Cryptography module, Exercises 1 (unassessed)

You can submit your answers on Canvas and get feedback about your work. To do this, you must type your answers in a word processing system, and create a PDF. We will not accept handwritten and scanned or photographed answers. The deadline (if you want to get comments) is 16 October 2019 at 17:00.

Extra incentive: there is a prize for the person that gets the top mark!

1. As you know, the columnar transposition cipher is weak, because you can exhaustively try all the keys. Find the plaintext for the the following ciphertext encrypted with the columnar transposition cipher:

   AVUEVLETSEISBNACBOOLEOBTILBDLCOBOOE

2. Assume a simple two-round Feistel block cipher with an 8 bit key and a 16 bit block size. We write the key as a decimal number (from 0 to 255) and the input as two decimal numbers (also from 0 to 255). The key derivation is defined as $K_i = K + 75 * i \pmod{256}$, where $0 \leq i \leq 1$. The Feistel function is $f(K_i, R_i) = 127 * (K_i + R_i) \pmod{256}$ where R_i is the decimal representation of the right 8 bits of the input block. Encrypt the message $(86, 83)$ with the key 89.

3. What is the output of the first round of the DES algorithm when the plaintext and the key are both all zeros?

4. Remember that it is desirable for good block ciphers that a change in one input bit affects many output bits, a property that is called *diffusion* or *avalanche effect*. We will try to get a feeling for the avalanche property of DES. Let x be all zeros (0x0000000000000000) and y be all zeros except 1 in the 13th bit (0x0008000000000000). Let the key be all zeros.

   After just one round, how many bits in the block are different when x is the input, compared to when y is the input? What about after two rounds? Three? Four?

   (For this exercise, you might like to search for an implementation of DES on the web, and download it and modify it to output the answers.)