Exercise on Differential Fault Analysis

The goal of this exercise is to code, using the MATLAB environment[1], a differential fault analysis on the DES cipher.

- The provided file (`exercise_dfa.zip`) contains the dataset `assignment_dfa.mat` that contains 10 pairs of fault-free and faulted ciphertexts. Every ciphertext is stored in binary form. The correct key of DES in round 16 is also included.
- The provided file contains skeleton code on `main.m` that hints how to perform DFA on DES.
- The provided file contains the unimplemented functions of DES that will be needed to perform DFA.

▶ Write code in `main.m` and in the unimplemented DES functions such that you recover the full 48-bit 16-round key of DES.

Deliverables: Email your code to Stefan Wijnja [s.wijnja@uva.nl] and to Daphnèe Chabal [d.n.m.s.chabal@uva.nl] with email subject: "exercise on DFA". State your name and surname in the email.

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