CS 427/519: Homework 3

Due: Monday February 5, 10pm; **typed** and **submitted electronically**.

> **Important notes** for this homework and all future ones:
>
> - When asked to show that something is **secure**, please clarify what libraries you are going to show indistinguishable. List a sequence of hybrid libraries and briefly justify each step (that two consecutive hybrids are indistinguishable).
> - When asked to show that something is **insecure**, please clarify what libraries you are going to distinguish. Explicitly write the code of the distinguisher / calling program. Explicitly derive the output probability of the distinguisher in the presence of each library.

1. Let F be a secure PRF with λ-bit outputs, and let G be a PRG with stretch ℓ. Define

   $$F'(k, r) = G(F(k, r)).$$

   So F' has outputs of length $\lambda + \ell$. Prove that F' is a secure PRF.

2. Let F be a secure PRF. Let $\overline{x}$ denote the bitwise complement of the string x. Define the new function:

   $$F'(k, x) = F(k, x) \| F(k, \overline{x}).$$

   Show that F' is **not** a secure PRF. Describe a distinguisher and compute its advantage.

3. Let $f : \{0,1\}^{\mathsf{in}} \to \{0,1\}^{\mathsf{out}}$ be a (not necessarily invertible) function. The Feistel transform described in the text works only when $\mathsf{in} = \mathsf{out}$.

   Describe a modification of the Feistel transform that works even when the round function satisfies $\mathsf{in} \neq \mathsf{out}$. The result should be an invertible with input/output length $\mathsf{in} + \mathsf{out}$. Be sure to show that your proposed transform is invertible!

grad. Let F be a secure PRF, and define the following 3-round Feistel cipher:

$$\begin{array}{l} \underline{H((k_1, k_2, k_3), X_0 \| X_1):} \\ \quad X_2 := F(k_1, X_1) \oplus X_0 \\ \quad X_3 := F(k_2, X_2) \oplus X_1 \\ \quad X_4 := F(k_3, X_3) \oplus X_2 \\ \quad \text{return } X_3 \| X_4 \end{array}$$

Show that H cannot be a secure SPRP.