CS 165 Lab 3 Assignment

October 21, 2012

The year is 1815, and General Napoleon is about to attack Waterloo. Lucky for us, our spy has intercepted a message that says where Napoleon is keeping his armies. He thinks it's been encrypted with a shift cipher, but doesn't know the key. Decrypt it and find out where Napoleon keeps his armies:

```
VA UVF FYRRIVRF.
```

Whoops! Our spy has made a mistake. Napoleon is too smart to use a shift cipher. Substitution ciphers are the most secure encryption that has been invented yet, so that's what Napoleon is going to use for his communications. This is the real message we've intercepted:

```
O VOSS QZZQEA YKGD ZIT LGXZI VOZI QSS DN YGGZ LGSROTKL,
QFR YKGD ZIT TQLZ VOZI DN EQSCQKN.
```

Luckily, we've also intercepted a plaintext/ciphertext pair we can use to help us decrypt the message.

```
plaintext:  THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
ciphertext: ZIT JXOEA WKGVF YGB PXDHL GCTK ZIT SQMN RGU
```

RSA

1. Create a simple RSA cryptosystem by choosing two **distinct** primes $p > q \geq 7$, $n = pq$. Select values for e, d. Denote which pieces are part of the public key and which are part of the private key.

2. Select two messages $M_1, M_2 \in \mathbb{Z}_n$ such that: p, q are coprime with M_1, and q divides M_2. Include a third message $M_3 = 10$. Encrypt all three messages ($M_i^e \mod n$), and then decrypt each ($(M_i^e)^d \mod n$), showing that $(M_i^e)^d \equiv M \pmod{n}$.

I recommend you recopy the proof that the RSA algorithms works to make sure you can reproduce it on an exam.