Cryptography, winter 2006

PROF. DR. WERNER SCHINDLER, DIPL.-INF. DANIEL LOEBENBERGER

4. Exercise sheet (29.11.2006)
Hand in solutions to the homework exercises on Wednesday, December 20th, in the tutorial/the lecture.

Exercise 4.1 (Repetition: Power of 3).

Compute $3^{1\,000\,003} \bmod 101$ *by hand.* Note*: Only a small calculation is needed!*

Exercise 4.2 (Perfect secrecy).

In this exercise we study the impact of non-uniform key selection.

For this purpose consider the encryption system $y = e_k(x)$ *when* e *is the encryption function,* k *is the encryption key, that can belong to a set* $K = \{1, 2, 3, 4\}$*. The plain text* x *and the cipher text* y *belong both to same set* $P = C = \{a, b, c, d\}$*. We express mapping rule with a table as follows:*

	a	b	c	d
1	b	c	d	a
2	c	d	a	b
3	d	a	b	c
4	a	b	c	d

This means, for instance, that key 1 maps the character a to b while key 4 induces the identity mapping.

Suppose that the character a *appears as plain text with probability* $1/2$*, that is* $\text{prob}(\mathcal{P} = a) = 1/2$*. Suppose further that* $\text{prob}(\mathcal{P} = b) = 1/4$*,* $\text{prob}(\mathcal{P} = c) = 1/8$*,* $\text{prob}(\mathcal{P} = d) = 1/8$*. The key is selected independently from the plaintext.*

(i) Show the identity

$$\text{prob}(\mathcal{C} = y) = \sum_{x, e_k(x) = y} \text{prob}(\mathcal{P} = x) \cdot \text{prob}(\mathcal{K} = k).$$

(ii) Suppose $\text{prob}(\mathcal{K} = 1) = 1/3$*,* $\text{prob}(\mathcal{K} = 2) = 1/3$*,* $\text{prob}(\mathcal{K} = 3) = 1/3$*,* $\text{prob}(\mathcal{K} = 4) = 0$*.*

  (a) For each of characters a*,* b*,* c*,* d *compute probability of observing them as output.*

  (b) Compute conditional probability $\text{prob}\,(\mathcal{P} = x \,|\, \mathcal{C} = y)$ *that the plain text was* x *if we observe the cypher text* y *for each* $x \in \{a, b, c, d\}$*,* $y \in \{a, b, c, d\}$*.*

(iii) *Suppose* $\text{prob}(\mathcal{K} = 1) = 1/4$, $\text{prob}(\mathcal{K} = 2) = 1/4$, $\text{prob}(\mathcal{K} = 3) = 1/4$, $\text{prob}(\mathcal{K} = 4) = 1/4$. *Do the same as in (ii).*

(iv) *Which of these key schedules is better for a one-time pad system?*

Exercise 4.3 (Homework: Retail-CBC-MAC). (7 points)

7 Suppose that the CBC-MAC is combined with CBC encryption with IV $= 0$. Consider the following attack (taken from the lecture): For $k_1 = k_2 = k$ we have $\text{MAC}(p_1, p_2, \ldots, p_t, k) = \text{Enc}(c_{t-1} \oplus p_t, k) = c_t$. If the adversary alters any blocks c_j for $j < t - 1$ the CBC-MAC remains unchanged. The receiver will presumably not detect the loss of integrity.
Show that this attack also works against the strengthened CBC-MAC (Retail-CBC-MAC) if its first key k coincides with the encryption key.

Exercise 4.4 (Homework: Modes of operation). (13 points)

4 (i) Discuss advantages and disadvantages of each of the modes of operation presented in class: ECB (Electronic Codebook), CBC (Cipher Block Chaining), CFB (Cipher Feedback), OFB (Output Feedback), CTR (Counter).

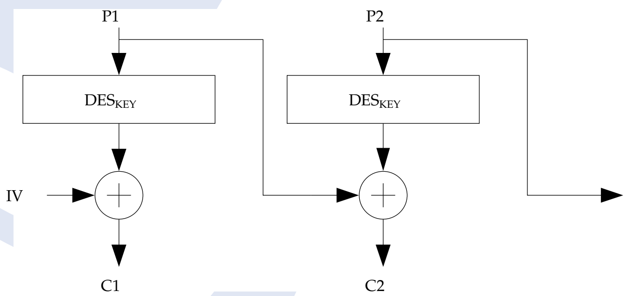
(ii) Answer the following questions concerning error propagation for each of the aforementioned modes.

3 (a) How many text blocks are false if one of the transmitted blocks is corrupted?

3 (b) How many text blocks are false if one of the transmitted blocks is dropped unnoticedly?

Try to draw conclusions from your observations.

3 (iii) We define a further mode PBC (Plain Block Chaining) that adds the message P_i to the encrypted message C_i as depicted in the following diagram.



Answer the questions under (ii) also for this mode.