lab3-part1.py README

Description

lab3-part1.py is a RSA encryption python project.

It first generates two prime numbers, whose size depends on the integer passed in as an argument. Then finds the multiplicitive inverse of the least common multiple of the two prime numbers and sets it as the value of 'd'. Finally we hardcoded the value of 'e' to be '65537'.

For the public key we return 'n' (the value of 'p' multiplied by 'q'), and 'e'.

For the private key we return 'n', and the value of our 'd'

After key creation, it encrypts the message "test,message" with both public and private key, and prints the cipher text to show they cipher to different strings. Finally it will decipher the message using the private key, redisplaying the message "test,message".

Requirements

Dependencies:

- Python
- prime.py

Usage Walkthrough

1. Navigate to the directory which the `lab3-part1.py` and `prime.py` are downloaded.
2. Run `lab3-part1.py` with an integer for the size of bits for the size of 'p' and 'q'

   Example: `python3 lab3-part1.py 50`

Requires a number >= 50

A value larger than 500 can cause crashes due to generating large prime numbers