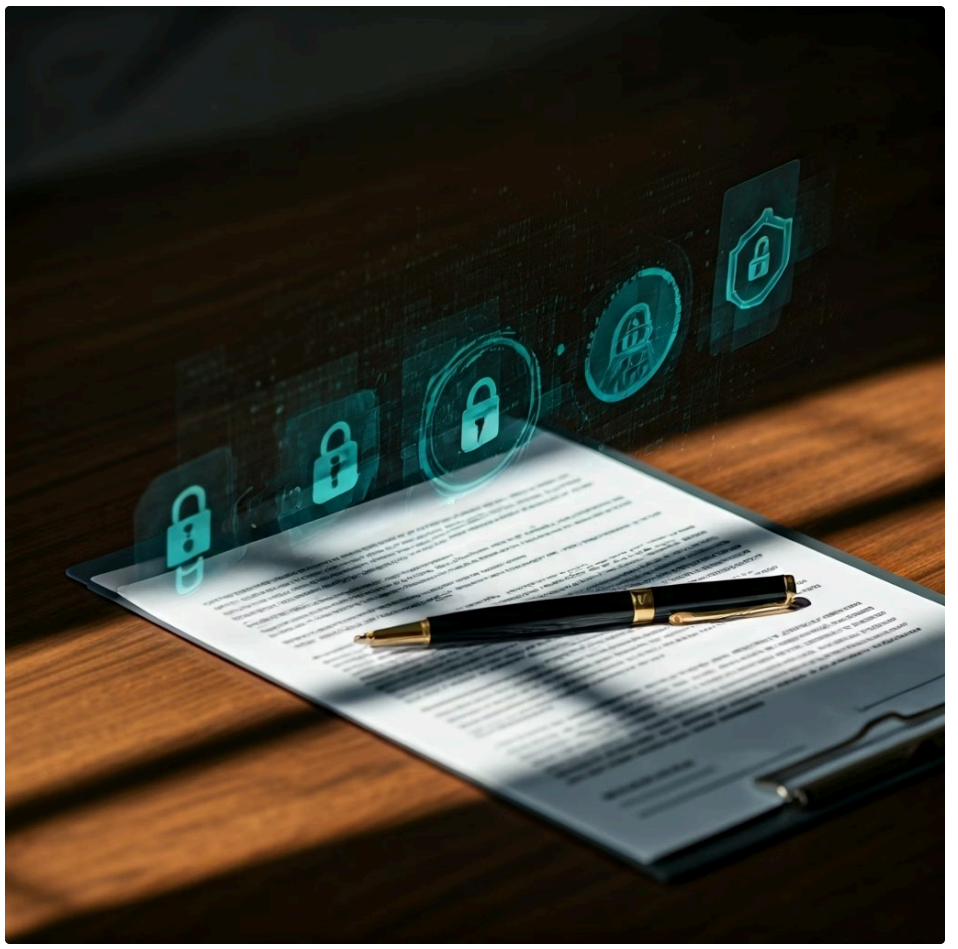
Suporta chaves de 128, 192 ou 256 bits

Pense no AES como o "carro esportivo" da criptografia moderna. Ele é rápido, eficiente e extremamente seguro. Diferente do DES, que usa uma estrutura de Feistel, o AES é baseado em uma **rede de substituição-permutação (SPN)**, o que o torna mais adequado para implementações de software e hardware. Ele opera em blocos de 128 bits e suporta chaves de 128, 192 ou 256 bits, oferecendo um nível de segurança que é considerado robusto contra ataques de força bruta por muitas décadas.

A escolha do AES não foi aleatória. Ele passou por um rigoroso processo de avaliação por criptógrafos de todo o mundo, que analisaram sua segurança, desempenho e flexibilidade. Sua arquitetura é projetada para ser eficiente em uma ampla gama de plataformas, desde pequenos dispositivos embarcados até supercomputadores. Isso o torna a escolha ideal para proteger uma vasta gama de aplicações, desde a segurança de redes Wi-Fi (WPA2/WPA3) até a criptografia de discos rígidos (BitLocker, FileVault) e a proteção de dados em trânsito na internet (TLS).

> A introdução do AES marcou um divisor de águas na criptografia simétrica, estabelecendo um novo patamar de segurança e eficiência. Sua ubiquidade e a confiança depositada nele por governos, empresas e indivíduos sublinham sua importância como a espinha dorsal da proteção de dados no século XXI.

Criptografia Simétrica e a Proteção de Dados: LGPD e GDPR



A compreensão dos algoritmos de criptografia simétrica não é apenas um exercício técnico; ela tem implicações diretas e profundas na conformidade com legislações de proteção de dados, como a **Lei Geral de Proteção de Dados (LGPD)** no Brasil e o **Regulamento Geral sobre a Proteção de Dados (GDPR)** na Europa. Ambas as leis exigem que as organizações implementem medidas técnicas e organizacionais adequadas para proteger os dados pessoais.

Privacy by Design

Segurança da informação e proteção desde a concepção

Pseudonimização

Dados cifrados reduzem riscos de vazamento

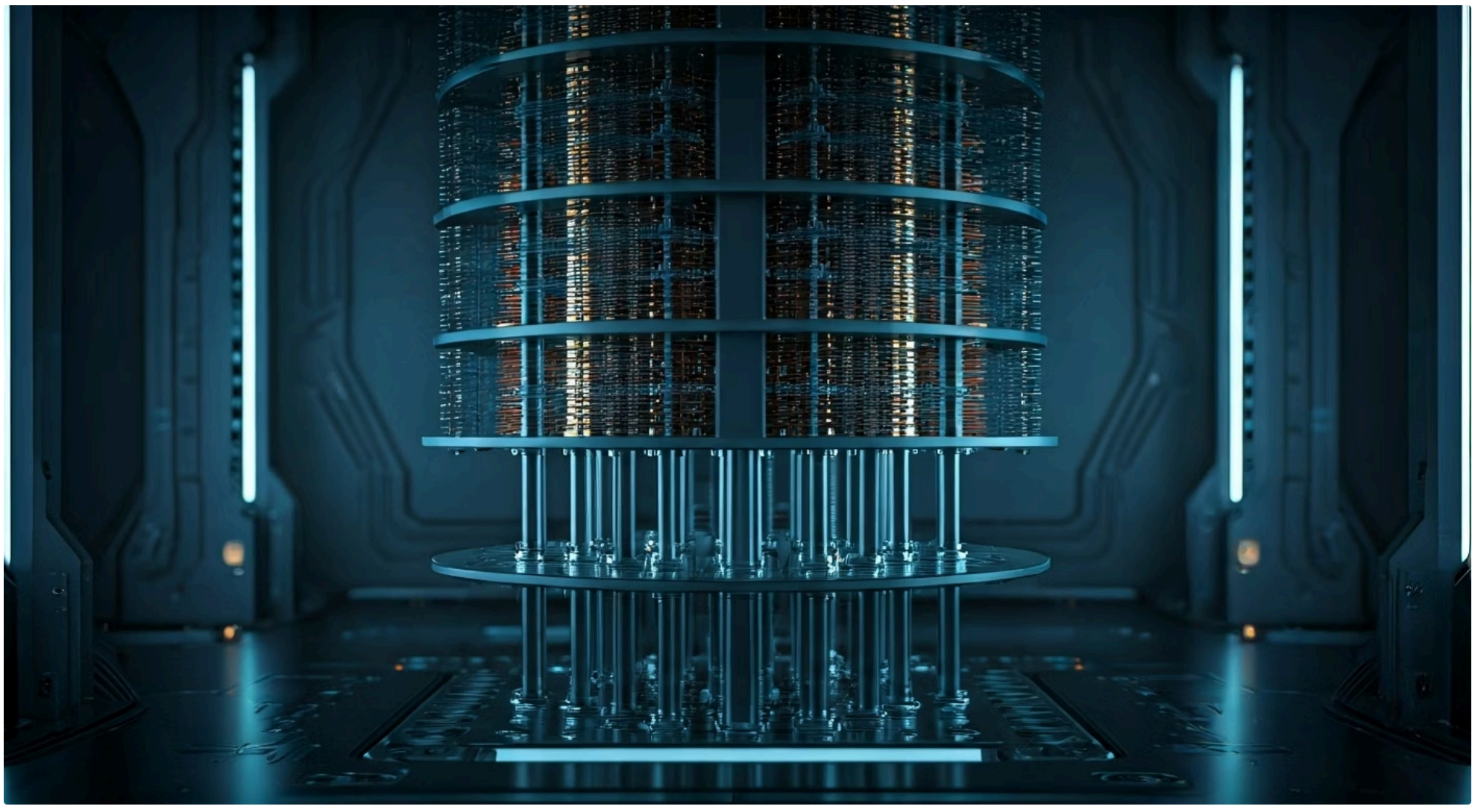
Conformidade

Criptografia adequada evita multas pesadas

Pense na criptografia como uma das ferramentas mais poderosas no arsenal de qualquer empresa que lida com dados pessoais. Quando a LGPD e a GDPR falam em "segurança da informação" e "proteção de dados desde a concepção e por padrão" (Privacy by Design), elas estão implicitamente apontando para a necessidade de usar técnicas como a criptografia. Um dado pessoal cifrado com um algoritmo robusto como o AES, e com uma chave bem gerenciada, é considerado "pseudonimizado" ou até mesmo "anonimizado" em certos contextos, reduzindo significativamente o risco de vazamento e as penalidades associadas.

A escolha do algoritmo e do modo de operação corretos é vital. Por exemplo, cifrar dados em repouso (armazenados em um banco de dados ou disco) com AES no modo CBC ou CTR é uma prática recomendada. Para dados em trânsito (enviados pela internet), a criptografia simétrica é usada dentro de protocolos como TLS/SSL, que primeiro estabelecem uma chave simétrica segura usando criptografia assimétrica, e depois usam essa chave para cifrar a comunicação de forma eficiente. A não utilização de criptografia adequada em cenários de risco pode resultar em multas pesadas e danos à reputação da organização, conforme previsto por essas legislações.

Criptografia Pós-Quântica (PQC): O Futuro Desafiador



Enquanto o AES é considerado seguro contra ataques de computadores clássicos, o horizonte da computação quântica apresenta um novo e formidável desafio para a criptografia atual. A **Criptografia Pós-Quântica (PQC)** é um campo de pesquisa que busca desenvolver algoritmos capazes de resistir a ataques de computadores quânticos em larga escala.

Algoritmo de Grover

Acelera ataques de força bruta contra chaves simétricas, reduzindo segurança efetiva de 256 bits para ~128 bits

Chaves Maiores

Necessidade de chaves simétricas ainda maiores ou algoritmos com maior resistência

Foco em Assimétricos

PQC prioriza substituição de RSA e ECC, mais vulneráveis ao algoritmo de Shor

Embora os algoritmos simétricos como o AES sejam menos diretamente ameaçados por computadores quânticos do que os algoritmos assimétricos (que podem ser quebrados pelo algoritmo de Shor), eles ainda enfrentam riscos. O algoritmo de Grover, por exemplo, pode acelerar ataques de força bruta contra chaves simétricas, reduzindo a segurança efetiva de uma chave de 256 bits para algo próximo a 128 bits. Isso significa que, para manter o mesmo nível de segurança no futuro quântico, talvez precisemos de chaves simétricas ainda maiores ou de algoritmos simétricos com maior resistência.

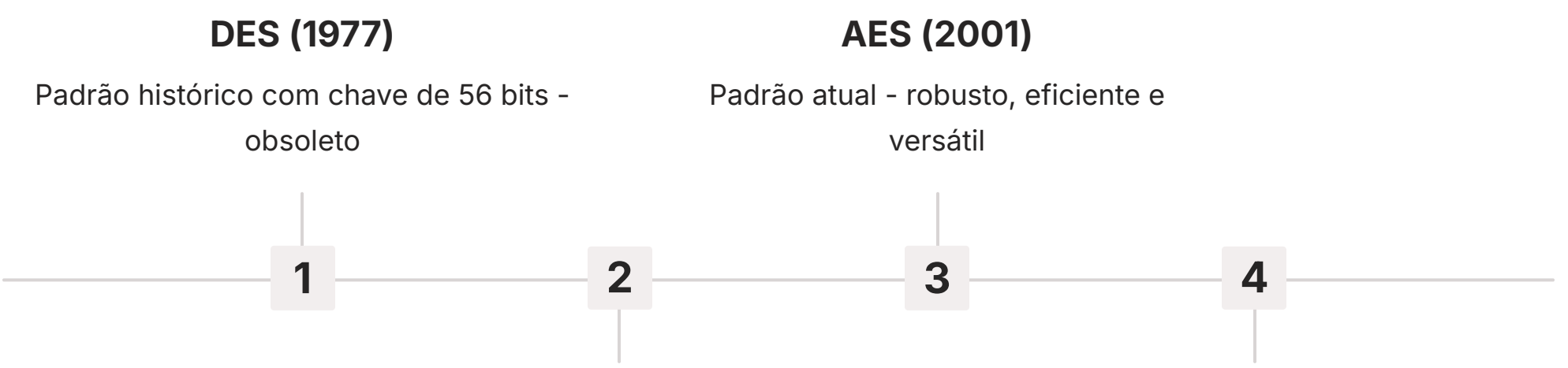
🔮 Privacy by Design no Futuro Quântico

A PQC está focada principalmente em substituir os algoritmos assimétricos (como RSA e ECC) que são usados para troca de chaves e assinaturas digitais, pois estes são os mais vulneráveis. No entanto, a transição para um mundo pós-quântico afetará todo o ecossistema criptográfico. A "Privacidade por Design" (Privacy by Design), um princípio fundamental da LGPD e GDPR, exigirá que as organizações considerem a resistência quântica em suas arquiteturas de segurança desde o início, garantindo que os sistemas de hoje possam ser atualizados para proteger os dados contra ameaças futuras.

A pesquisa em PQC está em pleno vapor, com o NIST liderando um esforço global para padronizar novas famílias de algoritmos. Embora o AES continue sendo a escolha robusta para a criptografia simétrica hoje, a conscientização sobre os desafios quânticos é crucial para planejar a segurança de longo prazo e garantir que a proteção de dados permaneça eficaz nas próximas décadas.

Consolidação e Aplicação Prática

Nesta aula, desvendamos os fundamentos dos algoritmos de criptografia simétrica, essenciais para a segurança digital. Começamos entendendo as **cifras de bloco** e seus **modos de operação** – ECB, CBC e CTR – cada um com suas particularidades e aplicações. Vimos que, enquanto o ECB é simples, mas vulnerável a padrões, o CBC e o CTR oferecem maior segurança e flexibilidade, sendo amplamente utilizados em cenários diversos, desde a proteção de arquivos até a comunicação em rede.



Em seguida, exploramos a história do **DES**, um algoritmo que marcou uma era, mas que sucumbiu ao avanço do poder computacional devido ao seu tamanho de chave limitado. Conhecemos o **3DES** como uma solução temporária engenhosa, que estendeu a vida útil do DES, mas com custos de desempenho. Finalmente, fomos apresentados ao **AES**, o padrão ouro da criptografia simétrica atual, reconhecido por sua robustez, eficiência e versatilidade, sendo a base da segurança de dados em todo o mundo.

Conectamos esses conceitos à realidade das **legislações de proteção de dados como LGPD e GDPR**, mostrando como a criptografia é uma ferramenta indispensável para a conformidade e a mitigação de riscos. E, olhando para o futuro, introduzimos a **Criptografia Pós-Quântica (PQC)**, um campo emergente que busca preparar nossos sistemas para os desafios impostos pela computação quântica, garantindo que a "Privacidade por Design" continue sendo uma realidade.

✅ Em prática

Ao projetar um sistema de segurança, sempre prefira o AES com chaves de 128 bits ou mais. Escolha modos de operação como CBC ou CTR para a maioria dos dados, evitando o ECB. Garanta que suas chaves sejam geradas e gerenciadas de forma segura. Lembre-se que a criptografia é uma camada vital na proteção de dados, mas não a única.

Autoavaliação

1

Questão 1

Qual dos modos de operação de cifra de bloco é mais suscetível à identificação de padrões no texto cifrado, caso o texto puro contenha repetições?

- a) CBC
- b) CTR
- c) ECB
- d) GCM

2

Questão 2

O principal motivo para o DES ter se tornado obsoleto foi:

- a) Sua arquitetura de Feistel ser inerentemente fraca.
- b) O tamanho de sua chave (56 bits) ter se tornado insuficiente frente ao poder computacional.
- c) A complexidade de sua implementação em hardware.
- d) A descoberta de falhas matemáticas em suas S-boxes.

3

Questão 3

Qual algoritmo de criptografia simétrica é o padrão atual e oferece chaves de 128, 192 ou 256 bits?

- a) DES
- b) 3DES
- c) RSA
- d) AES

4

Questão 4

A Criptografia Pós-Quântica (PQC) busca desenvolver algoritmos que:

- a) Aumentem a velocidade de cifragem em computadores clássicos.
- b) Sejam imunes a ataques de força bruta em qualquer cenário.
- c) Resistam a ataques de computadores quânticos em larga escala.
- d) Substituam completamente a criptografia simétrica.

Gabarito

1. c)

2. b)

3. d)

4. c)

Questão Discursiva

> Explique como a escolha de um modo de operação inadequado para uma cifra de bloco, como o ECB, pode comprometer a conformidade de uma organização com a LGPD ou a GDPR, mesmo que o algoritmo subjacente (como o AES) seja considerado forte.

Próxima Aula

> 📚 **Aula 7 – Algoritmos de Criptografia Simétrica: Parte 2**
>
> Na próxima aula, aprofundaremos em outros algoritmos simétricos, exploraremos o gerenciamento de chaves e discutiremos a integração da criptografia em sistemas complexos.

Recursos Adicionais

- **NIST Special Publication 800-38A:** Para detalhes técnicos sobre modos de operação.
- **Livro "Criptografia e Segurança de Redes" de William Stallings:** Uma referência completa sobre o tema.
- **Site oficial da ANPD (Autoridade Nacional de Proteção de Dados):** Para informações atualizadas sobre a LGPD.

NOTA IMPORTANTE: As informações regulatórias/legais/técnicas desta aula estão atualizadas até 2025. Consulte sempre fontes oficiais para verificar alterações.