Trent University
COIS-FRSC 2750H WEB
Winter 2020 Assignment 1
Marked out of 30

1. [5 marks] Let's get some practice with the binary and hexadecimal number systems
    a. Convert the hex value AB40E7C into binary
    b. Convert the binary value 11101101010110111001110011100 into hex
    c. What is A43FFFD + 4 equal to (assuming hex values)?
    d. What is EB + BE equal to (assuming hex values)?
    e. What is EDCBA9 + 12345 equal to (assuming hex values)?

2. [4 marks] Now let's get some practice converting text to its hex equivalent value.
    a. Give the ASCII representation in hex for the word *Virginia*
    b. Give the ASCII representation in hex for the phrase *Frosty the Snowman!*
    c. Give the ASCII representation in hex for the phrase Born-2-Run
    d. Give the text message represented by the following hex digits
    23 47 6F 6F 64 54 69 6D 65 73 25

3. [7 marks] Let's look at an old Roman age encryption scheme. Let's say we intercepted a message from a known Celtic hacker group. We know from experience that this group uses the characters from A to Z, then a space, and then the numerals from 0 to 9 and employs a wrap around (moving left from A gives us 9). The first leading pairs of letters tell us what the substitution code is using the code phrase "Trudy Jones". For example if the first two pairs are *uy du* the code is 24 and 32. This would mean that we move the first 2 letters 4 places to the right eg. A becomes E), and then the next 3 letters 2 places to the left (eg. A becomes 8), then 4 places to the right for the next 2 characters and so on to encrypt the message.
    a. What is the message hidden in: *yu dd VJG1SLIWPVGBOXUVCVB*? Remember that you will have to reverse the algorithm (i.e. shift left first then right then left etc.) to decrypt the message.
    b. The message is actually the nickname of one of a state in the US. What is the state (give it in upper case)? What would be the encrypted version this state using the same encryption scheme as the original message?

4. [9 marks] Now let's look at a more modern symmetric encryption. Assume that the algorithm for this system is to rotate the bits in the message left 2 positions, XOR the bits with the key, and rotate the bits 4 positions to the right.
    a. A key encoded within a spam email message will be emailed to you. Please be on the lookout for this message. Once you receive the email go to http://www.spammimic.com/ and click on Decode. Cut and paste the body of your email into the Decode window and get the key. The key will be 2 hex numerals. If you do not get 2 hex numerals when you decode the message, you haven't copied the entire email message correctly. What is the key?
    b. Using the key and the above algorithm, decrypt the following name (given in hex): 4F 48 4B 12 4F 4E CA 09 0E. Remember that you will have to reverse the order and direction of operations in order to decrypt the message (i.e. start by rotating 4 positions left). What is the message?
    c. The answer to Part (b) is the nickname of a famous actor. Find (and state) the last name of this actor in upper case. Using the key and the above algorithm, encrypt the last name of this actor (in upper case) and put in hex format.

5. [5 marks] One failing of an encryption system occurs if a letter (or number) **always** encodes to the same value. Let's see how we can exploit this weakness. Let's assume that we know that the word GOOD is in this intercepted message: *XLI3KSSH3HSGXIV*. What are the encrypted values (i.e., give the mappings) of the letters G, O, D (i.e., G -> ?, O -> C, and D -> ?) and what is the encryption algorithm?

    To test your detective skills, what is the exact original message? (It's a simple cipher where a letter or number always encodes to the same value). Hint: you need to find where GOOD would appear in the encrypted message.

Upload your answers to the Assignment 1 dropbox on Blackboard by the due date. Please use PDF format for your submission (**do not** submit Word documents). For Questions 3, 4 and 5, you are REQUIRED to show your work to earn full marks.

Late assignments will be penalized 10% (3 marks in this case) a day for each day late. Assignments later than 7 days late will not be accepted.