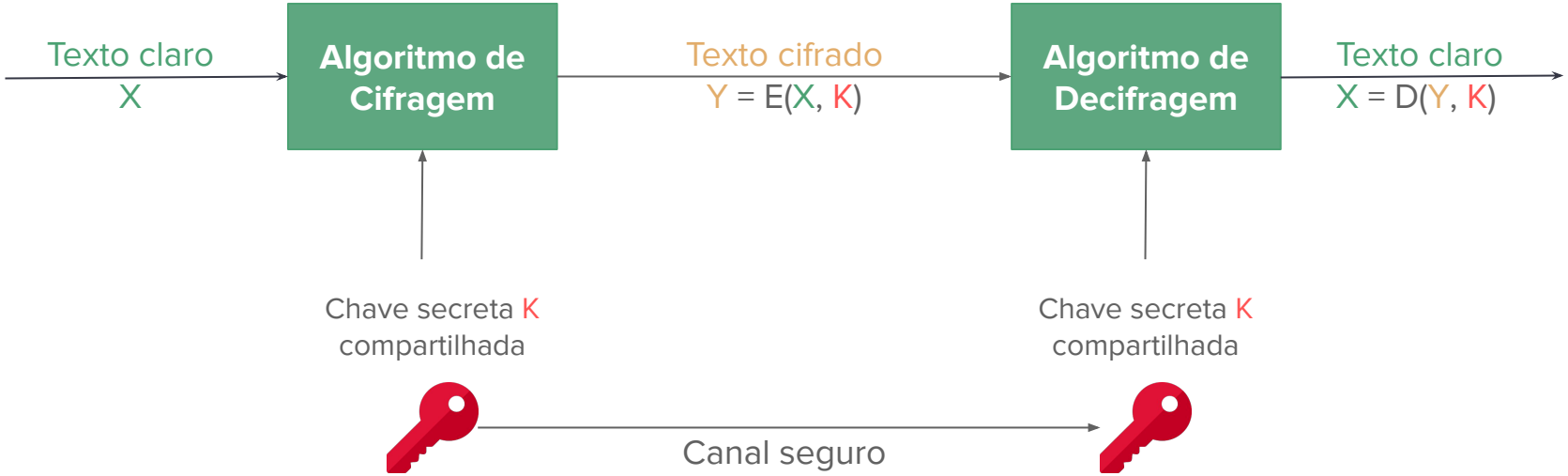
Criptografia Aplicada

Atividade prática com AES

Criptografia simétrica



AES - Advanced Encryption Standard

- Suporte a chaves de 128, 192 e 256 bits
- Blocos de 128 bits
- Número de *rounds* dependente do tamanho da chave

Key Size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext Block Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of Rounds	10	12	14
Round Key Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded Key Size (words/bytes)	44/176	52/208	60/240

Imagem: W. Stallings. *Cryptography and network security*. Cap 6.2

Modos de Operação

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

Electronic Codebook - ECB

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

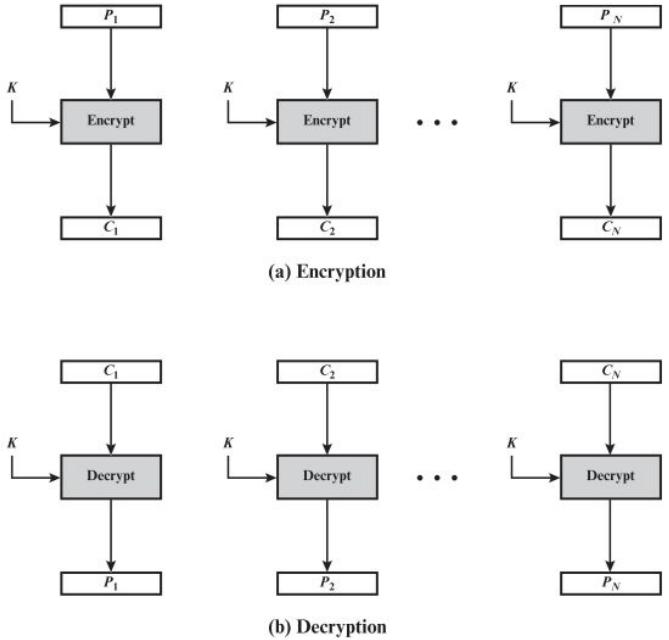


Figure 7.3 Electronic Codebook (ECB) Mode

LabSEC
Laboratório de Segurança em Computação

cpqd

Cipher Block Chaining - CBC

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

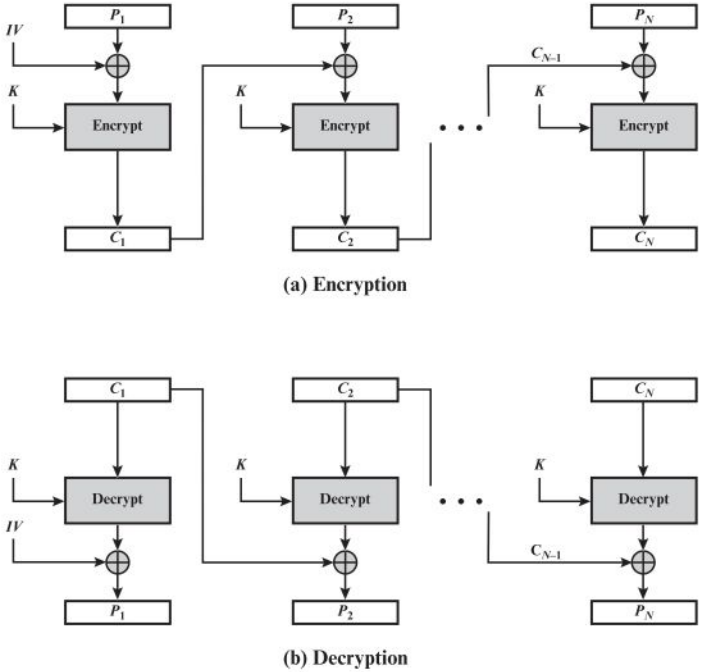


Figure 7.4 Cipher Block Chaining (CBC) Mode

LabSEC
Laboratório de Segurança em Computação

Cipher Feedback - CFB

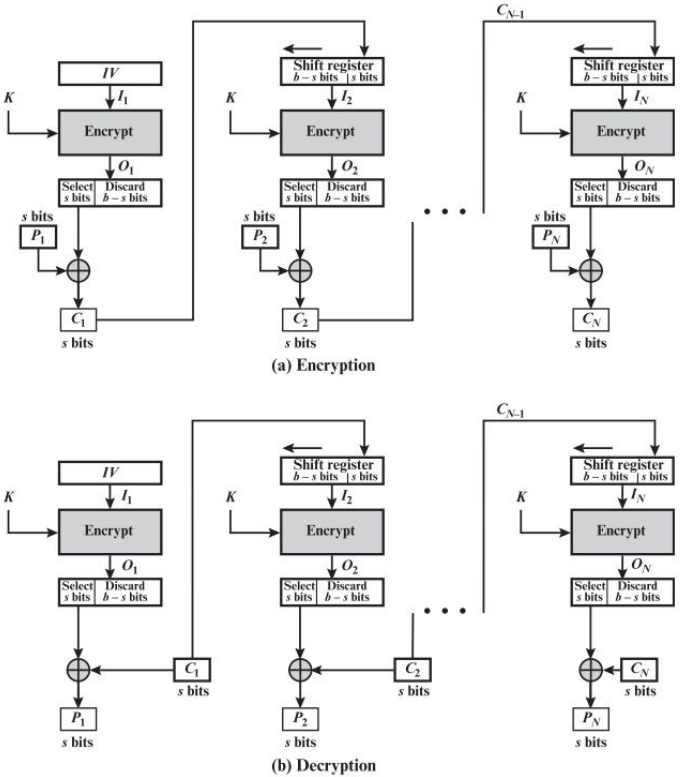


Figure 7.5 *s*-bit Cipher Feedback (CFB) Mode

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

Output Feedback - OFB

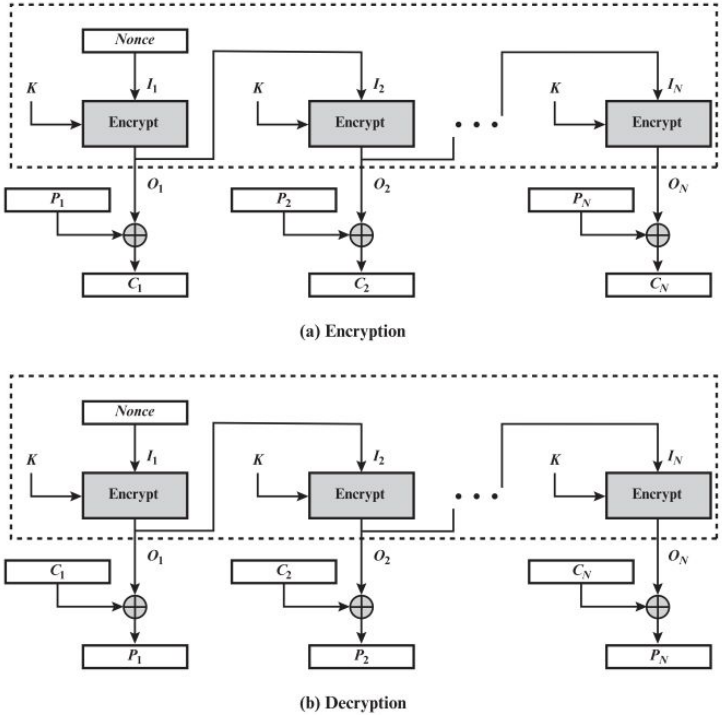


Figure 7.6 Output Feedback (OFB) Mode

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

Counter Mode - CTR

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

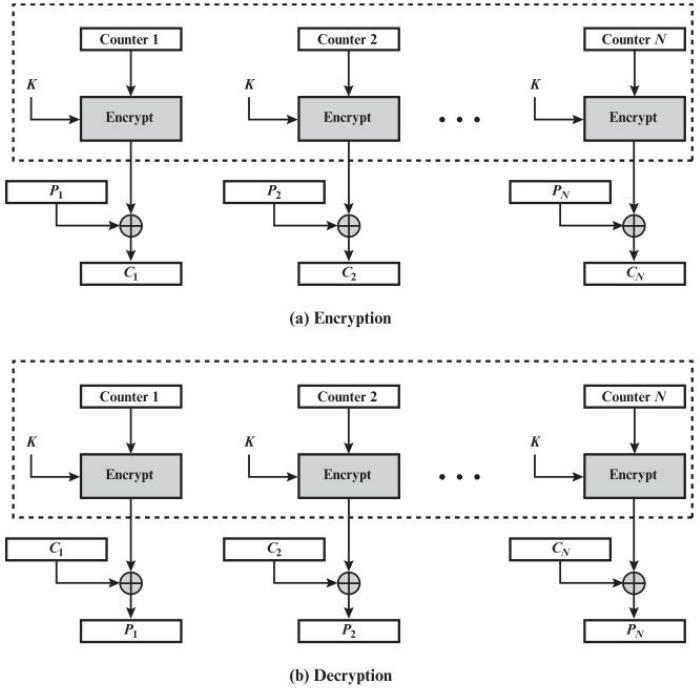


Figure 7.7 Counter (CTR) Mode

LabSEC
Laboratório de Segurança em Computação

cpqd

Atividade

- Vamos utilizar agora a biblioteca PyCryptodome
- Para instalar no linux, basta rodar o comando:
  - pip install pycryptodome
  - pip install pycryptodomex (alternativa se não funcionar a anterior)
- Importação da biblioteca:
  - `from Cryptodome.Cipher import AES`
  - `from Crypto.Cipher import AES`

Atividade 1

- Crie duas funções python, uma para **cifragem** e outra para **decifragem** de mensagens usando o AES
- **Cifragem:**
  - Ela precisa ser flexível para permitir diversos modos de operação
  - Ela deve salvar o IV e o texto cifrado em um arquivo
  - Veja a documentação para entender as particularidades de cada modo de operação
- **Decifragem**:
  - Ela precisa ser flexível para permitir diversos modos de operação
  - Ela deve obter o IV salvo na mensagem cifrada
- Cifre um arquivo de texto e envie aos colegas para decifragem
- Veja o esqueleto do código python no Canvas: `aes.py`

Vetor de inicialização IV

- Com exceção do modo ECB, todos os outros modos precisam de um IV ou counter/nonce para decifrar a mensagem cifrada.
- Geralmente, essa informação é transmitida junto com a mensagem cifrada
- No caso dessa aula, recomendo concatenar na mensagem cifrada da seguinte maneira, ambos em bytes:

```
iv + ciphertext
```

Atividade 2

- Um documento foi cifrado utilizando AES (trasure.txt.enc)
- A sua tarefa é decifrá-lo!
- Quais informações você precisa para fazer a decifragem?

Chave AES

- A chave foi cifrada usando uma técnica de cifragem **antiga** e resultou no seguinte texto:

dyhubvhfuhwnhbbbdyhubvhfuhwnhbbb

- Essa é uma chave de 32 bytes = 256 bits

Referências

Documentação PyCryptodome:
https://pycryptodome.readthedocs.io/en/latest/src/cipher/classic.html#