

**LAB 12**

**Part 1: One-Time Pad Cryptography**

**Copyright © (2022-2025) All Rights Reserved**

**Dr. Matthew Kisow**

VERSION 1

22-NOV-2024

**LAB**:NaCL Cryptography Programming – Part 1: One-Time Pad Cryptography

**OBJECTIVE**: Create a Python script that reads the one-time pad **part1.otp.bin** and ciphertext **part1.ciphertext.bin** files, and performs decryption using XOR operations to recover the original plaintext message.

**INSTRUCTIONS**: In this lab, you will write a Python script to decrypt the ciphertext in the **part1.ciphertext.bin** file using the one-time pad stored in **part1.otp.bin**. The decryption will reconstruct the original plaintext message. Ensure you follow these guidelines when building your **part1.otp\_decrypter.py** script. Please follow the instructions for submitting this assignment on Blackboard.

1. **Prerequisites**
2. **Setting Up Your Python Environment**

Before you start programming your client, set up your Python environment:

1. Create a virtual environment:

python3 -m venv .venv

1. Activate the virtual environment:

* **Linux/macOS:**

source .venv/bin/activate

* **Windows:**

.venv\Scripts\activate

1. Install the necessary dependencies:

pip install wheel pynacl requests

1. **Understand XOR Decryption:**

Encryption and decryption with a one-time pad work as follows:

* + Encryption: **ciphertext\_byte = plaintext\_byte ^ otp\_byte**
  + Decryption: **plaintext\_byte = ciphertext\_byte ^ otp\_byte**

1. **Writing the otp\_decrypter.py Script**
2. **Import Necessary Modules**

Use the **os** and **sys** , **pynacl** modules for file handling.

1. **Define Helper Functions**
   * **Read Binary Data from File:** Create a function to read binary data from the given file:

def read\_from\_file(filename):

"""Read binary data from a file."""

with open(filename, "rb") as file:

return file.read()

* + **Decrypt Using OTP:** Implement the XOR decryption logic:

def decrypt\_with\_otp(ciphertext, otp):

"""Decrypt ciphertext using the one-time pad."""

# XOR each byte of the ciphertext with the corresponding byte of the OTP

plaintext\_bytes = bytes([c ^ o for c, o in zip(ciphertext, otp)])

return plaintext\_bytes.decode('ascii')

1. **Build the Main Script Logic**
   1. Read the **part1.ciphertext.bin** and **part1.otp.bin** files.
   2. Ensure the files have matching lengths.
   3. Decrypt the ciphertext using the OTP.
   4. Print the recovered plaintext.
2. **Testing**
   1. Save the script as **part1.py**.
   2. Run it from the command line, providing the **part1.ciphertext.bin** and **part1.otp.bin** files as arguments:

python3 part1.py part1.ciphertext.bin part1.otp.bin

**DELIVERABLE**

Write a Python3 script named **part1.py** that communicates with the server, receives the ciphertext, and prints the plaintext message to the screen.