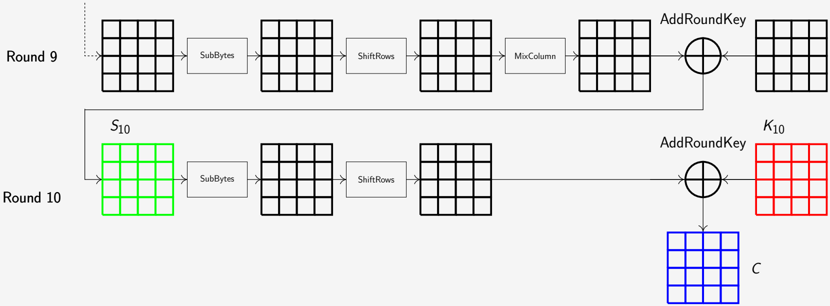
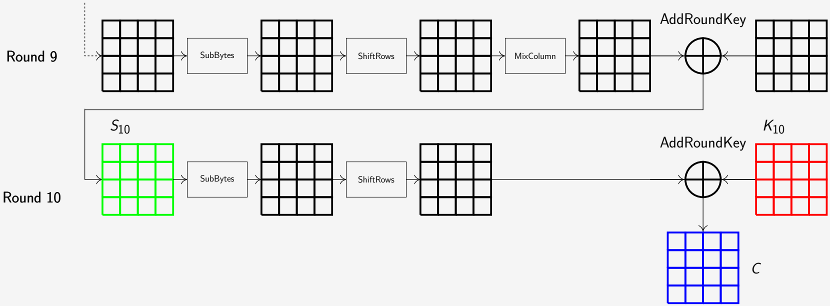
# AES-128 Assignment 3



- This time a developer left a debug option that prints out Hamming weights of bytes of the 10th round state $HW(S_{10})$ somewhere among other useless information and a ciphertext $C$. What can be wrong with that?

# AES-128 Assignment 3



- This time a developer left a debug option that prints out Hamming weights of bytes of the 10th round state $HW(S_{10})$ somewhere among other useless information and a ciphertext $C$. What can be wrong with that?
- Find $K_{10}$ and then get the master key using the provided code

# What to do: tip 1

- The only difference with the previous task is that you have more points
- Just increase iSample loop from 16 to 100 and enjoy the solution
- Am I right?

# What to do: tip 2

Sorry, no solution this time

# Thank you!

Roman Korkikian, Nicolas Oberli

Side-channels and Fault Attacks
February 23rd, 2023 - June 29th, 2023

heig-vd

HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD

www.heig-vd.ch