Introduction to Homomorphic Cryptosystems
Exercise Sheet 1: Mathematical Background

Task 1 – Groups (1/2)

The mathematical concept of groups was introduced in the lecture.

a) Justify whether the following tuple $(P, \heartsuit)$ represents a group. The Set P consists of all people on earth and the operation $\heartsuit$ is defined for $p_1, p_2 \in P$ as: $p_1 \heartsuit p_2 = p_1$ loves p_2.

b) Justify whether the following tuple $(G, *)$ represents a group. Where $G = \{a, b, c, d\}$ and the mapping rule $*$ is defined in table Tabelle 1.

$*$	a	b	c	d
a	b	d	a	a
b	c	b	a	b
c	a	d	a	d
d	a	b	c	d

Tabelle 1

Task 2 – Groups (2/2)

Proof the following theorems:

a) Each group has a unique identity.

b) Each element in a group has a unique inverse.

Task 3 – Group Homomorphism (1/2)

Show that the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = ax + b$, where $a, b \in \mathbb{R}$ and $b \neq 0$, is not a homomorphism between the group $(\mathbb{R}, +)$ and $(\mathbb{R}, +)$.

Task 4 – Group Homomorphism (2/2)

Show that the function $f : \mathbb{R}^+ \to \mathbb{R}$ defined by $f(x) = log(x)$ is a homomorphism between the group $(\mathbb{R}^+, *)$ and $(\mathbb{R}, +)$.

Task 5 – Paillier scheme

The Paillier scheme is a PHE scheme introduced in 1999. The keygeneration algorithm yields a public key (n, g) and a secret key (p, q).

Encryption Algorithm:
For each message $m \in \mathbb{Z}_n$ (integers smaller n), the number $r \in \mathbb{Z}_{n^2}^*$ (multiplicative group of integers smaller n^2) is randomly chosen and the encryption works as follows:

$$c = E(m) = g^m r^n \pmod{n^2}$$

Proof that the Paillier scheme is a PHE scheme.

Task 6 – PHE Schemes

PHE schemes have the disadvantage that they only support one operation (usually addition or multiplication), but this operation can be performed any number of times. In practice, there are also many practical applications where only one operation is required. Think of such an example and describe it

Task 7 – OpenFHE

OpenFHE is a C++ library which provides implementation of common FHE schemes. Compared to other HE libraries OpenFHE has the most features. We want to use the library in the following exercises, so in this task you should follow the instructions on `https://openfhe-development.readthedocs.io/en/latest/` and install all necessary prerequisites.

After that you should be able to run on of the example scripts, which are located in our cloned version of the OpenFHE repo. You can try this one as a test:

src/binfhe/examples/boolean.cpp