Problem 1: Malleability of ElGamal

Remember the auction example from the lecture: Bidder 1 produces a ciphertext $c = E(pk, bid_1)$ where $E$ is the ElGamal encryption algorithm (using integers mod $p$ as the underlying group). Given $c$, Bidder 2 can then compute $c'$ such that $c'$ decrypts to $2 \cdot bid_1 \mod p$. This allows Bidder 2 to consistently bid twice as much as Bidder 1.

Now refine the attack. You may assume that $bid_1$ is the amount of Cents Bidder 1 is willing to pay. And you can assume that Bidder 1 will always bid a whole number of Euros. (I.e., $bid_1$ is a multiple of 100.)

Show how Bidder 2 can consistently overbid Bidder 1 by only 1%. What happens to your attack if Bidder 1 suddenly does not bid a whole number of Euros?

**Hint:** Remember that modulo $p$, one can efficiently find inverses. For example, one can find a number $a$ such that $a \cdot 100 \equiv 1 \mod p$.

**Solution.** Let $a$ be the inverse of 100 modulo $p$. That is $100a \equiv 1 \mod p$. If Bidder 2 intercepts a message $c = E(pk, bid_1)$, he computes $c' = E(pk, (1 + a)bid_1 \mod p)$. This way he bids to $bid_2 := (1 + a)bid_1 \mod p$. We have to show that $bid_2 = 1.01 \cdot bid_1$.

We assumed that Bidder 1 always pays a whole amount of Euros. Hence $bid_1 = 100x$ for some integer $x$. Thus $1.01bid_1 = 101x$. Furthermore,

$$bid_2 \equiv (1 + a)bid_1 = (1 + a)100x \equiv 100x + (100a)x \equiv 100x + x \equiv 101x \mod p.$$  

Thus we know that $bid_2 \equiv 101x \mod p$. Furthermore, since $p$ is a large prime, it is to be expected that $101x < p$ (otherwise Bidder 1 would bid an unrealistically large amount). Thus $bid_2 = 101x$. Hence $bid_2 = 1.01bid_1$.

What happens if Bidder 1 does not bid a whole amount of Euros? For example, if $bid_1 = 1$ (1 Cent). In this case, Bidder 2 will bid $1 + a$ Cent. And $a$ is a very large number. (At least $a > p/100$ because otherwise $100a < p$ and hence $100a \not\equiv 1 \mod p$.) Thus in this case, Bidder 2 may end up bidding huge amounts. (Typically in the order of magnitude of $p$.)

Problem 2: Encoding messages for ElGamal (bonus problem)

The message space of ElGamal (when using the instantiation that operates modulo a prime $p > 2$ with $p \equiv 3 \mod 4$ and if we want to avoid the insecurity discussed in the practice) is the set $\mathbb{QR}_p = \{x^2 \mod p : x = 0, \ldots, p - 1\}$.

The problem is now: if we wish to encrypt a message $m \in \{0, 1\}^\ell$ (with $\ell \leq |p| - 2$), how do we interpret $m$ as an element of $\mathbb{QR}_p$?

---

1 As long as $bid_1 < p/2$, that is. Otherwise $2 \cdot bid_1 \mod p$ will not be twice as much as $bid_1$. However, for large $p$, $bid_1 \geq p/2$ is an unrealistically high bid.

2 You do not actually need to use this fact, but the hint that $-1 \not\in \mathbb{QR}_p$ below is only true in this case.
One possibility is to use the following function \( f : \{1, \ldots, \frac{p-1}{2}\} \rightarrow \text{QR}_p \):

\[
f(x) := \begin{cases} x & \text{if } x \in \text{QR}_p \\ -x \mod p & \text{if } x \notin \text{QR}_p \end{cases}
\]

Once we see that \( f \) is a bijection and can be efficiently inverted, the problem is solved, because a bitstring \( m \in \{0, 1\}^\ell \) can be interpreted as a number in the range \( 1, \ldots, \frac{p-1}{2} \) by simply interpreting \( m \) as a binary integer and adding 1 to it. (I.e., we encrypt \( f(m + 1) \).

We claim that the following function is the inverse of \( f \):

\[
g(x) := \begin{cases} x & \text{if } x = 1, \ldots, \frac{p-1}{2} \\ -x \mod p & \text{if } x \neq 1, \ldots, \frac{p-1}{2} \end{cases}
\]

We thus need to show the following: the range of \( f \) is indeed \( \text{QR}_p \), and that \( g(f(x)) = x \) for all \( x \in \{1, \ldots, \frac{p-1}{2}\} \).

(a) Show that \( f(x) \in \text{QR}_p \) for all \( x \in \{1, \ldots, \frac{p-1}{2}\} \).

\text{Hint:} You can use (without proof) that \(-1 \notin \text{QR}_p \) (this only holds in \( \text{QR}_p \) for \( p \) prime with \( p \equiv 3 \mod 4 \). And that the product of two quadratic non-residues is a quadratic residue (this only holds in \( \text{QR}_p \), but not in \( \text{QR}_n \) for \( n \) non-prime).

\text{Solution.} We distinguish two cases:

- “\( x \in \text{QR}_p \)” In that case, by definition \( f(x) = x \in \text{QR}_p \).
- “\( x \notin \text{QR}_p \)” Then \( f(x) \equiv -x \equiv (-1) \cdot x \mod p \). Since both \(-1\) and \( x \) are quadratic non-residues, \((-1) \cdot x\) is a quadratic residue. Hence \( f(x) \in \text{QR}_p \).

(b) Show that \( g(f(x)) = x \) for all \( x \in \{1, \ldots, \frac{p-1}{2}\} \).

(This then shows that \( f \) is injective and efficiently invertible. Bijectivity follows from injectivity because the domain and range of \( f \) both have the same size.)

\text{Hint:} Make a case distinction between \( x \in \text{QR}_p \) and \( x \notin \text{QR}_p \). Show that for \( x \in \{1, \ldots, \frac{p-1}{2}\} \) it holds that \(-x \mod p \notin \{1, \ldots, \frac{p-1}{2}\} \).

\text{Solution.} We distinguish two cases:

- “\( x \in \text{QR}_p \)” Then \( f(x) = x \in \{1, \ldots, \frac{p-1}{2}\} \), hence \( g(f(x)) = g(x) = x \).
- “\( x \notin \text{QR}_p \)” Then \( f(x) = (-x \mod p) = p - x \in \{p - \frac{p-1}{2}, \ldots, p - 1\} = \{\frac{p+1}{2}, \ldots, p - 1\} \). Since \( \frac{p+1}{2} > \frac{p-1}{2} \), this implies that \( f(x) \notin \{1, \ldots, \frac{p-1}{2}\} \). Thus \( g(f(x)) = (-f(x) \mod p) = (-(-x \mod p) \mod p) = (x \mod p) = x \).