Homework 5: Fault Attacks - INDIVIDUAL
Due date: 04/15/2022 (Friday 2:00 PM EDT)

Overview:

In this assignment you will practice fault attacks on AES and DES using Jupyter notebooks.

Part 1: AES

1. In Prof. Debdeep Mukhopadhyay's lecture (which was recorded and is available on Brightspace/Zoom), there was a demonstration of the use of an AES fault attack Jupyter notebook. This notebook is available for use here:
    - https://colab.research.google.com/drive/1oZO8AewxKM57Kc-IA3JZToN7c-bD-edm?usp=sharing
    - Your task:
        i. Open and make a copy of this notebook to your own NYU Drive.
        ii. Try and run the code and understand how it works. Change the Notebook to encrypt different messages, using fault attacks on different bytes. Understand how to break the key.

Part 2: DES

2. Now that you understand the fault attack AES notebook, you will make your own fault attack notebook on DES using Jupyter/Google Colab. Using the methodology demonstrated in the slides and associated papers, write a notebook of similar quality to the AES notebook. Use an existing open source DES implementation, e.g. https://github.com/RobinDavid/pydes. Your Jupyter notebook should:
    - Perform a fault attack on the DES in the 15th Round
    - Include code to derive the key from ciphertexts
    - Include an explanation of the attack, with diagrams
    - Walk the user through how to use the notebook

Part 3: Thoughts?

Now that you have performed AES and DES fault attacks, write a 5-6 sentence summary about your impressions of the attacks and their usefulness. Are they a practical form of attack? What is required to perform them? Should people be worried?
Include this paragraph at the end of your notebook.

Submission:

Submit your Jupyter notebook only by:

1. Downloading a copy of it and submitting it to Brightspace, AND
2. Sharing your notebook with "hammond.pearce@nyu.edu" and "ba1283@nyu.edu"