IV054 Coding, Cryptography and Cryptographic Protocols
2013 - Exercises VII.

1. Consider the ElGamal signature scheme with $p = 467$, $q = 2$ and $x = 127$. Perform in detail signing and verification procedures for the message $w = 100$ and $r = 213$.

2. Suppose Alice is using the ElGamal signature scheme with a prime p and $q \in \mathbb{Z}_p^*$, $q \equiv 2 \pmod p$ (note that for 2 to be a primitive element of $\mathbb{Z}_p^*$, $p \equiv 1 \pmod 4$) and let y be Alice's public key and $m \in \mathbb{Z}_{p-1}$ be a message.
Let $z(a)$ be a solution of the following equation:
$$q^{za} = y^a.$$
Show that Eve can sign message m on behalf of Alice, without knowing her secret key, as follows:
   (a) Let $a = \frac{p-1}{2}$. Show that Eve can easily calculate $z(a)$.
   (b) Let $a = \frac{p-1}{2}$, $t \equiv \frac{p-3}{2} \pmod{p-1}$ and $b = t(m - az) \pmod{p-1}$.
   Show that (a, b) is a valid signature of the message m.

3. Prove that the Ong-Schnorr-Shamir subliminal channel scheme is correct.

4. Consider the ElGamal signature scheme is used. After receiving a signature (a, b), the verifier should check that the condition $1 \leq a < p$ is satisfied. Why?

5. Consider the ElGamal signature scheme.
   (a) Let $p = 3061$ and $q = 307$.
      - Prove that q is a primitive element of the group $(\mathbb{Z}_p^*, \cdot)$.
      In the proof, you are only allowed to evaluate $q^e \pmod p$ for at most 5 different e.
      - Is $r = 17$ a valid choice?
   (b) In the description given at the lecture, it is assumed that we choose $r \in \mathbb{Z}_{p-1}^*$. Why cannot we just choose $r \in \mathbb{Z}_p^*$ instead?

6. Consider the Rabin signature scheme.
   (a) Prove that a lower bound for the cardinality of $QR(n)$ is $\sqrt{n}$.
   Using this lower bound, estimate the upper bound for the expected number of randomly generated $x \in Z_n$ that need to be tested in order to get $x \in QR(n)$.
   (b) Determine the probability that an event with chance to succeed equal to $1 - \epsilon$ takes at least k tries to succeed for the first time.
   (c) Why can we suppose that the step 2 of the signing process (finding a suitable U) finishes in polynomial time?

7. A lazy signer uses the DSS signature algorithm and has precomputed one pair (k, a) satisfying $a = (r^k \bmod p) \bmod q$ that always uses for generating a signature. Recover his secret key.