Project 2 Stage 1

You have successfully reached the first stage of Project 2. Be sure to record this URL on your submission. It is worth ten points. From here you will have to log in to each subsequent stage. **For all stages, your username will remain your NetId. You will have a different password for each stage.** This will involve more complicated password cracking. To start with the URL for the next page is the md5sum of your Netid without .html just end with a slash. From here you have to figure out the user id and password to log in to Stage 2.

The prefix for the next URL is http://netsec.engr.uconn.edu/Project2/Stage2/

Next password Your next password is in the source of this webpage. You must view the page source and look for comment lines.

Tips: If you use echo or certain text editors to feed data into a hash computation they often add a newline character. This needs to be removed. This can be accomplished easily for echo by using the -n flag. For vi, we recommend using head to select a subset of characters.

In this assignment you'll have to crack passwords. For some of the earlier stages this can be done using the command line (sha256sum). However, for later stages this will takes hours to crack. If you write a program it can be done much faster. The provided java can serve as a shell for this computation.

```
public static String hashToHex(String input) throws UnsupportedEncodingException, NoSuchAlgorithmException{
    MessageDigest md = MessageDigest.getInstance("SHA-256");
    byte[] mdbytes = md.digest(input.getBytes("US-ASCII"));
    StringBuffer hexString = new StringBuffer();
    for (int i=0;i<mdbytes.length;i++) {
    String hex=Integer.toHexString(0xff & mdbytes[i]);
    if(hex.length()==1) hexString.append('0');
    hexString.append(hex);
    }
        return hexString.toString();
        }
```

Project 2 Stage 2

Congratulations on reaching the second stage of project 2. Be sure to record this URL on your submission. It is worth ten points. Reaching stage 3 will require cracking a password. From here on your username will return to your NetID. For Stages 3-6 you need to figure out the URL to use and the correct password.

The prefix for the next URL is http://netsec.engr.uconn.edu/Project2/Stage3/

Your individualized URL is the encryption of the current randomized part of the URL (the 20 character hexadecimal string). Use AES-128 (this is different than the cipher we used in project 1) in ECB mode with the key **e0e0e0e0e0e0e0e0f1f1f1f1f1f1f1f1**. This ciphertext will contain non printable characters. The URL is the restriction of this string to only alphanumeric characters. So you should remove all other characters to form the next stage URL.

Next password Your next password is a 3 character string consisting of *lower case letters*. You need to write a program to crack the password. **Do not try to crack the password by repeatedly logging into the webpage**. Not only will this drain system resources but it will take way too long. Your password has a SHA256 hash of:23c8f1bdd488e9bc079b81e4f2f6f6e5651359fdb8ed43c4287d1eb1ef24697d.

You should use that hash value to recover your password. It is possible for you to compute a sha256 hash using the command line. However, writing a program will accomplish the task much faster. Feel free to use the hashing function provided in Stage1.

Project 2 Stage 3

Congratulations on reaching the third stage of project 2. Be sure to record this URL on your submission. It is worth twenty (20) points. Reaching stage 4 again will require cracking a password. From here on your username will return to your NetID. For Stages 3-6 you need to figure out the URL to use and the correct password.

The prefix for the next URL is http://netsec.engr.uconn.edu/Project2/Stage4/

Your individualized URL is the sha1sum (this is a linux command) of the current randomized part of the URL (the hexadecimal string after Stage 3). Use the first 10 characters of this string.

Next password Your next password is a random dictionary word from the dictionary file provided. You need to write a program to crack this password. **Do not try to crack the password by repeatedly logging into the webpage**. Not only will this drain system resources but it will take way too long. Your password has a sha256sum hash of:371f7e4223809d8bce3d52f6a5358e47c4b57aa00cbe0a4d8b47d74f010dffa6.

You should use that hash value to recover your password. To reach Stage 4 you'll need to compute roughly 10,000 hashes. Be sure your program is fast enough on a small sample before starting this computation.

Project 2 Stage 4

Congratulations on reaching the fourth stage of project 2. Be sure to record this URL on your submission. It is worth twenty (20) points. Reaching stage 5 requires cracking a password. From here on your username will return to your NetID. For Stages 3-6 you need to figure out the URL to use and the correct password.

The prefix for the next URL is http://netsec.engr.uconn.edu/Project2/Stage5/

Your individualized URL is the reverse of the current randomized part of the URL (the hexadecimal string after Stage 4).

Next password Your next password will be based on the same dictionary as the previous stage. However, a random digit (0-9) has been added at the end of the string. **Do not try to crack the password by repeatedly logging into the webpage**. Not only will this drain system resources but it will take way too long. Your password has a SHA256 hash of:6af51980d8dc0343ab8cd2acee45ce98d3a3db95b1eed66f634511da19220f83.

You should use that hash value to recover your password. To reach Stage 5 you'll need to compute roughly 100,000 hashes. Before starting the crack on the whole dictionary be sure your program is fast enough.

Project 2 Stage 5

Congratulations on reaching the fifth stage of project 2. Be sure to record this URL on your submission. It is worth twenty (20) points. Reaching stage 6 requires cracking a password. From here on your username will return to your NetID. For Stages 3-6 you need to figure out the URL to use and the correct password.

The prefix for the next URL is http://netsec.engr.uconn.edu/Project2/Stage5/

Your individualized URL for Stage 6 is the following, start from the randomized portion of your URL (the Hex pattern) and remove all of the letters. Note you need to include the final password in your submission so it is necessary to successfully complete the log in.

Next password Your next password will be based on the same dictionary as the previous stage. However, a random digit (0-9) at a **random location** instead of at the end of the string. **Do not try to crack the password by repeatedly logging into the webpage**. Not only will this drain system resources but it will take way too long. Your password has a SHA256 hash of:2958b6fb24a94cd6410ef5a47f1667966c764e515d2c85467660df2826672dbb.

You should use that hash value to recover your password. Making the number at a random position means you will need to compute roughly one million hashes. Good luck on the final crack!

Project 2 Stage 6

You've reached the end of the project. Record this URL and submit the 6 URLs you obtained as your project submission. This stage is worth twenty (20) points. Also write down your stage 6 password in your submission.