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

04/12/2023. Homework for Lecture 12.

Exercise 1. Let $n = 323 = 17 \cdot 19$. Find (without a computer) four numbers x in the set $\{1, \ldots, n-1\}$ such that $x^2 = 16 \mod n$.

Exercise 2. Prove that if $\mathrm{P} = \mathrm{NP}$ then there exists a deterministic polynomial-time algorithm that finds for every input n (an integer numbers given by its binary expansion) the list of all its prime factors.

Exercise 3. Let $p > 2$ be an prime number. Show that the number -1 is a quadratic residue modulo p (i.e., there exists an integer number x such that $x^2 = -1 \mod p$) if and only if p can be represented as $p = 4k + 1$ for some integer k. For example, -1 is a quadratic residue modulo 5, 13, 17 (prime numbers of the form $4k + 1$) but not a quadratic residue modulo $3, 7, 11$ (prime numbers of the form $4k + 3$).

Exercise 4 (optional)**.** Let p be a prime number and p can be represented as $p = 4k + 3$ for some integer k. Show that the mapping

$$x \mapsto x^2 \mod p$$

restricted on the set of quadratic residues modulo p is a bijection.

For example, for $p = 7$ the (non-zero) quadratic residues are the numbers 1 (since $1 = 1 \cdot 1 = 6 \cdot 6 \mod 7$), 2 (since $2 = 3 \cdot 3 \mod 7 = 4 \cdot 4 \mod 7$), and 4 (since $4 = 2 \cdot 2 \mod 7 = 5 \cdot 5 \mod 7$). Observe that

$$1^2 = 1,\ 2^2 = 4,\ 4^2 = 2 \mod 7,$$

i.e., the operation $[x \mapsto x^2 \mod 7]$ induces a bijection on the set of quadratic residues. We propose to prove that a similar property holds for all primes represented $p = 4k + 3$ (we do not claim this for the other prime numbers).