Homework 1 for 01410, 2021 (10 points)

Exercise 1.1 (3 points)
Consider CipherTwo from Figure 11.3 in the lecture notes. Let there be given the following pairs of messages and ciphertexts (m, c): $(0, e), (f, 9), (3, 6), (c, a), (2, 7), (d, b)$ all encrypted with the same secret key consisting of k_0, k_1 and k_2 (four bits each). Find the values of k_0, k_1 and k_2 used in the encryption using differential cryptanalysis. (Hint: use the characteristic $\mathtt{f} \rightarrow \mathtt{d}$ through the S-box).

Exercise 1.2 (4 points)
Consider CipherThree from Figure 11.4 in the lecture notes. Let there be given the following pairs of messages and ciphertexts:

Message	Ciphertext
0	1
1	d
2	8
3	a
4	4
5	3
6	0
7	2
8	f
9	6
a	e
b	c
c	5
d	b
e	7
f	9

all encrypted with the same secret key consisting of k_0, k_1, k_2 and k_3 (four bits each). Use differential cryptanalysis and the characteristic $\mathtt{f} \rightarrow \mathtt{d} \rightarrow \mathtt{c}$ of probability about 1/4 to find k_3.

Exercise 1.3 (3 points)
Consider again CipherThree. Find the best 2-round differential characteristics for this cipher.

What you should do

- Write the solutions to the exercises in one document.
- Upload your document via the "Assignments" link (DK: "Opgaver") on inside.
- Deadline: see course page on DTU Learn.
- You may work in groups of at most two students.
- The format of your document should be PDF.