Matt Muldowney
Homework 3 due 2/19

Written Problems

Problem 1

How many different ways are there to choose the values of the 8 bytes such that the most significant bits correspond to the 8-bit ASCII code for ‘q’?

In this case, the most significant bit of each byte is fixed (so that it corresponds to the 8-bit ASCII code for ‘q’). As a result, each of the other 7 bits of each byte can take 2 values (0 or 1). Therefore, the number of different ways to choose values are:

$((2)^7)^8 = 128^8 =$ **$7.21 * 10^{16}$**

How many different ways are there to choose the values of the 8 bytes such that the least significant bits correspond to the 8-bit ASCII code for ‘q’?

The same reasoning follows:

$((2)^7)^8 = 128^8 =$ **$7.21 * 10^{16}$**

Next assume that we do require that the 8 bytes spell out something comprehensible. Discuss how your answers to the previous questions would change under this new requirement.

The ASCII code assigns 128 characters to integer values [0, 127]. This means that in this scheme, the most significant bit is always 0, because all bytes are less than 10000000. Thus, it would not be possible to hide each bit of a character, e.g. ‘q’, in the most significant bit of each byte in a steganographic sequence and also make the

sequence spell out something comprehensible (unless the character was the null character, which wouldn't make sense). As for hiding each bit of a character in the least significant bit, the choices for bytes to use in the sequence are much less, not only because each byte must start with a 0, but also because the bytes must occur in certain patterns so as to spell out something comprehensible. Moreover, the first 32 characters in the ASCII scheme are control characters and therefore unusable if trying to spell out something comprehensible, further limiting the number of different ways to choose the values of the 8 bytes.

Suppose we restrict the 8 bytes to being selected from the set of 8-bit ASCII codes for letters in the alphabet and punctuation: would it be preferable to use the most significant bits or the least significant bits for steganography?

As explained above, it would be preferable to use the least significant bit, as it would not be possible to hide the bits of a character in the most significant bit of each byte in a steganographic sequence. This is because the most significant bit of each byte, which encodes an ASCII character, must be 0.