Cryptography ENEE/CMSC/MATH 456: Homework 4

Due by beginning of class on 3/6/2023.

1. Let $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be a pseudorandom function. For all $\text{SK} \in \{0,1\}^n$ and for all input $x \in \{0,1\}^n$, define $F'_{\text{SK}}(x) := F_{\text{SK}}(x)||F_{\text{SK}}((x+1) \mod 2^n)$. Is F' a pseudorandom function? If yes, prove it; if not, show an attack.

2. Consider the following keyed function F: For security parameter n, the key is an $n \times n$ Boolean matrix A and an n-bit Boolean vector b. Define $F_{A;b} := Ax + b$, where all operations are done modulo 2. Show that F is not a pseudorandom function.

3. Let F be a pseudorandom function and G be a psuedorandom generator with expansion factor $\ell(n) = n + 1$. For each of the following encryption schemes, state whether the scheme has indistinguishable encryptions in the presence of an eavesdropper and whether it is CPA-secure. (In each case, the shared key is a uniform $k \in \{0,1\}^n$.) Explain your answer.
   (a) To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m \rangle$.
   (b) To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.
   (c) To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1||m_2$ with $|m_1| = |m_2|$, then choose uniform $r \in \{0,1\}^n$ and send $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k((r+1) \mod 2^n) \rangle$.

4. What is the effect of a dropped ciphertext block (e.g., if the transmitted ciphertext $c_1, c_2, c_3, \ldots$ is received as $c_1, c_3, \ldots$) when using the CBC, OFB, and CTR modes of operation?

5. 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—a *block cipher*—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 in CBC mode 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.

Warmup for a problem on HW4

G PRG $G: |s| \to |s|+1$

$G'(s) = s \,||\, G(s)$

Is G' a PRG?

i.e. will $s||G(s)$ look pseudorandom?

Never pseudorandom

G is public. Adv can evaluate $G(s)$

$l(s)||G(s)$

if leakage can be arbitrary insecure.