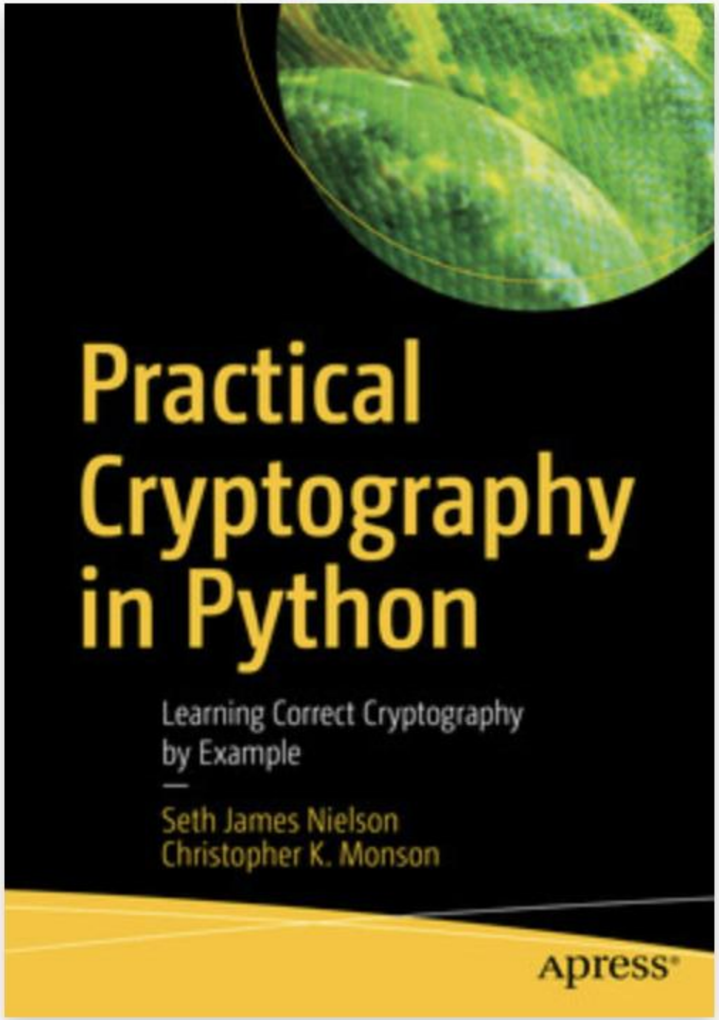
Week 13 Symmetric encryption

Recommended reading



Practical Cryptography in Python

Learning Correct Cryptography by Example

Seth James Nielson
Christopher K. Monson

Apress

The book is available to you via the library

Technology stack

- Python 3
  Link to a Python Cheat Sheet
- cryptography.io
  Link to the library

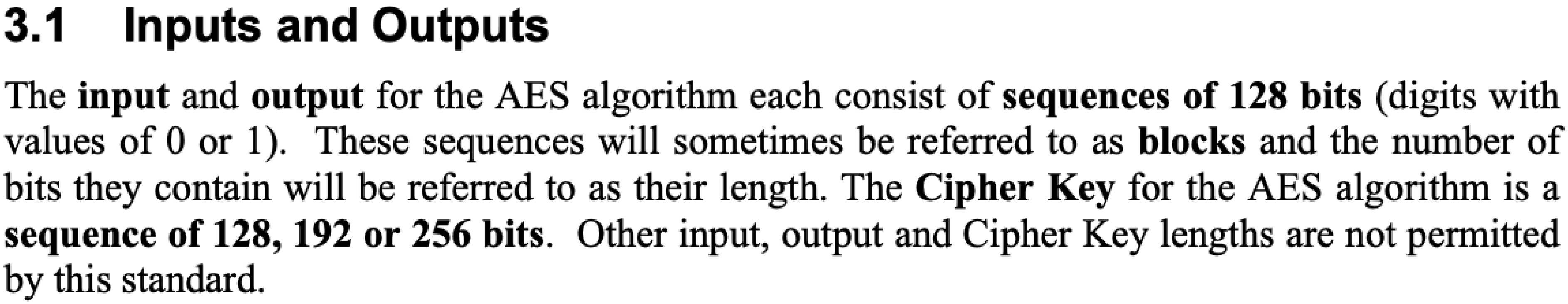
Topics

- AES – ECB
- Encrypt a B&W file in AES-ECB
- Padding
- AES-CTR

Recommended reading: Chapters 3 from the book of "Practical Cryptography in Python"

AES I/O

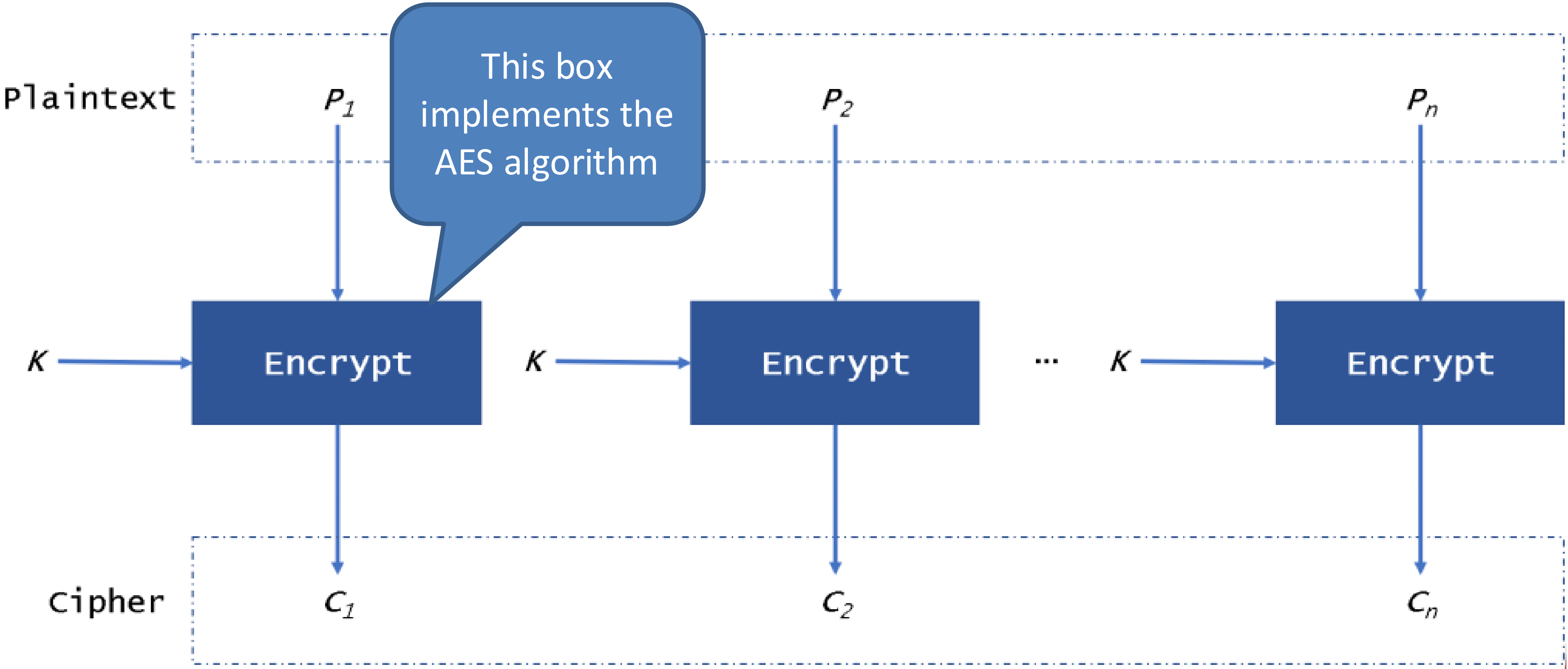
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf



3.1 Inputs and Outputs

The **input** and **output** for the AES algorithm each consist of **sequences of 128 bits** (digits with values of 0 or 1). These sequences will sometimes be referred to as **blocks** and the number of bits they contain will be referred to as their length. The **Cipher Key** for the AES algorithm is a **sequence of 128, 192 or 256 bits**. Other input, output and Cipher Key lengths are not permitted by this standard.

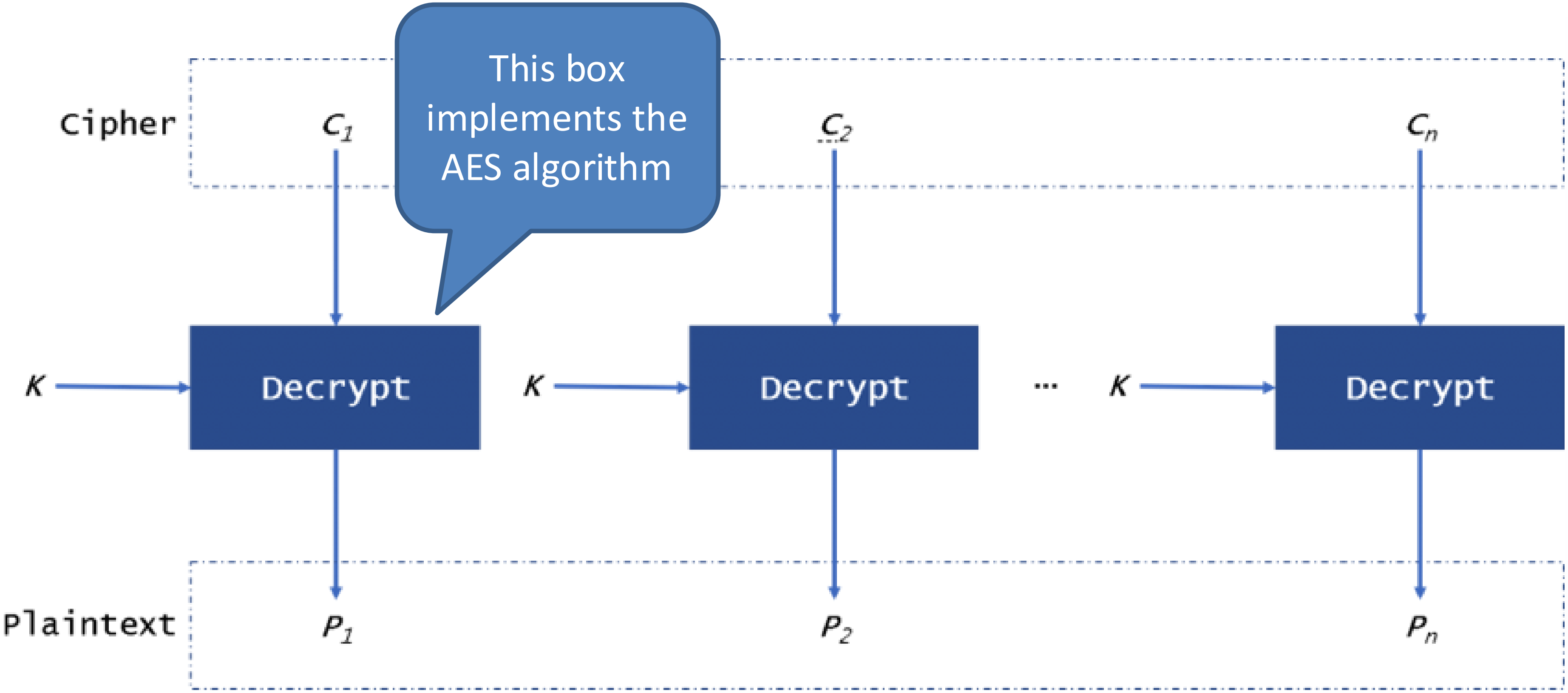
AES – Electronic Code Book (ECB) - Encrypt



This box implements the AES algorithm

https://www.highgo.ca/2019/08/08/the-difference-in-five-modes-in-the-aes-encryption-algorithm/

AES – Electronic Code Book (ECB) - Decrypt



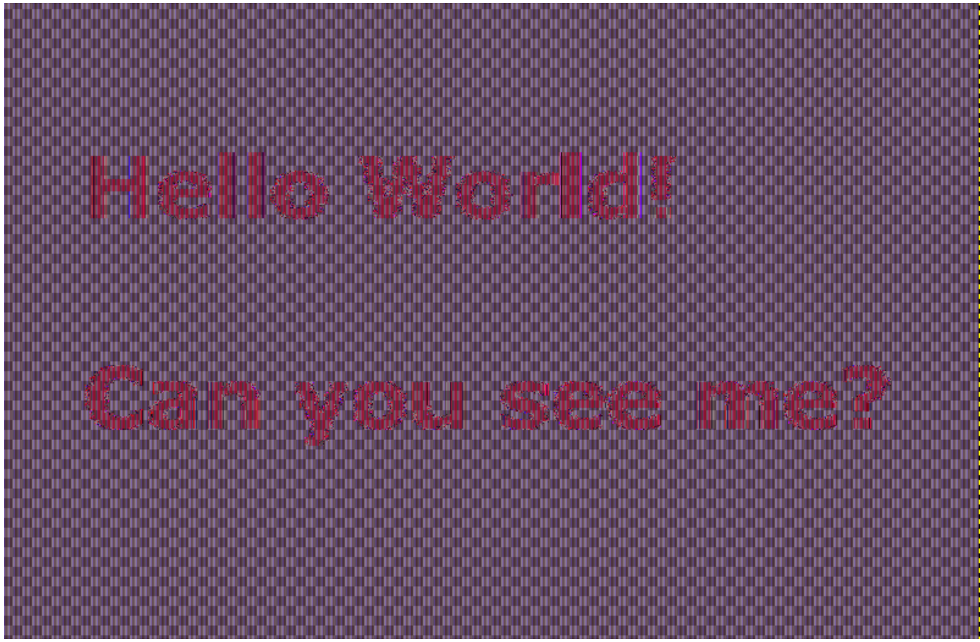
This box implements the AES algorithm

https://www.highgo.ca/2019/08/08/the-difference-in-five-modes-in-the-aes-encryption-algorithm/

Example

Hello World!

Can you see me?



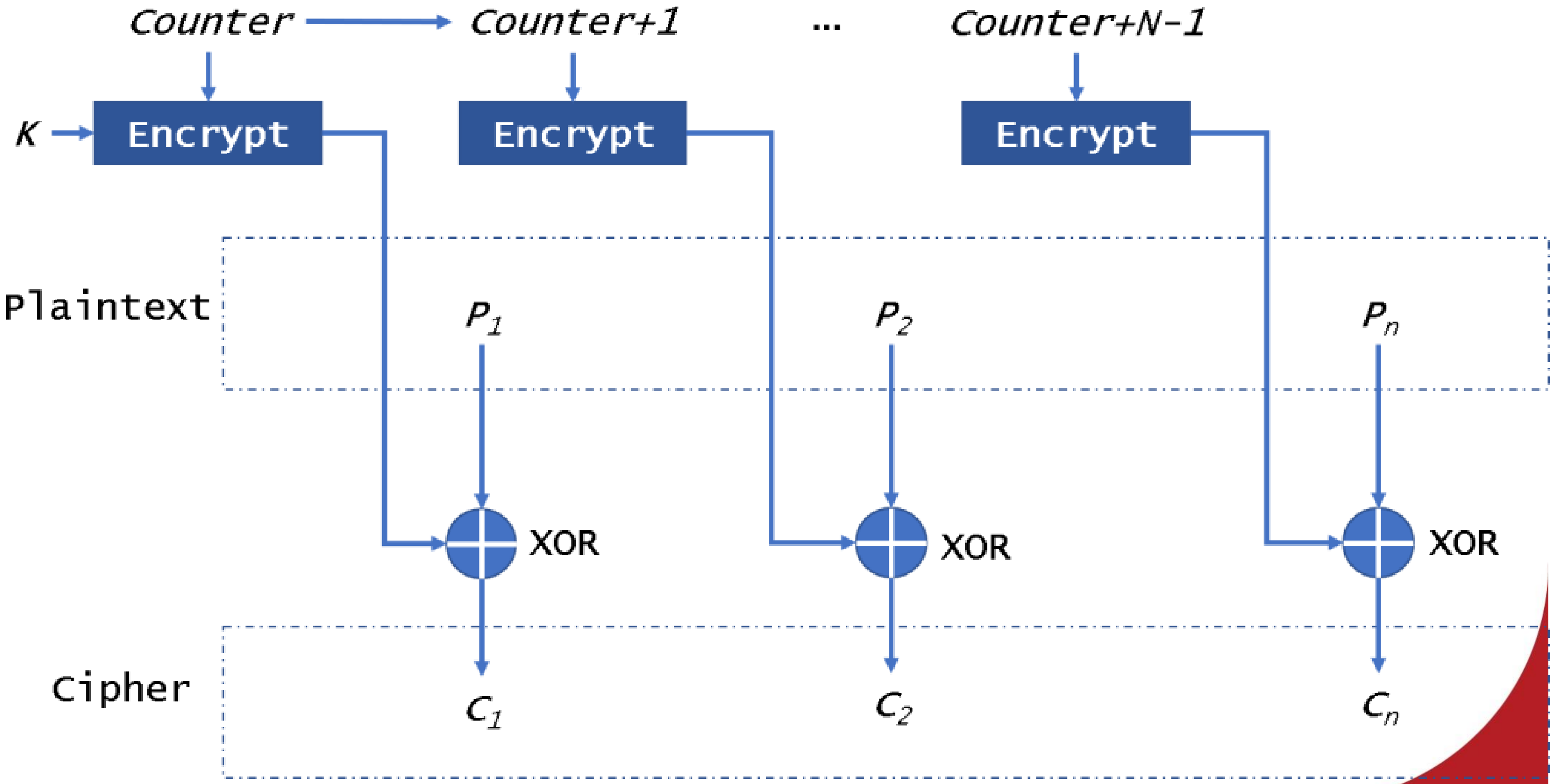
Are we forgetting something?

```
from cryptography.hazmat.primitives.ciphers import Cipher,
algorithms, modes
import os

def SimpleECB():
        key = os.urandom(32)
        aesCipher = Cipher(algorithms.AES(key), modes.ECB())
        aesEncryptor = aesCipher.encryptor()
        aesDecryptor = aesCipher.decryptor()

        message = b"Hello world"

        cipherText = aesEncryptor.update(message)
        print(cipherText)

        plainText = aesDecryptor.update(cipherText)
        print(plainText)
```

Padding – PKCS7

```
def SimpleECB():
        …
        message = b"Hello world"
        padder = padding.PKCS7(128).padder()
        unpadder = padding.PKCS7(128).unpadder()

        paddedMessage = padder.update(message) +
padder.finalize()
        cipherText = aesEncryptor.update(paddedMessage)
        print(cipherText)
        plainText = aesDecryptor.update(cipherText)
        plainText = unpadder.update(plainText) +
unpadder.finalize()
        print(plainText)
```

AES – Counter- CTR



Structure of your code…

Modules you want to import

```
import XYZ
```

List of functions you implement

```
def myFunction():
    # TODO

    return # TODO
```

Have a main section to call your functions

```
if __name__ == “__main__”:
    x = myFunction()
```