

## Exercise 5

### 1 Threshold Pseudorandom Function

Using a discrete log setting with  $G = \langle g \rangle$ , let  $x$  be a *seed* and define a  $F_x : \{0, 1\}^* \rightarrow \{0, 1\}^k$  as

$$F_x(s) = H'(H(s)^x),$$

where  $H : \{0, 1\}^* \rightarrow G$  and  $H' : G \rightarrow \{0, 1\}^k$  are hash functions. The family  $F = \{F_x\}$  is a pseudorandom function assuming the hardness of the DLP (which can be proven formally in the random oracle model).

Design a non-interactive threshold pseudorandom function based on  $F$  that is secure against a passive adversary.