Exercises Extra

Note: These exercises are exemplary for the ones appearing in the final exam.

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

i. *What is the order* $\mathsf{ord}(G)$ *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 2. *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 3. *Let* $\Pi = (Gen, Enc, Dec)$ *be a correct and secure symmetric encryption scheme. We build the following key-exchange protocol:*

Alice samples an ephemeral key $m_A \leftarrow Gen$ *and sends it to Bob. Bob samples 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 it is not secure (against an eavesdropper).*

Exercise 4 (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.*