CS 491 / 591 Spring 2021
Homework # 2
Due Tuesday April 13 AOE

Submission: Submit your homework as an attachment to email to yasodhan@pdx.edu
With subject: IntroSec HW 2

Part A: Written Exercises
Read textbook chapter 2, and watch the two assigned videos listed in the roadmap.

1. [10 points] What is the best hash function to use today? Give the name and bitlength.
2. [10 points] What does the Euler phi function compute?
3. [10 points] RSA public-key encryption requires two large primes. Why do they have to be large?

4. Given a key with 256 bits:
   a. [10 points] how many trials of exhaustive search must be done before success is expected?
   b. [15 points] Assume each exhaustive search trial (testing a single possible value to see if it is the key) requires a total of 16 floating point operations. Is a 256 bit key length a reasonable choice given today's most powerful supercomputer? [See the "top 500" list of November 2020 at https://top500.org/lists/top500/2020/11/ to find Floating Point Operations per Second or FLOPs]. Explain your answer.

Part B: Hands-on programming exercises
Symmetric encryption with OpenSSL

There are many open source options available for performing encryption-related functionality in our programs. In this assignment we will use the OpenSSL library to explore encryption and digital signatures.
OpenSSL is installed in the Linux lab machines. You can access a linux lab machine by:
ssh mylogin@linuxlab.cs.pdx.edu [*Note that is "linuxlab" NOT "linux".]*

What to turn in: For this part, turn in answers to the questions 1-3. [15 points each.]
The openssl library implements a wide variety of cryptographic operations. It is installed on all computers in the linux lab. Extensive documentation is available through the man pages, and through the program itself. Additional resources are listed on the OpenSSL site Documentation tab: https://www.openssl.org/docs/ For example, there is a free online book called OpenSLL Cookbook if you want to explore more deeply.

In these exercises we will use the `openssl` command at the linux command line.

The openssl `enc` command is used for encryption and decryption. A full explanation of all of the options for this command is included in the `enc` man page. Follow the listed steps, then answer the questions.

Step 1. Create a small text file with 15-20 lines of text, enough to be several aes blocks. Name it testfile.txt.

Step 2. Encrypt the file using 128 bit aes in Electronic Code Book (ecb) mode (each block is encrypted independently). Use this command:

```
openssl enc -aes-128-ecb -in testfile.txt -out testfile.txt.aes -
K 'E33202510575DF98CD66D5F35A1915D0' -iv
'582221FEB84119C54FC41FBED8E9D778'
```

This command is doing the following:

- We are telling openssl to encrypt testfile.txt and put its output in testfile.txt.aes.
- We are telling it to use 128 bit AES and in electronic code book mode.
- We are specifying the key to use (using -K).
- We are specifying the initialization vector (using -iv).

The key and IV can be any hex string of appropriate length. They are often randomly generated. Use the same key and IV for each command in this section.

Step 3. Now decrypt the ciphertext file with a similar command, but including the -d option to decrypt, and making some other small changes.

Question 1: What exact command did you use in Step 3?

Step 4. Make a copy of your plaintext, but try changing (replacing, not adding or deleting) a couple characters in the middle of it. Encrypt the modified version, and compare the result with the encrypted original version (it may be easier to compare hex dumps of each).

Question 2: How does the ciphertext (encrypted file) from this encryption differ from the ciphertext based on the original plaintext (what is the extent of the differences)?

Step 5. Repeat the above exercise, only this time encrypting and decrypting using aes-128-cbc. (note the cbc there at the end, different from the ecb we used before. It stands for Cipher Block Chaining

Question 3: What differences do you observe in your results? How does this difference impact security?