University of Edinburgh		Fall 16-17
Cryptography		Kiayias
Coursework 9.11.2016	Name :	
Due on 23 November 2016	ID :	

Let g be some deterministic function from $\{0,1\}^k$ to $\{0,1\}$ and $\mathcal{A}$ be a randomized algorithm that on input $x \in \{0,1\}^k$ outputs $y \in \{0,1\}$. It holds that $\mathcal{A}(x) = g(x)$ with probability p, and $\mathcal{A}(x) = 1 - g(x)$ otherwise. Note that k is in $\mathbb{N}$.

1. Assuming $p = 3/4$, describe an estimator algorithm $\mathcal{E}$ that estimates $g(x)$ for a specific input x using $\mathcal{A}$ as a subroutine and fails with probability less than e^{-k}. Describe your estimator, analyze its probability of success and also its running time.

2. Assuming $p = 1/2 + f(k)$, how small can $f(k)$ be so that an estimator invoking $\mathcal{A}$ at most polynomial number of times in k fails with probability less than e^{-k}?