Cryptography: Homework 4

(Deadline: 10am, 2021/11/05)

1. (20 points) Let F be a length-preserving PRF. Let $P : \{0,1\}^{2n} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ be a keyed function defined by a 2-round Feistel network:

   - key: $k = (k_1, k_2) \in \{0,1\}^n \times \{0,1\}^n$;
   - input: $x = (L_0, R_0) \in \{0,1\}^n \times \{0,1\}^n$;
   - output: $P_k(x) = (L_2, R_2)$, which is computed as follows
     - $L_1 = R_0, R_1 = L_0 \oplus F_{k_1}(R_0)$;
     - $L_2 = R_1, R_2 = L_1 \oplus F_{k_2}(R_1)$.

   Determine whether P is a PRP. Show your answers.

2. (30 points) Let F be a length-preserving PRF. Let $P : \{0,1\}^{n} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ be a keyed function defined by a 3-round Feistel network:

   - key: $k \in \{0,1\}^n$;
   - input: $x = (L_0, R_0) \in \{0,1\}^n \times \{0,1\}^n$;
   - output: $P_k(x) = (L_3, R_3)$, which is computed as follows
     - $L_1 = R_0, R_1 = L_0 \oplus F_k(R_0)$;
     - $L_2 = R_1, R_2 = L_1 \oplus F_k(R_1)$;
     - $L_3 = R_2, R_3 = L_2 \oplus F_k(R_2)$.

   Show that P is not a PRP.