

Cryptography Assignment 3

1. Suppose Alice and Bob share the same RSA modulus n but with different public encryption codes e_A and e_B with e_A and e_B relatively prime. Charlie sends the same message m to Alice and Bob by sending $c_A = m^{e_A} \bmod n$ to Alice and $c_B = m^{e_B} \bmod n$ to Bob. Suppose Eve intercepts both c_A and c_B . Show how Eve can get m .
2. Describe an RSA scheme where Bob chooses n to be the product of three large primes, p , q and r .
3. Compute the first several terms of the continued fraction for the Golden Ratio $(\frac{1+\sqrt{5}}{2})$. Do you recognize the sequence of numbers that arise?
4. We want to show that there is a short proof that a number n is prime.
 - (a) Show that n is prime if and only if there is an a such that
 - $\gcd(a, n) = 1$.
 - $a^{n-1} \equiv 1 \pmod n$.
 - For every prime factor p of $n - 1$, $a^{\frac{n-1}{p}} \not\equiv 1 \pmod n$.
 - (b) Use (a) to show that every prime n has a short proof of primality that can be quickly checked without using randomness. Note you may have to recursively show other numbers are prime. Do not worry about how hard it is to find the proof, only that the proof exists.