CMPSC 177 Homework 1

Task 1:

1. Violation of confidentiality and source integrity
2. Violation of confidentiality, source integrity, data integrity, and availability
3. Violation of confidentiality
4. Violation of source integrity and availability
5. Violation of confidentiality and data integrity
6. Violation of source integrity, availability
7. Violation of availability
8. Violation of availability

Task 2:

1. I used a brute force attack method. I converted every letter in the string into a corresponding integer, i.e. a = 0, b = 1, etc. Then, I put those numbers into a vector in the order that they were in the string. Then, I'd take the first key value, k = 1, add it to every integer in the vector, take the modulus of the sum and 26, and then put the new integer into a new vector in the corresponding position. Then, I'd take the new vector and convert the integers back into their corresponding characters. Next, I output the resulting string. Now, I repeat this process for every possible key, from 1 - 26. Key: 15 Deciphered text: icheckeditverythoroughlysaidthecomputerandthatquitedefinitelyistheanswerithinktheproblemtobequitehonestwithyouisthatyouveneveractuallyknownwhatthequestionis
2. I did this one by hand. It took a long time. First, I copied the ciphertext onto a word doc. Then, I used the find tool to count the frequency of each letter in the alphabet. The most frequent letter was T, which I assumed translated to the most frequent letter in English: E. Then, I used the find tool to search out the most common permutation of three letters ending with T. This got me RNT. The most common word in the English language is the word 'the', so I set R as T and N as H. Once I got that, I began to look for more words that used those three letters like 'then', 'that', 'this', etc. This got me to find that Q was A, Z was S, and G was I. After that, it was just continuing to look for more possible words, made difficult by the lack of whitespaces. Cipher (Plain/Cipher): A/Q, B/U, C/O, D/W, E/T, F/H, G/I, H/N, I/G, J/-, K/S, L/D, M/K, N/E, O/J, P/X, Q/-, R/P, S/Z, T/R, U/L, V/F, W/V, X/B, Y/Y, Z/- Deciphered Text: ITISANIMPORTANTANDPOPULARFACTTHATTHINGSARENOTALWAYSWHATTHEYSEEMFORINSTANCEONTHEPLANETEARTHMANHADALWAYSASSUMEDTHATHEWASMOREINTELLIGENTTHANDOLPHINSBECAUSEHEHADACHIEVEDSOMUCHTHEWHEELNEWYORKWARSANDSOONWHILSTALLTHEDOLPHINSHADEVERDONEWASMUCKABOUTINTHEWATERHAVINGAGOODTIMEBUTCONVERSELYTHEDOLPHINSHADALWAYSBELIEVEDTHATTHEYWEREFARMOREINTELLIGENTTHANMANFORPRECISELYTHESAMEREASONSCURIOUSLYENOUGHTHEDOLPHINSHADLONGKNOWNOFTHEIMPENDINGDESTRUCTIONOFTHEPLANETEARTHANDHADMADEMANYATTEMPTSTOALERTMANKINDOFTHEDANGERBUTMOSTOFTHEIRCOMMUNICATIONSWEREMISINTERPRETEDASAMUSINGATTEMPTSTOPUNCHFOOTBALLSORWHISTLEFORTIDBITSSOTHEYEVENTUALLYGAVEUPANDLEFTTHEEARTHBYTHEIROWNMEANSSHORTLYBEFORETHEVOGONSARRIVEDTHELASTEVERDOLPHINMESSAGEWASMISINTERPRETEDASASURPRISINGLYSOPHISTICATEDATTEMPTTODOADOUBLEBACKWARDSSOMERSAULTTHROUGHAHOOPWHILSTWHISTLINGTHESTARSPANGLEDBANNERBUTINFACTTHEMESSAGEWASTHISSOLONGANDTHANKSFORALLTHEFISHINFACTTHEREWASONLYONESPECIESONTHEPLANETMOREINTELLIGENTTHANDOLPHINSANDTHEYSPENTALOTOFTHEIRTIMEINBEHAVIOURALRESEARCHLABORATORIESRUNNINGROUNDINSIDEWHEELSANDCONDUCTINGFRIGHTENINGLYELEGANTANDSUBTLEEXPERIMENTSONMANTHEFACTTHATONCEAGAINMANCOMPLETELYMISINTERPRETEDTHISRELATIONSHIPWASENTIRELYACCORDINGTOTHESECREATURESPLANS

Task 3:

1. The function table on the left adequately describes a block cipher where k = n = 2, or where a key with two bits encodes a plaintext block of two bits into a ciphertext of two bits. The first one does this as, while plaintext blocks can be encoded into the same ciphertext block by different keys, no key encodes two different plaintext blocks into the same ciphertext block. The function table on the right fails to do so, which could lead problems when trying to decode the cipher text when, as an example, decoding the ciphertext block 00 with key 11 can either lead to a plaintext block of 01 or 10, and an algorithm would have no idea which the original plaintext was.
2. In order to prove that the function , such that E'(K, X) = X for all , is a block cipher, we must first understand what the properties of block ciphers are. The simplest definition of a block cipher is a algorithm or function that takes two inputs, the key and the plaintext, and outputs a block with the same number of bits as the plaintext. As the function takes in a key of size n bits and a plaintext block of size n bits and outputs a block of ciphertext of size n bits. Despite the fact that, for all plaintext blocks X and keys K of size n bits, the output of the function is the same as the plaintext block X, by definition, E' is a block cipher.
3. Again, to prove that , which is defined as for all where comes from flipping all bits of X, is a block cipher, we must first define block ciphers. As previously stated in part b, a block cipher is a algorithm or function that takes two inputs, the key and the plaintext, and outputs a block with the same number of bits as the plaintext. Again, we have two inputs, a key and plaintext block, that each have a size of n bits. Again, the output is of length n bits, the same as the inputted plaintext block. From this information alone, we know that E'' fits the basic definition of a block cipher. What exactly the output is does not really matter here.
4. E' does not qualify as a secure block cipher regardless of the value of n, as the ciphertext it outputs is exactly the same as the inputted plaintext. The only way that E' could possible succeed in hiding the contents is through reverse psychology. E'', on the other hand, is secure, as it manages to hide the contents of the plaintext block. And it's a good cipher too, as, with the key paired to the ciphertext, the original plaintext can be retrieved in its original condition due to the nature of the XOR operation.
5. Bob's belief in the insecurity of Alice's block cipher is legitimate as there is a clear pattern in the ciphertext blocks. Just as his series of plaintexts were all the exact same series of hexidecimal numbers, except for the last digit which incremented by one, the series of ciphertexts showed that exact same pattern. For this reason, it's easy to figure out the content of other encrypted plaintexts once you know what the pattern for the key used to encrypt that plaintext was.

Task 4:

1. The value of the ciphertext outputted by AES when using my unique value of X as both the key and the plaintext is: 473e1bb10f1397562d215dd2d10ebd73
2. The plaintext M whose first byte equals 00 when encrypted with AES using my unique X as the key is: 1fd31d6070709d50fdfb82acd00c1acb. I obtained this by setting my X as the key and putting a random 16 byte hexadecimal number that started with 00 in as the ciphertext to be decrypted. The resulting plaintext was my M.
3. The key k that results in the first byte being 00 when using it to encrypt my unique X is: 1fd31d6070709d50fdfb82acd00c1a51. I found this by taking the plaintext from the previous question and randomly changing the last byte.