Blake

Johnson

Homework 2

Task 1:

1. The only difference between the two cipher texts is that one of the bits has been flipped. The 131st bit has been flipped in the second cipher text. The only information we can figure out based solely on the cipher texts is their length. The difference in only 1 bit is not significant whatsoever since the encryption is randomized with a new iv each time. The length of the message is a negligible piece
2. A scenario where knowing the message length would be problematic is if you know the message could be one of three messages and two of the messages were significantly longer than the third. If a significantly shorter cipher text was received then you would know exactly which message was sent.
3. Since the 3DES encryption is only using 64 bits, the amount of messages is relatively small, and therefore the same random counter will statistically be used after 2^(64/2) blocks, whereas 256 bit AES encryption will be able to send significantly more messages before it reaches a birthday bound.

Task 2:

1. Original: FFBC1ADC607ACDDEAE7D837FA8123A3A9CFDD83A9CD55F15A8CD7F8CFA32A67B

Change:

FFBC1ADC607ACDDEAE7D837FA8123A3A9CFDD83A9CD55F15A8CD7F8CFA32A6**01**

1. Original:

FFBC1ADC607ACDDEAE7D837FA8123A3A9CFDD83A9CD55F15A8CD7F8CFA32A67B

Change:

FFBC1ADC607ACDDEAE7D837FA8123A3A9CFDD83A9CD55F15A8CD7F8CF**A030203**

Task 3: