Họ tên:Nguyễn Văn Duy
Mã sinh viên:22174600011
Lớp: DHKL16A1HN
BÀI THỰC HÀNH 2 : Xác thực bằng mật khẩu, OTP và 2FA

Bước 1: Xác thực bằng mật khẩu

```python
import hashlib

# Mật khẩu lưu trữ dưới dạng mã băm SHA-256
stored_password = hashlib.sha256(b"123456").hexdigest()

# Yêu cầu người dùng nhập mật khẩu
password = input("Nhập mật khẩu: ")
hashed_password = hashlib.sha256(password.encode()).hexdigest()

if hashed_password == stored_password:
    print("Xác thực thành công!")
else:
    print("Xác thực thất bại!")

```

✓ 3.1s

```
Xác thực thành công!
```

Bước 2: Xác thực bằng mã OTP

```python
import pyotp
import time

# Tạo khóa bí mật và mã OTP
secret = pyotp.random_base32()
totp = pyotp.TOTP(secret)

print("Mã OTP của bạn là:", totp.now())

# Yêu cầu nhập mã OTP
otp_input = input("Nhập mã OTP: ")

if totp.verify(otp_input):
    print("Xác thực thành công!")
else:
    print("Xác thực thất bại!")

```

✓ 5.6s

```
Mã OTP của bạn là: 227260
Xác thực thành công!
```

Bước 3: Mô phỏng xác thực hai yếu tố (2FA)

Họ tên:Nguyễn Văn Duy
Mã sinh viên:22174600011
Lớp: DHKL16A1HN

```python
import hashlib
import pyotp
import time

# Bước 1: Xác thực bằng mật khẩu
stored_password = hashlib.sha256(b"123456").hexdigest()  # Mật khẩu lưu trữ dưới dạng mã băm SHA-256

password = input("Nhập mật khẩu: ")
hashed_password = hashlib.sha256(password.encode()).hexdigest()

if hashed_password == stored_password:
    print("Xác thực mật khẩu thành công! Chuyển sang bước xác thực bằng mã OTP.")
else:
    print("Xác thực mật khẩu thất bại!")
    exit()  # Thoát chương trình nếu sai mật khẩu

# Bước 2: Xác thực bằng mã OTP nếu mật khẩu đúng
# Tạo khóa bí mật và mã OTP
secret = pyotp.random_base32()
totp = pyotp.TOTP(secret)

# In mã OTP (trong thực tế sẽ được gửi qua SMS hoặc Email)
print("Mã OTP của bạn là:", totp.now())

# Yêu cầu người dùng nhập mã OTP
otp_input = input("Nhập mã OTP: ")

if totp.verify(otp_input):
    print("Xác thực hai yếu tố thành công!")
else:
    print("Xác thực bước 2, mã OTP thất bại!")

```

```
Xác thực mật khẩu thành công! Chuyển sang bước xác thực bằng mã OTP.
Mã OTP của bạn là: 989896
Xác thực hai yếu tố thành công!
```

Bước 4: Tóm tắt kết quả thực hành

1. Tại sao xác thực hai yếu tố (2FA) lại an toàn hơn so với xác thực chỉ bằng mật khẩu?

Vì sao 2FA an toàn hơn?

- Ngăn chặn truy cập trái phép nếu bị lộ mật khẩu: Dù kẻ tấn công có được mật khẩu, họ vẫn không có thiết bị tạo mã OTP.
- Mã OTP thay đổi theo thời gian (thường 30 giây), giúp giảm rủi ro bị lộ/đoán.
- Giảm rủi ro tấn công brute-force, phishing, keylogger, v.v.

2. Có thể cải tiến thêm tính năng bảo mật nào cho chương trình này không?

- Không in mã OTP ra màn hình (giả lập gửi qua email/SMS)
- Giới hạn số lần nhập sai mã OTP hoặc mật khẩu

Họ tên:Nguyễn Văn Duy
Mã sinh viên:22174600011
Lớp: DHKL16A1HN

- Lưu trữ mật khẩu và secret trong file mã hóa hoặc sử dụng cơ sở dữ liệu an toàn
- Thêm chức năng kiểm tra thời gian tạo mã OTP
- Sử dụng thư viện quản lý xác thực chuyên nghiệp

3. Dựa trên kết quả thực hành, Anh/Chị rút ra được bài học gì về tính bảo mật của mật khẩu và mã OTP?

Mật khẩu không đủ an toàn nếu dùng một mình

- Mật khẩu dù được mã hóa bằng SHA-256 vẫn có thể bị lộ qua:
    - Phishing (lừa đảo qua email/web),
    - Keylogger (ghi lại phím bấm),
    - Tái sử dụng mật khẩu ở nhiều nơi.
- Dùng một yếu tố duy nhất là không đủ để bảo vệ tài khoản quan trọng.

Mã OTP tăng cường độ an toàn nhờ tính chất tạm thời và riêng biệt

- OTP (One-Time Password) được tạo ra ngẫu nhiên, thay đổi mỗi 30 giây.
- Ngay cả khi hacker biết mật khẩu, họ không thể đăng nhập nếu không có mã OTP, vì:
    - OTP liên kết với thiết bị cụ thể (điện thoại),
    - OTP có thời hạn ngắn, không thể tái sử dụng.

Kết hợp 2 yếu tố (mật khẩu + OTP) là phương án bảo vệ mạnh mẽ

- Đây là minh chứng rõ ràng cho mô hình xác thực hai yếu tố (2FA):
    - Nếu một yếu tố bị lộ, yếu tố còn lại vẫn ngăn chặn truy cập trái phép.
    - Phòng ngừa hầu hết các cuộc tấn công đánh cắp tài khoản thông thường.