

1. (a) Determine if 26266420821755846767903229943872448216978563775362413528739799570782012895729253611033166067023054701007436871995892469175515579020024909703 is prime or composite. If its composite, 100 bonus points for factoring it
(b) Determine if 36184610761562394272680651266207055831168764358131305459948367146751216733630536753099965144993218962709200955703292625048506291629497908601 is prime or composite. If its composite, 100 bonus points for factoring it
2. Suppose you recover the following message fragment: 62348969205948200001015241450024946722469332360051408575520798741304101490295396058778396576134441398730009329635347608130050922544165302799246527731 from Alice to you. Decipher it knowing it was enciphered with RSA and enciphering key $e = 53377331408955027727108017250378601596081494302212327907957945565307662932967575549444570386972435953271154290959344642055293725777469703970281665387$ and private keys: $p = 338924865013753917793198154466313280758349925364202530883974881671144457383$ and $q = 574140101975668414936274434241846579804042151401465513513902999781576300143$.
3. You and I set up a Diffie-Hellman key exchange with prime $p = 30174262332883194758233841730714906179003$, and primitive root $a = 2$. You choose as your private key, $x_{\text{you}} = 19644940962127358887148087983894438397661$. You look up my public key it is: $\alpha_{\text{my}} = 1888640642713829712382116813874012329412$.
 - (a) What is your public key?
 - (b) What is our common key?
 - (c) (100 Bonus Points) What is my private key?
 - (d) If you were unable to answer the previous question, what difficult problem were you unable to solve?
4. (a) Make a table of powers of 10 (mod 19).
 - (b) Use that table (you must show you are using the table to get full credit) to find $7^{12} \pmod{19}$.
 - (c) Use that table (you must show you are using the table to get full credit) to find, x such that $12^x \equiv 8 \pmod{19}$.
 - (d) Use the table to find all primitive roots of 19.