202 Final Project Example

Michael Ceccarelli

May 2021

1 Example

Bob and Alice are trying to exchange messages on an insecure server. They are going to use RSA encryption to do so.

Bob chooses two large primes, p and q. This time, he chooses $p = 17$ and $q = 19$. Bob then computes a number that is hard to factor, N,

$$N = pq = 17 * 19 = 323.$$

He then needs an exponent, e, which he will make public. He chooses $e = 65$. The condition for this number is

$$gcd(e, (p-1)(q-1)) = gcd(65, 288) = 1.$$

Alice then turns her message into an integer that is less than N, 243. Using Bob's published N and e, Alice computes c, which looks like this

$$c \equiv m^e \pmod{N}, c \equiv 243^{65} \equiv 22.$$

Bob takes her ciphertext and, because he knows $(p-1)(q-1) = 288$, he is able to compute

$$ed \equiv 1 \pmod{288}, d * 65 \equiv 1 \pmod{288}.$$

He finds that $d = 257$. Now he computes the message from the formula

$$c^d \pmod{N}, 22^{257} \equiv 243 \pmod{323}.$$