Exercise 1

1 Protection goals:

1.1

A common scenario in which IT-Security is important is the *car-to-car* communication. What kind of benefits do you see in this technology/communication with other road users, the infrastructure or even with the driver's home?

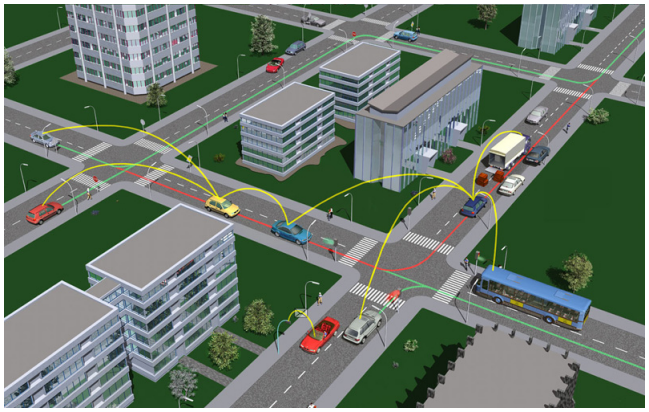

Abbildung 1: Car-to-Car communication

1.2

For each of the following protection goals describe possible effects that may occur if it is attacked in the *car-to-car* scenario.

a) Confidentiality:

b) Integrity:

c) Authenticity:

d) Accountability:

2 Shared secret

Imagine that the CEO of a nuclear power plant is the only person with the master key to shut it down in case of problems. In the company are 7 co-manager. Next week the CEO have an appointment on a very important nuclear power plant symposium on Hawaii so he decides to give each of the 7 co-manager one piece of the master key. It should be possible to reconstruct the master key with at least 3 persons. The master key is: **6**

2.1

What are the 7 points(secret pieces) for the polynomial if you use shamir's secret sharing scheme in $\mathbb{Z}$. Please use $a_1 = 5$ and $a_2 = 9$ as coefficients.

2.2

During the symposium at the beach of Hawaii the CEO get a message that something goes wrong in the power plant. Because this symposium is really very important he can't come back to solve the problem on his own. Of course he also can't send the master key because the telephone line is not secure. The next problem is that the first co-manager is sick and no. 4, 5 and 7 are not available.

The last option to avoid a big catastrophe is to reconstruct the master key with the help of co-manager no. 2, 3 and 6. Because you are the CSO it's your job to do it. Look sharp! (Use Lagrange interpolation)

3 Fair Exchange Protocols:

In the course you have seen an example for a simple fair exchange protocol.

3.1

Think about some (real world) examples for what a fair exchange protocol can be used.

3.2

What are requirements for a fair exchange protocol?

3.3

In an *optimistic* protocol you suppose that most entities are honest. The TTP intervenes only in case of problems. In the picture below you see such a optimistic contract protocol.

In this situation the protocol is fair but what happens if Alice, after sending the first message get stuck? In this case one of the requirements mentioned above is violated. Which one and how would you solve this problem?

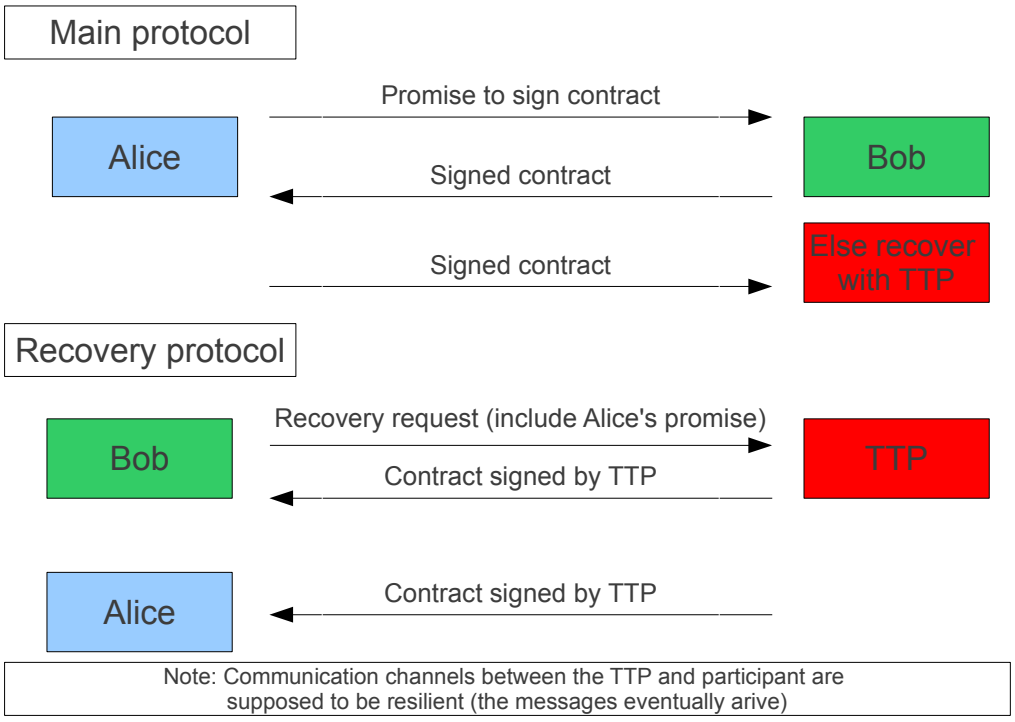

Abbildung 2: Example for a simple optimistic fair exchange protocol