1. Explain why the Chinese Remainder Theorem allows RSA decryption to be done 4 times faster.

2. Show how to find the plaintext $x$ from its ciphertext $x^e \pmod{n}$ if the Top/Down oracle is correct 99% of the time.

3. Formally prove that when $R$ is sufficiently large ($|Rn| > |m^2| + 100$), any algorithm for computing $X$ from a sampled $x^2 + Rn$ (i.e., $R$ is chosen at random) is equivalent to an algorithm for computing $x$ from $x^2 \pmod{n}$. 

Public Key Cryptography

Exercise 5 - due May 21

May 7, 2007