Project 0

Due Friday, October 19th, in class

Problem 1. I have encrypted some message with the following OpenSSL command:

```
% openssl enc -aes128 -base64 < secret-message
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
U2FsdGVkX196x5b9Md2JX6D11gTcALXeInqFpRYWBtajOTE9fF0vUa54t6WSjE/Z
/Uk7GT3Tfw1eoisEzo7oOyo75AoXh4k6ZInzk0F95DIBkpvE8Es2Mhv87kekrM6s
%
```

Your mission is to find the secret message. That sounds impossible, right? I mean, we have encrypted with CBC-AES-128, which is supposed to be virtually unbreakable. BUT, I will tell you that I used a password that is **three lowercase letters**. In other words, it's aaa, aab, $\cdots$, zzz. You must find it.

This is simply an exercise in your ability to find a working version of OpenSSL (the simplest solution is to use the CSEL machines, but you could also install it on a home-machine). Then you need to find an efficient way to do a key-search (don't type them all by hand... write a script or something!).

Please turn in:

- The password I used
- The secret message
- The script you used to find the key
- Your opinion about the article: should Martin begin training for next year's competition?

You can find a copy of the above ciphertext string on our course web page (so you don't have to type it in!).