Exp no 4 Rollno:220701249

Date:11-02-2025

BREAKING RSA

PROCEDURE

1. Log in to TryHackMe

Go to https://tryhackme.com and log in or create a free account.

2. Search and Join the Room

In the search bar, type "RSA" or "Crypto", and join one of these rooms:

- "RSA" (TryHackMe original room)
- "Intro to Crypto"
- "Maths of Cryptography"
- "Cryptography is Fun"

Click "Join Room" and read the intro.

3. Start the Machine (if applicable)

Most RSA rooms don't require a machine — you can solve challenges using the AttackBox or your own terminal.

3. Understand RSA Basics (from the Tasks) Read

through tasks explaining:

- $n = p \times q \pmod{u}$
- e (public exponent)
- d (private key)
- c = m^e mod n (encryption)
- m = c^d mod n (decryption)

You'll usually be given n, e, and ciphertext and asked to decrypt or find m.

5. Use Online Tools or Python Scripts

You'll often need to factor n or crack weak RSA using tools like:

Option 1: RsaCtfTool

bash CopyEdit

git clone https://github.com/Ganapati/RsaCtfTool.git cd

RsaCtfTool

python3 RsaCtfTool.py --publickey pubkey.pem --uncipherfile cipher.txt

Option 2: Use factordb.com

- Go to https://factordb.com
- Paste n into the search bar
- If it's a weak key, it will give you p and q
- Use them to compute d and decrypt c

Option 3: Write a custom Python script

Use Python with Crypto.Util.number or built-in pow():

python CopyEdit

from Crypto.Util.number import inverse, long_to_bytes

```
p = 61 q = 53 e = 17
n = p * q phi = (p -
1) * (q - 1)
d = inverse(e, phi)

c = 2790 m =
pow(c, d, n)
print(long_to_bytes(m))
```

6. Submit Answers

TryHackMe will ask things like:

- "What is the plaintext?"
- "What is the value of d?"
- "What was the original message?" Paste your correct answers to proceed.

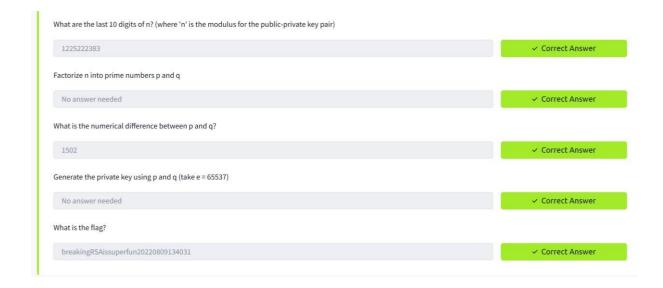
7. Complete the Room

After solving all RSA challenges, the room will be marked as "Completed".

TASKS

Task 1 Capture the flag





RESULT

Thus the introduction to breaking rsa has been successfully studied and implemented successfully



