CS 469 – Security Engineering
Homework #3

Due Date: See Blackboard

Instructions: Submit a Text, Word or PDF document with answers to the following questions through Blackboard. Blackboard does not accept late submissions… so be on time! Answer each question with a brief, clear response.

I have provided you with a program authCheck1.c This program accepts a username and a numeric password. Without changing the program I want you to force it to accept another password "17476". Use a buffer overflow attack to make that happen.

Some hints:

- When you copy a character into memory, it goes in as its ASCII number.
- It's probably easier to work in hexadecimal. (Although the number 17476 is a decimal number).

Questions:

1. **What is the input needed to change the password to 17476 ?**
2. **How did you figure it out.**

I have provided you with an executable crypto that encrypts a file using a static password. I have also provided you with a file encrypted by crypto. Your job is to decrypt this file using whatever means you can (some methods are far easier than others ☺).

Sample run:

```
   ...te/classes/cs469/fall13/non_web/hw3 >  ./crypto

 Enter filename to encrypt:
plaintext.txt
aO/4mLKxoBJ64+UJyYBNTuGE601PzjmKQdcMqV+Qu6BtZ0Yim9CwSOjTTuo/NcDg
OX6TJ1jaGeAjE8h4iMWe6jA9LQW55zDSU7mq+NEj4Hk5sTJEWyTvgr4Y9rpBwkHI
Tp840eQY/aBUd7f28ekJf9mWvmOM2U1KC4lKoNot7E8=

      Some hints:
      -    Crypto executes a separate openssl program to do the encryption
      -    The more you think about this problem, the easier it can be.
```

Questions:

3. What is the plaintext for the given encrypted.txt file?

4. How did you figure it out?