CS 30
Fall 2019
Discrete Mathematics

Class Exercises: 2019-10-10

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

1. Dr. Speedy proposes a cryptosystem that would work faster than RSA by working modulo a large *prime*.

   - Bob chooses a public key of the form (P, e), where P is a very large (say 300-digit) prime.
   - When Alice wants to send a message $M \in \mathbb{Z}_P$ to Bob, she will send $C := M^e \pmod{P}$.
   - Bob has a secret key d such that $ed \equiv 1 \pmod{P-1}$; using it, he decrypts $M' := C^d \pmod{P}$.

   1.1. Show that Dr. Speedy's cryptosystem is sane, in the sense that $M' = M$ always.

   1.2. Why aren't we all using Dr. Speedy's cryptosystem instead of RSA, which is more complicated?

2. The security of RSA would be compromised if you could find an algorithm $\mathscr{A}$ to quickly compute $\phi(N)$, given N. We believe that factoring is hard, but why should computing ϕ be hard?

   Prove that if computing ϕ were easy—i.e., algorithm $\mathscr{A}$ exists—then $\mathscr{A}$ can be used to quickly factor the RSA modulus N. You'll need to use the fact that N is the product of *exactly two* primes.

3. In class (see the slides), we used a clever method to compute $a^{42} \bmod n$, based on the decomposition $42 = 32 + 8 + 2$.

   3.1. Find a connection between the above decomposition and the binary representation of 42.

   3.2. Explain how you would compute $a^{83} \bmod n$ along similar lines.