

## BREAKING RSA

EXP.NO: 4

DATE: 01-02-2025

AIM:

### Breaking RSA in TryHackMe Using Fermat's Factorization Algorithm

The goal is to break an RSA encryption challenge in TryHackMe by factoring the modulus  $N$  using Fermat's Factorization Algorithm. This method works best when the two prime factors  $p$  and  $q$  are close to each other, meaning their difference is small. Once  $p$  and  $q$  are found, the private key and decrypt messages can be found.

### A brief overview of RSA

The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem". RSA key pair is generated using 3 large positive integers –

A constant, usually 65537

Known as the modulus of public-private key pair. It is a product of 2 large random prime numbers,  $p$  and  $q$ .

$n = p \times q$

A large positive integer that makes up the private key. It is calculated as,

$d = \text{modinv}(e, \text{lcm}(p - 1, q - 1))$

Where modinv is the modulus inverse function and lcm is the least common multiple function.

$(e, n)$  are public variables and make up the public key.  $d$  is the private key and is calculated using  $p$  and  $q$ . If we could somehow factorize  $n$  into  $p$  and  $q$ , we could then be able to calculate  $d$  and break RSA. However, factorizing a large number is very difficult and would take some unrealistic amount of time to do so, provided the two prime numbers are **randomly** chosen.

### Fermat's Factorization Algorithm Mathematical Basis:

RSA uses a modulus  $N$  calculated as:

$$N = p \times q$$

$$N = p \times q$$

where  $p$  and  $q$  are prime numbers.

If  $p$  and  $q$  are close, they can be rewritten as:

$$p = (a - b), q = (a + b)$$

where  $a$  is the midpoint between  $p$  and  $q$ , and  $b$  is the offset.

Rearranging, we get:

$$N=(a-b)(a+b)=a^2-b^2$$

which can be rewritten as:

$$a^2-N=b^2$$

Thus, the problem reduces to finding an integer  $a$  such that  $a^2-N$  is a perfect square.

### ALGORITHM:

1. **Find an initial estimate of  $a$ :**

$$a = \lceil \sqrt{N} \rceil$$

(Round up the square root of  $N$ ).

2. **Iterate until  $a^2-N$  is a perfect square:**

- Compute  $b^2=a^2-N$
- Check if  $b^2$  is a perfect square.
- If it is, set  $b = \sqrt{b^2}$
- Compute  $p=a-b$  and  $q=a+b$ .

3. **Verify  $p$  and  $q$  by checking if  $p \times q = N$**

4. **Use  $p$  and  $q$  to compute  $\phi(N)$  and the private key  $d$ :**

$$\phi(N)=(p-1)(q-1)$$

$$d=e^{-1} \bmod \phi(N)$$

using the Extended Euclidean Algorithm.

5. **Decrypt the ciphertext using:**

$$M=C^d \bmod N$$

### When Fermat's Factorization Works Well:

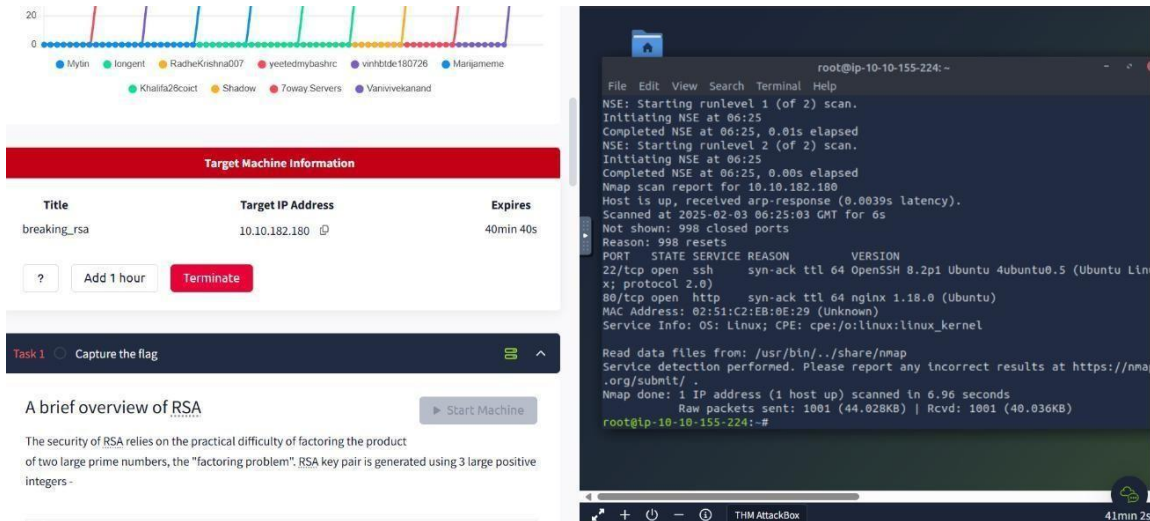
- When  $p$  and  $q$  are close.
- For small or medium-sized RSA moduli.
- When the difference  $q - p$  is small, making  $b$  small.

**OUTPUT:**

- How many services are running on the box?

**\$ sudo nmap -sV -Pn -vvv -T3 10.10.182.180**

**Ans: 2**



The screenshot shows a web application interface on the left and a terminal window on the right. The web application displays 'Target Machine Information' for 'breaking\_rsa' at IP '10.10.182.180'. It includes a 'Task 1' section with a 'Capture the flag' button and a brief overview of RSA. The terminal window shows the output of the command 'sudo nmap -sV -Pn -vvv -T3 10.10.182.180'. The scan results indicate that the host is up and two services are running: SSH (22/tcp) and HTTP (80/tcp).

**Target Machine Information**

Title	Target IP Address	Expires
breaking_rsa	10.10.182.180	40min 40s

Task 1 ☐ Capture the flag

A brief overview of RSA

The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem". RSA key pair is generated using 3 large positive integers -

Start Machine

```

root@ip-10-10-155-224: ~
File Edit View Search Terminal Help
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 06:25
Completed NSE at 06:25, 0.01s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 06:25
Completed NSE at 06:25, 0.00s elapsed
Nmap scan report for 10.10.182.180
Host is up, received arp-response (0.0039s latency).
Scanned at 2025-02-03 06:25:03 GMT for 6s
Not shown: 998 closed ports
Reason: 998 resets
PORT      STATE SERVICE REASON      VERSION
22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Lin
x; protocol 2.0)
80/tcp    open  http     syn-ack ttl 64 nginx 1.18.0 (Ubuntu)
MAC Address: 02:51:C2:EB:0E:29 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.96 seconds
Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.036KB)
root@ip-10-10-155-224: ~#
  
```

```

(0xb0b0kali)~[~/Documents/tryhackme]
$ nmap -sT -p- 10.10.72.68 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 14:37 EST
Nmap scan report for localhost (10.10.72.68)
Host is up (0.048s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 23.40 seconds

(0xb0b0kali)~[~/Documents/tryhackme]
$ nmap -sT -sV -sC -p 22,80 10.10.72.68 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 14:40 EST
Nmap scan report for localhost (10.10.72.68)
Host is up (0.045s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 ff:8c:c9:bb:9c:6f:6e:12:92:c0:96:0f:b5:58:c6:f8 (RSA)
|_ 256 67:ff:d4:09:ee:2c:8d:eb:94:b3:af:17:8e:dc:94:ae (ECDSA)
|_ 256 81:0e:b2:0e:f6:64:76:3c:c3:39:72:c1:29:59:c3:3c (ED25519)
80/tcp    open  http     nginx 1.18.0 (Ubuntu)
|_ http-title: Jack Of All Trades
|_ http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.11 seconds
  
```

**Q. 2 What is the name of the hidden directory on the web server? (without leading '/') Ans: development**

```
(0xb0b@kali)-[~]
$ gobuster dir -u http://10.10.72.68 -w /usr/share/wordlists/dirb/big.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.72.68
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/development (Status: 301) [Size: 178] [→ http://10.10.72.68/development/]
Progress: 20469 / 20470 (100.00%)

Finished
```

**Q.3 What is the length of the discovered RSA key? (in bits)**

To determine the length in bits of the public we can issue the following command:

```
(0xb0b@kali)-[~/Documents/tryhackme/breaking-rsa]
$ ssh-keygen -l -f id_rsa.pub
SHA256:DIqTDIhboydTh2QU6i58JP+5aDRnLBPT8GwVun1n0Co no comment (RSA)
```

**Ans: 4096**

**Q.4 What are the last 10 digits of n? (where 'n' is the modulus for the public-private key pair) Ans: 1225222383**

```
(0xb0b@kali)-[~/Downloads]
$ python
Python 3.11.7 (main, Dec 8 2023, 14:22:46) [GCC 13.2.0] on linux
Type "help", "copyright", "credits" or "license()" for more information.
>>> from Crypto.PublicKey import RSA
>>> f = open("id_rsa.pub", "r")
>>> key = RSA.importkey(f.read())
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
AttributeError: module 'Crypto.PublicKey.RSA' has no attribute 'importkey'. Did you mean: 'importKey'?
>>> key = RSA.importKey(f.read())
>>> print key.n
File "<stdin>", line 1
print key.n
^^^^^^^^^
SyntaxError: Missing parentheses in call to 'print'. Did you mean print( ... )?
>>> print(key.n)
65537
```

**Q.5** What is the numerical difference between p and q? Ans: 1502

```
(0xb0b@kali) ~/Documents/tryhackme/breaking-rsa
$ python rsa-pwn.py
Modulus (n): 96034377877549488806716229688022562692463185460664314559819511657255292180827209174624059690060629715513180527734160798185034958883650709727032190772084959
116259664047922715427522089353727952666824433207585440395813418471678775729954222480081084629807905584769933629196395161205383625169276223151872749717340814352300791532
0575075102064295675711703085205308814697656053158344700335513546035992885701019624149760424915137435365349168421481367813639664170694912845352656665112316213880689811602
792891825813671342737677561872513645198489630078846560491474187297017386854194067540032500667966203078757098669524390301792312110548393534289783830664260722704673471688
470355688980584136674278172580377180144541078809082817312226041629366155542892744715230386667609942603158299822306406688112504470300034623177406032045771239056157186
878330153255448883608789888414723660898930212117229236863767234940525477258174288343104837605293733299563014179392865499007896747519472415182168911702601044530537574860
4757116271353498403318409547515058838447618537811182917198454172161072247021099572638700461507432831248944781465511414308770376182766366160748136532693805002316728842876
51909139940867222673058844554058431161474308624683491225222383
Public Exponent (e): 65537
p:
q:
Difference between q and p:
Private Key (d):
Private Key generated and saved as 'id_rsa'.
```

**Q.6** What is the flag?

Ans: breakingRSAissuperfun20220809134031

```
(0xb0b@kali) ~/Documents/tryhackme/breaking-rsa
$ chmod 600 id_rsa
(0xb0b@kali) ~/Documents/tryhackme/breaking-rsa
$ ssh -i id_rsa root@10.10.72.68
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-124-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

System information as of Fri 16 Feb 2024 07:55:05 PM UTC

System load:  0.0          Processes:      112
Usage of /:   70.1% of 4.84GB Users logged in:   1
Memory usage: 24%         IPv4 address for eth0: 10.10.72.68
Swap usage:   0%

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Fri Feb 16 19:33:29 2024 from 10.8.211.1
root@thm:~# ls -lah
total 36K
drwx----- 5 root root 4.0K Feb 16 19:33 .
drwxr-xr-x 19 root root 4.0K Aug 13 2022 ..
-rw----- 1 root root 30 Aug 13 2022 .bash_history
-rw-r--r-- 1 root root 3.1K Dec 5 2019 .bashrc
drwx----- 2 root root 4.0K Feb 16 19:33 .cache
-r----- 1 root root 36 Aug 13 2022 flag
-rw-r--r-- 1 root root 161 Dec 5 2019 .profile
drwx----- 3 root root 4.0K Aug 13 2022 .snap
drwx----- 2 root root 4.0K Aug 13 2022 .ssh
root@thm:~# cat flag
```

Answer the questions below

How many services are running on the box?

2

✓ Correct Answer

What is the name of the hidden directory on the web server? (without leading '/')

development

✓ Correct Answer

What is the length of the discovered RSA key? (in bits)

4096

✓ Correct Answer

What are the last 10 digits of  $n$ ? (where ' $n$ ' is the modulus for the public-private key pair)

1225222383

✓ Correct Answer

Factorize  $n$  into prime numbers  $p$  and  $q$

No answer needed

✓ Correct Answer

What is the numerical difference between  $p$  and  $q$ ?

1502

✓ Correct Answer

Generate the private key using  $p$  and  $q$  (take  $e = 65537$ )

No answer needed

✓ Correct Answer

What is the flag?

breakingRSAissuperfun20220809134031

✓ Correct Answer

## RESULT:

Thus, Breaking RSA in TryHackMe is Completed Successfully