None of the problems on this assignment are graded. Instead, after completing it, please fill out the associated Google form. That form is the only graded component.

Exercise 1. *Explain, in your own words (not mine or ChatGPT's) why it is okay that* n *is part of the public key but* p *and* q *are part of the private key.*

Exercise 2. *Find a partner to exchange messages with. Choose an integer that is meaningful to you in some way. This will be your plaintext.*

Generate RSA key elements $(p, q, n, \varphi(n), d, e)$*. Exchange public keys with you partner and encrypty your message with their encryption key. Recieve the encrypted ciphertext from your partner and decrypt it with your private dcecryption key.*

It will be useful to do some of the calculations with python or a calculator. Write your process here.

Bonus

Exercise 3. *RSA is breakable with quantum computers. This is due to how fundamentally different they are that normal computers. Some algorithms that increase exponentially in dificulty with the problem size increase polynomially on a quantum computer (makes them much easier). One of these algorithms is Shor's algorithm. Read the part of it's wikipedia page titles "classical reduction". Try and use it to factor 21.*