Introduction to Computer Security, Exercise 1, March 22-26, 2010.

1. Assume that the national agency for medicines would like to collect information from various registers (hospital, cause of death, cancer, malformation etc registers) in order to study the side effects of medicines. The aim is to combine the information in various registers. However, the protection of privacy prevents this in Finland. How could the registers send their information to the agency in such a way that the identities are not revealed, but the agency can combine the information from the registers? The information should also be confidentially sent through the internet. You can use symmetric encryption and, if needed, hash functions.

2. There has been a lot of discussion on illegal copying and delivering of files in internet. What are the current methods to prevent this kind of activity? Suppose that the control will be increased in the future. What kind of techniques could be used to prevent copying and delivering? Are they realistic? Would it make necessary to change some laws (in Finland, in your country)?

3. What are the consequences of the following criminal acts in your country: breaking into computer systems, illegally using other people's or companies' computers, disturbing data communication? What are the laws that consider these actions?

4. There has been a lot of talk about Lex Nokia, a new law making it possible for companies to follow employers' emails. Find out some details of this law. (There should be some English material in the web.) What are the practices in your country in this respect?

5. In your country, when can the police listen to calls and data traffic, unravel the people calling to some number. What do you think, are the practices in your country fine or are some actions needed?

6. What do the following abbreviations mean and what kind of activity do they contain?

   a) OWASP

   b) GSSP

   c) CSSLP

   d) Microsoft SDL