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?

Sol: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)

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.

If bit 4 in C1⊕C3 is 1, C1 is a space & if bit 4 in C1⊕C3 is 0, C1 is a decimal digit.

So C1 is the ciphertext for '8' = ' 0011 1001'

Exclusive or '8' with C1 and we get the key:

C1: 1 0 0 0 0 0 1 1 '8': 0 0 1 1 1 0 0 0

C1⊕'8' = 1 0 1 1 1 0 1 1 This is the key (8-bit RC4 stream)