William Graf **Homework 13** **Due 12-12-2014**

1. (a) What is the SHA256 hash value for the string "William Graf" (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 a96fcaf350a67 75ae223f0c2af52f6319a2bef6d96a99b8bd32c9f0888fa80a3.

2. Suppose you recover the following message fragment: 143588649132805804936983783918 540985210452440465798994395080546889056750253796872840638418607399948947852893 6 from Alice to you.
   (a) Alice used your public enciphering key. Decipher it knowing your deciphering private key is $d = 111814948483918120581878936829338928038554721670133583993340824002415633547789079125104883085706345805952997 9$ and $n = 155290399740904176594420983723321170573647539181824773988764706318264943149088390200279275484879390862588613 7$.
   (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 $1b20221ed90a0937e625b909f822bb22824239a381f85e200c6031512e59b86f8f006014820fff7f0be04982effe$. You look up her public decipher key it is $d = 9801ee8180a8517b8f14823977b272120a8df98bd23ca7b1d3f88807d1dde81f1057d672e557ade450c19d7b65$ and $n = 2494661dfe7a3fcb1e4c5292c801f468267283035987d2b7a9c990b0334cdc0bb07658d6f54cdfc2b20b7074207$. Verify it came from her. (Remember she is hashing the original message which may have spaces in it).

3. (a) Express the number 687 in binary.
   (b) What number has the hexadecimal expression $12e4c4$.

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 William Graf. 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.