Hướng dẫn thực hành: Cài đặt giải thuật Tấn công với khóa bí mật nhỏ (Tấn công Wiener)

1. **Mục đích**
   - Giúp sinh viên tìm hiểu thuật toán tấn công wiener, xây dựng thuật toán tấn công wiener tìm ra khóa bí mật của giải thuật rsa.
2. **Yêu cầu đối với sinh viên**
   - Hiểu được tấn công lên khóa bí mật nhỏ (tấn công wiener), điều kiện tấn công và các bước tấn công.
   - Tìm hiểu được cách code chương trình python tấn công wiener, code chương trình giải mã RSA.
3. **Nội dung thực hành**

Khởi động bài lab:

imodule https://github.com/baprang186/labtainer/raw/main/imodule_cryp-attk-rsa_wiener.tar

Vào terminal, gõ:

labtainer cryp-attk-rsa_wiener

(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

Sau khi khởi động xong, màn hình sẽ xuất hiện 1 terminal với người dùng **student.** Bài lab cho sẵn một thư mục venv, nơi chứa các biến môi trường và thư viện cho môi trường ảo hóa. Khởi động môi trường ảo, thực hiện lệnh:

source venv/bin/activate

Thực hiện sinh khóa và bản mã bằng chương trình genkey.py cho trước, thực hiện lệnh:

python3 genkey.py

Đầu ra của chương trình trên là một khóa công khai gồm n, e và bản mã c ở dạng *long*.

Để tìm được khóa bí mật d, sinh viên cần thay giá trị n, e vừa tìm được vào chương trình tấn công wiener.py. Sau khi thay giá trị, gõ lệnh:

python3 wiener.py

Nếu bàn hình output in ra được kết quả tìm thấy d thì cho thấy đã tấn công wiener thành công. Sinh viên thực hiện viết chương trình python tìm bản rõ từ khóa công khai, bản mã và khóa bí mật vừa tìm được theo công thức sau:

m = c^d mod n

Ví dụ, chương trình giải mã RSA bằng python như sau:

```
from Crypto.Util.number import *
def decrypt_rsa(ciphertext, d, n):
    # Giải mã bản mã
    plaintext = pow(ciphertext, d, n)
    return plaintext

ciphertext = <Nhập giá trị ciphertext>
d= <Nhập giá trị khóa bí mật>
n=  <Nhập giá trị modulus>

# Giải mã
plaintext = decrypt_rsa(ciphertext, d, n)
m = long_to_bytes(plaintext)
print("Ban ro:", m)
```

Kết thúc bài lab:

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

stoplab cryp-attk-rsa_wiener

Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

Khởi động lại bài lab:

Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

labtainer –r cryp-attk-rsa_wiener