

Homework 4 – Due Tuesday, April 21 in class or online

Reminders: Collaboration is permitted on homeworks, but you must (a) list your collaborators on the problem set and (b) **understand and write your solutions yourself**.

Clarity is an important component of the grade on your problem sets. Poorly explained solutions will not receive full marks, even if they are correct.

Problems to be handed in:

1. **(Bounding the number of divisors)** Show that for integers N , the ratio $\frac{\phi(N)}{N}$ is $\Omega(N^{-\epsilon})$, for every constant $\epsilon > 0$. (This ratio is the fraction of elements in \mathbb{Z}_N that are relatively prime to N).

Hint: How many different prime factors can N have? How small can they be?

Recall: If $N = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime factorization of N , then $\phi(N) = \prod_{i=1}^k p_i^{e_i-1} (p_i - 1)$ (this follows from the Chinese Remainder Theorem).

2. **(Better Hashing from the Discrete Logarithm Assumption)** KL, Exercise 7.22.
3. **(Signatures)**
 - (a) KL, Exercise 12.4 (RSA signatures via encoding)
 - (b) KL, Exercise 12.11 (Making Lamport-type schemes stateless)
4. **(Random Self-Reducibility)**
 - (a) KL, Exercise 10.7 (Random self-reducibility of RSA)
 - (b) KL, Exercise 10.17 (coin flipping) — do only parts (a) and (b). (You should feel free to think about (c), too, but you do not need to hand it in.)