IDATT2503 - Kryptografi - Høst 2022

Extra Assignment/practice problems

Exercise 1

- What does Kerchoffs principle (the one we have covered) say? Why is it an important principle?
- What in general is a good approach to develop a secure cryptographic algorithm? Give an example of "good" and "less good" examples in this respect.

Exercise 2

a) Explain in general what a "mode of operations" are for block ciphers.

b) What is a basic difference between CBC and CTR modes?

Exercise 3

a) The security of cryptographic hash functions can be described as the hardness of three "problems". What are these?

b) You are given the following attampt at a hash function:

Split the cipher into equal length blocks, bitwise XOR all the blocks. Pad the message with the pattern 010101... so that the message is equal to a whole multiple of the block length.

Assess the security of this hash function considering the criteria in part a)

Exercise 4

Give the most important differences between a public key and a private key cryptosystem.

Exercise 5

1. What can we say about perfect secrecy and key size compared to message size?
2. What is the One Time Pad, and why is it called that?
3. What type of cipher is an approximation to the One Time Pad?

Exercise 6

Consider affine ciphers on the message and cipher space $\mathcal{P} = \mathcal{C} = \mathbf{Z}_{32}$, where encryption with a key (a, b) is given by the formula

$$\mathcal{E}(x) = ax + b \mod 32,$$

a) Why is $(14, 4)$ not a valid key in this setup?

b) Encrypt $x = (10\ 11\ 20)$ (three blocks) in ECB mode, with the key $(5, 11)$

c) Encrypt the same message in CBC mode, with same key, and use IV = 17. (Use bitwise xor)

d) What is a serious weakness of the affine cipher, even if we used very large blocks, using for example 512 bits for a and b?

Exercise 7

Consider the following security goals:

1. Integrity
2. Secrecy
3. Autheticity
4. Non-repudiation

a) Which of the security goals are achieved by

   1. A Message Authentication Code?
   2. A digital signature?