KALAIYARASI 231901503

DATE: 26/2/25

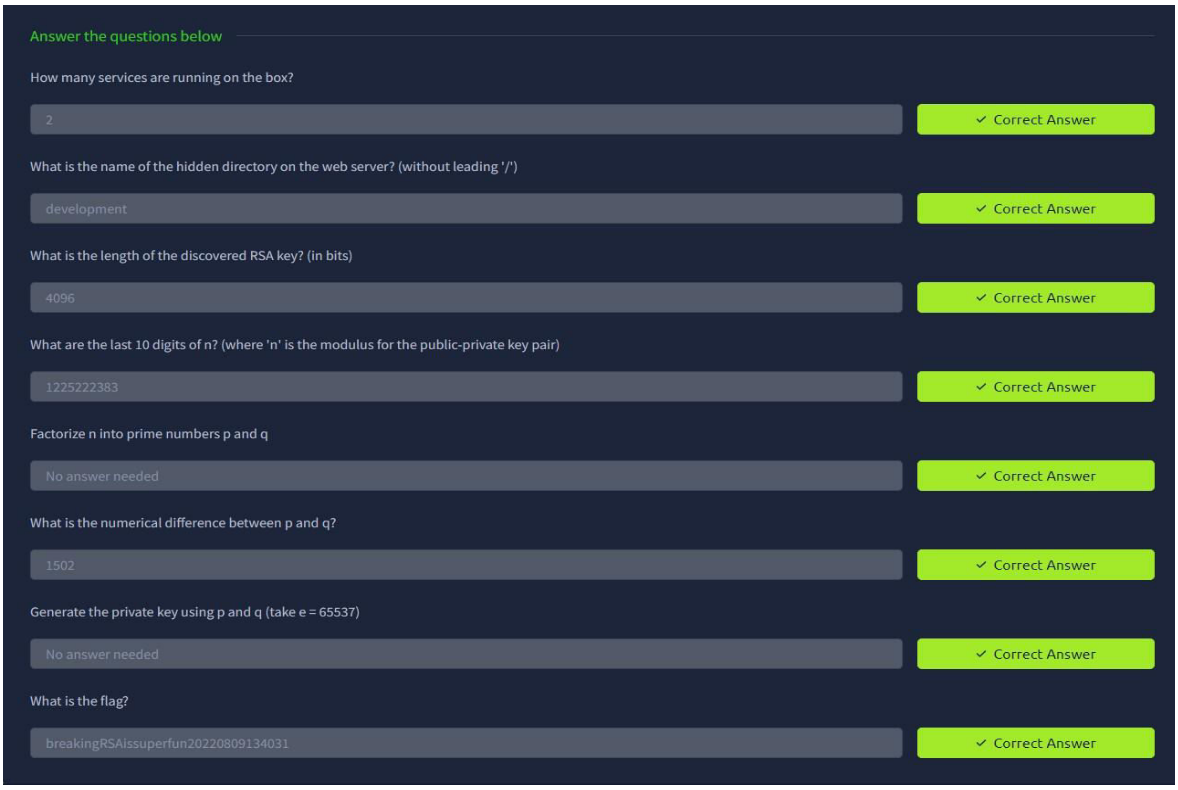
BREAKING RSA

AIM:

To implement RSA using Fermat’s Factorization Algorithm.

PROCEDURE:

Task 1. Capture the Flag



Answer the questions below

How many services are running on the box?

2

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

development

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

4096

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

1225222383

Factorize n into prime numbers p and q

No answer needed

What is the numerical difference between p and q?

1502

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

No answer needed

What is the flag?

breakingRSAissuperfun20220809134031

RESULT:

Hence, RSA is implemented using Fermat’s Factorization Algorithm.