University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

Homework 3

Due at the *beginning* of class on Oct. 13

Note: In all the following questions, you should show insecurity by *demonstrating and analyzing an explicit attack*, but you can claim security by giving a convincing argument (a formal proof of security is welcome, but not required).

1. Let G be a pseudorandom generator, and define $G'(x_1 \cdots x_n) = G(x_1 \cdots x_n) \| (x_1 \vee x_2)$. Is G' a pseudorandom generator?

2. Let G be a pseudorandom generator that maps n-bit inputs to $(n+1)$-bit outputs, and define $F_k(x) = G(x) \oplus k$. (Note F has an $(n+1)$-bit key, takes n-bit inputs, and has $(n+1)$-bit outputs.) Is F a pseudorandom function?

3. Let F be a pseudorandom permutation.

   (a) Consider the encryption scheme for the message space $\{0,1\}^n$ defined as follows: $\mathsf{Gen}(1^n)$ chooses two random keys $k_1, k_2 \in \{0,1\}^n$. Encryption is done as $\mathsf{Enc}_{k_1,k_2}(m) = F_{k_1}(k_2 \oplus m)$, and decryption is done in the natural way. Does this scheme have indistinguishable encryptions in the presence of an eavesdropper? Is this scheme CPA-secure?

   (b) Consider the encryption scheme where the message space is $\{0,1\}^{n/2}$ and encryption of a message m is done by choosing random $r \leftarrow \{0,1\}^{n/2}$, and then outputting the ciphertext $F_k(r \| m)$. (Decryption is done in the natural way.) Does this scheme have indistinguishable encryptions in the presence of an eavesdropper? Is this scheme CPA-secure?

4. (Exercises 4.8, 4.9.) Show that the following variants of CBC-MAC are not secure:

   (a) Basic CBC-MAC when used to authenticate messages of different lengths.

   (b) A variant of CBC-MAC where a random IV is used each time a tag is computed (and the IV is included as part of the tag); cf. Exercise 4.9(a).

   (c) A variant of CBC-MAC where all intermediate blocks are included as part of the tag; cf. Exercise 4.9(b).