ECS 227: Modern Cryptography
Homework 3

Phillip Rogaway

Out: 6 February 1996. Due: Tuesday, 20 February 1996

7. I give you a coin of some unknown bias, p. You want to estimate p. Develop and analyze the running time of an algorithm $A(\epsilon, \delta)$ which does this. Your algorithm returns an estimate p^* which is within ϵ of p a fraction $1 - \delta$ of the time.

8. Show that if a one-way function exists then $\mathbf{P} \neq \mathbf{NP}$.

9. Recall the (stateful) symmetric encryption scheme we based on a pseudorandom generator $g : \{0,1\}^\ell \to \{0,1\}^L$: the encryption of message x_i using key $a \in \{0,1\}^\ell$, where $\sum_{j=1}^{i} |x_j| \leq L$, is $\langle s, x_i \oplus g(a)[s..t] \rangle$, $s = \sum_{j=1}^{i-1} |x_j| + 1$ and $t = \sum_{j=1}^{i} |x_j|$. Call this scheme $\Pi[g]$. Prove the following theorem, which we stated in class:

> Let A be an adversary that (t, q, μ, ϵ)-breaks the encryption scheme $\Pi[g]$, in the sense of indistinguishability. Then there exists an adversary A' that (t', μ', ϵ')-break the PRG g, where $t' = t + O(\mu)$, $\mu' = \mu$, and $\epsilon' = e$.

10. In class we sketched a proof that, for symmetric encryption, security in the sense of indistinguishability implies semantic security. State and prove a converse to this theorem.