In class assignment

1. Three ASCII characters are believed to have been encrypted by the same 8-bit RC4 stream producing the cipher-text bytes:

   C1 = 1 0 0 0 0 0 1 1

   C2 = 1 0 0 1 1 0 1 1

   C3 = 1 0 0 0 1 0 1 0

   If they are all assumed to be decimal digits 0 to 9 or a space as listed in table 1, what are the three digits and what is the 8-bit RC4 stream?

   Ascii table :

   0 - 0011 0000

   1 – 0011 **0001**

   2 – 0011 0010

   3 – 0011 0011

   4 – 0011 0100

   5 – 0011 0101

   6 – 0011 0110

   7 – 0011 0111

   8 – 0011 1000

   9 – 0011 1001

   Sp - 0010 0000

Solution:

C1⊕C2 = 0 0 0 1 1 0 0 0
As per ASCII code, Upper 4 bits are identical for numbers 0-9
If C1 and C2 are numbers then all of the upper 4-bits of C1⊕C2 should be 0.

Since one of the upper 4 bits of C1⊕C2 is 1, C1 (or) C2 contains a space and therefore is not a number.

C1⊕C3 = 0000 1001
Since all upper 4-bits are zeros, C1 and C3 are numbers and C2 is a space.

C2 = space = 0 0 1 0 0 0 0 0
C1⊕C2 = 0 0 0 1 1 0 0 0 => C1=0 0 1 1 1 0 0 0 = 8 in decimal
So C1 is 8 and C2 is space

Key = C1⊕8 = 1 0 0 0 0 0 1 1 + 0 0 1 1 1 0 0 0 = 1 0 1 1 1 0 1 1

C2⊕C3 = 0 0 0 1 **0 0 0 1**

The last 4 digits give us one.

Therefore,

First character ‘C1’ is 8

Second character ‘C2’ is space

Third character ‘C3’ is 1

And the key is 10111011.