

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:

- $n = p \times q$ (modulus)
- e (public exponent)
- d (private key)
- $c = m^e \bmod n$ (encryption)
- $m = c^d \bmod n$ (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

$p = 61$ $q = 53$ $e = 17$

$n = p * q$ $\phi = (p - 1) * (q - 1)$

$d = \text{inverse}(e, \phi)$

$c = 2790$ $m =$

$\text{pow}(c, d, n)$

$\text{print}(\text{long_to_bytes}(m))$

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

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

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



