ECE599 - Assignment Homework 3

Opeyemi Ajibuwa

Question 1

a. Device B has higher algorithmic noise. This is because device B implements the AES with 16 S-Boxes to do a full AES round within just one clock cycle. This means that each byte in the state goes through a different S-Box during each round of AES, resulting in a higher variance (noise) for each byte value. In contrast, device A implements the AES with just a single S-Box in hardware, which means that all bytes in the state go through the same S-Box during each round, resulting in lower variance (noise) for each byte value.

b. Device B will be more difficult to attack because of the higher noise resulting from using multiple S-Boxes. This increases the complexity of the power consumption pattern and makes it more difficult for an attacker to distinguish between different values of the same byte based on power consumption. Therefore, more traces are required for a successful key extraction attack, making the attack more difficult. In contrast, device A uses the same S-Box for all bytes in the state during each round of AES, making it easier for an attacker to distinguish between different values of the same byte based on power consumption. Therefore, fewer traces are required for a successful key extraction attack, making the attack less difficult.

c. To adapt the attack on device of type B such that when attacking the first round of AES, the attack would behave similar to device of type A, we can adopt any one of the following techniques:

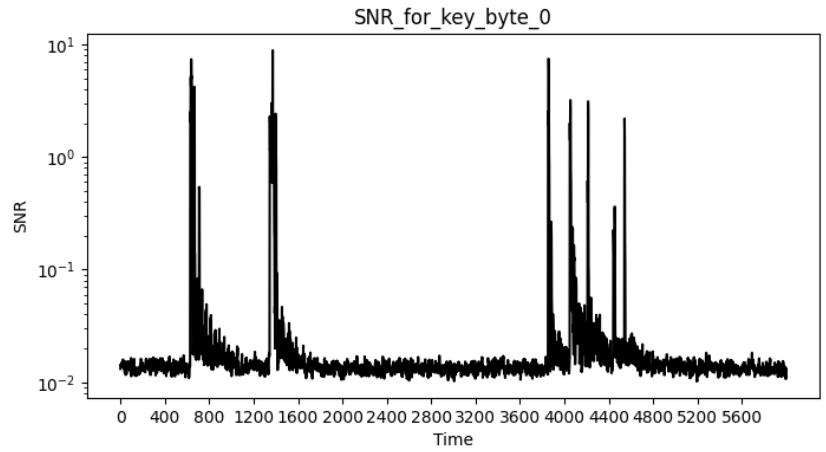
- We can carefully choose the plaintext input to force each byte in the state to go through the same S-Box during the first round of AES. This can be achieved by setting the same byte value for each byte in the state during the first round, which will cause all bytes to have the same S-Box input and, therefore, the same S-Box output. For example, suppose we want to attack the first round of AES on device B using a plaintext input of all zeros. In this case, we can force each byte in the state to go through the same S-Box by setting all bytes in the state to zero during the first round. This will cause all bytes to have the same S-Box input (i.e., zero) and, therefore, the same S-Box output. As a result, the power consumption pattern for all bytes in the state will be the same, making the attack similar to device A.

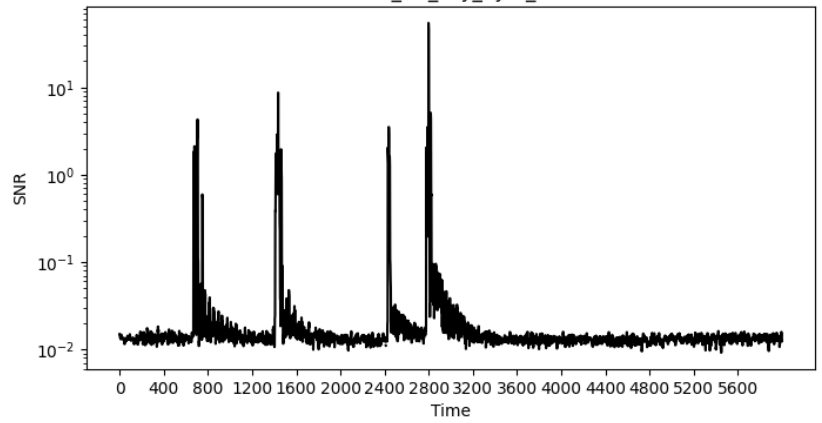
- We can also attack each byte of our plaintext individually, i.e., attack on one byte while keeping the other 15 bytes fixed (and consequently their S-Boxes idle). This way, we can collect traces only corresponding to one plaintext byte ignoring the other 15 bytes as noise to recover the keybyte for the first round. This can be repeated for all the other bytes to recover all the keys for the first round.

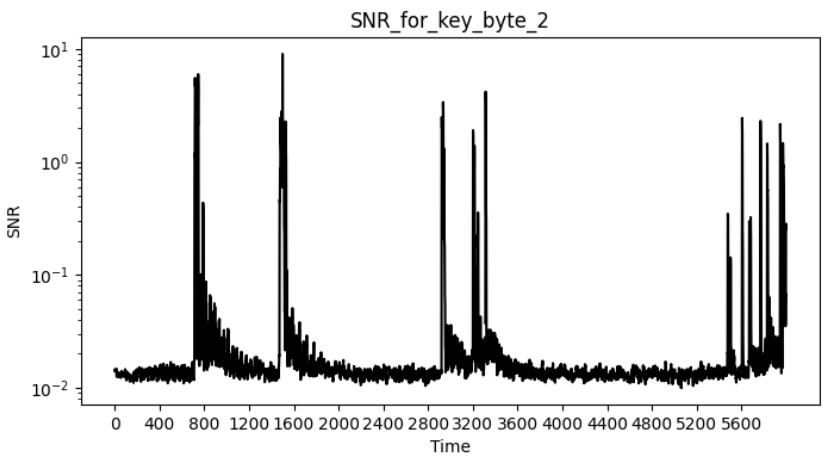
However, it is worth noting that this attack only works for the first round of AES and does not apply to subsequent rounds, as each byte in the state goes through a different S-Box during each subsequent round. Therefore, even if the attacker successfully extracts the key for the first round, the attacker needs to repeat the attack for each subsequent round of AES to extract the complete key.

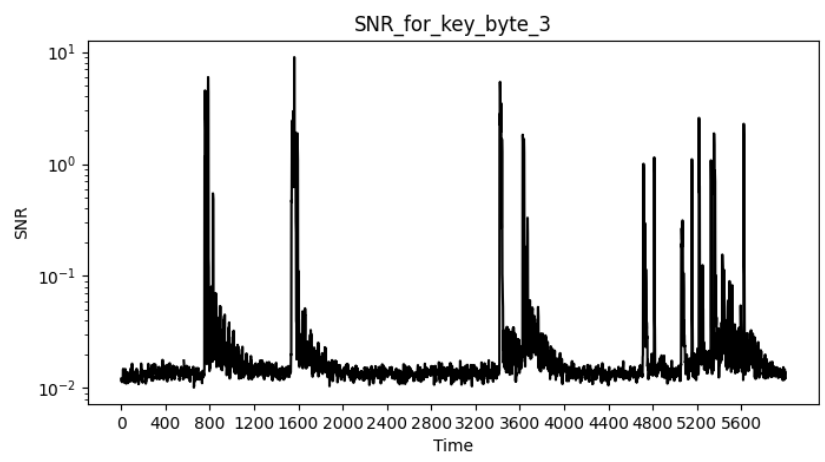
Question 2

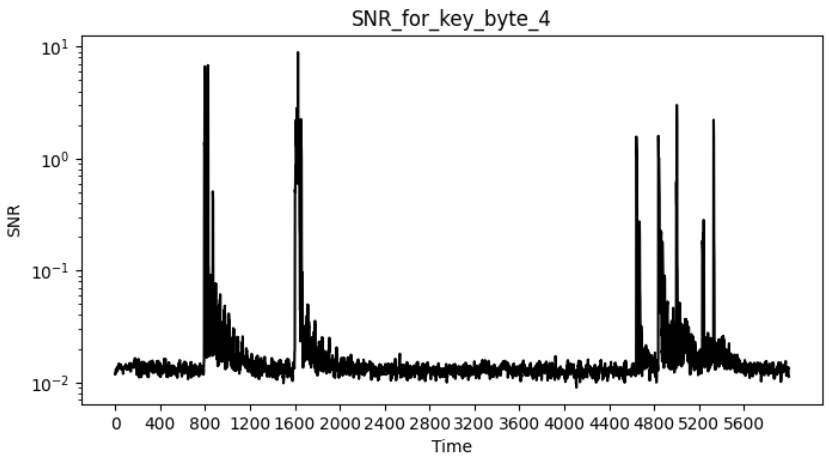
a. I narrowed the points of interest (PoI) to the regions of the highest peak for all the SNR figures of the 16 bytes.

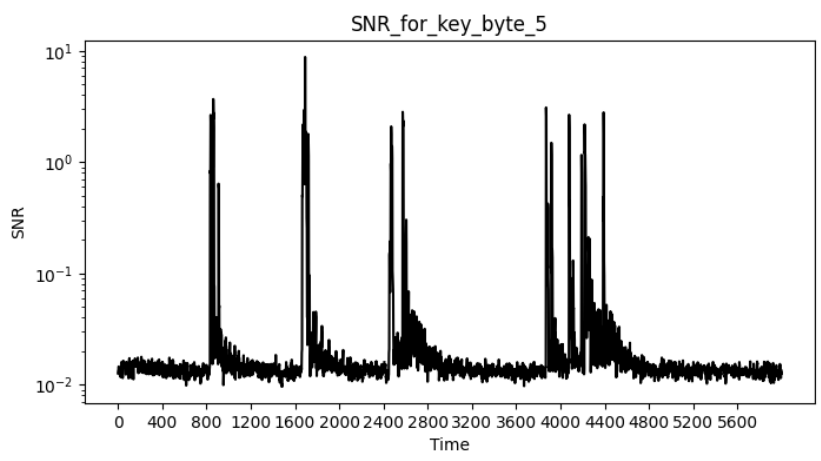


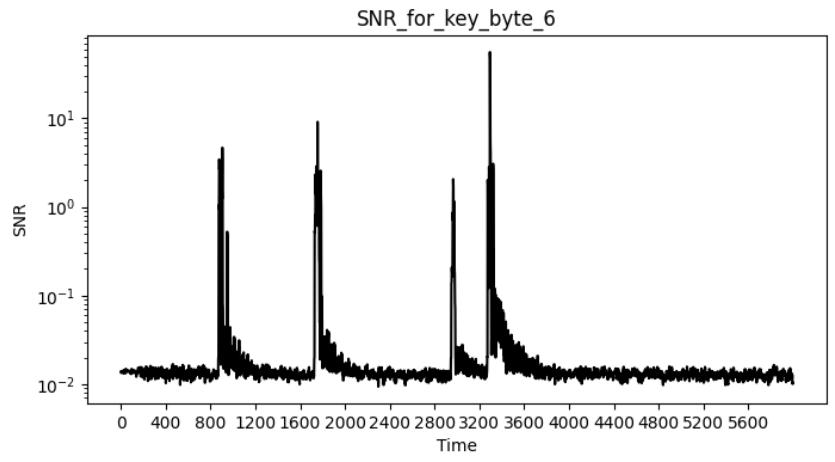


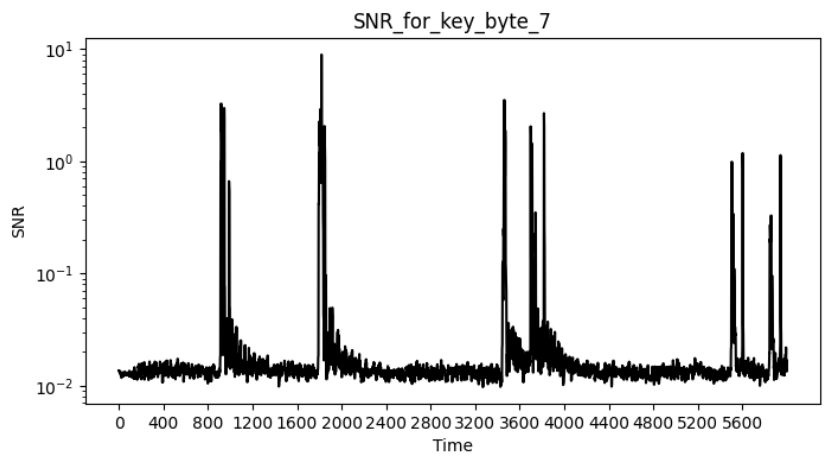


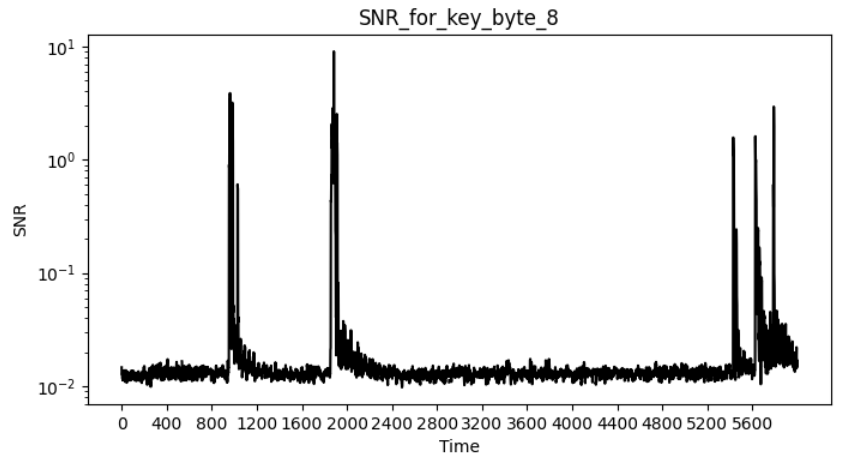


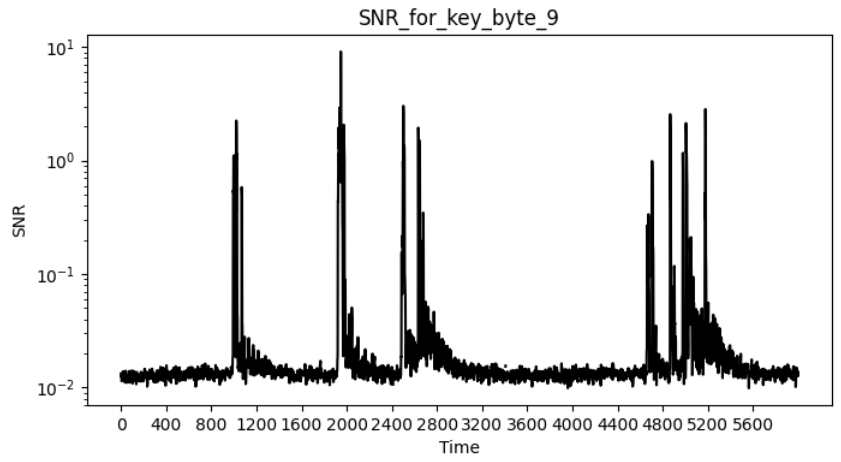


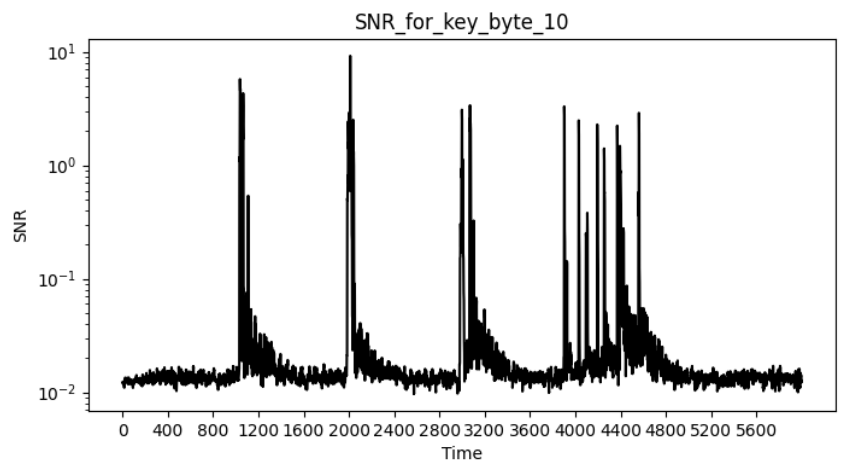


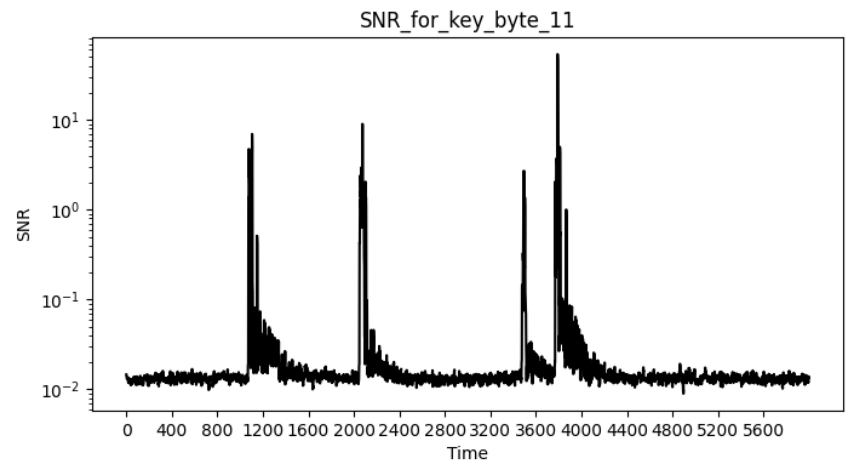

SNR_for_key_byte_6
SNR
Time

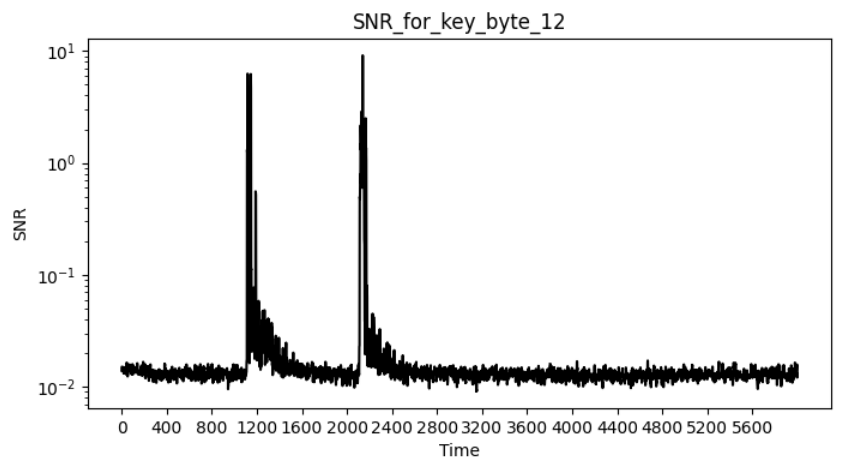

SNR_for_key_byte_7
SNR
Time

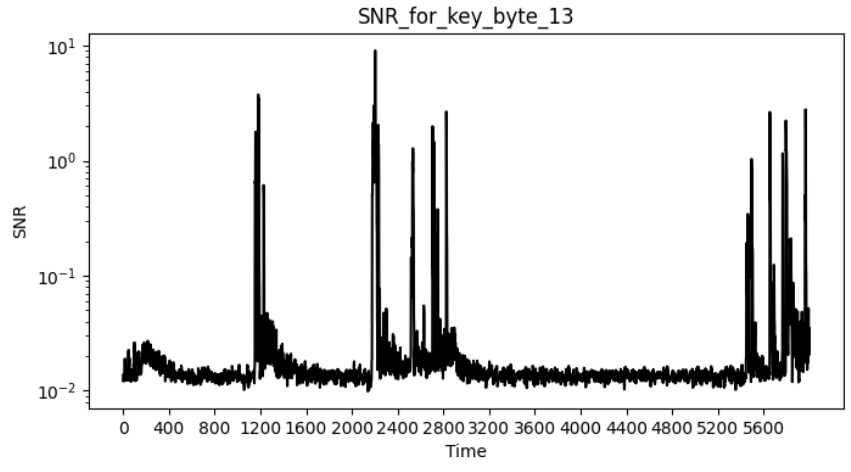

SNR_for_key_byte_8
SNR
Time

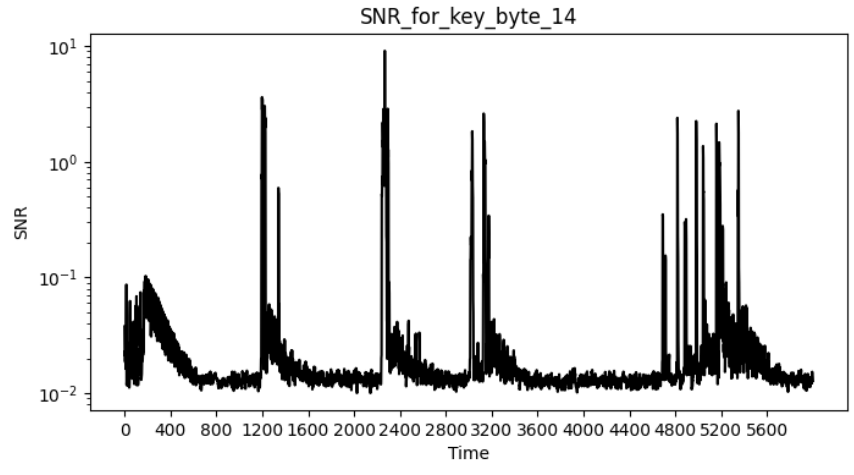

SNR_for_key_byte_9
SNR
Time

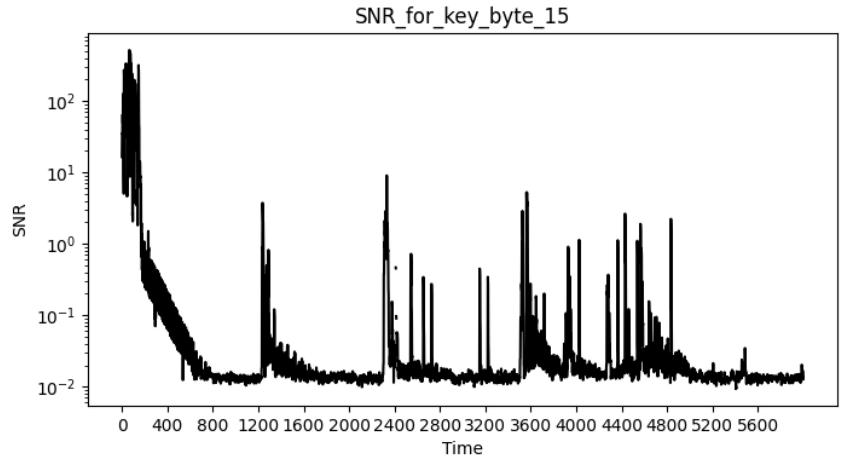

SNR_for_key_byte_10
SNR
Time


SNR_for_key_byte_11
SNR
Time

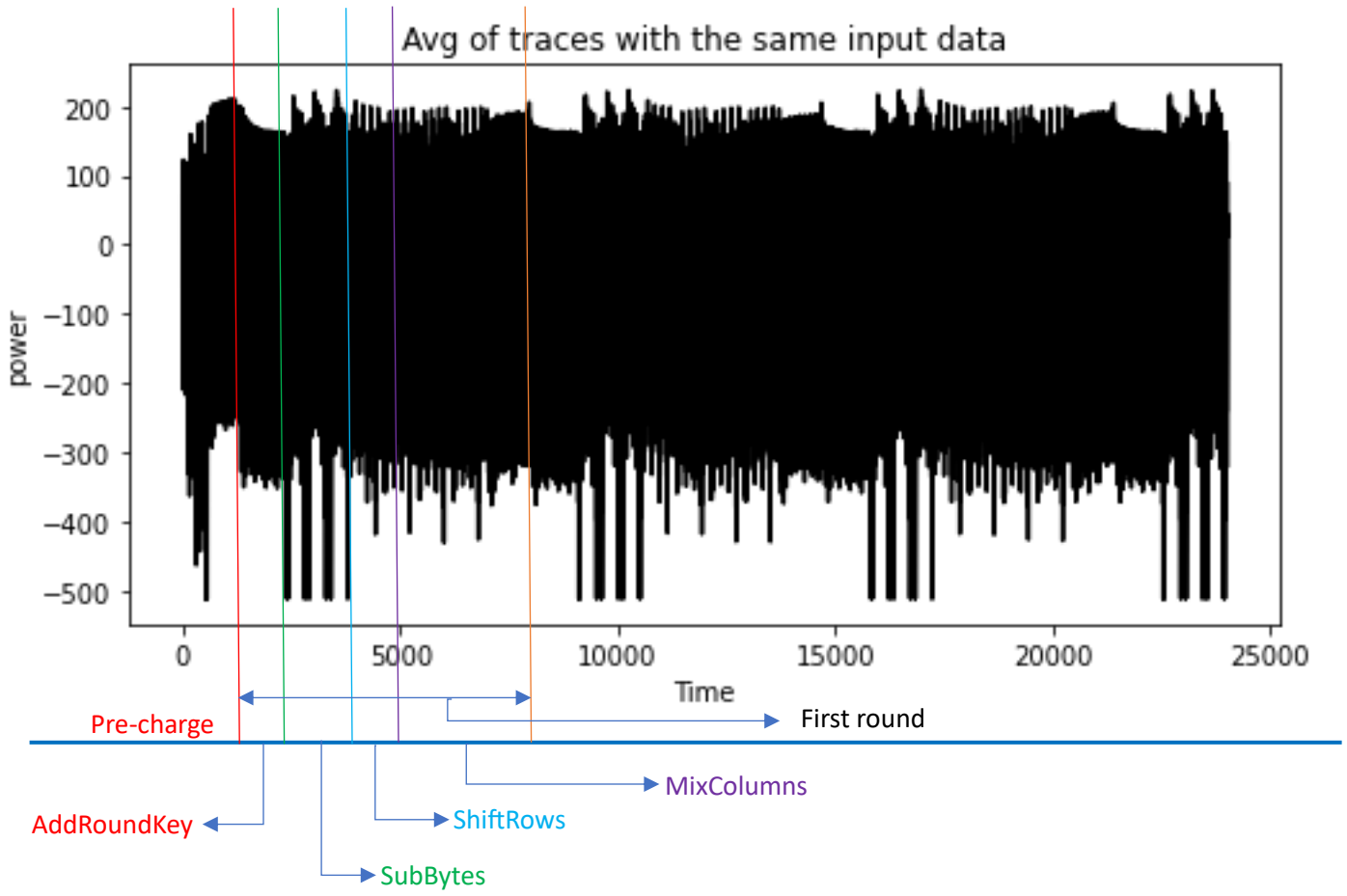

SNR_for_key_byte_12
SNR
Time


SNR_for_key_byte_13
SNR
Time


SNR_for_key_byte_14
SNR
Time

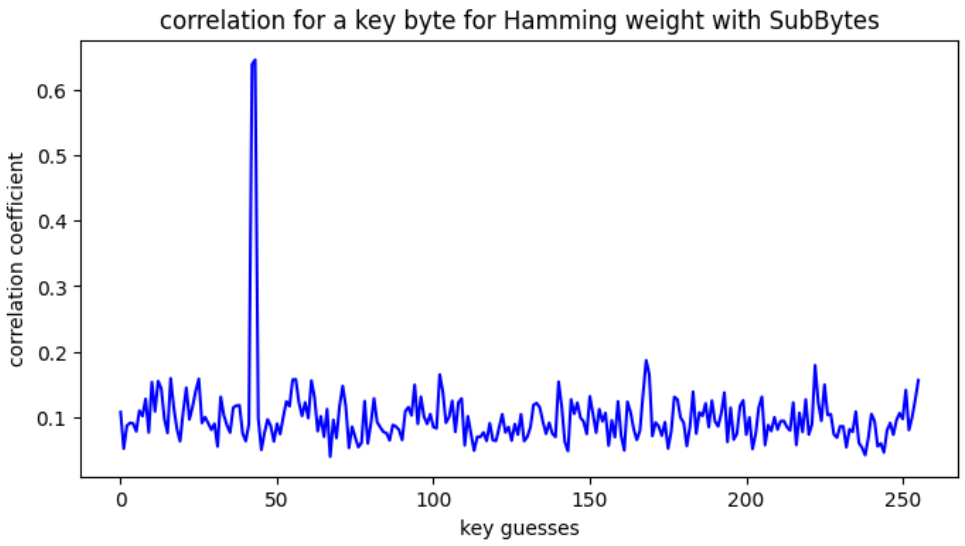

SNR_for_key_byte_15
SNR
Time

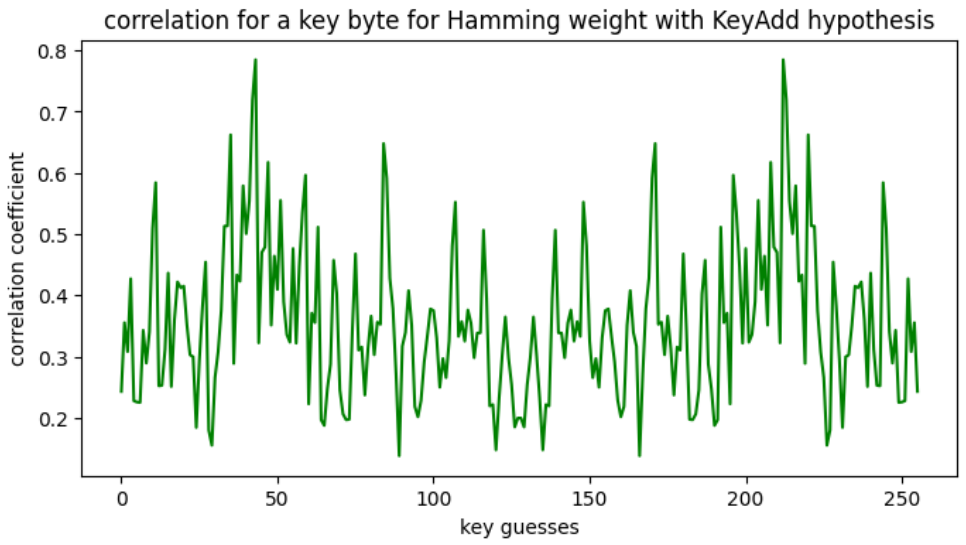
b. The plot below averages all the traces corresponding to when byte value = 0

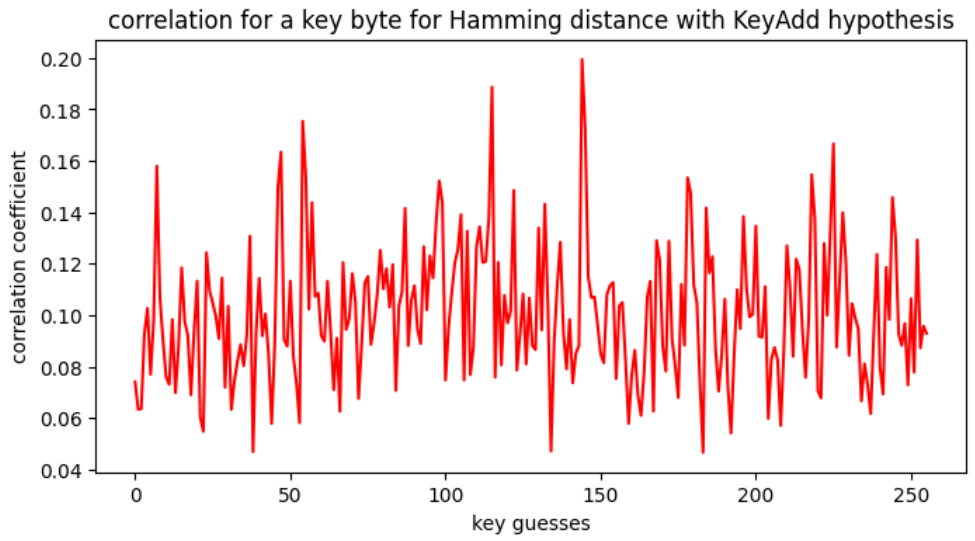


c. The correlation plots and extracted keys for different hypotheses and their respective intermediate values are presented below. Based on the plots and table, the Hamming weight hypothesis with SubBytes intermediate values appears to be the most effective. This is because a single peak corresponding to the best guessed key is expected to be present in the correlation curve for accurate key extraction. Such a peak is only observed in the correlation plots associated with the Hamming weights with SubBytes hypothesis. In contrast, the other hypotheses examined displayed multiple peaks without a clear peak. Consequently, we conclude that using the Hamming weights power model with SubBytes intermediate values is the most reliable approach for extracting the keys correctly.

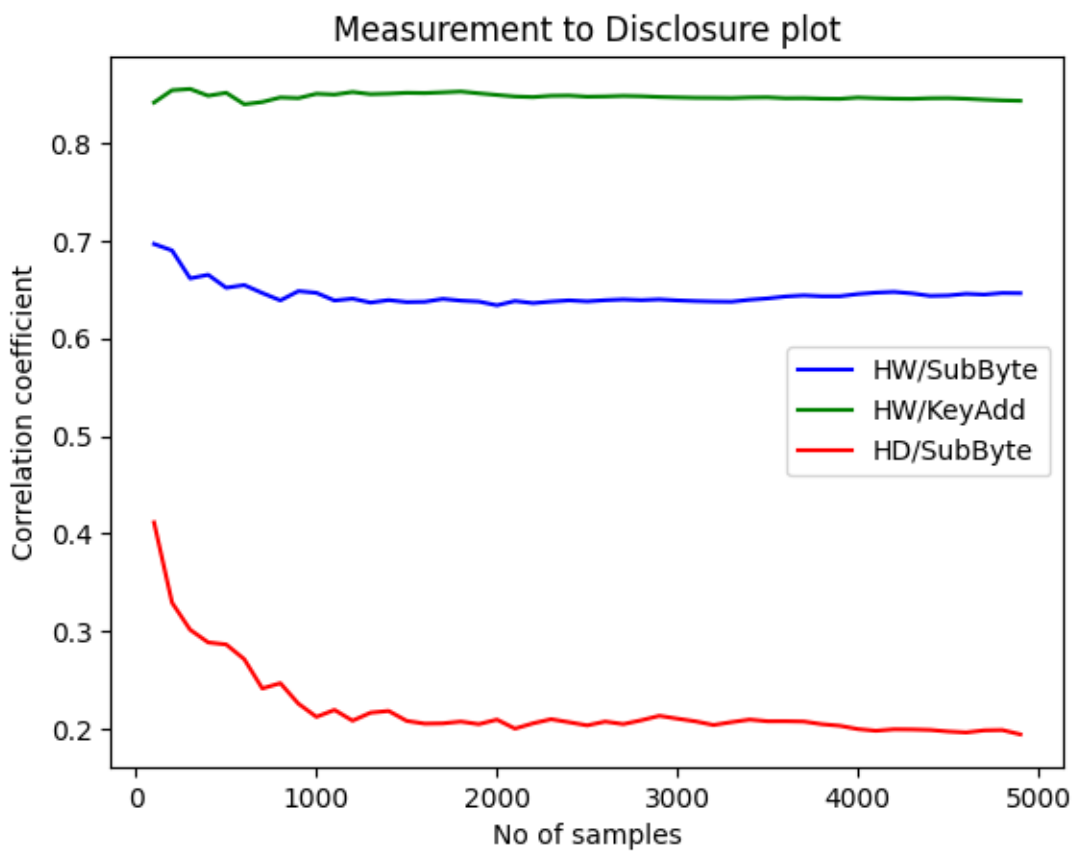
	Extracted Keys (for all 16 bytes)	**Corresponding Correlations**
Hamming Weight/Sub-Byte	43, 126, 21, 22, 40, 174, 210, 166, 170, 247, 21, 136, 9, 207, 79, 60	0.6453865771241162, 0.8535502084653921, 0.6710423206635319, 0.6760507503410397, 0.6262555091739614, 0.66895841642514, 0.8406618120987825, 0.6426888828996733, 0.6283705626632339, 0.6376922817827257, 0.6522624435573907, 0.8659636331381121, 0.6256287081699976, 0.6488194470081117, 0.7206034642781088, 0.8614645060813655
Hamming Weight/KeyAdd	43, 177, 21, 233, 215, 81, 29, 89, 84, 247, 234, 71, 9, 207, 79, 0	0.7849189798997483, 0.19118411088604684, 0.7940733202552364, 0.7625738600628336, 0.7788662710407364, 0.7392218751997908, 0.23201387235126658, 0.7306338466904104, 0.7373240212825029, 0.7161306945730432, 0.758654093830553, 0.22778067204251903, 0.75402861449555, 0.7153766513765992, 0.7937618358023023, 0.8959185570744564
Hamming Distance/Sub-Byte	144, 136, 175, 172, 147, 20, 36, 29, 16, 76, 175, 126, 179, 116, 244, 100	0.1995430120412925, 0.23974159198777964, 0.21284540288289755, 0.21232439338354317, 0.22158889961788408, 0.21032613459124222, 0.18427211957986464, 0.19085464809436603, 0.22607967655615424, 0.21010623909055773, 0.2036004930614009, 0.18501177175423247, 0.20695872423435102, 0.20356913257646206, 0.2098397463592359, 0.22963781540796144
Hamming Distance/KeyAdd	All O's for all key bytes	n/a







d. The MTD plots for all 3 valid hypotheses are shown below. I determined the minimum MTD for first two hypotheses as 100 and 300 for the third hypothesis.



Question 3

The plot below is the result of the standard Welch t-test performed on the traces. Leakages were observed across the following time instants: [**535, 543, 2915, 9619, 10099, 10115, 10519, 16735, 23539**]