Cryptography: Homework 4

(Deadline: 10am, 2022/10/21)

1. (20 points) Let F be a length-preserving PRF. Let $F' : \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{2n}$ be a keyed function such that $F'_k(x) = F_k(0\|x)\|F_k(x\|1)$, where $\|$ denotes the concatenation of two strings (e.g., $000\|111 = 000111$). Determine whether F' is a PRF. Show your proof or attack.

   Hint: Since F' is not length-preserving, you need to slightly generalize the definition of PRF. More precisely, you need to determine if $\{F'_k\} \equiv_{\text{c.i.}} \{f\}$, where $k \leftarrow \{0,1\}^n$ and f is a random function from $\{0,1\}^{n-1}$ to $\{0,1\}^{2n}$.

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.