LAB 3

Fuzzing - Reverse Engineering - Cryptography

Họ tên và MSSV:……..   Lớp: …….
Link youtube: Link github

- *Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho tất cả bài thực hành của môn này.*
- *Bài nộp phải ở dạng docx, hình minh họa phải rõ ràng chi tiết.* Hình minh hoạ chỉ cần chụp ở nội dung thực hiện, không chụp toàn màn hình.
- *Quay quá trình làm có face để gv biết anh chị đang làm*
- *Anh chị nào không có video trên kênh sẽ không chấm bài*

Câu 1: Thực hiện kỹ thuật Reverse Engineering với công cụ IDA Pro

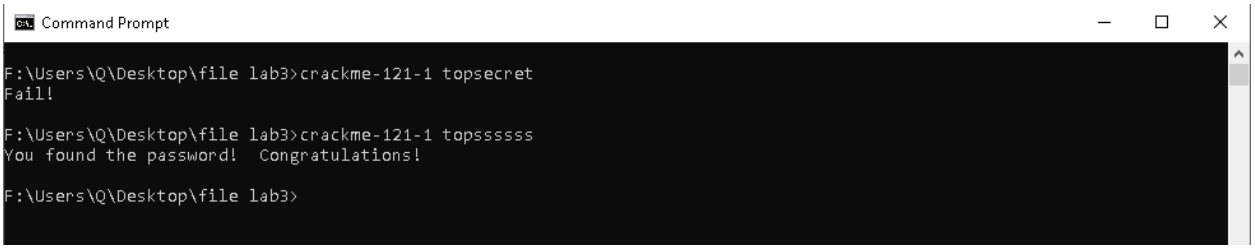
Tham khảo và thực hiện hướng dẫn thực hiện kỹ thuật Reverse Engineering với công cụ IDA Pro. Chụp hình minh hoạ các bước thực hiện như trong hướng dẫn.

https://samsclass.info/126/proj/p2x-126-IDA.html

* Kết quả thực hiện:

- Chạy lại chương trình crackme thì chương trình báo Fail!:

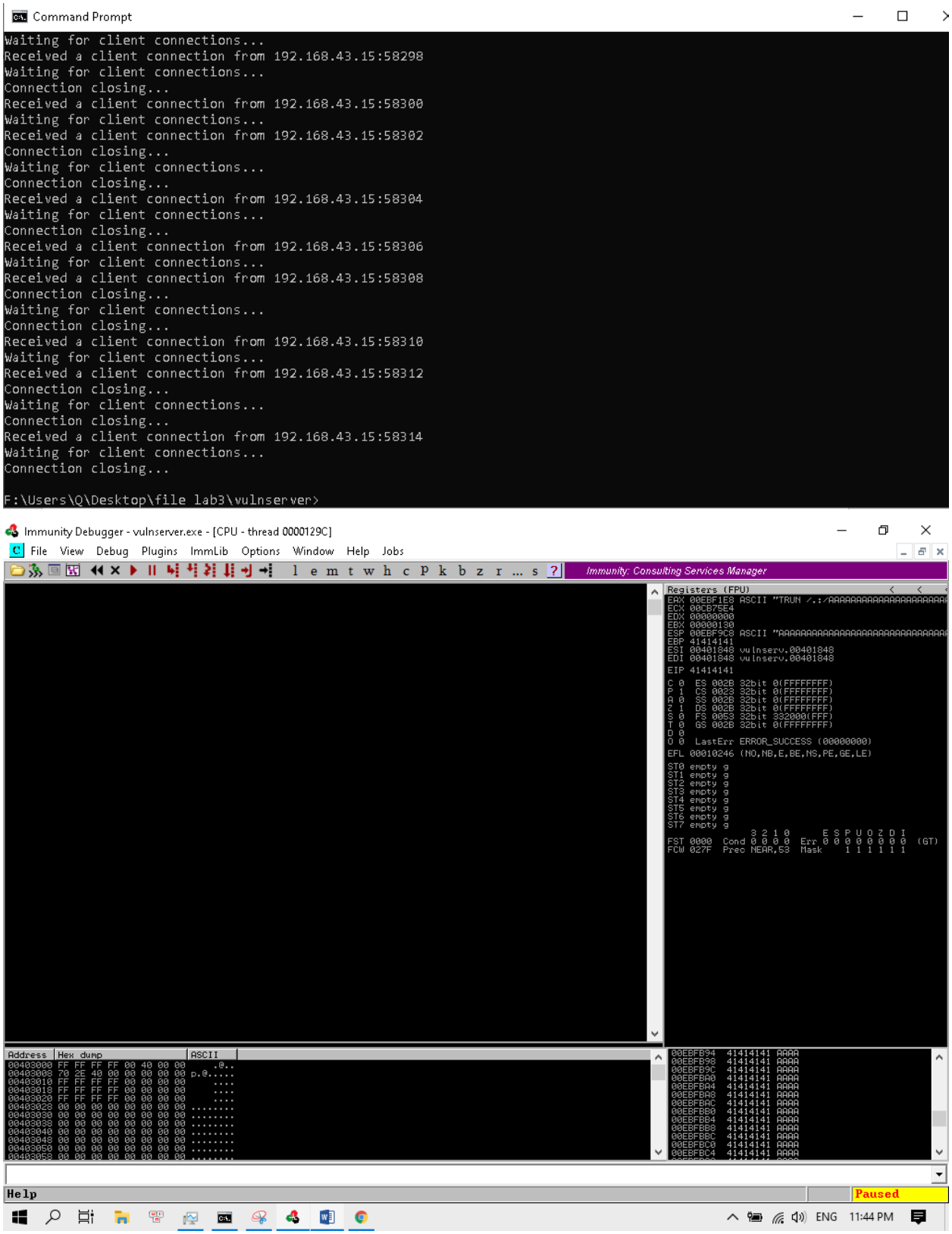
- Chúng ta nhập vào chuỗi mới sửa lại thì chương trình báo thành công:

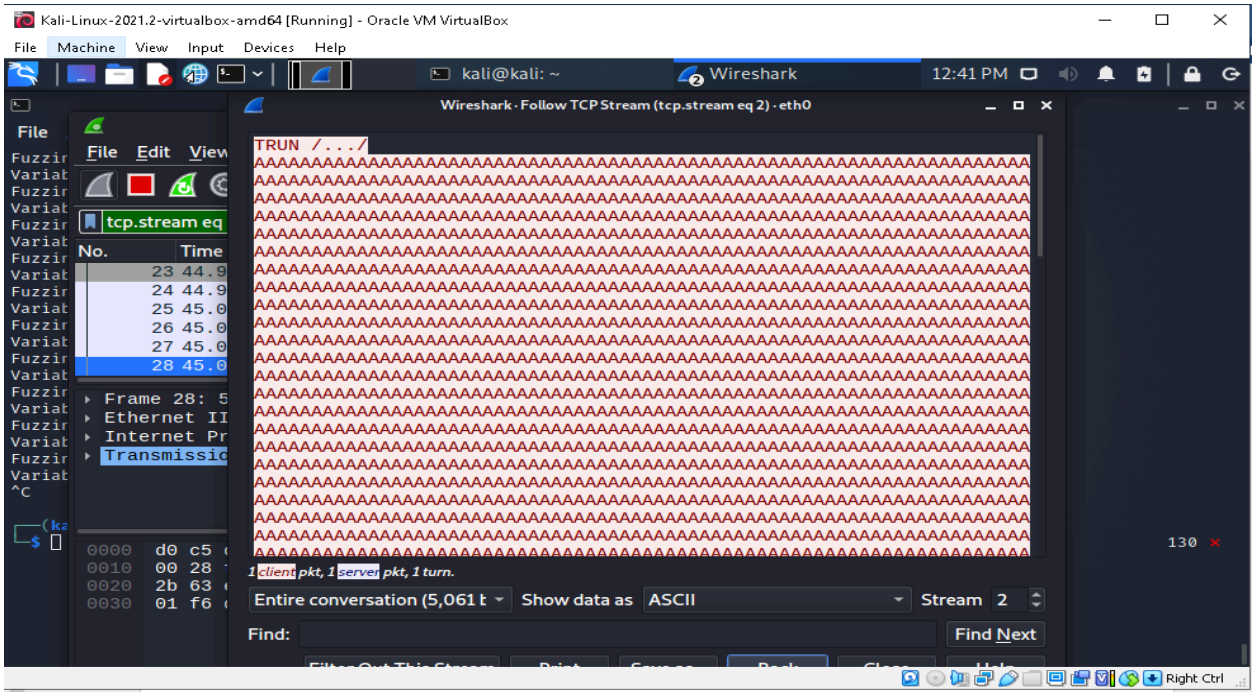


Câu 2: Thực hiện kỹ thuật Fuzzing với công cụ Spike

Tham khảo và thực hiện hướng dẫn thực hiện kỹ thuật Fuzzing sử dụng công cụ Spike trên Kali Linux. Chụp hình minh hoạ các bước thực hiện như trong hướng dẫn.

https://samsclass.info/127/proj/p16-spike.htm


Command Prompt
Waiting for client connections...
Received a client connection from 192.168.43.15:58298
Waiting for client connections...
Connection closing...
Received a client connection from 192.168.43.15:58300
Waiting for client connections...
Received a client connection from 192.168.43.15:58302
Connection closing...
Waiting for client connections...
Connection closing...
Received a client connection from 192.168.43.15:58304
Waiting for client connections...
Connection closing...
Received a client connection from 192.168.43.15:58306
Waiting for client connections...
Received a client connection from 192.168.43.15:58308
Connection closing...
Waiting for client connections...
Connection closing...
Received a client connection from 192.168.43.15:58310
Waiting for client connections...
Received a client connection from 192.168.43.15:58312
Connection closing...
Waiting for client connections...
Connection closing...
Received a client connection from 192.168.43.15:58314
Waiting for client connections...
Connection closing...
F:\Users\Q\Desktop\file lab3\vulnserver>
Immunity Debugger - vulnserver.exe - [CPU - thread 0000129C]
File View Debug Plugins ImmLib Options Window Help Jobs
Immunity: Consulting Services Manager
Registers (FPU)
Address Hex dump ASCII
Help
Paused
ENG 11:44 PM



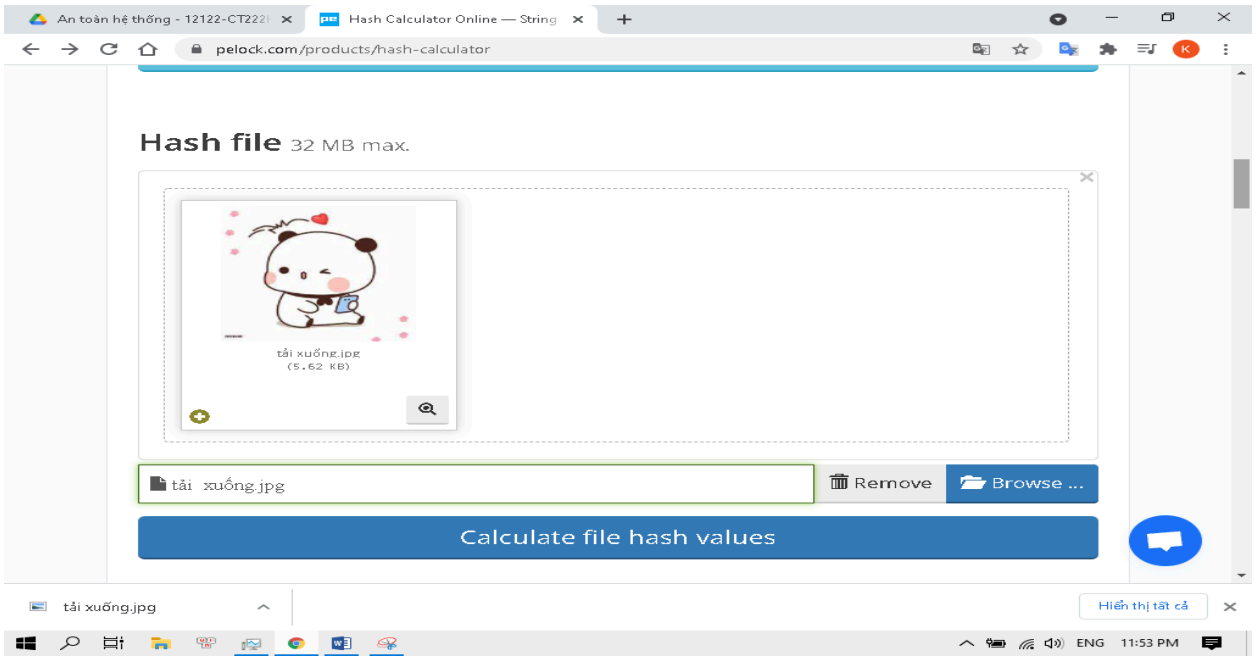
Câu 3: Giải thuật băm

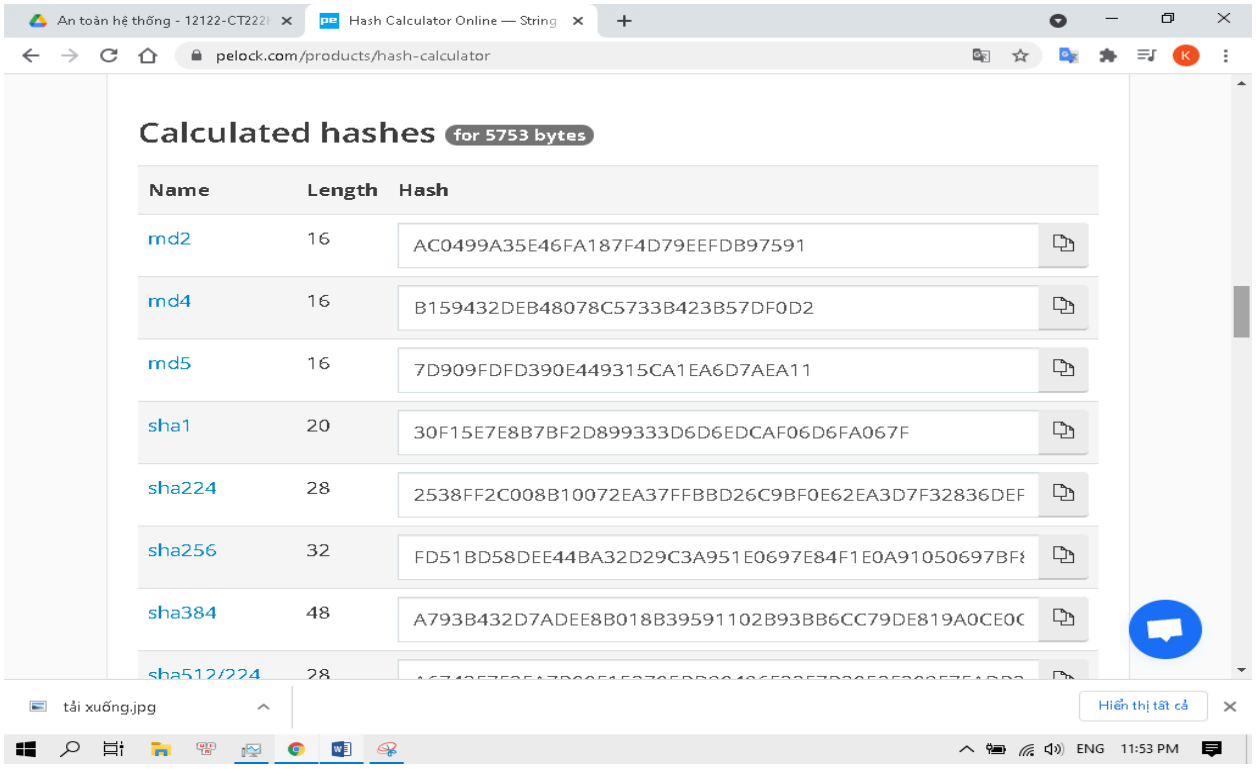
Sử dụng một trang web online cho phép thực hiện giải thuật băm, ví dụ (https://www.pelock.com/products/hash-calculator) thực hiện các công việc sau:

3.1. Tìm giá trị băm của chuỗi "@ntoanhethong_ct222" sử dụng giải thuật MD5 và SHA512

- Giá trị băm của giải thuật MD5 là: CDF279EC13F76CB3C87EE5D362463F88
- Giá trị băm của giải thuật SHA512 là: E6F3A3A5B5FBE1E4BEAF185ED958839EC2C51E219AB0E69FA8ABA23F626B4B894D4E362F98F5505CB55D01A365F775630152F56BE6032CDCE5106C7F2D93D493

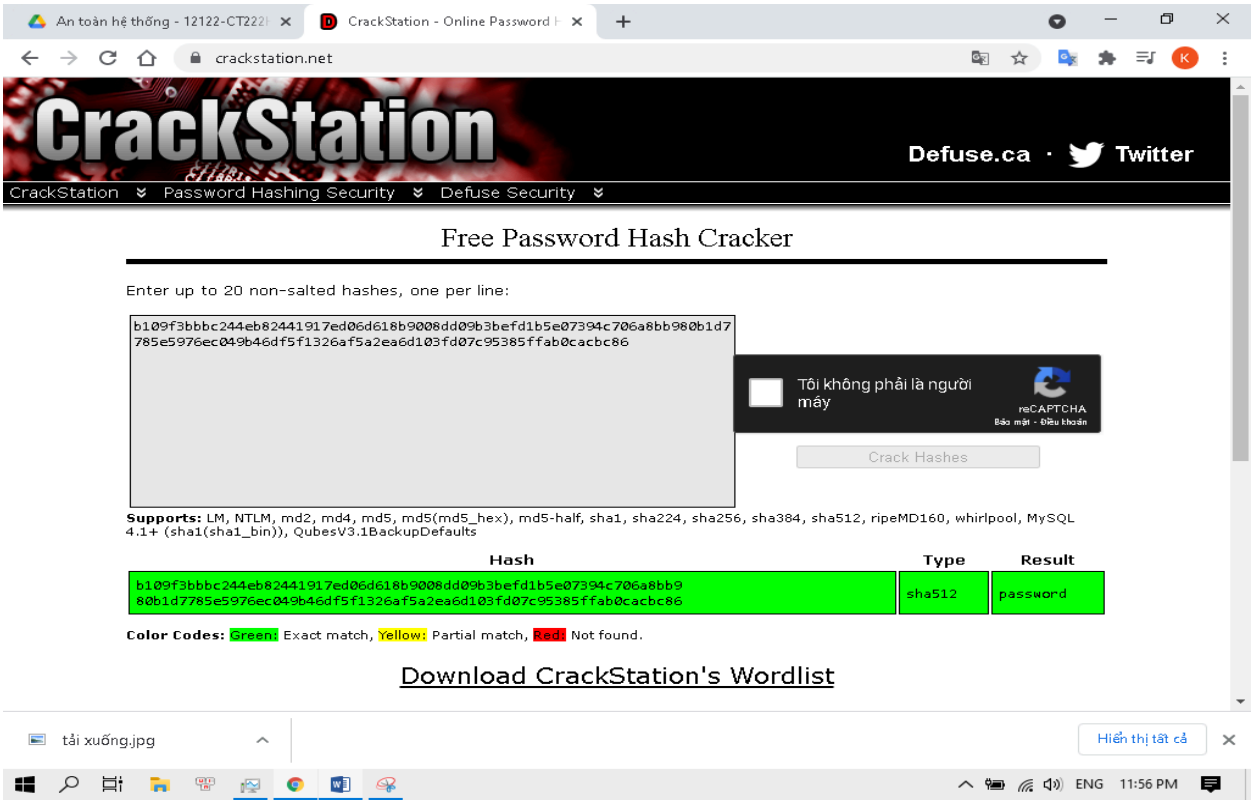
3.2. Upload 1 tập tin và tìm giá trị băm của tập tin đó sử dụng giải thuật MD5 và SHA512



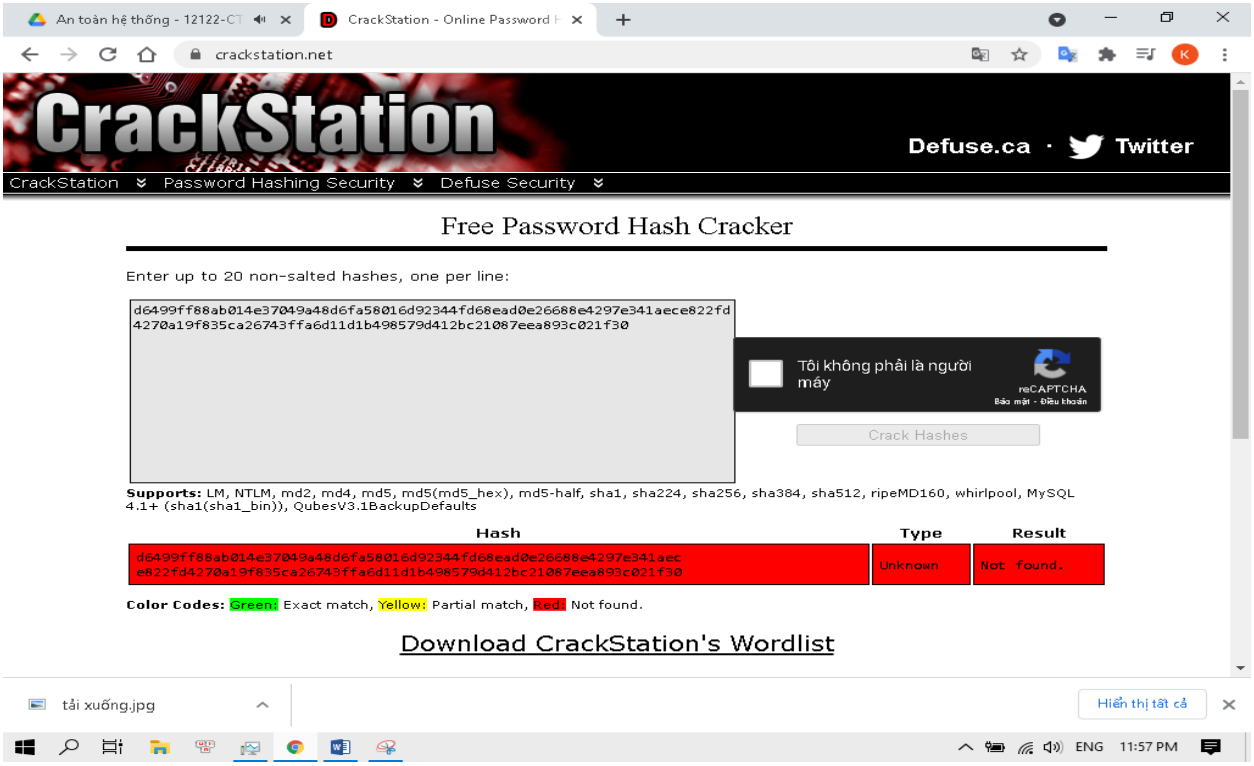


3.3. Sử dụng một trang web cho phép dịch ngược giá trị băm, ví dụ: https://crackstation.net/, để tim giá trị ban đầu của 2 giá trị băm sau:

- "b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e07394c706a8bb980b1d7785e5976ec049b46df5f1326af5a2ea6d103fd07c95385ffab0cacbc86"



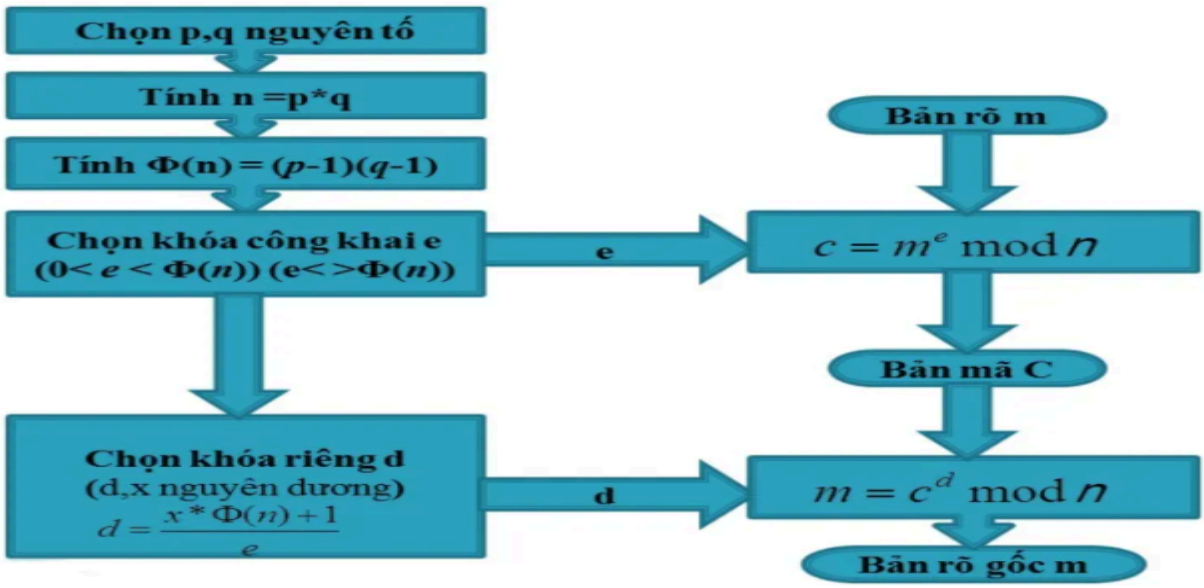
- ”d6499ff88ab014e37049a48d6fa58016d92344fd68ead0e26688e4297e341aece822fd42
70a19f835ca26743ffa6d11d1b498579d412bc21087eea893c021f30”



Câu 4: Tìm hiểu giải thuật RSA

Truy cập đến địa chỉ http://people.cs.pitt.edu/~kirk/cs1501/notes/rsademo/index.html để tạo khóa, mã hóa, giải mã sử dụng giải thuật RSA. Sau đó mô tả ngắn gọn (sử dụng mã giả hoặc flow chart) cách RSA tạo khóa, mã hóa và giải mã.

Sơ đồ tạo khóa, mã hóa và giải mã theo RSA



Câu 5: Chứng chỉ số

Sử dụng một trình duyệt web truy cập đến địa chỉ https://www.ctu.edu.vn/,, sau đó tìm chứng chỉ số (SSL Server Certificate) của địa chỉ nói trên và trả lời các thông tin sau:

- Đơn vị phát hành chứng chỉ: AlphaSSL CA –SHA256 –G2
- Ngày hết hạn chứng chỉ: 29/05/2022
- Khóa công khai (public key) của chứng chỉ: RSA (2048 Bits)

```
30 82 01 0a 02 82 01 01 00 c5 43 0d 01 e0 ae d1 c9 26 f0 bc d7 6e bb ac e0 21 58 45 20 e2
34 2d ae 59 dd 93 73 25 3f ef 94 04 97 a5 e8 a3 91 b9 05 4a ce c1 0e 6d 2b 6f 8e e6 c4 63
af 14 ca a8 dc 8c 0f cc bc 7d 07 4b 94 b3 3a f9 88 72 60 27 74 d9 14 e0 a3 01 28 6a 62 77
81 dc 0f 67 50 b3 c5 cb 0c b0 01 5d 9c 20 03 7c 50 28 8b 2a 94 0e 3a 92 73 bf 27 80 81 bc
ee 2b 6e 38 f6 82 d1 a7 c1 a5 6a f7 8e a9 ae 0f 9f dc 23 fc 59 dd b0 4a ff c9 cf db e2 b8
2a 33 8f 9c 4b 00 db f6 0f 03 13 fa 87 e7 0d 55 ed 2c 2b 8d aa f4 33 ce 37 2d 02 c5 04 0b
08 a1 c3 aa 28 63 90 45 eb ce 2f 13 69 7c 94 24 c8 df fa dc ec 89 91 68 ad ac 2b 13 61 0f
b1 f2 48 68 7b e2 64 f2 00 39 59 d2 d6 00 8e f0 8d ac b9 71 ea cc 44 f6 93 d2 b3 01 95 7d
81 f0 0e 2f 91 5a b7 de 18 22 50 f8 86 02 f0 7f 68 7f fa f6 1d b6 e5 db 8d 02 03 01 00 01
```

Câu 6: Bẻ khoá giải thuật RSA sử dụng khoá ngắn (Không bắt buộc)

Tham khảo và thực hiện hướng dẫn thực hiện bẻ khoá giải thuật RSA (sử dụng khoá ngắn). Chụp hình minh hoạ các bước thực hiện (chỉ cần thực hiện bước 5a trong hướng dẫn)

https://samsclass.info/141/proj/p5RSA2.htm

---HẾT---