HAI709I : Fondements cryptographiques de la sécurité, Université de Montpellier, 2023

20/11/2023. Homework for Lecture 10.

Exercise 1. (a) Propose an polynomial time algorithm that takes a k-bit integer number n (i.e., an integer number such that $2^{k-1} \leq n < 2^k$) and checks whether $n = m^{13}$ for some integer m.

Remark: The algorithm should run in time $\mathrm{poly}(k)$, so you cannot try every integer number below n.

Hint: The problem is simpler if you need to *find* such a number m.

(b) the same question for the properties $n = m^k$ with $k = 2, 3, \ldots, \lceil \log_2 n \rceil$.

Exercise 2. (a) Let us take the pair $(n = 59 \cdot 61, d = 7)$ as a public key of the RSA scheme. Try to find the matching private key.

(b) Let us take the pair $(n = 59 \cdot 61, d = 5)$ as a public key of the RSA scheme. Try to find the matching private key.

(c) Let us take the pair $(n = 59 \cdot 69, d = 3)$ as a public key of the RSA scheme. Try to find the matching private key.

One of these questions has no solution. Which one?