Exercises, set 1

Computer Security

- You do not have to hand this in. You can completely ignore these exercises if you wish.
- These exercises are given for you to check your knowledge during the course.
- These exercises are based on material in Chapter 2, 3 and 14. Some exercises may require you to look for information outside the textbook as well.
- Exam questions can be based on some or none of the exercises.
- The teachers are happy to help you out if you run into problems.

Exercise 1.1

Medical records pose particular security problems. Assume that your medical records can be accessed on-line. On one hand, this information is sensitive and should be protected from disclosure. On the other hand, in an emergency it is highly desirable that whoever treats you have access to your record. How would you use prevention, detection, and recovery to secure your records?

Exercise 1.2

The birthday paradox can be used in hash function attacks.
a) Explain how you could use a birthday attack to claim that a victim has signed a contract he has not signed. In other words, you let the victim sign a seemingly "good" document, and later you claim that he has actually signed another, "evil", document.
b) How many contracts do you have to create according to the birthday paradox if the hash function used is SHA-1?

Exercise 1.3

Show with an example how the DSA algorithm works. To simplify your calculations, select q and p such that $20 < q < p < 100$. Create a public and a private key, sign a message m and check the signature using the public key. Assume $h(m) = 11$. (You are not required to know DSA by heart in the course.)

Exercise 1.4

Encrypting an entire message with a private RSA component does not create a digital signature. Explain how, and to which extent, an attacker could forge signatures if there is no redundancy check, e.g. hash value, on the message that has been signed.

Exercise 1.5

a) What are the problems with the electronic code book (ECB) mode of operation for block ciphers?
b) How are these problems dealt with in cipher block chaining (CBC)?
c) Describe counter mode.

Exercise 1.6

Someone has invented a new brilliant way to send messages securely over an insecure channel. This person has read about how to send a box securely between Alice and Bob. The new idea is based on the fact that the same thing can be done with a one-time-pad. Assume that Alice and Bob each have a secret random string, denoted S_A and S_B respectively. The protocol is as follows:

1. Alice encrypts the message using her string S_A, and sends it to Bob.
2. Bob encrypts the received string using S_B, and sends it back to Alice.
3. Alice decrypts the received string using S_A, and sends it to Bob.
4. Bob decrypts the received string using S_B, and obtains the message.

Encryption and decryption uses simple xor of the two strings. Is this a good protocol?

Exercise 1.7

In RSA encryption, choose the two primes p and q as $p = 11, q = 17$. Let the public encryption exponent be chosen as $e = 9$.
a) Compute the private decryption exponent d.
b) Encrypt the message $m = 14$.

Exercise 1.8

Compare a MAC value and a hash value as a means of providing integrity protection for a message sent over an insecure channel.

Exercise 1.9

Assume that a hash function constructed using Merkle-Damgård is used as a MAC. Show that the construction $h(k||x)$ is insecure, where k is the secret key, x is the message and $\|$ denotes concatenation of strings.