ECS 227: Modern Cryptography
Homework 5

Phillip Rogaway

Out: 5 March 1996. Due: 12 March 1996

No late homeworks will be accepted: sorry!

15. **Part A.** Adapt Definition 8.4.2 to come up with a directly analogous definition for asymmetric encryption in the random oracle model. Assume you have will have two random oracles, G and H. Your definition would begin:

> Let $\mathcal{G}$ be an encryption scheme, and let A be an adversary. Then A is said to (t, q, q_G, q_H, μ)-break $\mathcal{G}(1^k)$ if $\cdots$

Part B. Suppose you have an adversary A that (t, q, q_G, q_H, μ)-breaks OAEP$[\mathcal{F}, k, k_0, n]$, with respect to the definition you just gave. Describe an inverting algorithm I which does a good job inverting the trapdoor permutation $\mathcal{F}$, You need not prove the particular bounds (t', e') which your inverter I achieves. *Hint: this problem is simply asking you to adapt 9.5 to a slightly different definition of secure encryption.*

16. Let $\Pi = (\mathit{Gen}, \mathit{Sign}, \mathit{Verify})$ be a signature scheme. It lets you sign messages of arbitrary length. But suppose *Sign* is slow when you ask it to sign strings which are more than a couple hundred bits. Otherwise it's fast.

Describe a new signature scheme, Π_H, based on Π and a fast-to-compute collision-intractable hash functions H (eg., H =SHA). Signing under Π_H should now be fast. *Hint: do what's obvious.*

Give a convincing argument which establishes that Π_H is secure as long as Π is a secure and H is a collision-intractable hash function. That is, given an adversary A which does a good job at forging under Π_H, you should either be able to do a good job at forging against Π, or else you be able to find collisions in H.