Problem Set 8

Due: Monday November 23, 2009, in class.

Collaboration is allowed on this problem set. See the course information sheet for collaboration rules.

Problem 1. **[40 points]** Let $\mathcal{K}_{\rm rsa}$ be an RSA generator with associated security parameter k. The associated RO model SRSA KEM $\mathcal{KEM} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is defined via

algorithm $\mathcal{K}$	algorithm $\mathcal{E}^H_{pk}$	algorithm $\mathcal{D}^H_{sk}(C_a)$
$(N, p, q, e, d) \xleftarrow{\$} \mathcal{K}_{\rm rsa}$	$x \xleftarrow{\$} \mathbf{Z}_N^*$	$x \leftarrow C_a^d \bmod N$
$pk \leftarrow (N, e)$	$K \leftarrow H(x)$	$K \leftarrow H(x)$
$sk \leftarrow (N, d)$	$C_a \leftarrow x^e \bmod N$	return K
return (pk, sk)	return (K, C_a)	

Here we view $H\colon\ \mathbf{Z}_N^* \to \{0,1\}^k$ when the public key is (N, e). Let A be an ind-cpa adversary that makes 1 **Enc** query and q queries to the RO H. Show that there is a OW-adversary I such that

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{KEM}}(A) \le \mathbf{Adv}^{\text{owf}}_{\mathcal{K}_{\rm rsa}}(I)\ .$$

The running time of I should be about that of A plus the time for q RSA operations.
