Cryptography: Homework 8

(Deadline: 11:59am, 2019/11/20)

1. (30 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: $x = (L_0, R_0) \in \{0,1\}^n \times \{0,1\}^n$
   - $L_1 = R_0, R_1 = L_0 \oplus F_{k_1}(R_0)$; $L_2 = R_1, R_2 = L_1 \oplus F_{k_2}(R_1)$; output $P_k(x) = (L_2, R_2)$

   Show that P is not a PRP.

2. (30 points) Let $\mathcal{G}$ be a cyclic group generator that on input n and output (q, G, g), where q is an n-bit prime, $G = \langle g \rangle$ is a cyclic group of order q and generated by g. Let $\Pi = (\mathbf{Gen}, h)$ be a hash function defined as below.

   - $s \leftarrow \mathbf{Gen}(1^n)$: generate $(q, G, g) \leftarrow \mathcal{G}(1^n)$, choose $h \leftarrow G$ uniformly and at random, output $s = (q, G, g, h)$.
   - h: given $s = (q, G, g, h)$ and $(x, y) \in \mathbb{Z}_q^2 = \{0, 1, \ldots, q-1\}^2$, output $h^s(x, y) = g^x h^y \in G$. ($h^s$ is a function with domain $\mathbb{Z}_q^2$ and range G.)

   Show that if the problem of computing discrete logarithm is hard with respect to $\mathcal{G}$, then Π is a collision-resistant hash function.

   (Hint: Assume that Π is not collision-resistant. Construct an algorithm for computing discrete logarithms.)