Problem 1. (How not to use the ElGamal cryptosystem) Alice and Bob are using the ElGamal cryptosystem. The public key of Alice is \((p, a, y) = (3571, 2, 2905)\). Bob encrypts the messages \(m_1\) and \(m_2\) as
\[C_1 = (1537, 2192)\] and \(C_2 = (1537, 1393)\).

a) Show that the public key is valid.
b) What did Bob do wrong?
c) The first message is given as \(m_1 = 567\). Determine the message \(m_2\).

Problem 2. (Euler’s criterion) Prove Euler’s criterion (Proposition 9.2): Let \(p > 2\) be prime, then
\[c \in \mathbb{Z}_p^*\text{ is a quadratic residue modulo } p \iff c^{\frac{p-1}{2}} \equiv 1 \mod p.\]

Problem 3. (Properties of quadratic residues) Let \(p\) be prime, \(g\) a primitive element modulo \(p\) and \(a, b \in \mathbb{Z}_p^*\). Show the following:

a) \(a\) is a quadratic residue modulo \(p\) if and only if there exists an even \(i \in \mathbb{N}_0\) with \(a \equiv g^i \mod p\).
b) If \(p\) is odd, then exactly one half of the elements \(x \in \mathbb{Z}_p^*\) are quadratic residues modulo \(p\).
c) The product \(a \cdot b\) is a quadratic residue modulo \(p\) if and only if \(a\) and \(b\) are both either quadratic residues or quadratic non-residues modulo \(p\).

Problem 4. (Rabin cryptosystem) Alice and Bob are using the Rabin Cryptosystem. Bob uses the public key \(n = 4757 = 67 \cdot 71\). All integers in the set \(\{1, \ldots, n-1\}\) are represented as a bit sequence of 13 bits. In order to be able to identify the correct message, Alice and Bob agreed to only send messages with the last 2 bits set to 1. Alice sends the cryptogram \(c = 1935\). Decipher this cryptogram.