Exercise

Algorithmic Cryptography

Sheet 11

Exercise 11.1: (4 points)

After Knud Knudson’s arrival at the North Pole, the Inuit told him that there is the Treasure of the Unknown Harbor Seal near the Geographic North Pole. In order to find it, Knud Knudson has to discover the coordinates of the Stones of the Average, each given by a point \((x_i, y_i)\), \(i \in \{1, \ldots, n\}\). The treasure is located at the average point of them, i.e., at \((\frac{1}{n} \cdot \sum_{i=1}^{n} x_i, \frac{1}{n} \cdot \sum_{i=1}^{n} y_i)\).

Unfortunately, Knud Knudson’s mental calculation skills do not allow him to calculate the average point using only his brain. So he uses his new Peach yPhone, which has a connection to a server that can compute complicated calculations. As a result of a misapprehension, the vendor sent Knud Knudson a smartphone that can save only one point at the same time. So Knud Knudson must use the server to do the computation. But he does not trust the server operator. So he does not want that the server can see any point or the result. Hence, the computation has to be done using encrypted data.

Can you design a protocol that guarantees Knud Knudson’s privacy requirements? The Inuit gave Knud Knudson a machine that can compute the discrete logarithm efficiently, i.e., given a prime number \(p\), a generator \(g\) of \(\mathbb{Z}_p^*\), and a \(y \in \mathbb{Z}_p^*\), it can compute a \(x \in \mathbb{Z}_p^*\) with \(y \equiv g^x \mod p\).

Exercise 11.2: (4 points)

Construct an electronic money protocol for the following problem:

A couple wants to share a bank account in such a way that each of them can do transactions. The bank must not distinguish between who has done a transaction, but both spouses must be able to differentiate who has done the transaction using the receipts of the bank.

Exercise 11.3: (4 bonus points)

Let an ElGamal system be given by the private key \((p, g, x)\) and the public key \((p, g, y = g^x \mod p)\). Furthermore, let \(k \in \{2, \ldots, p - 2\}\) with \(\gcd(k, p - 1) = 1\). The message \(m\) was encrypted to \((a, b) = (g^k \mod p, m \cdot y^k \mod p)\).

Prove: It can be determined efficiently, whether \(m\) is a quadratic residue or not, using only \(g, g, p, a,\) and \(b\).
Exercise 11.4: (4 bonus points)

Construct a Zero-Knowledge-Proof based on the following problem:

**DOMINATING INDUCED MATCHING**

*Input:* Graph $G = (V, E)$ and $b, w \in \mathbb{N}$ with $b + w = |V|$.

*Question:* Is there a partition of $V$ in $w$ white vertices which form an independent set, and $b$ black vertices which induce a matching?

**Deadline:** Wednesday, January 16, 2013, 15:00, in the letterbox in front of i1.