

1. (a) Determine if 68262167090434536483016370451346396376442408190705614718283527980861698751267529884700972316914157912917880376231218363813620069605718499027 is prime or composite. If its composite, 100 bonus points for factoring it
(b) Determine if 7630965276720711551797316643758214579677551837114908953263991848460834844527129974412947213652146294237519225394068376854654663085734148909 is prime or composite. If its composite, 100 bonus points for factoring it
2. Suppose you recover the following message fragment: 319135106829632087177398031600927238728942029131336983002860985530050539907485789529652305698352873333238126119029823889380677824538007604772145406330 from Alice to you. Decipher it knowing it was enciphered with RSA and enciphering key $e = 213056105601650188305469094898084471727934916088044536473279752367780177601763477096359957414334591708364335590230551562547010893447790765427535989571$ and private keys: $p = 743551830017989111422689100463645319018265740623025771118153269016028485457$ and $q = 437586425035627102849834098328007349679057638746527343251015100557675335419$.
3. You and I set up a Diffie-Hellman key exchange with prime $p = 15003344356724570157855951747441787386419$, and primitive root $a = 2$. You choose as your private key, $x_{\text{you}} = 14034587278233989637225741339618218740358$. You look up my public key it is: $\alpha_{\text{my}} = 5889814413724144052268312403762851518092$.
 - (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.