Lab Eight

Exersise One

Question One

a. How long are the primes

> ~30 digits

$$2^{128}$$

b. how many decimal digits long will the RSA public modulus n be?

> ~60 digits

c. How many bits long will the RSA public modulus be?

$$2^{128} \times 2^{128}$$

d. Is this RSA key large enough to be used in modern applications such as TLS?

> No, the industry standard is 2048 - 4096 bits

Question Two

What happens when changing cryptool key e? Try changing it to 8

> In the cryptosystem, 8 is not invertible, meaning that gcd(8, n) != 1

Question Three

> It would be a bad idea, because then all pre-evaluated cipher text could be reversed with the public key?

Question Four

a. How long did the encryption take?

> ~1 second

b. Press stop then change the range to 1024

> ~ 5 second

c. Press stop then change the range to 2048

> ~ 10 second

d. Do you think the delay was key generation, encryption or both?

Both

e. What practical lessons can we extract from examining these timings

Exersise Two

Question Six

> ~2 seconds