Name : Punyaja Mishra
Student Id : 0660001

COIS-FRSC 2750H WEB
Winter 2020 Assignment 1

1. **Let's get some practice with the binary and hexadecimal number systems**
   a. **Convert the hex value AB40E7C into binary**

   Answer :

   Binary numbers are in 1 and 0. The simple way to do so is to just think, what powers of 2 will add up to give that hex value, and then write a 1 for the power used and 0 for not. That is, convert the hex value to 4 binary equivalents (2^3 2^2 2^1 2^0).

   For example, hex value =9, can be written as 8+0 = $2^3 + 2^0$, and hence 1001.
   Also, we need to keep in mind that A=10, B=11, C=12, D=13, E=14, F=15

   Thus A = 1010, B=1011, 4=0100, 0=0000, E=1110, 7=0111, C=1100

   Hence $(AB40E7C)_{16} = (1010\ 1011\ 0100\ 0000\ 1110\ 0111\ 1100)_2$

   b. **Convert the binary value 11101101010110111001110011110 0 into hex**

   Answer :

   To convert binary to hex, we group them into fours, starting from right and then in each group, multiply the binary digit to 2 to the power the place they are on (0 or 1 or 2 or 3) and then add them. And write it's hex equivalent, that is 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.
   And if there are less than 4 digits, we add 0s at the left end to get 4 digits.

   So after grouping we get from the right,
   11 1011 0101 0110 1110 0111 0011 1100
   1100 = $1*2^3 + 1*2^2 + 0*2^1 + 0*2^0 = 12 = C$
   0011 = $0*2^3 + 0*2^2 + 1*2^1 + 1*2^0 = 3$
   0111 = $0*2^3 + 1*2^2 + 1*2^1 + 1*2^0 = 7$
   1110 = $1*2^3 + 1*2^2 + 1*2^1 + 0*2^0 = 14 = E$
   0110 = $0*2^3 + 1*2^2 + 1*2^1 + 0*2^0 = 6$
   0101 = $0*2^3 + 1*2^2 + 0*2^1 + 1*2^0 = 5$
   1011 = $1*2^3 + 0*2^2 + 1*2^1 + 1*2^0 = 11 = B$
   0011 = $0*2^3 + 0*2^2 + 1*2^1 + 1*2^0 = 3$
   Now, writing the answer form bottom,

Thus, $(11101101010110111001110011110 0)_{10} = (3B56E73C)_{16}$

c. What is A43FFFD + 4 equal to (assuming hex values)?

Answer :

Hex value addition is same as normal addition, but after adding, we write its hex equivalent. So for example, if I get 10, I write A. If I get any number greater than equal to 16, I write whatever the remainder is on subtracting 16 from the number and carry over the number of 16 left. For example, 19 = 16 + 3, so I write 3 and carry over 1 (since one 16).

```
    A 4 3[1] F[1] F[1] F[1] D
             +      4
---------------------------
    A 4 4  0 0  0  1
---------------------------
```

Thus answer is A540001.

d. What is EB + BE equal to (assuming hex values)?

Answer :

Similar to question above,

```
     E[1] B    B + E = 11 + 14 = 25 = 16 + 9
    +B E       E + 1 + B = 26 = 16 + 10
---------------
     1 A 9
---------------
```

Therefore, answer is 1A9.

e. What is EDCBA9 + 12345 equal to (assuming hex values)?

Answer :

Similar as above,

```
 E D C B A 9          9 + 5 =14 = E, A +4 = 14 = E, B+3=14 = E, C+2=14 = E, D+1 = E, E=E
+  1  2 3 4 5
------------------
 E E  E  E  E  E
-----------------
```

Therefore, answer is EEEEEE

2. Now let's get some practice converting text to its hex equivalent value.

a. Give the ASCII representation in hex for the word Virginia

Answer :

We first convert the letters to ASCII values and then convert the ASCII values which are in decimal, to hex, by using the same method we did to convert hex to binary, but instead this time we consider powers of 16 instead of 2. So $65 = 64 + 0 = 16^1 * 4 + 16^0 * 1$

V =86 i=105 r=114 g=103 i=105 n=110 i=105 a=97
Converting to hex :
$86 = 16^1 * 5 + 16^0 * 6 = 56$
$105 = 16^1 * 6 + 16^0 * 9 = 69$
$114 = 16^1 * 7 + 16^0 * 2 = 72$
$103 = 16^1 * 6 + 16^0 * 7 = 67$
$105 = 16^1 * 6 + 16^0 * 9 = 69$
$110 = 16^1 * 6 + 16^0 * 14 = 6E$
$105 = 16^1 * 6 + 16^0 * 9 = 69$
$97 = 16^1 * 6 + 16^0 * 1 = 61$

Therefore, Virginia = $(56\ 69\ 72\ 67\ 69\ 6E\ 69\ 61)_{16}$

b. Give the ASCII representation in hex for the phrase Frosty the Snowman!

Answer : Similar as the question above
$F = 70 = 16^1 * 4 + 16^0 * 6 = 46$
$r = 114 = 16^1 * 7 + 16^0 * 2 = 72$
$o = 111 = 16^1 * 6 + 16^0 * 15 = 6F$
$s = 115 = 16^1 * 7 + 16^0 * 3 = 73$
$t = 116 = 16^1 * 7 + 16^0 * 4 = 74$
$y = 121 = 16^1 * 7 + 16^0 * 9 = 79$
$space = 32 = 16^1 * 2 + 16^0 * 0 = 20$
$t = 116 = 16^1 * 7 + 16^0 * 4 = 74$
$h = 104 = 16^1 * 6 + 16^0 * 8 = 68$
$e = 101 = 16^1 * 6 + 16^0 * 5 = 65$
$space = 32 = 16^1 * 2 + 16^0 * 0 = 20$
$S = 83 = 16^1 * 5 + 16^0 * 3 = 53$
$n = 110 = 16^1 * 6 + 16^0 * 14 = 6E$
$o = 111 = 16^1 * 6 + 16^0 * 15 = 6F$
$w = 119 = 16^1 * 7 + 16^0 * 7 = 77$
$m = 109 = 16^1 * 6 + 16^0 * D = 6D$
$a = 97 = 16^1 * 6 + 16^0 * 1 = 61$
$n = 110 = 16^1 * 6 + 16^0 * 14 = 6E$
$! = 33 = 16^1 * 2 + 16^0 * 1 = 21$

Therefore the hex form of Frosty the Snowman is
$(46726F7374792074686520536E6F776D616E21)_{16}$

c. Give the ASCII representation in hex for the phrase Born-2-Run

Answer :
Similarly, as above.

B= 66 = $16^1 * 4 + 16^0 * 2$ =42
o= 111 = $16^1 * 6 + 16^0 * 15$ =6F
r= 114 = $16^1 * 7 + 16^0 * 2$ =72
n= 110 = $16^1 * 6 + 16^0 * 14$ =6E
-= 45 =$16^1 * 2 + 16^0 * 13$ =2D
2= 50 = $16^1 * 3 + 16^0 * 2$ =32
-= 45 = $16^1 * 2 + 16^0 * 13$ =2D
R= 82 = $16^1 * 5 + 16^0 * 2$ =52
u= 117 = $16^1 * 7 + 16^0 * 5$ =75
n = 110 = $16^1 * 6 + 16^0 * 14$ =6E
Thus, the hex form of Born-2-Run is
$(426F726E2D322D52756E)_{16}$

d. Give the text message represented by the following hex digits 23 47 6F 6F 64 54 69 6D 65 73 25

Answer :
23 =$16^1 * 2 + 16^0 * 3$ = 35 = #
47= $16^1 * 4 + 16^0 *7$= 71 =G
6F= $16^1 * 6 + 16^0 * 15$ =111 =o
6F= $16^1 * 6 + 16^0 * 15$ =111 =o
64= $16^1 * 6 + 16^0 * 4$ =100 =d
54= $16^1 * 5 + 16^0 * 4$ =84 =T
69= $16^1 * 6 + 16^0 * 9$ =105 =i
6D= $16^1 * 6 + 16^0 * 13$ =109 =m
65= $16^1 * 6 + 16^0 * 5$ =101 =e
73= $16^1 * 7 + 16^0 * 3$ =115 =s
25= $16^1 * 2 + 16^0 * 5$ =37 =%

Therefore, the text message is
#GoodTimes%

3. 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.

Answer :

T r u d y J o n e s
0 1 2 3 4 5 6 7 8 9

ABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789

For example, on moving 2 left from V, we get a T.

Code :
yu dd VJG1SLIWPVGBOXUVCVB

Now, looking at the code
yu dd : 42 33

Algorithm : first 4 characters move 2 right, next 3 characters move 3 left
Decryption : move first 4 characters 2 left then move the next 3 characters 3 right.

Moving 2 left
V =T J=H G=E 1= space
Moving 3 right
S=V L=O I=L
Moving 2 left
W=U P=N V=T G=E
Moving 3 right
B=E O=R X= space
Moving 2 left
U=S V=T C=A V=T
Moving 3 right
B= E

Now, putting them all together,
THE VOLUNTEER STATE

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?
Answer : THE VOLUNTEER STATE is TENNESSEE in US.
Encrypting TENNESSEE would be following steps as algorithm.
First 4 characters move 2 right and then the next 3 characters move 3 left

Moving 2 right
T=V E=G N=P N=P
Moving 3 left
E=B S=P S=P
Moving 2 right

E=G E=G

Therefore, the encrypted message would be

VGPPBPPGG

4. **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?
   Answer : Key : A5 ➔ Binary – $(1010\ 0101)_2$

   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?
   Answer :
   Algorithm : Rotate the bits in the message left 2 positions, XOR the bits with key, rotate the bits 4 positions to right.

   Coded message is in hex so converting it to binary
   4F = 0100 1111
   48 = 0100 1000
   4B = 0100 1011
   12 = 0001 0010
   4F = 0100 1111
   4E = 0100 1110
   CA = 1100 1010
   09 = 0000 1001
   0E = 0000 1110

   To decode we need to do reverse steps of the algorithm. So first 4 positions to left and then XOR with key and then 2 positions to right.

   Rotating 4 position left and then XOR with key

   1111 0100 1000 0100 1011 0001 0010 0100 1111 0100 1110 1100 1010 0000 1001 0000 1110 0100
   1010 0101 1010 0101 1010 0101 1010 0101 1010 0101 1010 0101 1010 0101 1010 0101 1010 0101

   0101 0001 0010 0001 0001 0100 1000 0001 0101 0001 0100 1001 0000 0101 0011 0101 0100 0001

Rotate 2 position right and the converting the binary into hex

0101 0100 0100 1000 0100 0101 0010 0000 0101 0100 0101 0010 0100 0001 0100 1101 0101 0000
5 4 4 8 4 5 2 0 5 4 5 2 4 1 4 13=D 5 0

Hexadecimal = $(54\ 48\ 45\ 20\ 54\ 52\ 41\ 4D\ 50)_{16}$

$54 = 16^1 * 5 + 16^0 * 4 = 84 =$ T
$48 = 16^1 * 4 + 16^0 * 8 = 72 =$ H
$45 = 16^1 * 4 + 16^0 * 5 = 69 =$ E
$20 = 16^1 * 2 + 16^0 * 0 = 32 =$ space
$54 = 16^1 * 5 + 16^0 * 4 = 84 =$ T
$52 = 16^1 * 5 + 16^0 * 2 = 82 =$ R
$41 = 16^1 * 4 + 16^0 * 1 = 65 =$ A
$4D = 16^1 * 4 + 16^0 * D = 77 =$ M
$50 = 16^1 * 5 + 16^0 * 0 = 80 =$ P
Using Ascii values and hex values we convert it into text

THE TRAMP

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.
Answer : THE TRAMP is nickname of CHARLIE CHAPLIN.
Writing their ASCII values and then converting it to hex values. Then, converting it to binary numbers and using algorithm on it.

$C = 67 = 16^1 * 4 + 16^0 * 3 = 43 =$ 0100 0011
$H = 72 = 16^1 * 4 + 16^0 * 8 = 48 =$ 0100 1000
$A = 65 = 16^1 * 4 + 16^0 * 1 = 41 =$ 0100 0001
$P = 80 = 16^1 * 5 + 16^0 * 0 = 50 =$ 0101 0000
$L = 76 = 16^1 * 4 + 16^0 * 12 = 4C =$ 0100 1100
$I = 73 = 16^1 * 4 + 16^0 * 9 = 49 =$ 0100 1001
$N = 78 = 16^1 * 4 + 16^0 * 14 = 4E =$ 0100 1110

0100 0011 0100 1000 0100 0001 0101 0000 0100 1100 0100 1001 0100 1110

Shift 2 position left and then XOR with the key A5

0000 1101 0010 0001 0000 0101 0100 0001 0011 0001 0010 0101 0011 1001
1010 0101 1010 0101 1010 0101 1010 0101 1010 0101 1010 0101 1010 0101

1010 1000 1000 0100 1010 0000 1110 0100 1001 0100 1000 0000 1001 1100

Shift 4 position right and then converting it to hex value

1100 1010 1000 1000 0100 1010 0000 1110 0100 1001 0100 1000 0000 1001
12=C 10=A 8 8 4 10=A 0 14=E 4 9 4 8 0 9

Thus encrypted value is

CA884A0E494809

5. **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.

Answer :

Since, we need to find "GOOD", logically thinking, as there are 2 'O' in GOOD, thus wherever there are two same encrypted characters, that is the place for the letter 'O' and then the letters before and after the two O's are G and D.

XLI3 KSSH 3HSGXIVD
GOOD

Now trying to figure the algorithm out,

ABCDEFGHIJKLMNOPQRSTUVWXYZ ➔K is at 4 places to the right of G
ABCDEFGHIJKLMNOPQRSTUVWXYZ ➔S is at 4 places to the right of O
ABCDEFGHIJKLMNOPQRSTUVWXYZ ➔H is at 4 places to the right of D

Algorithm : shift 4 places to the right.

ABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789

Thus, we can say that since there are same algorithm, that the mapping for G, O, D would be
G→K
O→S
D→H

To Decode : shift 4 places to left

So, now decoding this,
X= T
L= H
I= E
3= space

K= G
S= O
S= O
H= D
3= space
H= D
S= O
G= C
X= T
I= E
V= R
D=9

Thus, the decoded message is
“THE GOOD DOCTER9”