

1. (a) Determine if 5269911107906438655174317335612552990124325817909354725376097716838726181454264990580879438022419512936342955614702292920993449665435036191 is prime or composite. If its composite, 100 bonus points for factoring it  
(b) Determine if 31877216048965921721844738987479938702110448783219522840288607758517700294341101121244905091662953431068992891742924907113151015783105446267 is prime or composite. If its composite, 100 bonus points for factoring it
2. Suppose you recover the following message fragment: 59604646887994921793026917866167917442758685911203990447989230307855935258107163106727084953722603196709411710388584443590115535403845543006088913729 from Alice to you. Decipher it knowing it was enciphered with RSA and enciphering key  $e = 60369025206924734307246920295895897665876047445689211618869863085684389992843625303600827804702996488422816547331719883525692025914512266306946195661$  and private keys:  $p = 297688443874092526428727395487150607795639546051103299558207029508439020891$  and  $q = 305889120488689105035232247613707229145456811190431290963567338702545307781$ .
3. You and I set up a Diffie-Hellman key exchange with prime  $p = 85482255806997241493421711311327040445619$ , and primitive root  $a = 2$ . You choose as your private key,  $x_{\text{you}} = 25049544335343176369054617643065295675317$ . You look up my public key it is:  $\alpha_{\text{my}} = 26077606113312565572977731597744897876627$ .
  - (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.