Introduction to Cryptology ENEE459E/CMSC498R: Homework 3

Due by beginning of class on 2/24/2015.

1. For each of the following encryption schemes, state whether the scheme achieves perfect secrecy. Justify your answer using Definition 2.3, Lemma 2.4, Theorem 2.10 and/or Theorem 2.11.

   - Message space $\mathcal{M} = \{1, \ldots, 6\}$. Key space $\mathcal{K} = \{1, \ldots, 6\}$. $\mathsf{Gen}()$ chooses a key k at random from $\mathcal{K}$. Let k' be such that $k \cdot k' \equiv 1 \mod 7$. $\mathsf{Enc}_k(m)$ returns $m \cdot k \mod 7$. $\mathsf{Dec}_k(c)$ returns $c \cdot k' \mod 7$.

   - What happens when we use the same scheme as above except with $\mathcal{M} = \{1, \ldots, 8\}$ and $\mathcal{K} = \{1, \ldots, 8\}$?

2. Write a program that increments a counter $2^{24}, 2^{25}, 2^{26}, ..., 2^{33}$ times, and measure how many seconds your program takes to run in each case. Estimate how many years your program would take to increment a counter 2^{64} or 2^{128} times.

3. The best algorithm known today for finding the prime factors of an n-bit number runs in time $2^{c \cdot n^{\frac{1}{3}} (\log n)^{\frac{2}{3}}}$. Assuming 4Ghz computers and $c = 1$ (and that the units of the given expression are clock cycles), estimate the size of numbers that cannot be factored for the next 100 years.

4. OpenSSL is a utility that allows to perform various cryptographic operations. It should be pre-installed on your unix account. One of the cryptographic schemes implemented by OpenSSL is called AES (the Advanced Encryption Standard). AES is a symmetric key encryption scheme which is used to encrypt Internet traffic. Later in the semester, we will study AES in depth. In this exercise, you will use the OpenSSL AES implementation to encrypt a file (see course webpage for the file), using your student id as the secret key. You will then use a cryptographic hash function (SHA1) to hash the ciphertext to a short string. The resulting short string should be submitted as the final answer to this exercise.

   As we will see below, an AES secret key is only 256 bits (32 bytes), but we will use it to encrypt a file of size nearly one million bytes. This is in contrast to perfectly secret schemes, where the key must be as long as the message.

   Here are some more details:
   - Read about OpenSSL here: http://wiki.openssl.org/index.php/Enc
   - We will be using AES-256-CBC to encrypt the file linked to on the course webpage. Make sure to explicitly set the key and the IV.
   - The AES-256 key is 256 bits and the IV is 128 bits For the IV, use a string of all 0s. For the key, use the 9 digits of your student ID appended with an appropriate number of zeros. For example, if your student id is 123456789, your secret key should be 12345678900. . .00.
   - Use OpenSSL to encrypt the file and place it in a temporary file.
   - Use the unix command gsha1sum (see documentation here: http://manned.org/gsha1sum/392b94d5) to output the cryptographic hash of the temporary file (we will cover cryptographic hash functions later this semester as well). Submit this final value as the answer to this exercise.
   - I will be precomputing the correct SHA1 hash for each student and will check that your final hash value matches mine.