Homework 1 for 6.875

Teacher: Silvio Micali, TA: Yevgeniy Dodis

Due Date: **Wednesday, September 23**

Problem 1

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, where p_i are distinct *odd* primes and $\alpha_i > 0$. Let $x \in \mathbb{Z}_n^*$ be a quadratic residue.

(a) Show that x has *exactly* 2^k distinct square roots $(\bmod\ n)$.

(b) Why did we require that none of the $p_i = 2$?

Problem 2

Assume RSA is invertible in polynomial time. Give an efficient algorithm that, given two integers n and S, decides whether S is relatively prime to $\varphi(n)$.

Problem 3

Assume one is using RSA with the same modulus n but different relatively prime public exponents e_1 and e_2 to encrypt a message m. Prove that the adversary can reconstruct m from the 2 encryptions (i.e. from $m^{e_1} \bmod n$ and $m^{e_2} \bmod n$).

Problem 4

Assume Alice, Bob and Carol have 3 randomly chosen moduli n_A, n_B and n_C, s.t. 3 is a common RSA exponent for all of them (i.e. $gcd(3, \varphi(n_X)) = 1$, $X = A, B, C$). A user U encrypts the same message m using their public keys. Show that an adversary can reconstruct m from the 3 encryptions (i.e. from $m^3 \bmod n_A$, $m^3 \bmod n_B$ and $m^3 \bmod n_C$).