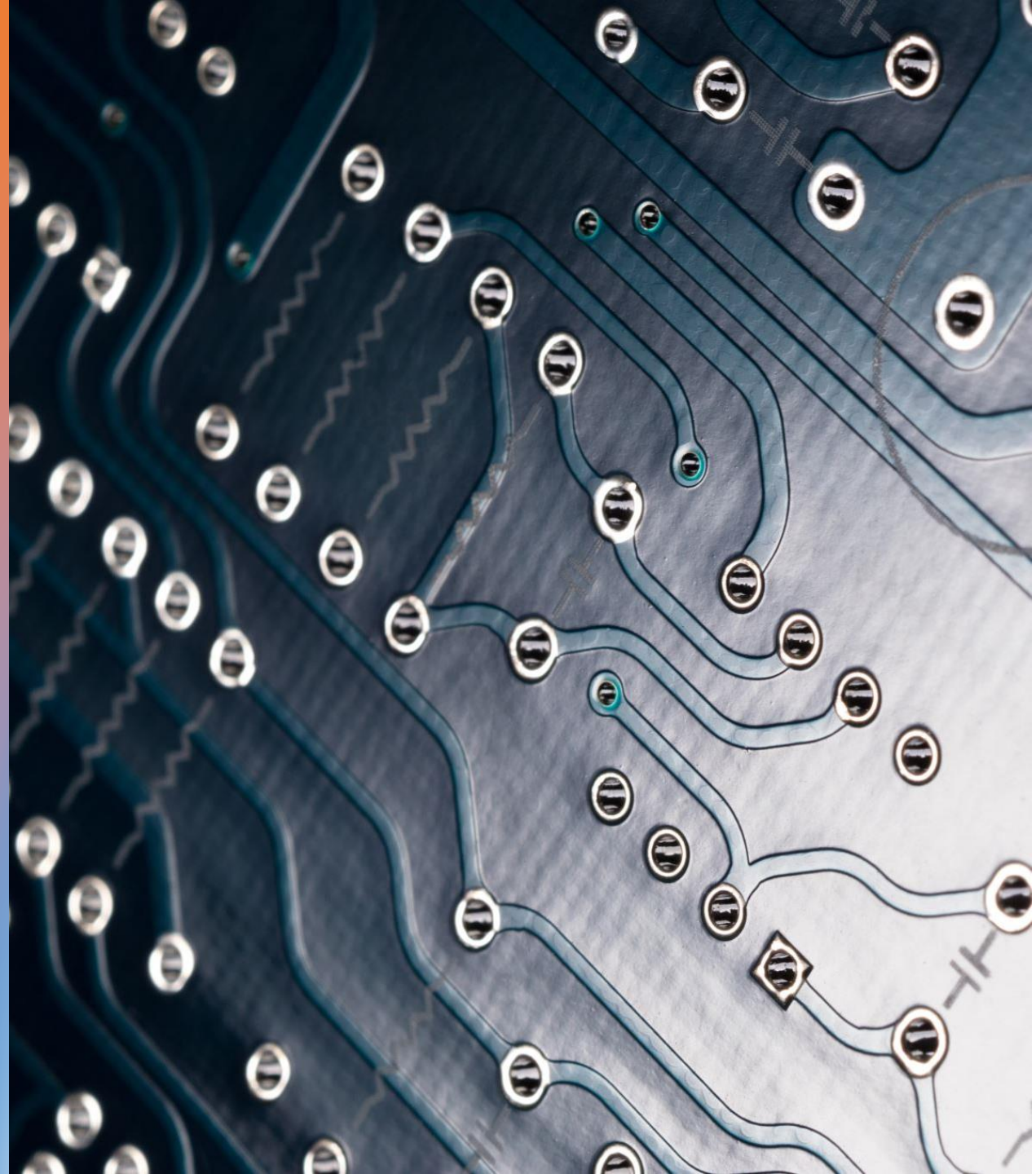
Criptografia

Prof. Dr. Gerson Pastre de Oliveira

Criptografia

- **Criptografia** é o processo de transformar dados legíveis em um formato cifrado, tornando-os inacessíveis para qualquer pessoa que não possua a chave necessária para decifrá-los;
- Esse processo assegura a confidencialidade, integridade e, em alguns casos, a autenticidade das informações.



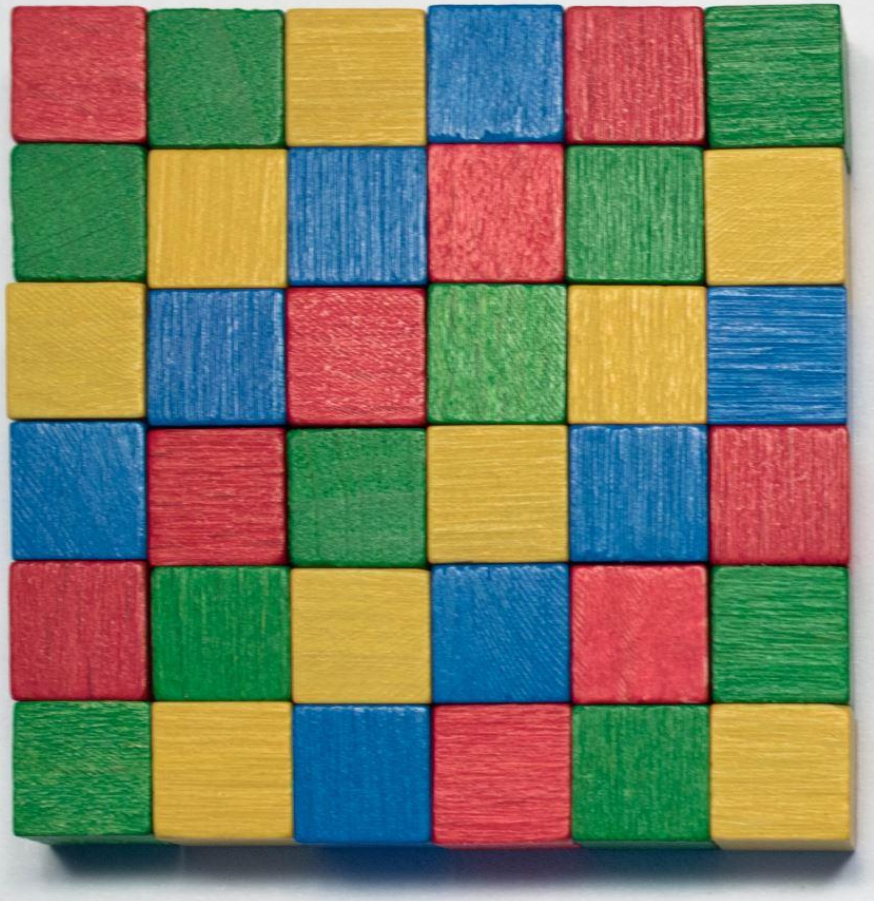
Tipos de criptografia

- **Criptografia simétrica:** usa uma única chave para cifrar e decifrar os dados;
- Mais rápida e eficiente em termos de processamento;
- A chave deve ser compartilhada entre as partes envolvidas, o que pode ser um risco de segurança;
- Exemplos: AES (Advanced Encryption Standard), DES (Data Encryption Standard).

Criptografia simétrica – DES (Data Encryption Standard)

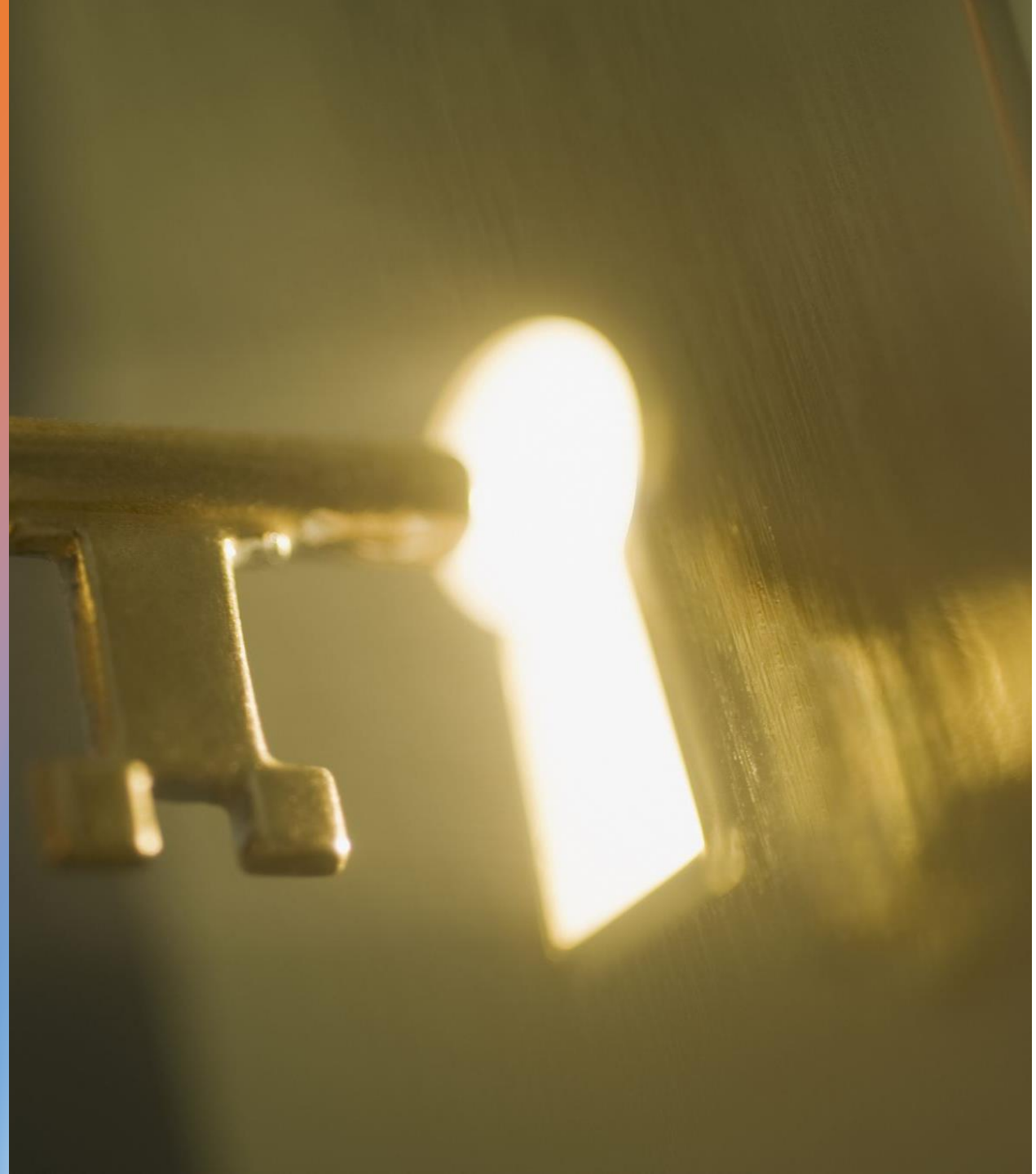
DES foi adotado como um padrão de criptografia pelo governo dos Estados Unidos em 1977;

Originalmente desenvolvido pela IBM, foi selecionado pelo *National Institute of Standards and Technology* (NIST) para proteger informações federais.



Fundamentos DES

- **Tamanho da Chave:** 56 bits;
- **Bloco:** cifra de bloco que opera em blocos de 64 bits;
- **Estrutura:** utiliza uma estrutura de rede Feistel, que divide o bloco de dados em duas metades e aplica uma série de operações repetitivas chamadas de rodadas (16 rodadas no total).



Características DES

- **Segurança:** Inicialmente considerado seguro, o DES tornou-se vulnerável a ataques de força bruta à medida que o poder computacional aumentou;
- Hoje, a chave de 56 bits é considerada insuficiente para proteger dados contra ataques modernos;
- **Velocidade:** relativamente rápido, mas a segurança limitada tornou-o obsoleto;

Características DES

Segurança: Inicialmente considerado seguro, o DES tornou-se vulnerável a ataques de força bruta à medida que o poder computacional aumentou;

Hoje, a chave de 56 bits é considerada insuficiente para proteger dados contra ataques modernos;

Velocidade: relativamente rápido, mas a segurança limitada tornou-o obsoleto;

Uso: substituído por algoritmos mais seguros, mas ainda pode ser encontrado em sistemas legados;

3DES (Triple DES): uma versão mais segura do DES, na qual o processo de cifragem é repetido três vezes com duas ou três chaves diferentes – isso aumenta a segurança, mas também diminui a eficiência.

Criptografia simétrica – AES (Advanced Encryption Standard)

AES foi adotado como o sucessor do DES pelo NIST em 2001;

Foi desenvolvido pelos criptógrafos belgas Joan Daemen e Vincent Rijmen e também é conhecido como o algoritmo Rijndael.

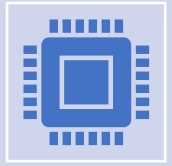
Fundamentos AES

- **Tamanho da Chave:** 28, 192, ou 256 bits;
- **Bloco:** cifra de bloco que opera em blocos de 128 bits;
- **Estrutura:** utiliza uma rede de substituição-permutação (SPN), que envolve uma série de operações de substituição e permutação organizadas em várias rodadas – o número de rodadas depende do tamanho da chave (10 rodadas para 128 bits, 12 para 192 bits e 14 para 256 bits).

Características AES

Segurança: considerado altamente seguro e resistente a ataques de força bruta: o tamanho da chave permite proteção robusta contra ataques, sendo adequado para uso em aplicações de segurança de dados de alto nível;

Velocidade: altamente eficiente tanto em software quanto em hardware: AES é mais rápido que 3DES e outros algoritmos mais antigos, tornando-o ideal para criptografar grandes volumes de dados;



Uso: amplamente adotado em diversas aplicações, incluindo criptografia de discos, comunicações seguras e como o algoritmo de cifragem padrão para muitos protocolos de segurança (como SSL/TLS);

Técnicas clássicas de encriptação

Cifras simétricas

Prof. Dr. Gerson Pastre de Oliveira

Criptografia simétrica

- Também chamada de encriptação convencional ou encriptação de chave única, era o único tipo em uso antes do desenvolvimento da encriptação por chave pública na década de 1970;
- Ainda é o tipo mais usado;
- Algoritmos simétricos, como o AES (*Advanced Encryption Standard*) e o 3DES (*Triple Data Encryption Standard*), são particularmente eficientes em termos de velocidade e desempenho, tornando-os ideais para criptografia de dados em grande escala, como em comunicações de rede e armazenamento de dados

Criptografia simétrica

Embora algoritmos de criptografia assimétrica, como RSA e ECC, sejam frequentemente utilizados para propósitos específicos, como estabelecimento de chaves e assinaturas digitais, a criptografia simétrica ainda desempenha um papel crucial em muitos aspectos da segurança da informação;

Em muitos casos, uma combinação de criptografia simétrica e assimétrica é empregada para fornecer maior segurança em diferentes cenários e contextos de uso.

Um esquema de encriptação simétrica possui cinco itens:

- Texto claro: essa e a mensagem ou dados originais, inteligíveis, que servem como entrada do algoritmo de encriptação.
- Algoritmo de encriptação: realiza diversas substituições e transformações no texto claro.
- Chave secreta: também e uma entrada para o algoritmo de encriptação. A chave e um valor independente do texto claro e do algoritmo. O algoritmo produzira uma saída diferente, dependendo da chave usada no momento. As substituições e transformações exatas realizadas pelo algoritmo dependem da chave.

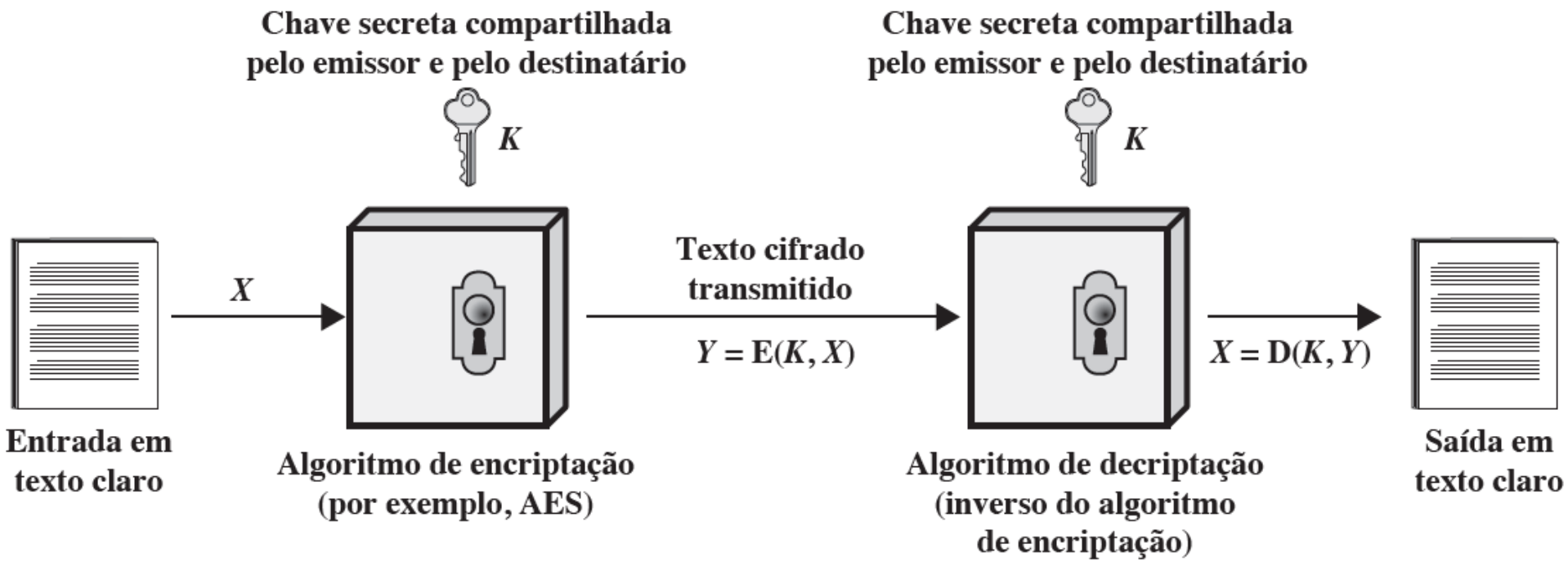
Um esquema de encriptação simétrica possui cinco itens:

- Texto cifrado: essa é a mensagem embaralhada, produzida como saída do algoritmo de encriptação. Ela depende do texto claro e da chave secreta. Para determinada mensagem, duas chaves diferentes produzirão dois textos cifrados distintos. O texto cifrado é um conjunto de dados aparentemente aleatório e, nesse formato, ininteligível.
- Algoritmo de decriptação: esse é basicamente o algoritmo de encriptação executado de modo inverso. Ele apanha o texto cifrado e a chave secreta e produz o texto claro original.

Requisitos para uso seguro de criptografia simétrica

1. Precisamos de um algoritmo de encriptação forte. No mínimo, gostaríamos que o algoritmo fosse tal que um oponente que conheça o algoritmo e tenha acesso a um ou mais textos cifrados seja incapaz de decifrar o texto cifrado ou descobrir a chave. Esse requisito normalmente é indicado de maneira mais forte: o oponente deverá ser incapaz de decriptar o texto cifrado ou descobrir a chave, mesmo que possua diversos textos cifrados com seus respectivos textos claros.
2. Emissor e receptor precisam ter obtido cópias da chave secreta de uma forma segura e mantê-la protegida. Se alguém conseguir descobrir a chave e o algoritmo, toda a comunicação usando essa chave poderá ser lida.

Figura 2.1 Modelo simplificado da encriptação simétrica.



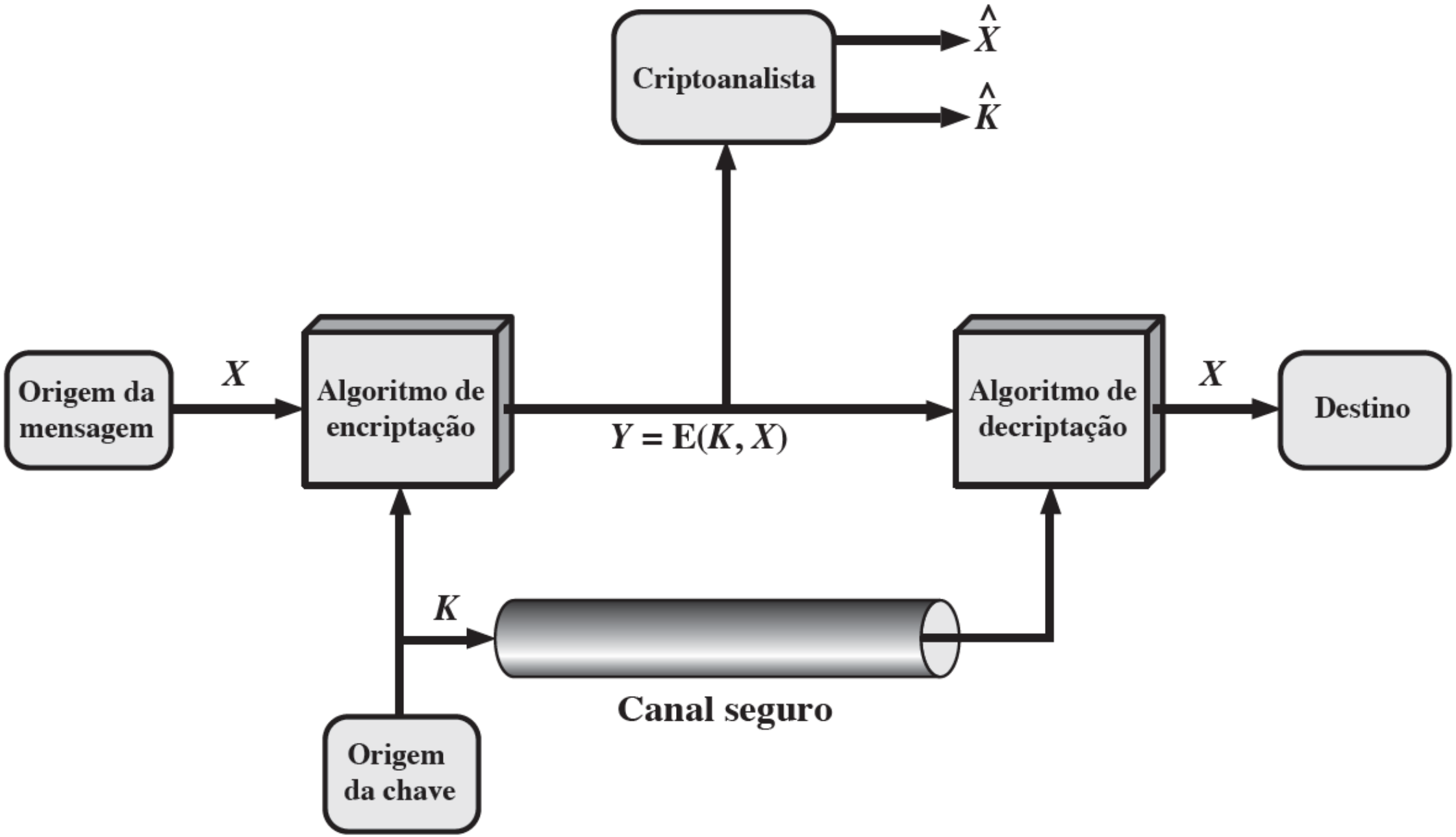
Criptografia simétrica

Podemos manter apenas a chave secreta (o algoritmo pode ser conhecido)

Um oponente, tendo acesso à saída cifrada, mas sem acesso ao texto claro e à chave, pode tentar recuperá-los, considerando que conheça o algoritmo

O oponente pode tentar recuperar apenas a mensagem atual (sob ataque) ou mensagens futuras

Figura 2.2 Modelo de criptossistema simétrico.



Criptografia

Os sistemas criptográficos são caracterizados ao longo de três dimensões independentes:

1. **O tipo das operações usadas para transformar texto claro em texto cifrado**: todos os algoritmos de encriptação são baseados em dois princípios gerais: substituição, em que cada elemento no texto claro (bit, letra, grupo de bits ou letras) é mapeado em outro elemento, e transposição, em que os elementos no texto claro são rearranjados. O requisito fundamental é que nenhuma informação seja perdida (ou seja, que todas as operações sejam reversíveis). A maioria dos sistemas envolve vários estágios de substituições e transposições (sendo chamados de *sistemas de produto*);

Criptografia

Os sistemas criptográficos são caracterizados ao longo de três dimensões independentes:

2. **O número de chaves usadas:** se tanto o emissor quanto o receptor utilizarem a mesma chave, o sistema é considerado de encriptação simétrica, de chave única, de chave secreta ou convencional. Se emissor e receptor usarem chaves diferentes, o sistema é considerado de encriptação assimétrica, de duas chaves ou de chave pública;

3. **O modo em que o texto claro é processado:** uma *cifra de bloco* processa a entrada de um bloco de elementos de cada vez, produzindo um de saída para cada de entrada; uma *cifra em fluxo* processa os elementos da entrada continuamente, proporcionando a saída de um elemento de cada vez;

Criptoanálise e ataque por força bruta

- *Em geral, o objetivo de atacar um sistema de encriptação e recuperar a chave em uso, em vez de simplesmente recuperar o texto claro a partir de um único texto cifrado;*
- *Existem duas técnicas gerais para o ataque a um esquema de encriptação convencional:*

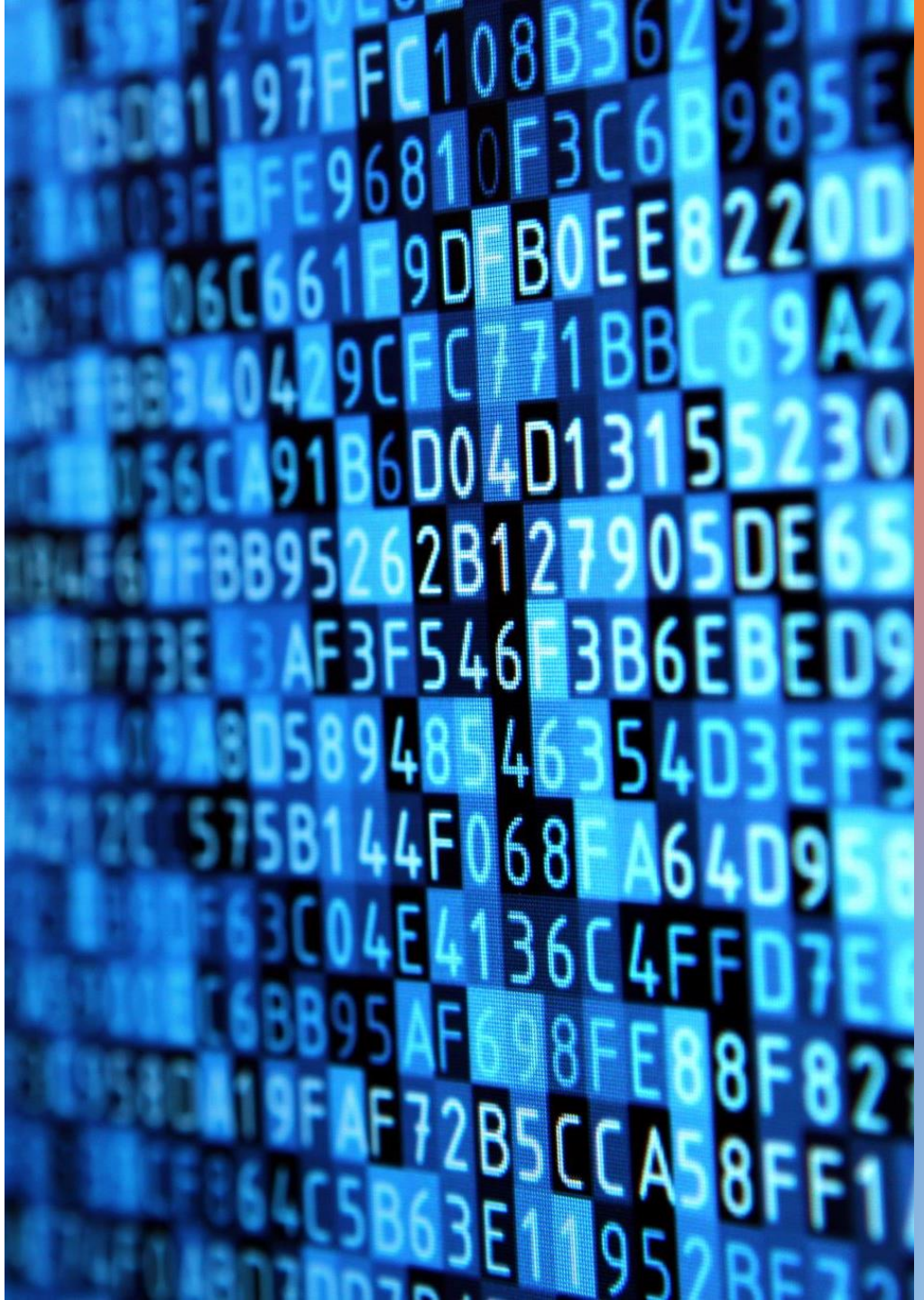
1. **Criptoanálise:** os ataques informação utilizam-se da natureza do algoritmo, e talvez de mais algum conhecimento das características comuns ao texto claro, ou ainda de algumas amostras de pares de texto claro-texto cifrado. Esse tipo de ataque explora as características do algoritmo para tentar deduzir um texto claro especifico ou a chave utilizada;
2. **Ataque por força bruta:** o atacante testa todas as chaves possíveis em um trecho do texto cifrado, até obter uma tradução inteligível para o texto claro. Na média, metade de todas as chaves possíveis precisam ser experimentadas para então se obter sucesso (ou não);

Quadro 2.1 Tipos de ataque sobre mensagens encriptadas.

TIPO DE ATAQUE	CONHECIDO AO CRIPTOANALISTA
Apenas texto cifrado	■ Algoritmo de encriptação ■ Texto cifrado
Texto claro conhecido	■ Algoritmo de encriptação ■ Texto cifrado ■ Um ou mais pares de texto claro-texto cifrado produzidos pela chave secreta
Texto claro escolhido	■ Algoritmo de encriptação ■ Texto cifrado ■ Mensagem de texto claro escolhida pelo criptoanalista, com seu respectivo texto cifrado gerado com a chave secreta
Texto cifrado escolhido	■ Algoritmo de encriptação ■ Texto cifrado ■ Texto cifrado escolhido pelo criptoanalista, com seu respectivo texto claro decriptado produzido pela chave secreta
Texto escolhido	■ Algoritmo de encriptação ■ Texto cifrado ■ Mensagem de texto claro escolhida pelo criptoanalista, com seu respectivo texto cifrado produzido pela chave secreta ■ Texto cifrado escolhido pelo criptoanalista, com seu respectivo texto claro decriptado produzido pela chave secreta

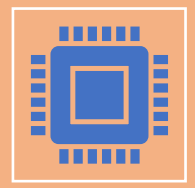
Criptoanálise e ataque por força bruta

- Somente algoritmos relativamente fracos não conseguem resistir a um ataque de texto cifrado;
- Em geral, um algoritmo de encriptação é projetado para aguentar a um ataque de texto claro conhecido;
- Um esquema de encriptação é incondicionalmente seguro se o texto cifrado gerado por ele não tiver informação suficiente para determinar exclusivamente o texto claro correspondente, não importa quanto texto cifrado esteja a disposição – ou seja, é indiferente quanto tempo um oponente tem, ele não tem como decriptar o texto cifrado, simplesmente porque a informação exigida não está lá;



Criptoanálise e ataque por força bruta

Com a exceção de um esquema conhecido como *one-time pad*, não existe algoritmo de encriptação que seja incondicionalmente seguro – portanto, tudo o que os usuários de um algoritmo de encriptação podem se esforçar para obter é um algoritmo que atenda a um ou a ambos os critérios a seguir:



1) O custo para quebrar a cifra ultrapassa o valor da informação encriptada;

2) O tempo exigido para quebrar a cifra supera o tempo de vida útil da informação.

Criptoanálise e ataque por força bruta

- Um ataque por força bruta envolve a tentativa de cada chave possível até que seja obtida uma tradução inteligível de texto cifrado para texto claro;
- Em média, metade de todas as chaves possíveis precisa ser experimentada para se obter sucesso – ou seja, se houver X chaves diferentes, um intruso descobriria a verdadeira após X/2 tentativas, em média;
- É importante observar que há mais coisas em um ataque por força bruta do que simplesmente testar todas as chaves possíveis – por exemplo, a menos que seja fornecido um texto claro conhecido, o analista deverá ser capaz de reconhecê-lo como tal;

Criptoanálise e ataque por força bruta

- Se a mensagem for simplesmente texto claro em inglês, então o resultado aparece facilmente, embora a tarefa de reconhecer o inglês tenha que ser automatizada – se a mensagem de texto foi compactada antes da encriptação, então o reconhecimento é mais difícil;
- Se a mensagem for de algum tipo mais geral de dado, como um arquivo numérico, e este tiver sido compactado, o problema se torna ainda mais difícil de automatizar – assim, para suplementar o método por forca bruta, é preciso haver algum grau de conhecimento sobre o texto claro esperado, além de algum meio de distinguir automaticamente o texto claro de dados aleatórios.

Técnicas de Substituição

Cifra de César;

Cifras monoalfabéticas;

Cifra *playfair;*

Cifra de Hill;

Cifras polialfabéticas;

One-time-pad.