CSIC 4331/6331 October 1, 2018

Quiz 4

Name:

Let F_k be a strong pseudorandom permutation (i.e., it is indistinguishable from a random permutation even when an adversary has access to an oracle for $F_k^{-1}(\cdot)$).

1. Consider an encryption scheme for message space $\mathcal{M} = \{0,1\}^n$ defined as follows: $Gen(1^n)$ chooses a random key $k \leftarrow \{0,1\}^n$. Encryption works by choosing $r \leftarrow \{0,1\}^n$ and computing $c = (r, F_k(\overline{r}) \oplus m)$ (where $\overline{r}$ represents the string that is derived from r by flipping each of its bits). Decryption works in the natural way.

   (a) Is this scheme CPA-secure? Why or why not?

   (b) Is this scheme CCA-secure? Why or why not?

   (c) Is this scheme an authenticated encryption scheme? Why or why not?

2. Now, consider an encryption scheme for message space $\mathcal{M} = \{0,1\}^{n/2}$ defined as follows: $Gen(1^n)$ chooses a random key $k \leftarrow \{0,1\}^n$. Encryption works by choosing $r \leftarrow \{0,1\}^{n/2}$ and computing $c = F_k(m||r)$. Decryption works in the natural way.

   (a) Is this scheme CPA-secure? Why or why not?

   (b) Is this scheme CCA-secure? Why or why not?

   (c) Is this scheme an authenticated encryption scheme? Why or why not?