

## BREAKING RSA

DATE: 19-02-2025

### AIM:

Hop in and break poorly implemented RSA using Fermat's factorization algorithm.

### PROCEDURE:

- Task 1: Capture the flag

### Task 1: Capture the 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?

breakingRSAisuperfun20220809134031 ✓ Correct Answer

### RESULT:

Thus the Breaking RSA is successfully completed in tryhackme platform.

**NAME: HARINI.D.S**

**ROLL NO: 231901009**