Criptografia

Redes e Segurança Informática

2º semestre > 1º ano

Mário Pinto | mjp@ua.pt

Cofinanciado por:
NORTE2020 PORTUGAL 2020 UNIÃO EUROPEIA Fundo Social Europeu

Index

Criptografia

- *The **mathematical science** that deals with **transforming data to render its meaning unintelligible** (i.e., to hide its semantic content), prevent its undetected alteration, or prevent its unauthorized use. If the transformation is reversible, cryptography also deals with restoring encrypted data to intelligible form.*

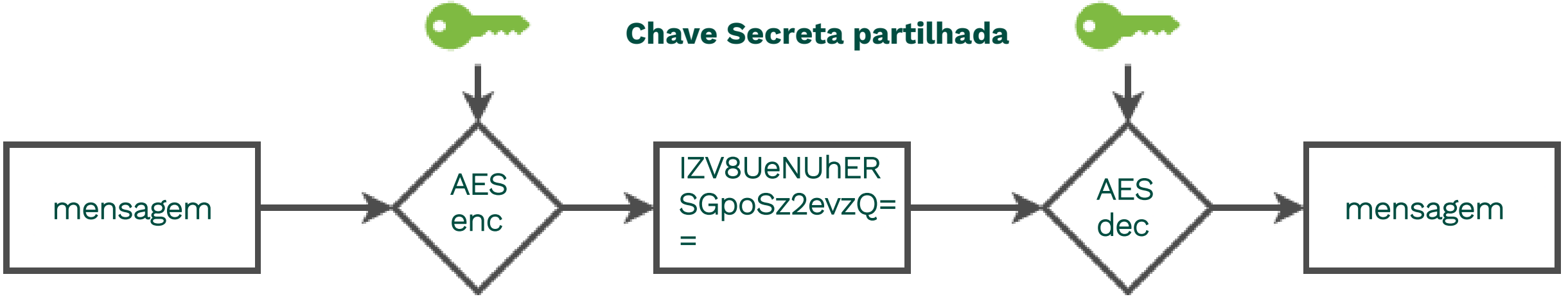
RFC 4949: Internet Security Glossary, version 2 (2007)

Criptografia

- Sistemas que utilizam Criptografia podem ser classificados em três dimensões:
  - **Tipo de operações** utilizadas para a transformação do original no encriptado
  - **Número de chaves** utilizadas
  - **Forma de processamento** do original

Criptografia

- Princípios da **Encriptação Simétrica**
  - Texto Original
  - Algoritmo de Encriptação
  - Chave Secreta (partilhada entre emissor e recetor)
  - Texto encriptado
  - Algoritmo de Desencriptação
  - Texto Final/Original



Criptografia

- Tipo de **operações** utilizadas para a transformação do original no encriptado
  - **Substituição**: cada elemento é mapeado para outro
  - **Transposição**: os elementos são reordenados
  - Não há perda de informação
  - Maior parte dos algoritmos utilizam várias etapas de substituições e transposições
  - Exemplos:

Substituição

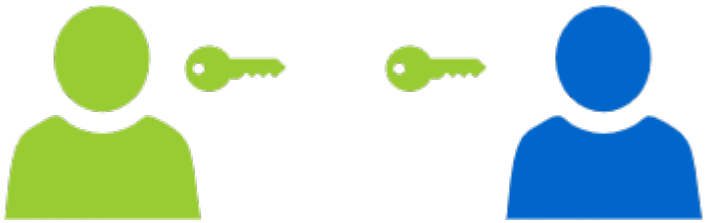
```
A ↔ N    PBZRORZ
B ↔ O
C ↔ P
D ↔ Q
E ↔ R
...
M ↔ Z
```

Transposição

```
C . . . B . .    CBOEEMM
. O . E . E .
. . M . . . M
```

Criptografia

- Número de **chaves** utilizadas
  - Chave única
    - Também designado de **Simétrico** (chave secreta ou convencional)
    - Chave secreta partilhada apenas pelo emissor e recetor
  - Chave pública
    - Também designado por **Assimétrico** (chave dupla ou chave única)
    - Emissor e Recetor possuem chaves secretas distintas



Simétrico

Assimétrico

Criptografia

- Forma de **processamento** do original
  - Encriptação por **Bloco**: elementos são agrupados em blocos que são processados isoladamente
    - Utiliza 64 ou mais bits
    - Complexo de implementar
    - Difícil de reverter
    - Utilizado em software
  - Encriptação por **Stream/Fluxo**: cada elemento (normalmente 8 bits) é processado isoladamente
    - Utiliza 8 bits
    - Simples de implementar
    - Fácil de reverter
    - Utilizado em hardware

Criptoanálise

- Processo de tentar **obter o texto original ou a chave** de encriptação
- A estratégia a utilizar depende da natureza da encriptação e da informação disponível
  - **Texto encriptado** apenas: por vezes também é possível determinar o algoritmo utilizado
  - **Original conhecido**: sabendo pares originais-encriptados que utilizem a mesma chave
  - **Original escolhido**: analista escolhe o original e o correspondente encriptado
  - **Encriptado escolhido**: analista escolhe o encriptado e o final correspondente
  - **Texto escolhido**: analista escolhe original e o correspondente encriptado, e ainda o encriptado e o final correspondente

Criptoanálise

- Texto encriptado
  - É possível determinar o algoritmo de encriptação
  - É possível utilizar força bruta com todas as chaves possíveis
    - Se o domínio das chaves for muito grande é impraticável
  - É possível saber mais sobre o Original:
    - Tipo de informação encriptada: executável, texto, código fonte, imagem, etc
  - É possível determinar padrões existentes no Original:
    - Tipos de ficheiros têm cabeçalhos comuns
    - Tipos de mensagens têm características comuns
    - Original com partes comuns: indicação de copyright, contactos, rodapés, cabeçalhos, etc

Criptoanálise

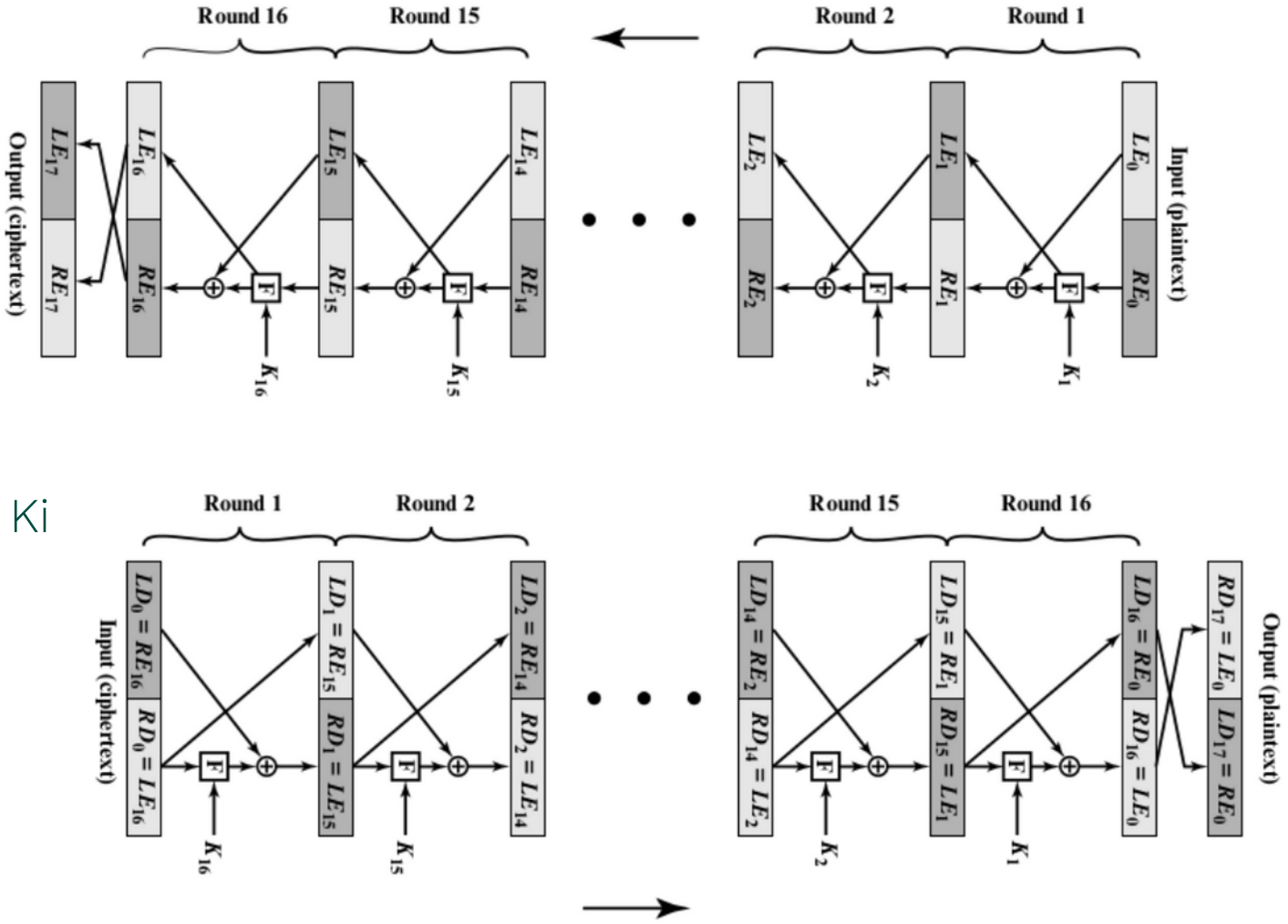
- Muitas possibilidades de ataque
- Um esquema de encriptação é **computacionalmente seguro** se:
  - O custo de quebrar a encriptação excede o valor da informação encriptada
  - O tempo para quebrar a encriptação excede o tempo de vida útil da informação

Encriptação Simétrica

- Encriptação simétrica mais comum utiliza **blocos**
  - Blocos de tamanho pré-definido no Texto Original e no Encriptado
- Chave de encriptação é partilhada
- Algoritmos importantes:
  - Data Encryption Standard (DES)
  - Triple DES (3DES)
  - Advanced Encryption Standard (AES)

Encriptação Simétrica | Feistel

- Encriptação de Feistel
  - Desenvolvida em 1973 por Horst Feistel para a IBM
  - 16 etapas de processamento
  - Bloco dividido em dois
    - LEi e REi
  - É gerada subchave de cada etapa Ki
  - É aplicada uma função F a Ri
    - Operação de Substituição
  - É aplicado XOR ao resultado anterior e a Li



William Stallings: Network Security Essentials Applications and Standards, 6th Edition

DES

- DES | Data Encryption Standard
  - Definido em 1977 como standard federal para processamento de informação (FIPS) pelo NIST
  - Utiliza a estrutura da Encriptação de Feistel
  - Utiliza blocos de 64 bits
  - Chave tem 56 bits
    - $2^{56} = 7{,}2 \times 10^{16}$ chaves possíveis
  - Possui 16 etapas de processamento
    - A partir da chave de 56 bits são geradas 16 sub-chaves
    - Cada sub-chave é utilizada numa das etapas
  - Desencriptação consiste na simples inversão do processo
  - Atualmente é **Muito inseguro**

3DES

- 3DES | Triple Data Encryption Standard
  - Introduzido em 1985 foi incorporado em 1999 como parte do DES
  - Utiliza **três chaves** (K1, K2, K3)
    - $2^{168} = 3{,}7 \times 10^{50}$ chaves possíveis
  - Faz **três execuções** do algoritmo DES (EDE: Encripta – Desencripta – Encripta)
  - Descontinuado em 2023, atualmente é **Inseguro** (mas é muito utilizado...)

Encriptar

```
E(K3, D(K2, E(K1, Original ) ) ) = Encriptado
```

Desencriptar

```
D(K1, E(K2, D(K3, Encriptado ) ) ) = Original
```

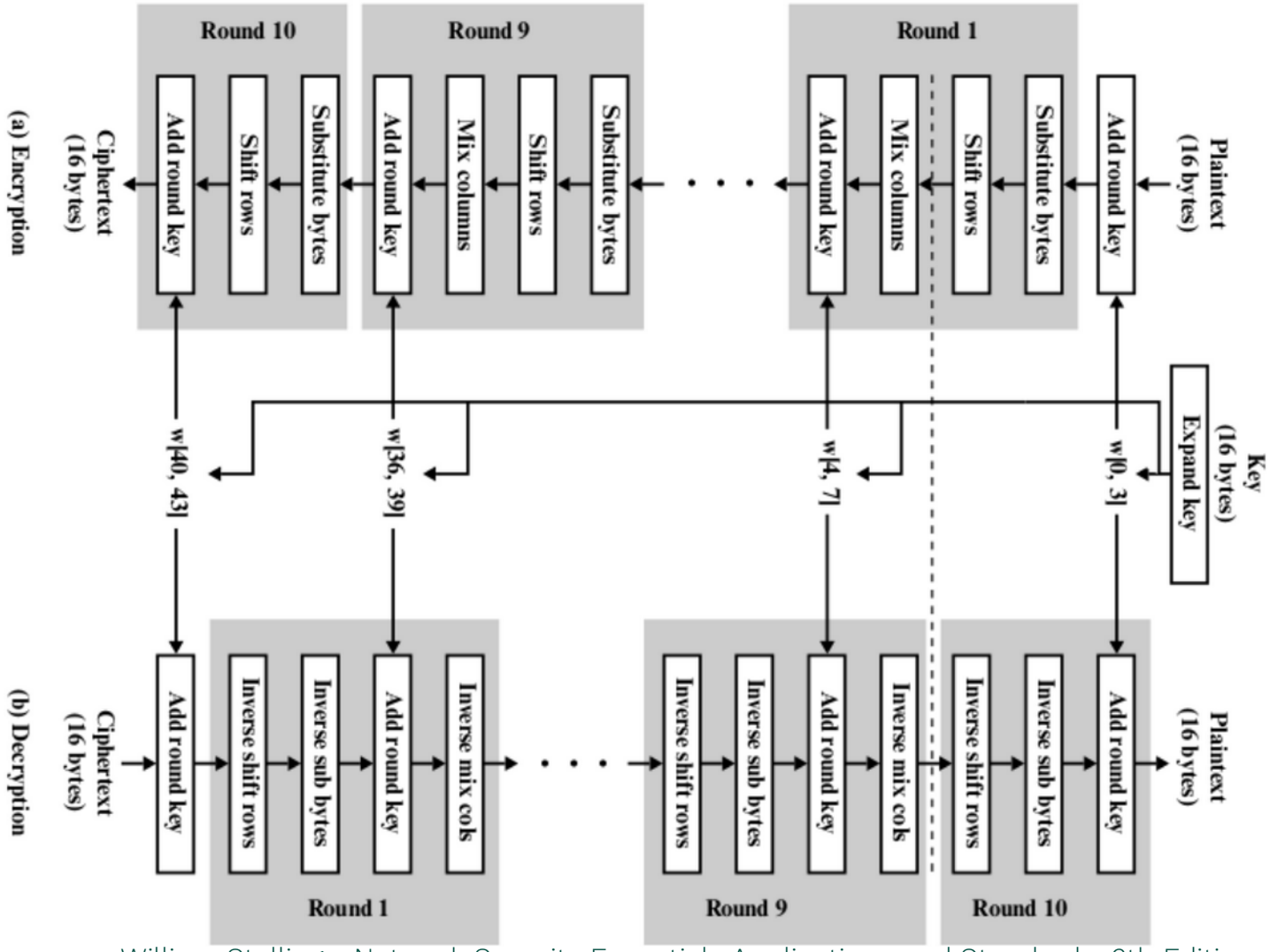
AES

- AES | Advanced Encryption Standard
  - Em 1997 NIST pediu propostas para um novo standard de encriptação (AES)
  - 2001 foi selecionada a proposta *Rijndael Block Cipher*
    - Elaborada por Dr. Joan Daemoen e Dr. Vincent Rijmen
  - **Blocos** com **128 bits**
    - Torna a encriptação mais complexa e mais difícil de atacar
  - Chaves com **128**, **192** ou **256 bits**
    - Torna a encriptação mais segura
  - Não utiliza a estrutura da encriptação Feistel

AES Proposal: Rijndael | https://cs.ru.nl/~joan/papers/JDA_VRI_Rijndael_V2_1999.pdf

AES

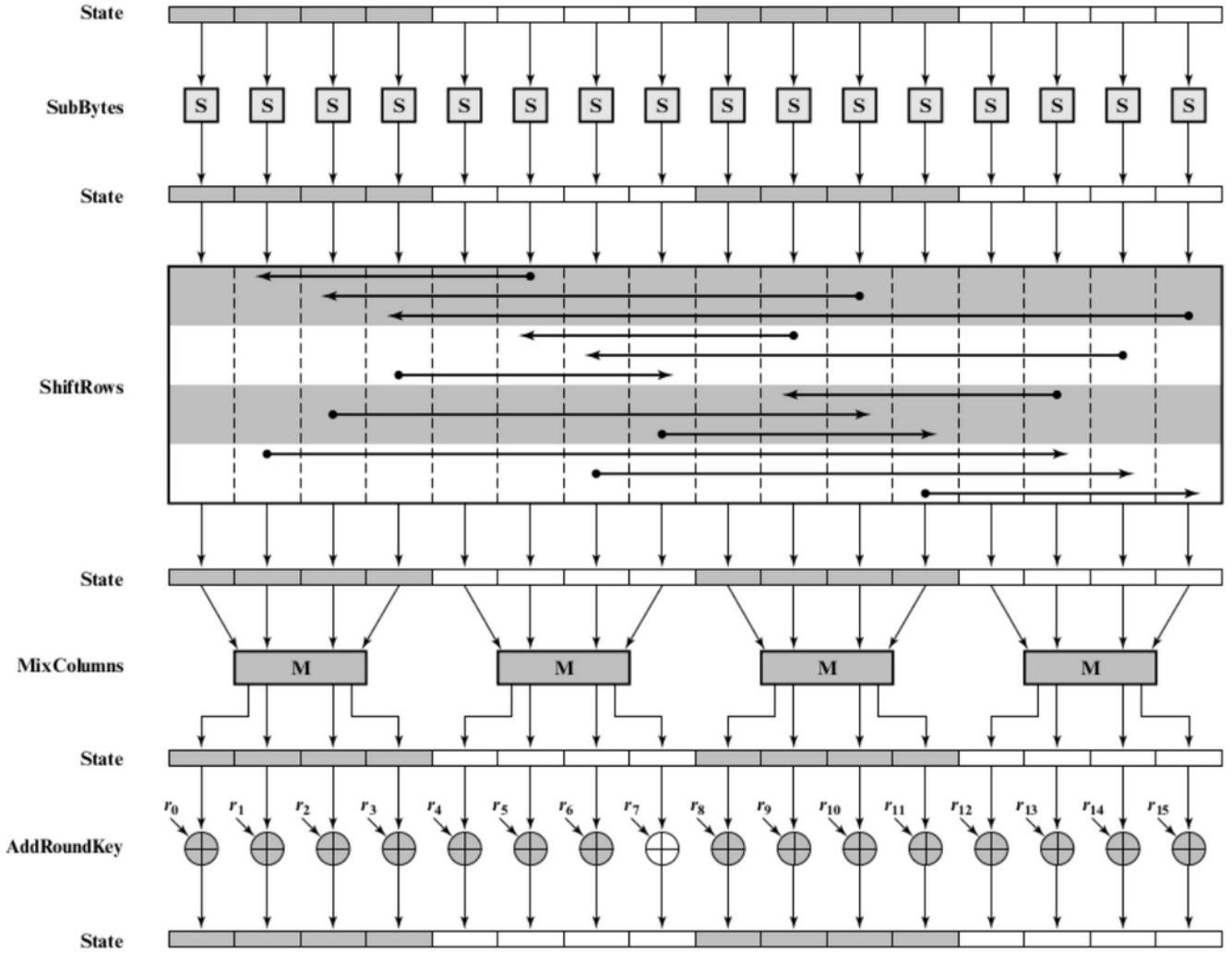
- AES encriptação
- AES desencriptação



William Stallings: Network Security Essentials Applications and Standards, 6th Edition

AES

- Exemplo de uma etapa



William Stallings: Network Security Essentials Applications and Standards, 6th Edition

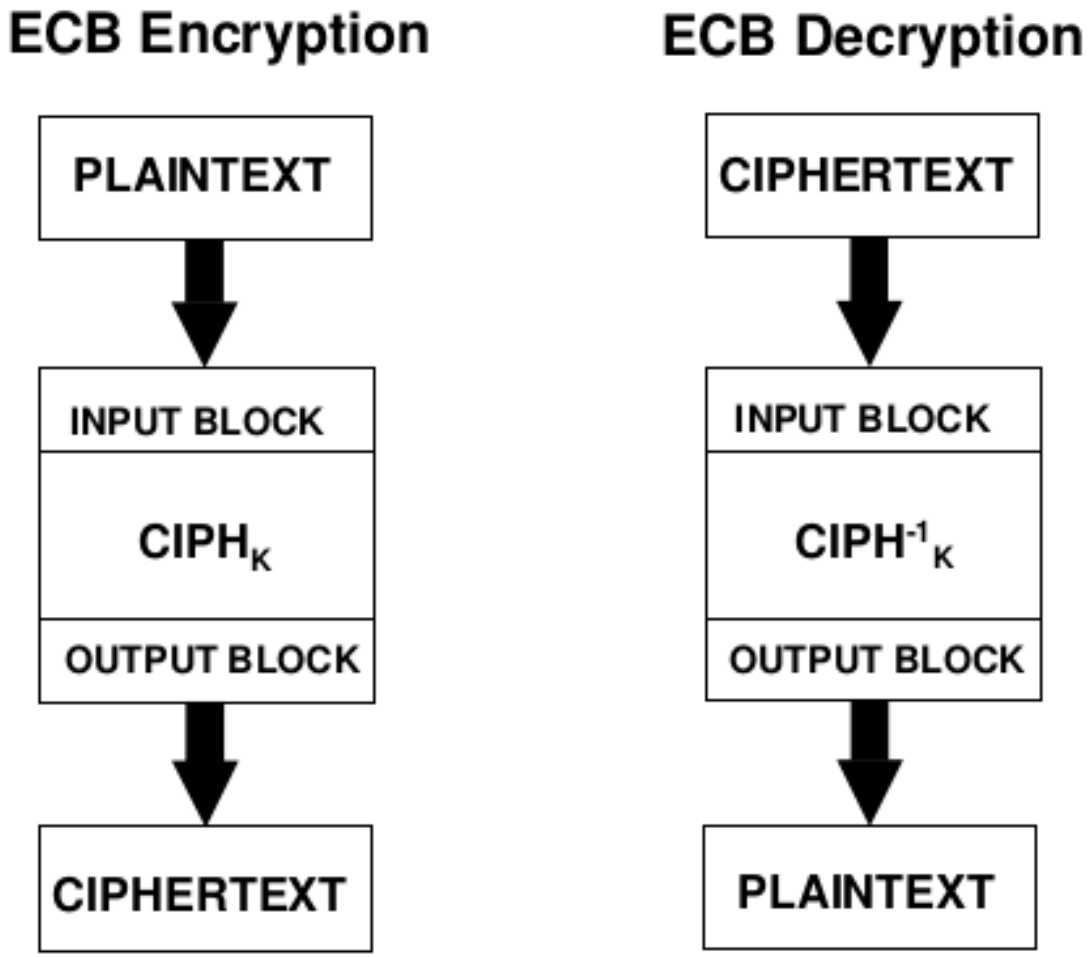
Modo de Operação

- A encriptação simétrica utiliza **Modos de Operação** na encriptação por blocos
- A definição do NIST prevê vários modos
- Destacam-se:
  - ECB | Electronic Codebook Mode
  - CBC | Cipher Block Chaining
  - CFB | Cipher FeedBack
  - OFB | Output FeedBack
  - CTR | Counter

ECB | Electronic Code Book

- Modo mais simples
- Utiliza blocos de 128 bits = 16 Bytes
- Cada bloco é encriptado com a mesma chave
  - Assim, seria possível ter um codebook
  - Todas as possibilidades de blocos e o bloco correspondente encriptado
  - O mesmo bloco original origina sempre o mesmo bloco encriptado
- Permite processamento paralelo
- Fácil de perceber repetições
- Facilita a análise e o ataque

ECB | Electronic Code Book

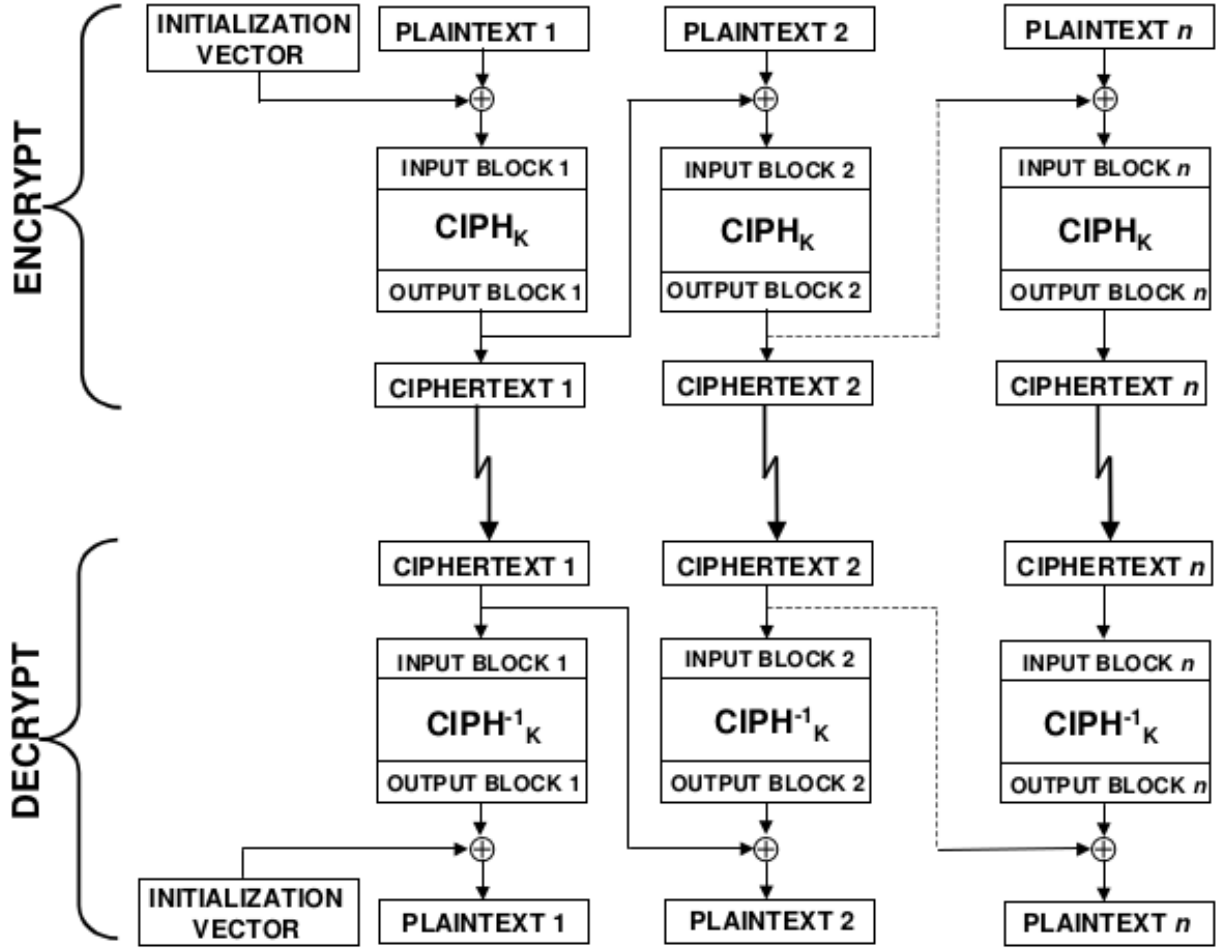


NIST SP 800-38A | Recommendation for Block Cipher Modes of Operation: Methods and Techniques

CBC | Cipher Block Chaining

- Utiliza blocos de 128 bits = 16 Bytes
- Utiliza um **vetor de inicialização** (IV – Initialization vector)
  - Garante que cada encriptação tem um resultado diferente
- Utiliza o resultado da encriptação do bloco anterior (*chaining*)
  - Operação XOR entre bloco original e bloco encriptado anterior
- Um erro num bloco inviabiliza a recuperação do resto dos blocos
- Não é possível processamento paralelo
  - Precisa dos dados da encriptação anterior
  - É um algoritmo mais lento

CBC | Cipher Block Chaining

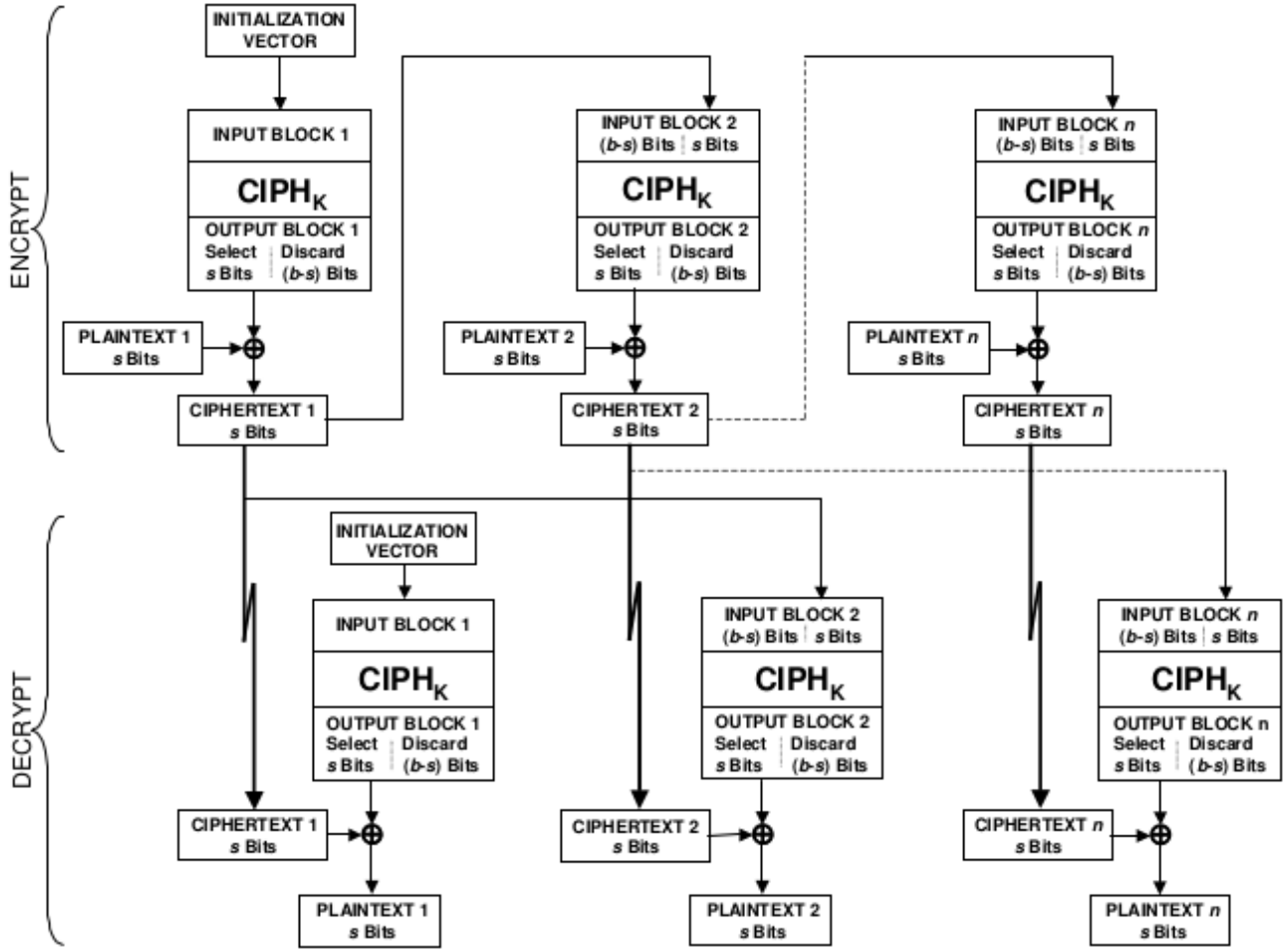


NIST SP 800-38A | Recommendation for Block Cipher Modes of Operation: Methods and Techniques

CFB | Cipher FeedBack

- Converte para uma **encriptação por stream/fluxo**
- Trabalha com cada byte
  - Aceita Dados de qualquer tamanho
- Não é possível processamento paralelo
  - Precisa dos dados da encriptação anterior
  - É um algoritmo mais lento

CFB | Cipher FeedBack

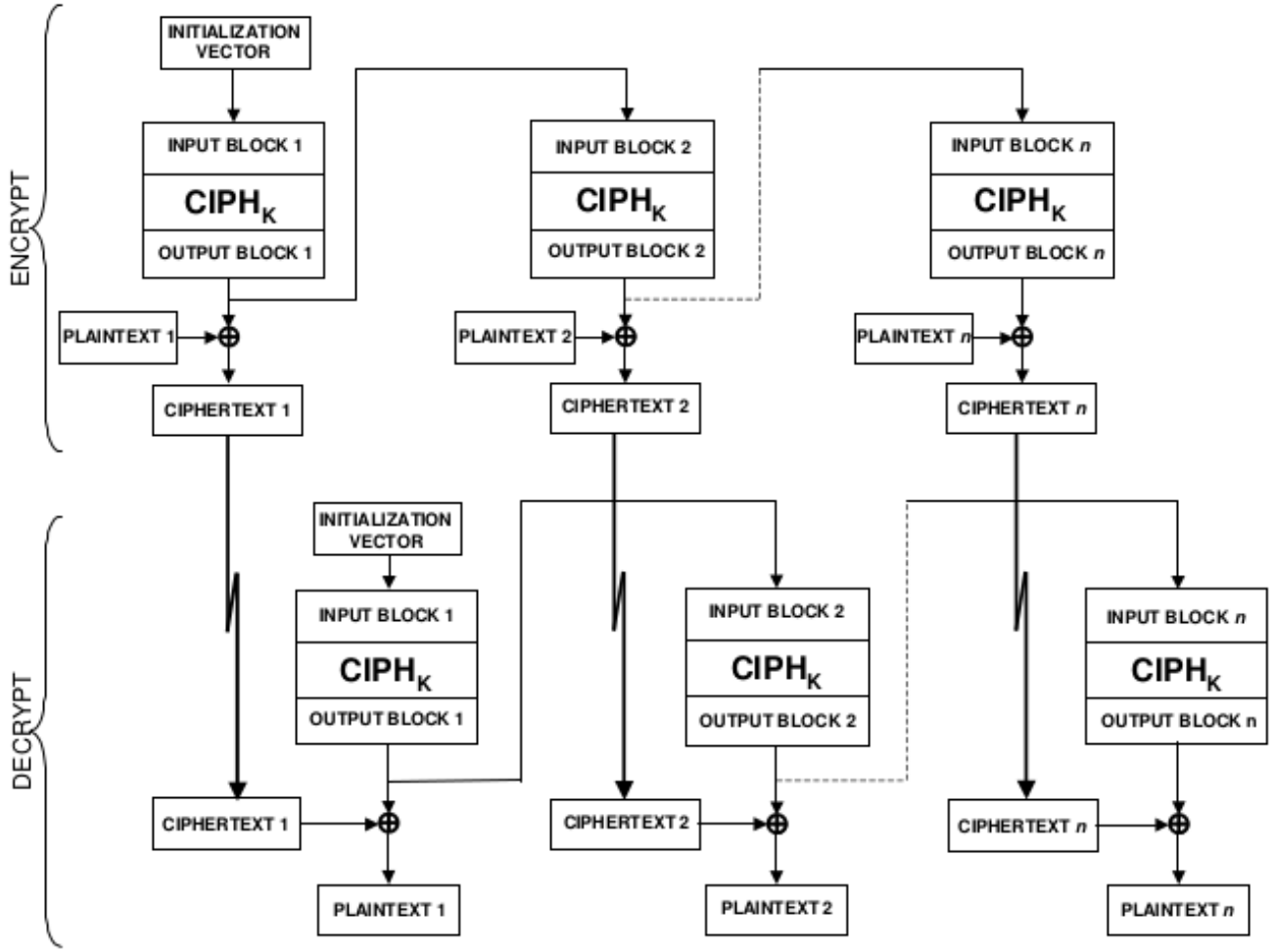


NIST SP 800-38A | Recommendation for Block Cipher Modes of Operation: Methods and Techniques

OFB | Output Feedback

- Utiliza blocos de 128 bits = 16 Bytes
- Utiliza um **vetor de inicialização** (IV – Initialization Vector)
  - Garante que cada encriptação tem um resultado diferente
- Utiliza o bloco de output anterior para a operação
  - Operação XOR entre bloco original e bloco de output

OFB | Output Feedback

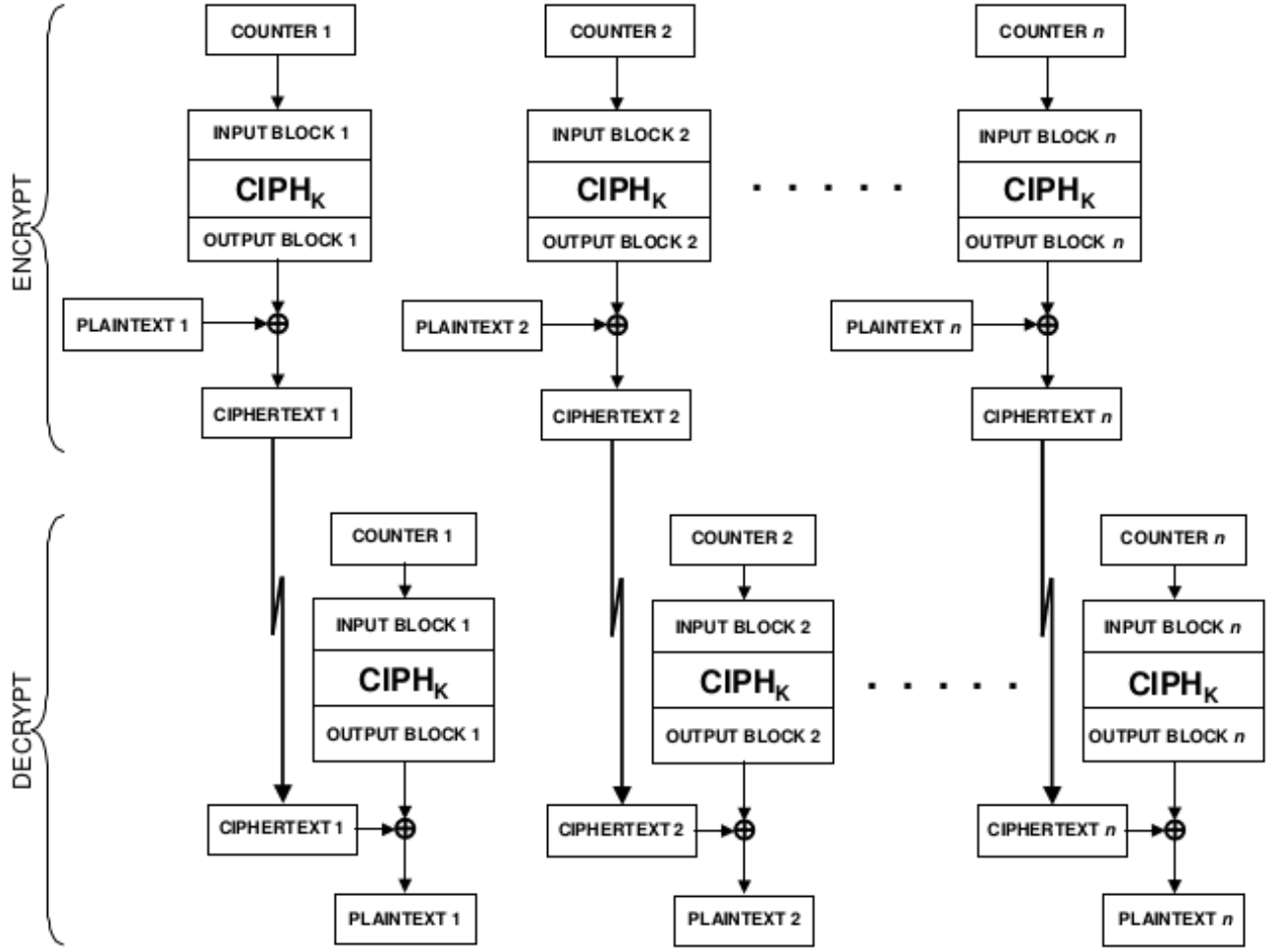


NIST SP 800-38A | Recommendation for Block Cipher Modes of Operation: Methods and Techniques

CTR | Counter

- Contador para a geração pseudoaleatória
  - É necessário proteger os CV Counter Values
  - Não devem ser reciclados
- Permite processamento paralelo
  - Permite desencriptar dois blocos independentemente
- É um dos mais utilizados

CTR | Counter



NIST SP 800-38A | Recommendation for Block Cipher Modes of Operation: Methods and Techniques