Criptografia Aplicada

Criptografia Simétrica - Modos de Operação

Modos de operação

- Quando múltiplos blocos de texto claro são cifrados usando uma cifra de bloco, alguns problemas de segurança podem aparecer
- Modos de operação são técnicas definidas pelo NIST para melhorar o efeito de um algoritmo criptográfico ou adaptar o algoritmo para uma aplicação
  - por exemplo, aplicar uma cifra de bloco em uma sequência de blocos ou fluxo de dados
- As recomendações do NIST se encontram em NIST SP 800-38A
- Cinco modos de operação foram desenvolvidos para o DES em 1980, mas aplicáveis em qualquer cifra de bloco

Sumário

- Modos de Operação:
  - Electronic Codebook - ECB
  - Cipher Block Chaining - CBC
  - Cipher Feedback - CFB
  - Output Feedback - OFB
  - Counter Mode - CTR
- Modos de operação na prática

Electronic Codebook - ECB

- Cada bloco é codificado de forma independente usando a mesma chave
- Pode ser necessário fazer padding no último bloco para atingir *b* bits
  - b = 56 para DES
  - b = 128, 192 ou 256 para AES
- *Codebook* refere-se ao fato de que para uma dada chave, existe um único texto cifrado para cada bloco de texto claro

Imagem: W. Stallings. *Cryptography and network security*. Cap 7.2

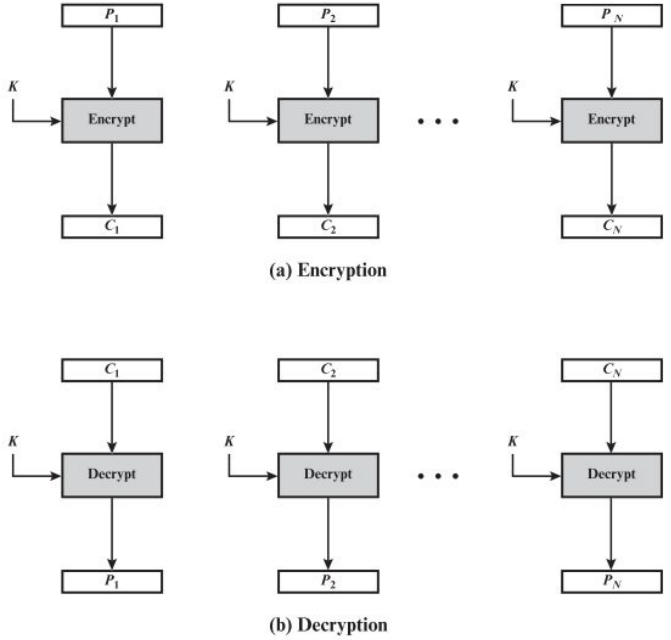
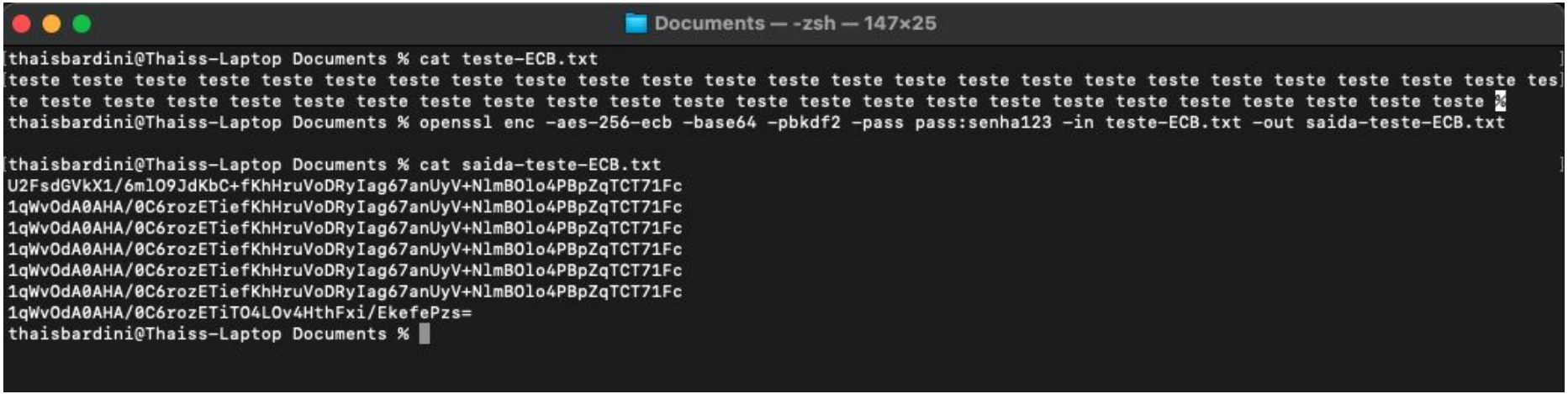


Figure 7.3 Electronic Codebook (ECB) Mode

ECB	$C_j = E(K, P_j) \quad j = 1, \ldots, N$	$P_j = D(K, C_j) \quad j = 1, \ldots, N$

Electronic Codebook - ECB



LabSEC
Laboratório de Segurança em Computação

cpqd

Electronic Codebook - ECB

- **Problema**: repetição de blocos de entrada produzem a mesma saída
  - auxilia na criptoanálise
- Segurança para transmissão de dados únicos/pequenos
  - menores que o tamanho de um bloco

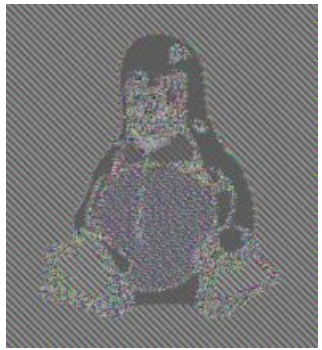


Imagem: https://tinyurl.com/ecb-tux

Imagem: W. Stallings. *Cryptography and network security*. Cap 7.2

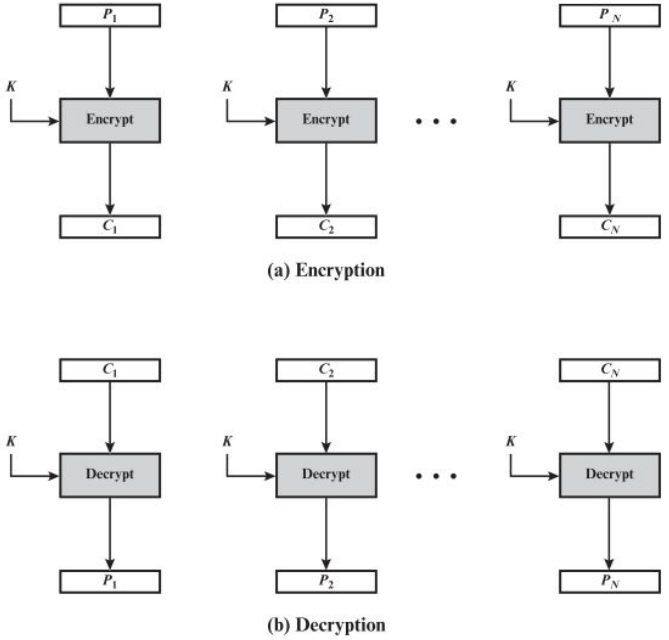


Figure 7.3 Electronic Codebook (ECB) Mode

Outros modos de operação

Propriedades para a avaliação de modos de operação superiores ao ECB:

- overhead
  - operações adicionais necessárias para cifragem e decifragem
- recuperação de erros
  - um erro no i-ésimo bloco cifrado (C_i) afeta apenas alguns blocos decifrados
- propagação de erros
  - um erro na transmissão do i-ésimo bloco cifrado (C_i) afeta o bloco decifrado P_i e todos os blocos subsequentes
- difusão
  - como a estatística do texto em claro é refletida no texto cifrado, previsibilidade, falta de aleatoriedade
- segurança
  - se os blocos de texto cifrados vazam informações sobre os textos em claro

Cipher Block Chaining - CBC

- É feito um XOR do próximo bloco de texto claro com o bloco anterior cifrado
- Um mesmo bloco de texto claro, quando repetido, produz blocos cifrados diferentes
- A mesma chave K é utilizada em todos os blocos

Imagem: W. Stallings. *Cryptography and network security*. Cap 7.2

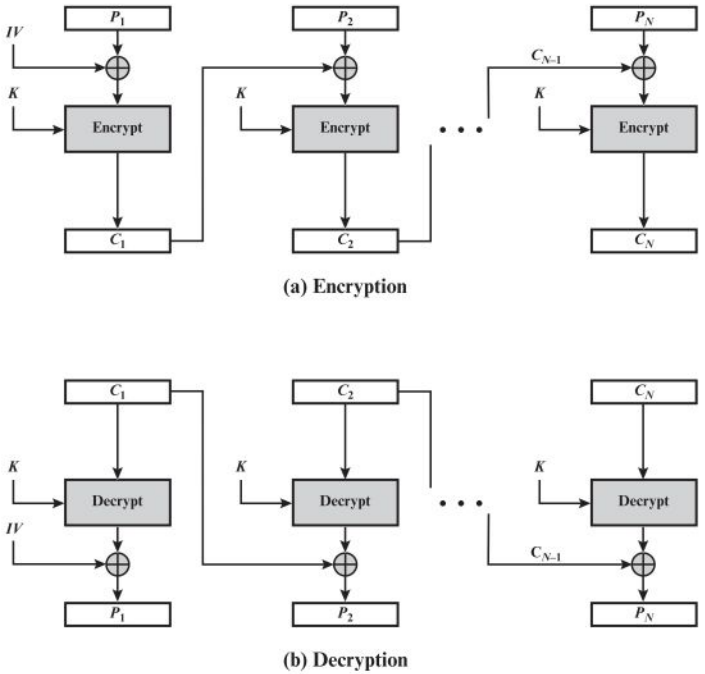


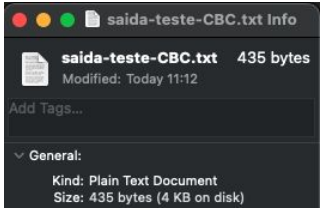
Figure 7.4 Cipher Block Chaining (CBC) Mode

CBC	$C_1 = \mathrm{E}(K, [P_1 \oplus \mathrm{IV}])$ $C_j = \mathrm{E}(K, [P_j \oplus C_{j-1}]) j = 2, \ldots, N$	$P_1 = \mathrm{D}(K, C_1) \oplus \mathrm{IV}$ $P_j = \mathrm{D}(K, C_j) \oplus C_{j-1}\, j = 2, \ldots, N$

Cipher Block Chaining - CBC

```
Documents — -zsh — 116×23
thaisbardini@Thaiss-Laptop Documents % cat teste-ECB.txt
teste teste teste teste teste teste teste teste teste teste teste teste teste teste teste teste teste teste te
ste teste teste teste teste teste teste teste teste teste teste teste teste teste teste teste teste teste test
e teste teste teste teste teste teste teste teste %
thaisbardini@Thaiss-Laptop Documents % openssl enc -aes-256-cbc -base64 -pbkdf2 -pass pass:senha123 -in teste-ECB.tx
t -out saida-teste-CBC.txt

thaisbardini@Thaiss-Laptop Documents % cat saida-teste-CBC.txt
U2FsdGVkX19lWn07ptHBzZjPQSDAsnT8dUEPTJfOpUfe1+wRCpOagjSyKF2D/t7L
hI+nuDxBm+IyZm2XWOBdkg4LlHFVxu2e2Cp648w9QYlMhL3GLHAfZ9/0B4Jb7ped
D10qcWGg+wfDfrLLOtmMieJQ2FwTD18ctN3iEgh0mFda2CRkS5zlLM3VdegBNNgy
iU4cqI7TaOrlsV+TS6YfNsPJZAkqeBc6j1UhxIA+g66iZy03nbc0ZU4WM3vD7ytX
3WGPAZhNirtVVvO0xtbWc3jUu8o0svKs3MOkXbuaMfY867iRPmpRXc+JETddllaj
9Jy0op4MZUUbWxlKDGQao3+bdPxyrD4Dg9Rne384+CKg1XbHgE8U0hTE/gFVCjPd
rOxGKSSaMQI1Yg0o8I3Ts+RklhHE5k9SuI336QOc08U=
thaisbardini@Thaiss-Laptop Documents %
```



LabSEC
Laboratório de Segurança em Computação

cpqd

Cipher Block Chaining - CBC

- Uso para autenticação de dados (MAC) e transmissões de propósito geral
- Apropriado para cifragem de mensagens longas
- IV deve ser conhecido pelo emissor e receptor, mas imprevisível para um atacante
  - não é necessariamente secreto, mas não deve ser reusado com a mesma chave
  - Usar número pseudo-aleatório
- **Problema**: Não é paralelizável

Imagem: W. Stallings. *Cryptography and network security*. Cap 7.2

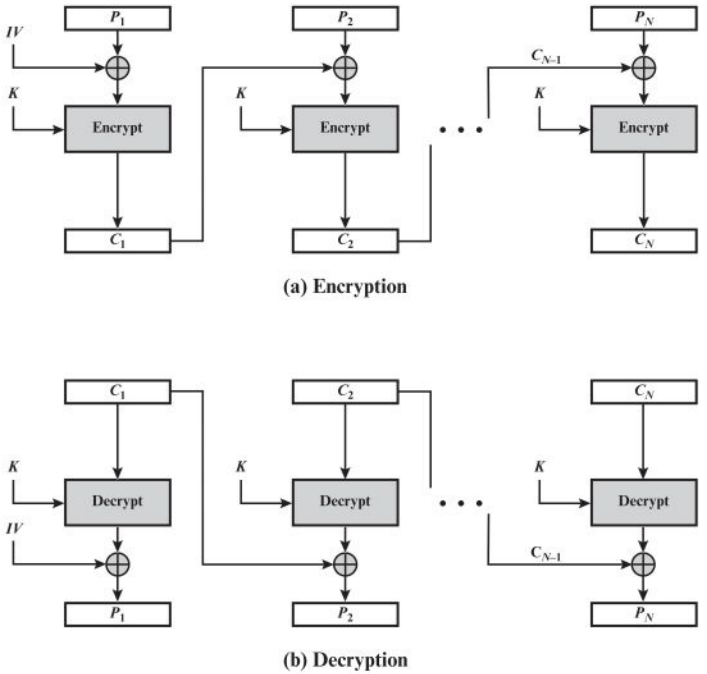


Figure 7.4 Cipher Block Chaining (CBC) Mode

LabSEC
Laboratório de Segurança em Computação

cpqd

Cipher Feedback - CFB

- Bloco cifrado anterior usado como entrada do algoritmo de cifragem. XOR entre essa saída e o texto claro
- Pode ser usado para converter uma cifra de bloco em cifra de *stream*
  - o texto claro é processado *s* bits por vez, s ≤ b
  - não há a necessidade de *padding* caso o texto plano tenha um número de bits múltiplo de s

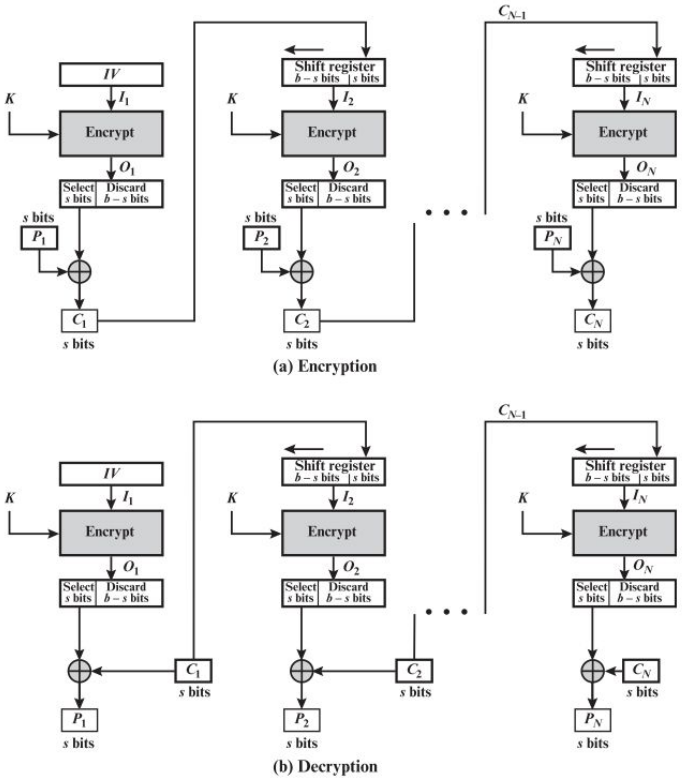


Figure 7.5 *s*-bit Cipher Feedback (CFB) Mode

Imagem: W. Stallings. *Cryptography and network security*. Cap 7.2

CFB	$I_1 = IV$ $I_j = \text{LSB}_{b-s}(I_{j-1}) \| C_{j-1}$ $j = 2, \ldots, N$ $O_j = \text{E}(K, I_j)$ $j = 1, \ldots, N$ $C_j = P_j \oplus \text{MSB}_s(O_j)$ $j = 1, \ldots, N$	$I_1 = IV$ $I_j = \text{LSB}_{b-s}(I_{j-1}) \| C_{j-1}$ $j = 2, \ldots, N$ $O_j = \text{E}(K, I_j)$ $j = 1, \ldots, N$ $P_j = C_j \oplus \text{MSB}_s(O_j)$ $j = 1, \ldots, N$

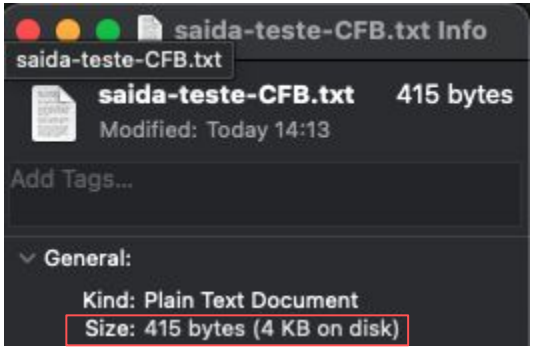
LabSEC Laboratório de Segurança em Computação

cpqd

Cipher Feedback - CFB

```
Documents — -zsh — 147×25
[thaisbardini@Thaiss-Laptop Documents % openssl enc -aes-256-cfb -base64 -pbkdf2 -pass pass:senha123 -in teste-ECB.txt -out saida-teste-CFB.txt

[thaisbardini@Thaiss-Laptop Documents % cat saida-teste-CFB.txt
U2FsdGVkX19jy1EU5jb7bKS0bG+RYc6Bo1/F8os5ry9JsLXTxCKzfrfn3Jza20Z2
m1tprDDwp4H8u66kLX3+pFPZPfu/IWo/e1LGb0ZimVoTMHRUpuBtJc2DPsB7Jeov
ymfL+VM3G6ZleUmidkeC8cXDJZrYoukQucVsrshP5rlgf626tojiplOt6dxoX6FJ
3Y10qZUqBb+G8qchraKQJRXxMygOZO0ehJ87+vRNACfOABkxMhvDZr5GQLrqWQAK
Cwr57UWeYRXnpVgh2ZTMOxFQnRiue09+GlX/2GeNvNBHYrmX2ZPqUG1DTXDos4FZ
DFFTHMdzsjEDNyPp9oAJBS0eZ2OPtbqS43hFkJ2Flns5Mv/Sc2B41NNvjOhv5WWq
18T3wxqqD0EQdgKbVuqg5A==
thaisbardini@Thaiss-Laptop Documents %
```



LabSEC
Laboratório de Segurança em Computação

cpqd

Cipher Feedback - CFB

- O mesmo algoritmo de cifragem é usado para cifrar e decifrar
  - Isso acontece pois a cifragem do texto claro acontece na operação de XOR entre P_j e O_j
  - portanto, para decifrar, basta fazer XOR entre C_j e O_j
- Uso para transmissão de dados e autenticação, opera em tempo real
- **Problemas**: Não é paralelizável

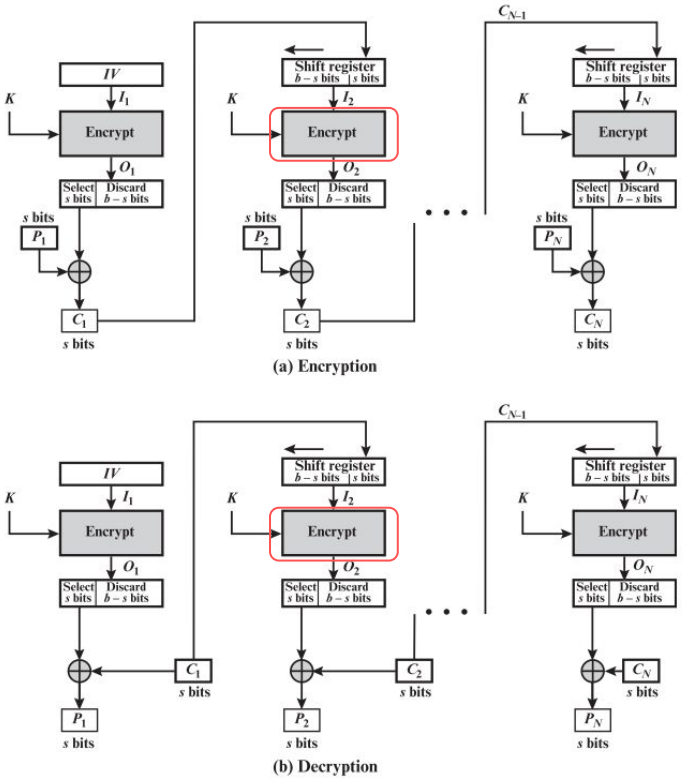


Figure 7.5 *s*-bit Cipher Feedback (CFB) Mode

Imagem: W. Stallings. *Cryptography and network security*. Cap 7.2

CFB	$I_1 = IV$	$I_1 = IV$
	$I_j = \text{LSB}_{b-s}(I_{j-1}) \| C_{j-1}$ $\quad j = 2, \ldots, N$	$I_j = \text{LSB}_{b-s}(I_{j-1}) \| C_{j-1}$ $\quad j = 2, \ldots, N$
	$O_j = \text{E}(K, I_j)$ $\quad j = 1, \ldots, N$	$O_j = \text{E}(K, I_j)$ $\quad j = 1, \ldots, N$
	$C_j = P_j \oplus \text{MSB}_s(O_j)$ $\quad j = 1, \ldots, N$	$P_j = C_j \oplus \text{MSB}_s(O_j)$ $\quad j = 1, \ldots, N$

LabSEC
Laboratório de Segurança em Computação

cpqd

Output Feedback - OFB

- A saída do cifrador é retroalimentada para gerar um *stream* de bits
  - gerando uma *keystream* que é independente do texto em claro
- Texto em claro é cifrado utilizando XOR com a saída do algoritmo de cifragem
- O mesmo algoritmo de cifragem é usado para cifrar e decifrar
- Todos os blocos de texto claro tem tamanho de *b* bits
  - se o último tiver u < b bits, são usados apenas os *u* bits mais significativos da saída O_N

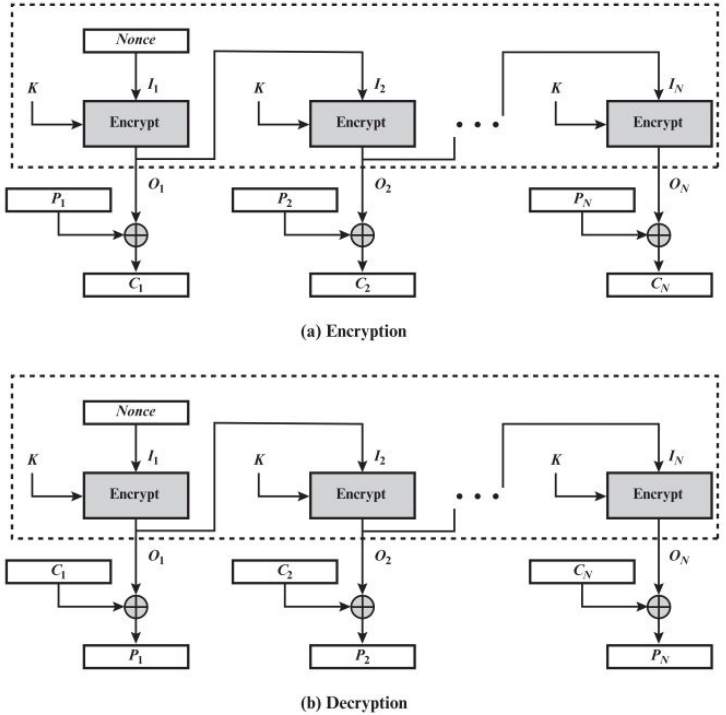


Figure 7.6 Output Feedback (OFB) Mode

OFB	$I_1 = Nonce$ $I_j = O_{j-1}$ $j = 2, \ldots, N$ $O_j = \mathrm{E}(K, I_j)$ $j = 1, \ldots, N$ $C_j = P_j \oplus O_j$ $j = 1, \ldots, N-1$ $C_N^* = P_N^* \oplus \mathrm{MSB}_u(O_N)$	$I_1 = Nonce$ $I_j = O_{j-1}$ $j = 2, \ldots, N$ $O_j = \mathrm{E}(K, I_j)$ $j = 1, \ldots, N$ $P_j = C_j \oplus O_j$ $j = 1, \ldots, N-1$ $P_N^* = C_N^* \oplus \mathrm{MSB}_u(O_N)$

Imagem: W. Stallings. *Cryptography and network security*. Cap 7.2

LabSEC
Laboratório de Segurança em Computação

cpqd

Output Feedback - OFB

- Usado em canais ruidosos
  - já que erros em um C_i não se propagam na decifragem
- IV precisa ser um *nounce* por questões de segurança
  - O_i depende apenas de K e IV
  - se reusado em duas mensagens que tem um ou mais blocos idênticos em posições idênticas, pode revelar informações sobre O_i
- **Problema**:
  - Não é paralelizável
  - Se os blocos cifrados chegam foram de ordem, precisa guardar a keystream inteira para decifragem

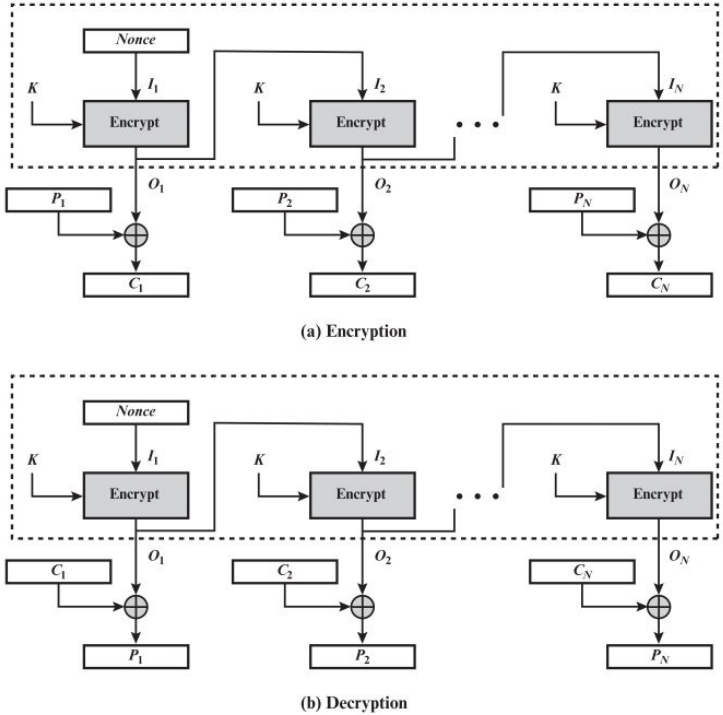


Figure 7.6 Output Feedback (OFB) Mode

Imagem: W. Stallings. *Cryptography and network security*. Cap 7.2

LabSEC
Laboratório de Segurança em Computação

cpqd

Counter Mode - CTR

- A saída do cifrador é retroalimentada para gerar um *stream* de bits
  - a diferença é que a entrada da cifragem é um contador
- Texto em claro é cifrado utilizando XOR com a saída do algoritmo de cifragem
  - se o último tiver u < b bits, são usados apenas os *u* bits mais significativos
- Counter precisa ser um *nounce* por questões de segurança
  - se reutilizado com a mesma chave, pode ser explorado por ataques conhecidos

Imagem: W. Stallings. *Cryptography and network security*. Cap 7.2

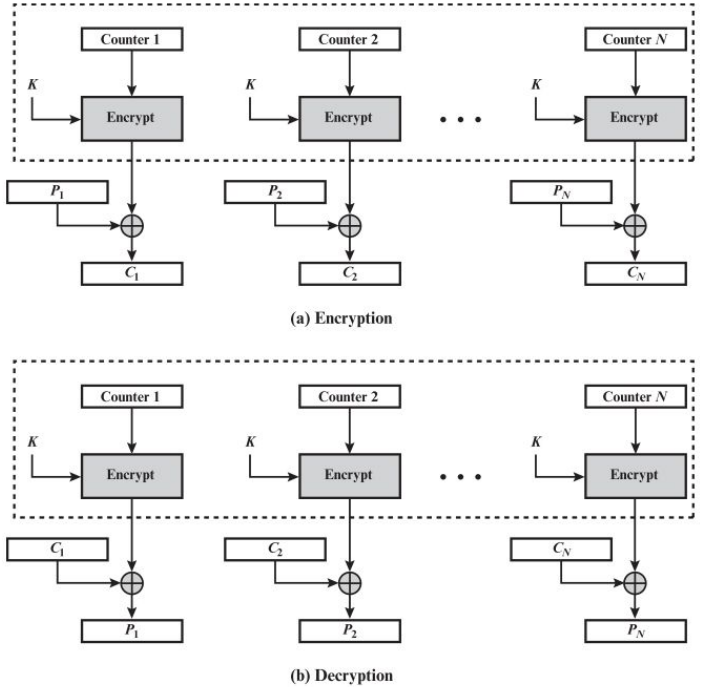


Figure 7.7 Counter (CTR) Mode

CTR	$C_j = P_j \oplus \mathrm{E}(K, T_j) \quad j = 1, \ldots, N-1$ $C_N^* = P_N^* \oplus \mathrm{MSB}_u[\mathrm{E}(K, T_N)]$	$P_j = C_j \oplus \mathrm{E}(K, T_j) \quad j = 1, \ldots, N-1$ $P_N^* = C_N^* \oplus \mathrm{MSB}_u[\mathrm{E}(K, T_N)]$

Counter Mode - CTR

- Lida com blocos fora de ordem
  - Sabendo o número do bloco, é possível decifrá-lo
  - não precisa guardar a *keystream* inteira
- Uso geral em transmissão de dados e em links de alta velocidade
- Permite implementações eficientes em software e hardware com **paralelismo**
  - além disso, permite pré-processamento
- Para informações sobre geração de counter: NIST 800-38A

Imagem: W. Stallings. *Cryptography and network security*. Cap 7.2

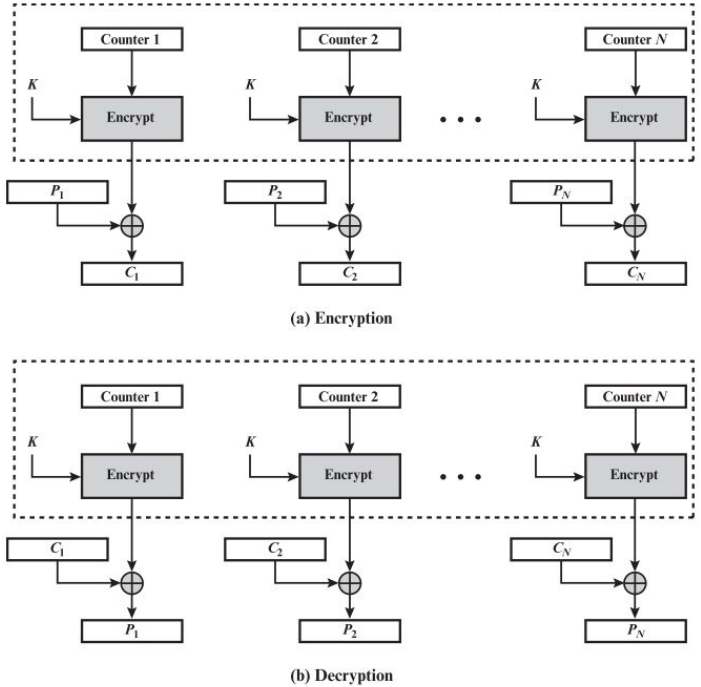


Figure 7.7 Counter (CTR) Mode

LabSEC
Laboratório de Segurança em Computação

cpqd

Resumo

Table 7.1 Block Cipher Modes of Operation

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of plaintext bits is encoded independently using the same key.	• Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next block of plaintext and the preceding block of ciphertext.	• General-purpose block-oriented transmission • Authentication
Cipher Feedback (CFB)	Input is processed *s* bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	• General-purpose stream-oriented transmission • Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output, and full blocks are used.	• Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	• General-purpose block-oriented transmission • Useful for high-speed requirements

Imagem: W. Stallings. *Cryptography and network security*. Cap 7.2

LabSEC
Laboratório de Segurança em Computação

cpqd

Padding

- Nos modos ECB, CBC e CFB, o texto plano precisa um comprimento múltiplo do tamanho dos blocos considerados
  - *b* para ECB e CBC ou *s* para CFB
- Se não for o caso, o texto plano será concatenado com alguns bits extras - *padding*
- Um exemplo de padding é 1 seguido dos 0's necessários para complementar o tamanho necessário

Vetores de inicialização

- Os modos CBC, CFB e OFB requerem um vetor de inicialização IV
- IV deve ser gerado em cada cifragem de uma nova mensagem
- O mesmo IV é necessário para a decifragem
  - por esse motivo, ele não é secreto, e deve ser transmitido no texto cifrado
- Para informações sobre IV: NIST 800-38A apêndice C
- O modo CTR precisa de algo similar, chamado de *counter* ou *nonce*

Sumário

- Modos de Operação:
  - Electronic Codebook - ECB
  - Cipher Block Chaining - CBC
  - Cipher Feedback - CFB
  - Output Feedback - OFB
  - Counter Mode - CTR
- **Modos de operação na prática**

Usos indevidos dos modos de operação

- Microsoft Office 365 Message Encryption usou ECB na cifragem de emails (2022)
- Alguns drivers USB usaram ECB na cifragem dos dados, podendo permitir que atacantes extraiam informações sobre dados cifrados (2022)
- Zoom utilizava AES-128 no modo ECB para a garantia de segurança das chamadas (2020)
- Reutilização de IV pela Samsung permite que atacante extraia informações sobre chaves em ~100 milhões de smartphones (2022)

Atividade: experimentando modos de operação

- Vamos praticar utilizando o openssl:

```
openssl enc -aes-256-ecb -base64 -pbkdf2 -pass pass:chave -in texto-claro.txt -out texto-cifrado.txt
```

- Crie diferentes arquivos de texto claro de tamanhos diferentes, com e sem repetições, etc.
- Experimente com diferentes modos de operação.
  - são eles: ecb, cbc, cfb, ofb, ctr
- O tamanho do arquivo cifrado varia de acordo com o modo de operação utilizado?
- Como podemos decifrar a mensagem cifrada?

Para a próxima aula

- Programação python utilizando a biblioteca PyCryptodome
- Requisito: fazer as instalações necessárias para a utilização da biblioteca
- https://pycryptodome.readthedocs.io/en/latest/src/installation.html

Referências

- W. Stallings. *Cryptography and network security*. 7a edição.
  - Capítulos 7.2, 7.3, 7.4, 7.5, 7.6
- NIST SP 800-38A