CS 70 Discrete Mathematics and Probability Theory
Spring 2018 Satish Rao and Babak Ayazifar

DIS 4B

1 RSA Warm-Up

Consider an RSA scheme modulus $N = pq$, where p and q are distinct prime numbers larger than 3.

(a) Recall that e must be relatively prime to $p-1$ and $q-1$. Find a condition on p and q such that $e = 3$ is a valid exponent.

(b) Now suppose that $p = 5$, $q = 17$, and $e = 3$. What is the public key?

(c) What is the private key?

(d) Alice wants to send a message $x = 10$ to Bob. What is the encrypted message she sends using the public key?

(e) Suppose Bob receives the message $y = 24$ from Alice. What equation would he use to decrypt the message?

2 Just a Little Proof

Suppose that p and q are distinct odd primes and a is an integer such that $\gcd(a, pq) = 1$. Prove that $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$.

3 RSA with Three Primes

Show how you can modify the RSA encryption method to work with three primes instead of two primes (i.e. $N = pqr$ where p, q, r are all prime), and prove the scheme you come up with works in the sense that $D(E(x)) \equiv x \pmod{N}$.

4 RSA Exponent

What's wrong with using the exponent $e = 2$ in a RSA public key?