# 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.

### Løsningsforslag

- Only the key should be taken as secret, not the algorithm, when considering the security. This is because its much easier to change key if compromised, than to change the algorithm.
- The design and analysis of a cryptographic system should be developed openly, so that it can be scrutinized and tested by so many as possible. This will make it more probable that any weaknesses are exposed, and also that there will be a general trust that the algorithms are secure. AES was developed in this way, while DES was not.

### 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?

### Løsningsforslag

a) Modes of operations are used to increase the security of a block cipher, by extending diffusion between blocks. In ECB mode, encryption of a block will always be the same with the same key. THis is avoided by modes such as CBC mode.

b) CBC mode encrypts the actual message, while CTR mode encrypts a nonce together with a counter, which generates a key stream to be used as a stream cipher, xor-ing the keystream with the message.

### 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)

**Løsningsforslag**

a) Pre-image resistance: Given hash tag $y$, find som $x$ that has $y$ as hash. Second pre-image resistance: Given $x$ and its hash tag $y$, find another $x'$ with same hash tag. Collision resistance: Find any two $x$ and $x'$ with equal hashes.

b) This is not resistant to any of the attacks: Pre-image: A message with length equal to block length is its own hash, so its trivial to find a pre-image. Second pre-image: Simply append a block of zeros, or flip any two bits in two blocks that are in same position relative to block length. If we can solve second pre-image, we have also solved collision problem.

### Exercise 4

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

**Løsningsforslag**

- Public key system uses two related but different keys for encryption and decryption, while private key uses same key.
- No secret information needs to be shared beforehand in a public key system, while this is required for private key systems.
- Private key systems are in general much more computationally efficient than public key systems.
- Public keys are usually used to exchange limited information, for example keys or certificates, while private systems are used for bulk encryption, due to its computational efficiency.
- A public system can only be computationally secure, since there is no real secret: The private key can with enough computational resources, be calculated from public key, without use of any use plaintexts or ciphertexts. For private key systems, there is really a secret, and can only be attacked by getting some informaton (ciphertexts, known plaintexts, etc)

### 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?

**Løsningsforslag**

1. A system can only be perfectly secure if the key is at least as long as the message it encrypts.
2. It is the encryption of a message by XOR-ing it with at randomly generated key, of equal length as the (binary) message. It is called One Time Pad, since it is only perfectly secure if the key is used used once.

3. A stream cipher is an approximation to the One time pad. From a master key, it generates a pseudo-random keystream, that is then XOR'ed with the message.

**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 $b$?

**Løsningsforslag**

a) Encryption has to be invertible. $\gcd(14, 32) = 2$, so 14 is not relative prime to 32. It does not have a mulitplicative inverse modulo 32, so the encryptions has no inverse (we cannot invert the formula). For example, adding 16 to a message does not change its encryption:

$$14(x + 16) \equiv 14x + 14 \cdot 16 \equiv 14x + 7 \cdot 32 \equiv 14x \mod 32$$

b) We encrypt each block separately, and concatenate the results:

$$e(10) \equiv 61 \equiv 29,\ e(11) \equiv 2,\ e(20) \equiv 15, \quad \text{all modoulo } 32$$

c)
$$e(10 \oplus 17) = e(27) \equiv 18,\ e(11 \oplus 18) = e(25) \equiv 8,\ e(20 \oplus 8) = e(28) \equiv 23$$

d) A legal key is $(a, b)$ where $0 \leq a, b < 2^{512}$, with $a$ an odd number. This gives essentially a 1023-bit long key. This prevents brute force attacks, and frequency analysis in only cipher-text attacks is also hard. However, one needs in general only two known plaintext-ciphertext pairs to find the key, and break the cipher completely. This is because we get two *linear* equations in the two unknowns $a$ and $b$, which we can solve.

**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?

**Løsningsforslag**

a)
   1. With a Message Authentication Code one achieves: Integrity and authenticity.
   2. With a digital signature one achieves: Integrity, authenticity and non-repudiation.

   Note that secrecy is not the purpose of a MAC or signature, but of course can be combined with such.