# Cryptology 5.2

Ryan Kellar

April 2024

## 1 Problem 1

$C = M^E$
$C = 2^5$
$C = 32$
Alice sends Bob 32 as the message. The idea is that the encrypted message can be found by doing $M^E$ (assuming the plaintext is a number). We are given that E is 5 and the problem tells us that Alice is sending 2 as the plaintext to Bob, so by performing this process we get 32 as the encrypted text.

## 2 Problem 2

For this problem we need to use shortcuts for modular exponentiation and break down our exponent into smaller exponents and modulating the values in between each. For the last problem, $C = \mathbb{Z}_{(p-1)(q-1)} = \mathbb{Z}_{192}$, so we didn't need to mod it. However, in this problem $(M^E = 2^150) >> 192$, so we need to mod it so that $C \subset \mathbb{Z}_{192}$.
$2^{150} \mod 192 = (2^{50} \mod 192)^3 \mod 192 = ((2^{10} \mod 192)^5 \mod 192)^3 \mod 192$
$(64^5 \mod 192)^3 \mod 192$
$(64^3 \mod 192)^5 \mod 192$
$64^5 \mod 192$
$64 = C$
In this case, Alice sends Bob 64 as the encoded ciphertext message.

## 3 Problem 3

### 3.1 a)

The idea of a multiplicative inverse is that $\exists m | n * m mod k \equiv 1$.
For example, the multiplicative of 2 in mod 3 is 2 since $2 * 2 \mod 3 = 4 \mod 3 \equiv 1$
So for this problem, we just have to apply this to test if 77 is the multiplicative inverse of 5 in mod 192.
$5 * 77 \mod 192 = 385 \mod 192 \equiv 1$
QED 77 is the multiplicative inverse of 5 in $\mathbb{Z}_{192}$.

### 3.2 b)

The RSA Cryptosystem Crux states that for any message $M$, encoding number $E$, and decoding number $D$, $M^{ED} \mod (p * q) = M$.
Essentially what this means is that whenever you encrypt a message and then decrypt that encrypted message (while keeping it in $\mod pq$), you will get back the original message's plaintext.
Since the point of $D$ is to counteract $E$, applying both operations is essentially the same as doing nothing at all.
$M^{ED} \mod pq$
$M^{5*77} \mod 291 = M$