lab3-part1.py README

Description

lab3-part1.py is a RSA decryption project, given:

- Cipher text: (c) = 768916070269816102747332979141020881585
- Public key: (n, e) = (20564417702267663739075887386762470065 87,65537)

With such a small value of 'n', we can use online resources (WolframAlpha) to determine the prime factors that make it up, which come out to be:

- p = 40822754178477882469
- q = 50374890465154864223

To find 'd' we first need to find the least common multiple (lcm) between the prime factors, and then find the modular multiplicitve inverse of 'e' modulo 'lcm'.

Once 'd' is calculated, we find the message with:

m = c^(d) % n

Requirements

Dependencies:

- Python

Usage Walkthrough

1. Navigate to the directory where the `lab3-part2.py` is downloaded.
2. Run `lab3-part2.py`

   Example: `python3 lab3-part2.py`