HAI709I : Fondements cryptographiques de la sécurité, Univ Montpellier, 2024
Exercises for the second part of the semester.

The colors help to distinguish between the exercises for lectures by **Katharina Boudgoust** and **Andrei Romashchenko**.

Exercise 1. Let p be a prime number. Prove that $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) = -1 \mod p$. For example, for $p = 5$ we have

$$1 \cdot 2 \cdot 3 \cdot 4 = 24, \text{ and we see that } 24 = -1 \mod 5.$$

Exercise 2. Let p, q be two different prime numbers, each of them is strictly greater than 2, and $n = p \cdot q$.

(a) Prove that if $a^2 = 1 \mod n$, then $a^2 = 1 \mod p$ and $a^2 = 1 \mod q$.

(b) Prove that if $a = 1 \mod p$ and $a = -1 \mod q$, then $a \neq \pm 1 \mod n$ but $a^2 = 1 \mod n$.

(c) Prove that there exists 4 different numbers x_1, x_2, x_3, x_4 in the set $\{1, 2, \ldots n-1\}$ such that $x_i^2 = 1 \mod n$.

(d) Let $n = 29 \cdot 31$. Find at least three different numbers x in $\{1, \ldots, n-1\}$ such that $x^2 = 1 \mod n$. (Try to do it without computer.)

Exercise 3. Assume that there exists a randomized polynomial time algorithm $\mathcal{A}$ such that for every composite number n (represented by its binary expansion), $\mathcal{A}(n)$ with probability $p > 1/2$ returns a non-trivial factor k of n (i.e., $k \neq 1$, $k \neq n$, and k divides n). With probability $1-p$ the algorithm may return a number that is not a factor of n or stop without any answer.

Prove that there exists another randomized polynomial time algorithm $\mathcal{B}$ such that for every composite number n (again, represented by its binary expansion), $\mathcal{B}(n)$ with a probability $> 0{,}99$ returns a non-trivial factor k of n.

Exercise 4. (a) Prove that there exists an integer number n_0 such that for all integers $n > n_0$ (i.e., for all large enough integer numbers) there exists an integer x

$$2^n < x < 2^{n+2}$$

such that $x = p \cdot q$, where p and q are two different prime numbers.

(b) Show that there exists a a randomized algorithm that takes n as input and in time $\mathrm{poly}(n)$ with probability $> 0{,}99$ produces an instance of such a number x. (You may use the Miller–Rabin test as a subroutine.)

(c) The same two questions as above but with a higher precision: $2^n < x < 2^{n+1}$.

Exercise 5. We consider the group $(G, \cdot, 1)$, where $G = (\mathbb{Z}/25\mathbb{Z})^\times$.

i. What is the order $\mathrm{ord}(G)$ of the group? List its elements.

ii. Compute the inverse of 13 in the group.

iii. Compute (by hand!) 2^{2777} in the group.

iv. Compute the subgroup $\langle 6 \rangle$ generated by 7.

Exercise 6. We define the following *squared exponent* problem: Let g be a generator of a cyclic group G and let t be sampled uniformly at random from $\{0, \ldots, \mathsf{ord}(G) - 1\}$. Given (g, g^t, g^{t^2}), the problem asks to find t.

Prove that there exists a reduction from the squared exponent problem to the computational Diffie-Hellman (CDH) problem, introduced in class. In other words, prove that an adversary having non-negligible success probability in solving CDH leads to an adversary having non-negligible success probability in solving the squared exponent problem.

Exercise 7. Let $\Pi = (Gen, Enc, Dec)$ be a correct and secure symmetric encryption scheme. We build the following key-exchange protocol:

Alice samples a ephemeral key $m_A \leftarrow Gen$ and sends it to Bob. Bob sample the key k_B and encrypts it under the symmetric encryption scheme using m_A as the key, i.e., $m_B \leftarrow Enc(k_B, m_A)$, and sends m_B to Alice. Alice computes $k_A \leftarrow Dec(m_B, m_A)$.

i. Prove that the scheme above is a correct key-exchange protocol.

ii. Prove that is not secure (against an eavesdropper).

Exercise 8 (Bonus)**.** Let $N = 41 \cdot 47$ and $e = 3$. Let us take the pair (N, e) as a public key of the RSA signature scheme. Find the corresponding private key.

Exercise 9. If $\mathrm{P} = \mathrm{NP}$ then there is no one-way functions.

Exercise 10. (a) Prove that every pseudo-random generator is a one-way function.

(b) Prove that if there exist one-way functions, then not all of them are pseudo-random generators. In other words, if there exists a pseudo-random generator $g : \{0,1\}^* \to \{0,1\}^*$ (which must be a one-way function), then there exists another one-way function $f : \{0,1\}^* \to \{0,1\}^*$ that is *not* a pseudo-random generator.

(c) Prove that if there exist one-way functions, than at least for some one-way function $f(x)$ the first bit of the argument x is *not* a hard-core predicate (which means that the construction of a one-way function with a hard core predicate is not trivial).

Exercise 11. Let $h : \{0,1\}^* \to \{0,1\}^*$ be a function computable in polynomial time by a deterministic algorithm such that for every $x \in \{0,1\}^n$ the value $y = h(x)$ is a binary string of length $\lfloor n/2 \rfloor$. (This function obviously cannot be one-to-one; one image y may have many different pre-images x such that $h(x) = y$.)

Assume that this function is *not pre-image resistant* in the following sense. There exists a polynomial-time algorithm $\mathcal{A}$ such that for every n, for a randomly chosen $x \in \{0,1\}^n$, with probability $> 0{,}5$ on the input $y = h(x)$

$$\mathcal{A}(y) \text{ returns an } x' \in \{0,1\}^n \text{ such that } h(x') = y$$

(algorithm $\mathcal{A}$ finds one of many h-pre-images of y, which is possibly not equal to the original x).

(a) Prove that this function is *not collision-resistant*: there exists a polynomial-time algorithm $\mathcal{B}$ such that for every even number n

- with probability $> 0{,}5$: $\mathcal{B}(n)$ stops in $\mathrm{poly}(n)$ steps and returns two numbers x_1, x_2 of length n such that $x_1 \neq x_2$ and $f(x_1) = f(x_2)$ (i.e., $\mathcal{B}$ finds a *collision* for f)

- with probability $< 0{,}5$: $\mathcal{B}(n)$ returns the symbol $\perp$ (which means *no answer*).

(b) Prove a stronger property: there exists a polynomial-time algorithm $\mathcal{B}'$ that for every even number n

- with probability > 0.99 : $\mathcal{B}'(n)$ stops in $\mathrm{poly}(n)$ steps and returns two numbers x_1, x_2 of length n such that $x_1 \neq x_2$ and $f(x_1) = f(x_2)$
- with probability < 0.01 : $\mathcal{B}'(n)$ returns symbol $\perp$

Exercise 12. (a) Let $\Pi = \langle Enc(), Dec(), Gen() \rangle$ with the space of clear message $\mathcal{M} = \{0,1\}^n$. Assume that there exists an algorithm $\mathcal{A}$ with the following property. For a uniformly randomly chosen message $(m^1 \dots m^n) \in \mathcal{M}$, a randomly chosen secret key $k \leftarrow Gen(1^n)$, and the encrypted message $e \leftarrow Enc(m, k)$, the value

$$res \leftarrow \mathcal{A}(e)$$

computed by $\mathcal{A}$ with probability $> 0{,}99$ is equal to (m^1, m^2, m^3). In other words, the adversary can reveal with a very high probability the first three bits of the clear message. Prove that in this case Π does not respect the formal definition of a scheme *secure against an adversary computable in polynomial time*.

(b)* The same question if with probability $> 0{,}33$ we have $res = (m^1, m^2)$.

(c)** The same question if with probability $> 0{,}13$ we have

$$res = (m^1, m^2 \oplus m^3, m^4 \oplus m^5 \oplus m^6).$$

(d) Prove that even for a secure scheme Π there exist randomized polynomial time algorithms $\mathcal{A}_2$, $\mathcal{A}_3$, and $\mathcal{A}_6$ such that

$$\mathrm{Prob}\left[\, \mathcal{A}_2(e) = m^1 m^2 \,\right] = \frac{1}{4},$$

$$\mathrm{Prob}\left[\, \mathcal{A}_3(e) = m^1 m^2 m^3 \,\right] = \frac{1}{8},$$

$$\mathrm{Prob}\left[\, \mathcal{A}_6(e) = m^1 m^2 m^3 m^4 m^5 m^6 \,\right] = \frac{1}{64}.$$

Exercise 13 (optional; not necessary for the final exam)**.** Assume there exists a one-way length preserving permutation f with a hard-core bit h. Suggest a protocol of the game rock-paper-scissors between Alice and Bob connected by a communication channel. It is assumed that both players are able to perform computations in polynomial time. If one of the players tries to cheat and deviates from the prescribed protocol, this should give only negligibly small advantage in the probability to win.