Practice Problem Set 1 (Ungraded)

February 14, 2017

Exercise 1. (Encryption: From Midterm Spring 2015) Let f be a pseudorandom function (PRF) taking key k and input x and producing output $f_k(x)$.
The key k, input x and output $f_k(x)$ all have bit length n.

The following is a **CPA-secure** symmetric encryption scheme:
To encrypt n-bit message m under key k, select fresh random n-bit string r and output

$$r||(f_k(r) \oplus m)$$

(The symbol $\oplus$ is the bitwise XOR; recall that $a \oplus a \oplus b = b$.)
(The symbol $||$ denotes concatenation.)

1. **(2 points).** Write down the decryption algorithm.
2. **(2 points).** Write down the definition of **CCA-secure symmetric encryption**.
3. **(4 points).** This encryption scheme is **CPA-secure**.
   Prove that this scheme is **NOT CCA-secure**.

Exercise 2. Does it suffice to use CPA-secure encryption in the following scenario? Why or why not?

A user A wants to send his password to a server B, and suppose A and B have a shared symmetric key k. The password is encrypted under key k.

If the password is correct, then A receives the message “OK” encrypted under k from B, and then is allowed to interact with the server B, downloading webpages and sending and receiving other information.

Otherwise, then A receives the message “Fail” encrypted under k from B, and then communication stops.

Exercise 3. (MACs & Encryption schemes.)

Let f be a pseudorandom function (PRF). f takes in a key of length n and an input of length $2n$ and produces an output of length n (*i.e.,* it is length shrinking). In the question below, the symbol $||$ means concatenation and the symbol $\oplus$ is a bit-wise XOR and the symbol $|m| = n$ means the bitstring m has length n bit.

- Prove that the following "MAC" for messages of length $4n$ is an insecure MAC.

  The shared key is a random bitstring $k \in \{0,1\}^n$. To authenticate a message $m1||m2$ where $|m1| = |m2| = 2n$, compute the tag

  $$f_k(m1)||f_k(f_k(m2)||0^n)$$

- The following is a CPA-secure encryption scheme. The shared key is a random bitstring $k \in \{0,1\}^n$. To encrypt a message m of length n bits, choose a random $2n$-bit string r and output the ciphertext

  $$r||(f_k(r) \oplus m)$$

  Now suppose we slightly modify the encryption scheme above, as follows. The shared key is a random bitstring $k \in \{0,1\}^n$. To encrypt a message m of length $2n$ bits, choose a random n-bit string r and output the ciphertext

  $$r||(f_k(m) \oplus r)$$

  Explain why this is not an encryption scheme.

- Now we slightly modify the encryption scheme again. We use a collision resistant hash function H that maps $2n$-bit string to an n bit strings. The key is a random bitstring $k \in 0, 1^n$.

  To encrypt a message m of length n, choose a random $2n$-bit string r and output the ciphertext

  $$r||(H(r) \oplus m \oplus k)$$

  Prove that this is not a CPA secure encryption scheme.

Exercise 4. In Lab2 (the minilab), you were asked to prove that AES in CTR mode cannot satisfy the definition of CCA2-secure encryption. In other words, present an algorithm for an Adversary that wins the CCA2 security game described in the lab handout.

Now, suppose that you used an *authenticated* version of AES in CTR mode. That is, you secret keys are (k_1, k_2), and to encypt a message m you first take $c = Enc_{k_1}(m)$, where Enc is encryption using AES in CTR mode, and then you take $t = MAC_{k_2}(c)$ where MAC is a secure MAC algorithm. You then output the ciphertext (c, t).

- Write down the decryption algorithm.
- Explain why the attack you presented in Lab2 (*i.e.,* the algorithm for an Adversary that wins the CCA2 security game) no longer works.