In class assignment

1. Two bytes are known to have been encrypted by the same 8-bit RC4 stream producing C1 = 1111 0011 and C2 = 1111 1001 respectively. The bytes are believed to be non-capitalised vowels ‘a’:61(Hex) ‘e’:65, ‘i’:69, ‘o’:6F ‘u’:75. What are they? What is the 8 bit key?

3 Two bytes are known to have been encrypted by the same 8-bit RC4 stream producing C1 = 1111 0011 and C2 = 1111 1001 respectively. The bytes are believed to be non-capitalised vowels ‘a’:61(Hex) ‘e’:65, ‘i’:69, ‘o’:6F ‘u’:75. What are they? What is the 8 bit key?

Solution: C1 xor C2 = 0000 1010

Which combination of two vowels will produce 0000 1010 ? Think!!

‘a’ 0110 0001

‘e’ 0110 0101

‘i’ 0110 1001

‘o’ 0110 1111

‘u’ 0111 0101

Cannot be ‘u’ & another & can’t be same letter, or we’d get ‘0000 0000’ .

Over to you; (answer is what a donkey says).

(Don’t forget, they can be in either order.)