1. Bài thực hành: Hastad Broadcast Attack

1.1 Nội dung và hướng dẫn bài thực hành

1.1.1 Mục đích

Mục tiêu của bài lab này là giúp sinh viên hiểu rõ cách khai thác các lỗ hổng mã hóa liên quan đến thuật toán RSA với tham số công khai e nhỏ với thuật toán dùng Hastad Broadcast Attack kết hợp định lí số dư Trung Hoa để tìm được bản rõ

1.1.2 Yêu cầu đối với sinh viên

Hiểu được thuật toán Hastad Broadcast Attack và định lí số dư Trung Hoa

Tìm hiểu được cách code chương trình python tấn công wiener, code chương trình giải mã RSA.

1.1.3 Nội dung thực hành

Khởi động bài lab:

Vào terminal, gõ:

labtainer hba

(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 terminal. Trong terminal có 2 file là john.py và output.txt. Xem tệp johan.py:

cat johan.py

Sau đó xem tệp output.txt nhận thấy tệp johan.py dùng để thực hiện mã hóa RSA đơn giản cho các thông điệp trong danh sách "messages". Kết quả được lưu vào file output.txt

Đọc code bài cho và thấy e = 3 và chó nhiều cặp (ei,ni) nên dùng Hastad Broadcast Attack kết hợp định lí số dư Trung Hoa để hoàn thành bài lab

```
from itertools import combinations
from Crypto.Util.number import *
from gmpy2 import iroot
def crt(remainders, mod):
    assert len(remainders)== len(mod)
    N  = 1
    for i in mod:
        N*=i
```

```
    Ni = []
    for i in range(len(mod)):
        Ni.append(N//mod[i])
    Y=[]
    for i in range(len(mod)):
        Y.append(pow(Ni[i],-1,mod[i]))
    res = 0
    for i in range(len(mod)):
        res+=remainders[i]*Ni[i]*Y[i]
    return res%N
```

n0 =

e = 3

c0 =

n1 =

e = 3

c1 =

n2 =

e = 3

c2 =

n3 =

e = 3

c3 =

n4 =

e = 3

c4 =

n5 =

e = 3

c5 =

n6 =

e = 3

c6 =

```
n=[n0,n1,n2,n3,n4,n5,n6]
c=[c0,c1,c2,c3,c4,c5,c6]
for i,j,k in combinations(range(len(n)),3):
    mod=[n[i],n[j],n[k]]
    remains =[c[i],c[j],c[k]]
    m =iroot(crt(remains,mod),3)
    flag=long_to_bytes(m[0])
    if b'crypto{' in flag:
        print(flag)
```

Kết thúc bài lab:

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

stoplab

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

Khởi động lại bài lab:

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

labtainer –r hba