4. 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? (Last yrs exam)

Solution: C1 ⊕ C2 = 0 0 0 1 1 0 0 0

Looking at ASCII table, one character has to be a 'space' (0010 0000)

(Because of the 4th bit being 1).

So the other one must be '8'.(0011 1000) , But which way round?

Is C1 the encrypted space and C2 the encrypted '8' or vice-versa?

Look at C3 to find out.

C1⊕C3 = 0000 1001

C3 is not identical to C1 or C2, so it must be a decimal digit.

'm' 0110 1101 'p' 0111 0000' '3' '0011 0011'

C1 xor C2 = 0000 0111 0000 1101 0000 0000 = E say

E xor 'the' = 0111 0011 0110 0101 0110 0101 'see'
E xor 'sex' = 0111 0100 0110 1000 0111 1000 'thx'
E xor 'mp3' = 0110 1010 0111 1110 0011 0011 'j)3'.

So C1 must be 'the' & C2 is: 'see' (or vice versa)
Key is C1 xor 'the' = 10101010 10101010 11001100
or C1 xor 'see'