Math 100

1 RSA Encryption

1. Pick two prime numbers, p and q.
2. Find the product of these two prime numbers, $n = pq$ where n is a public number.
3. Find $m = (p-1)(q-1)$
4. Pick a number e that has no common factors with m where e is another public number.
5. Pick a number W that must be less than n that we want to encrypt.
6. To encode a message W, calculate $C = W^e \ mod\ n$, where C is the encrypted message.

2 RSA Decryption

1. Suppose we have an encoded message C.
2. Keep note of our public numbers n and e, and private numbers p, q, and m.
3. Use the values of e and m to find the natural numbers d and m such that $ed = 1 + my$, where d is the decoding power and is private.
4. Compute $W = C^d \ mod\ n$, which will give us back our original message.

3 Example

Encrypting the original message:

1. Let $p = 3$ and $q = 5$.
2. $n = pq \rightarrow n = (3)(5) \rightarrow n = 15$.
3. $m = (p-1)(q-1) \rightarrow m = (3-1)(5-1) \rightarrow m = (2)(4) \rightarrow m = 8$.
4. Let $e = 3$, 3 is not a common factor of 8.
5. Let $W = 7$.
6. $C = W^e \ mod\ n \rightarrow C = 7^3 \ mod\ 15 \rightarrow C = 343 \ mod\ 15 \rightarrow C = 13$.

Decrypting the encrypted message:

1. $C = 13$ from out previous calculation.
2. We know $n = 15$, $e = 3$, $p = 3$, $q = 5$, and $m = 8$.
3. $ed = 1 + my \rightarrow 3d = 1 + 8y$. Let $d = 3$ and $y = 1$. $(3)(3) = 1 + (8)(1) \rightarrow 9 = 9$.
4. $W = C^d \ mod\ 15 \rightarrow W = 13^3 \ mod\ 15 \rightarrow W = 2197 \ mod\ 15 \rightarrow W = 7$

Note that when encrypting a message we get an encrypted message. Decrypting the encrypted message should give us our original message and is a good way to check if your encryption is correct.