Faris Zahrah
Practical Cryptology
Differential Power Analysis
S181710

AES-128 allows for an attacker with access to the device implementing the encryption to observe the power that is leaked. Specifically, after the S-box substitution, the power leakage gives the attacker the information they need to deduce the key with cryptoanalysis.

The attached program uses the sample inputs sent to the AES encryption device and the power traces recorded to create a correlation table of the 256 possible key bytes. The program begins by xoring the 256 possible key bytes with the inputs0.dat file, creating a double array of 600x256 possible results. It then takes the sbox value of each of these elements and counts the number of 1 bits in this byte.

The number of 1 bits in each byte is important because this is what we use to find the correlation with the power traces we have acquired (or been given, as in the exercise). The power traces are correlated with the number of 1 bits because the bus is preset prior to being loaded with the correct btye. The more 1 bits in the byte, the more power required to set the byte, which will result in a higher power leakage in the trace files at the time the bus is set. Now that the 256x600 hamming weight table is complete, we use this to find the correlation with the trace file.

The next step is creating a table of correlations between each possible byte for every power sample at each time. I acquired the correlation double array, and **the highest correlation coefficient I received between T0.dat and Inputs0.dat was .295309 with byte 113 which is 0x71**. I tried two different versions of the correlation function just to ensure that the implementation of the correlation formula was not a bug on my part and I received the same result. Working backward to try to understand where a bug could have occurred is confusing because no operations are misleading (everything is quite straightforward and simple). I looked at the correlation array in excel and the byte 0x71 has far greater correlation than any other byte, although it still falls short of some sample correlation tables that I have seen online showing the correct byte with roughly a .9 correlation coefficient.