March 26, 2000

More binary homework: *ALIENS!*

Due Monday, April 3

Background assumptions We imagine an alien language which has only three words:

- 40% of the words are 1111111. Abbreviate this word with **A**. It is seven bits long.
- 30% of the words are 00000. Abbreviate this word with **B**. It is five bits long.
- 30% of the words are 10101010. Abbreviate this word with **C**. It is eight bits long.

1. Decipher the following messages. That is, describe the sequence of alien words which produced them. For example, if you believe the message is $\overbrace{00000}\overbrace{1111111}\overbrace{10101010}\overbrace{10101010}$ you would report that the aliens were signalling **BACC**.

a) The aliens have xored a message with a pseudorandom bit string with about 5% 1's.

`10111 11111 11111 01010 10111 11110 01001 01010 10000 00101 01010 11111 11101`
`01110 00000 10111 11101 01010 11101 11000 00`

b) The aliens have xored a message with a pseudorandom bit string with about 10% 1's.

`10101 00001 10011 01111 00000 11111 11000 10110 10111 01010 10111 11111 11011`
`10000 11000 11010 10100 00001 11111 11111 010`

2. The aliens now xor two messages and send the resulting bitstream.

`11111 11111 00000 10111 11101 01011 01001 01000 00101 00101 00000 01010 00010`
`10101 11100 11111 11110 10101 00000 00111 11`

Reconstruct <u>both</u> messages as well as you can from this information.

3. The aliens created a pseudorandom bitstream with 50% 1's and 50% 0's, **but** they made a major error. They used the <u>same</u> stream to conceal three different messages. The concealed messages are displayed below. Decipher as much as you can of all three messages.

First message

`00100 11011 10110 10110 10101 11110 11101 11111 11110 00000 10010 01110 10110`
`00011 01111 01011 00000 10110 11000 10010 00101 1`

Second message

`00100 11001 00011 01001 11010 01110 11100 10101 01110 00011 01111 01110 11100`
`10110 00000 10100 11111 00110 11011 01111 01111 0`

Third message

`01110 01110 11100 00110 11010 01110 00011 11111 11011 01010 00111 01110 00011`
`00110 00101 11110 01010 01100 01110 00101 110`

Hint

Xor of first and second messages

`00000 00010 10101 11111 01111 10000 00001 01010 10000 00011 11101 00000 01010 10101 01111 11111`
`11111 10000 00011 11101 01010 1`

Xor of first and third messages

`01010 10101 01010 10000 01111 10000 11110 00000 00101 01010 10101 00000 10101 00101 01010 10101`
`01010 11010 10110 10111 111`

Xor of second and third messages

`01010 10111 11111 01111 00000 00000 11111 01010 10101 01001 01000 00000 11111 10000 00101 01010`
`10101 01010 10101 01010 101`