Cryptography ENEE/CMSC/MATH 456: Homework 2

Due by beginning of class on 2/26/2024.

1. Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. For inputs s of length n, define $G'(s) = F_{0^n}(s)||F_{1^n}(s)$. Is G' necessarily a pseudorandom generator?

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

3. Prove unconditionally the existence of a pseudorandom function $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}$ with key length n, input length $\log_2(n)$ and output length 1 bit.

4. Define the keyed function F as $F_k(x) := k\&x$, where & denotes bitwise AND. Describe and analyze an attack showing that F is not a pseudorandom function.

5. 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.

6. Assume pseudorandom permutations exist. Show that there exists a keyed function F that is a pseudorandom permutation but is not a strong pseudorandom permutation.
   Hint: Construct F such that $F_k(k) = 0^{|k|}$.

7. Let F be a pseudorandom permutation, and define a fixed-length encryption scheme $(\mathsf{Enc}, \mathsf{Dec})$ as follows: On input a key $k \in \{0,1\}^n$ and message $m \in \{0,1\}^{n/2}$, algorithm Enc chooses a uniform string $r \in \{0,1\}^{n/2}$ and computes $c := F_k(r||m)$.
   Show how to decrypt, and prove that this scheme is CPA-secure for messages of length $n/2$.

8. 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 $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k((r+1) \mod 2^n) \rangle$.

9. 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?

10. Recall our construction of CPA-secure encryption from PRF (Construction 3.28 in the textbook). Show that while providing secrecy, this encryption scheme does not provide message integrity. Specifically, show that an attacker who sees a ciphertext $c := \langle r, s \rangle$, but does not know the secret key k or the message m that is encrypted, can still create a ciphertext c' that encrypts $m \oplus 1^n$.