John Slater **Homework 13** **Due 12-12-2014**

1. (a) What is the SHA256 hash value for the string "John Slater" (in hexadecimal)?
   (b) (100 Bonus Points) Find another string that has this hash value.
   (c) If you were unable to answer the previous question, what is the name of the property of SHA256 that makes this hard?
   (d) Find the student in your class whose hash value for his/her name is a00e8ff56a85e dfc03225031d09c52604049498819417292cb281b3d1f519651.

2. Suppose you recover the following message fragment: 14650834939237840996603524780951893683782033013061218828442972927109105517323753761812287713444044865564826 2 from Alice to you.
   (a) Alice used your public enciphering key. Decipher it knowing your deciphering private key is $d = 85768054277271102912074931063805844884778619223611756777476528998126938495392156781952070962182460564060136 3$ and $n = 115444325353295718538078799217884537181409925302476847673035169336311674817212198895125384544160753172439288 7$.
   (b) The following numbers are all in hexadecimal for your convenience. Alice also sends used SHA256 to hash the message and enciphered that with her priviate key and sends you the ciphered hash which is $66877e550f492a7b993af330ab8044db2c6050b3ba987a2e0696c7bac050b5b1f59b98d3bec005d4fcdf0f69bb8$. You look up her public decipher key it is $d = b30146661486d6a75c4216ba53dd2dc583fb96c27efec70087124cd6ce3f8f5fbe264c79392880350467204ffbd$ and $n = 128aa2b5bfa635f0ffa595965 76358c260f285d1338229c713826869c40daf81372bd788d09f5d7e2aa8f587cacb$. Verify it came from her. (Remember she is hashing the original message which may have spaces in it).

3. (a) Express the number 921 in binary.
   (b) What number has the hexadecimal expression $1c8ebf$.

4. One day I find your credit card and look you up and call you to tell you I have it. You ask me to send it to you but then I realize maybe this is another John Slater. So I ask you if you know your credit card number so that I can verify it is you. You say you do, but won't tell it to me since you don't know who I am or if I even have your credit card number. I won't read it to you for the same reason. What can we do? Hint: Think about what we have done recently in class.