Exercise on Differential Cryptanalysis

The goal of this exercise is to code, using the MATLAB environment[1], two differential cryptanalysis attacks on reduced-round lightweight block ciphers.

- The provided code (`differential_cryptanalysis.zip`) demonstrates how to attack the toy ciphers CipherOne and CipherTwo, using the files in folders `dc_cipherone` and `dc_cipherone`. Both attacks are implemented in the respective `main.m` files.
- The provided code (`differential_cryptanalysis.zip`) also contains skeleton code that hints how to attack ciphers CipherThree and CipherFour in folders `exercise_dc_cipherthree` and `exercise_dc_cipherfour`.

▶ Write code in `exercise_dc_cipherthree\main.m` that recovers the nibble-sized (4-bit) key k_3 used in CipherThree, by utilizing an appropriate differential characteristic

▶ Write code in `exercise_dc_cipherfour\main.m` that recovers the the 3rd nibble of 16-bit key k_6 used in CipherFour, by utilizing an appropriate differential characteristic

▶ You can use the code that implements CipherThree (`cipher_three.m`), CipherFour (`cipher_four.m`) and the sbox inversion (`inv_sbox.m`) included in the folders

Deliverables: The MATLAB code and all related files that you used to perform the DC attack on CipherThree and CipherFour.

[1] check https://datanose.nl/#byod to use the UvA MATLAB licence