1. Consider the concepts of C.I.A (confidentiality, integrity, availability) and A.A.A (assurance, authenticity, anonymity). With respect to the C.I.A. and A.A.A. concepts, what risks are posed by
   a) spam,
   b) computer viruses,
   c) packet sniffers, which monitor all the packets that are transmitted in a wireless Internet access point;
   d) someone burning songs from an online music store onto a CD, then ripping those songs into their MP3 player software systems and making dozens of copies of these songs for their friends;
   e) Trojan horses.

2. Suppose you could use all 128 characters in the ASCII character set in a password. What is the number of 8-character passwords that could be constructed from such a character set? How long, on average, would it take an attacker to guess such a password if he could test a password every nanosecond?

3. Consider the following method that establishes a secret session key $k$ for use by Alice and Bob. Alice and Bob already share a secret key $K_{AB}$ for encryption.

   i) Alice sends a random value $N_A$ to Bob along with her id, A.
   ii) Bob sends encrypted message $E_{K_{AB}}(N_A), N_B$, where $N_B$ is a random value chosen by Bob.
   iii) Alice sends back $E_{K_{AB}}(N_B)$.
   iv) Bob generates session key $k$ and sends $E_{K_{AB}}(k)$ to Alice.
   v) Now Alice and Bob exchange messages encrypted with the new session key $k$.

Suppose that the random values and the keys have the same number of bits. Describe a possible attack for this authentication method. Can we make the method more secure by lifting the assumption that the random values and the keys have the same number of bits? Explain.
4. Alice and Bob shared an n-bit secret key some time ago. Now they are no longer sure they still have the same key. Thus, they use the following method to communicate with each other over an insecure channel to verify that the key $K_A$ held by Alice is the same as the key $K_B$ held by Bob. Their goal is to prevent an attacker from learning the secret key.

i) Alice generates a random n-bit value $R$.

ii) Alice computes $X = K_A \oplus R$, where $\oplus$ denotes the exclusive-or boolean function, and sends $X$ to Bob.

iii) Bob computes $Y = K_B \oplus X$ and sends $Y$ to Alice.

iv) Alice compares $X$ and $Y$. If they are the same, she concludes that $K_A = K_B$.

Show how an attacker eavesdropping the channel can gain possession of the shared secret key.

5. 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 from 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.

6. Consider the ten principles of a secure design. These principles are old. Is there a need to update the principles by dropping some out, to add some new or to modify some? Discuss.