EE576 Cybersecurity: Homework 5 (100 points)

You can team up with at most one other student in the class to complete this homework. All answers need to be properly justified by logical arguments, scholarly literature, screenshots, sample runs, and/or source codes. The report in pdf format and other relevant computer artifacts should be submitted to the course shell on Canvas.

1. (10 pts) Consider the simplified case of a dam with a single outlet valve that releases water to the pipeline that supplies a city. The valve is controlled by a computer, the operating system of which has a known vulnerability. If exploited, the vulnerability allows any user to log in as an operator of the valve. Although a patch exists, the dam's engineers have not yet installed it, because that would require shutting down the facility for a few hours. They do not think that the valve is in any danger, since the computer that controls it is not connected to anything other than the valve. Their rationale is that since the computer is not connected to the internet or any other network, it would not be possible for a hacker to damage it or hijack its control. Is their rationale valid? Why or why not?

2. (20 pts) Which of the following could be categorized as "normal accidents"? Justify your answers.
    a. The Stuxnet attack against the centrifuges in Natanz
    b. The ruptured pipeline in Bellingham, Washington
    c. The hijacked trams in Lodz, Poland
    d. The 2011 failure at the Illinois water plant

3. (20 pts) Utility meters are far from new; they have existed since the commercial exploitation of electricity took off in the late nineteenth century. Bypassing and manipulating energy meters to avoid paying for electricity has also been going on since at least the 1930s. What are the newest types of meters characterized as smart meters and why are they seen as particularly attractive targets for misuse, especially from cyber attackers? Support your answers with at least one concrete example from literature.

4. (50 pts)[1] Differential Power Analysis or DPA is a technique that exploits the dependency of the processed data on the power trace of the device to extract some secret information that would not be otherwise available. The goal of this problem is for you to develop the software (in Matlab) needed to carry out a DPA attack.

    You are provided with two sets of power-trace data. The first set is created using a known key (`00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff`) so that you can use it to test and debug your code. The second set is created using an unknown key and the objective is to find that unknown key.

    Both sets of data have three files: `plaintext.txt`, `ciphertext.txt`, and `traces-DxS.bin`. The first two files are the input and output data to the hardware AES encryption of the device. Each row corresponds to the 16 bytes plaintext/ciphertext data blocks in

[1] This lab is based on a similar exercise prepared by Jiri Bucek, Martin Novotny & Filip Stepanek

hexadecimal format. The last file is the captured power trace of the device during the encryption. It is a binary file where each byte is a measurement. The number "D" represents the number of input data blocks and the number "S" is the number of samples captured. For the known-key dataset, D=200 and S=370,000. For the unknown-key dataset, D=150 and S=550,000.

Your implementation should be based on the skeleton MATLAB functions provided. They include:

i. `measurement.m` - the code template for the key recovery process
ii. `mycorr.m` – the code template for correlation calculation during the recovery process
iii. `myin.m` - loads the content of the text files (plaintext.txt, ciphertext.txt) generated during the measurement (complete)
iv. `myload.m` - loads the content of the binary files (traces.bin) generated during the measurement (complete)

Submit the following in your writeup:

a. (5 pts) Briefly explain the key steps of DPA.
b. (30 pts) Full listing of `measurement.m` and `mycorr.m` that used to recover the unknown key. Please provide adequate comments to explain your implemention.
c. (10 pts) Demonstrate with plots on how you identify the matching samples and key for both datasets.
d. (5 pts) Discuss any challenges that you encountered in this exercise.