# HW2

## Part 1 (5Pts): Symmetric Key Encryption Modes

Use the SDES calculator provided in the blackboard site to perform the following encryptions using the specified mode. Here is an example question and its answer (please follow the same format for answering):

*Encrypt 10101010010111111010101001011111 using the key 1011001101 in codebook mode. Identify the blocks of plaintext?*  
*Blocks of plaintext:*

* *b1: 10101010*
* *b2: 01011111*
* *b3: 10101010*
* *b4: 01011111*

*Ciphertext: 00110001100111010011000110011101*

1. (2pts) Encrypt 10101010 01111111 10101010 11111111 using the key 1010101010 in electronic codebook mode.
   1. Identify the blocks of plaintext?
   2. What is the ciphertext?
   3. How many bits are different between plaintext blocks 1 and 3? How many bits are different between their corresponding ciphertext blocks?
   4. How many bits are different between plaintext blocks 2 and 4? How many bits are different between their corresponding ciphertext blocks? (recall the concept of “changing one bit in plaintext changes ciphertext by half” that we talked about in class).
2. (1.5pts) Encrypt 10101010 01111111 10101010 11111111 using the key 1010101010 in CBC mode. Use IV 11000011. Use the symbol ⊕ for XOR. The calculator won’t do the XOR for you. You have to do it manually.
   1. What is the ciphertext?
   2. How many bits are different between plaintext blocks 1 and 3? How many bits are different between their corresponding ciphertext blocks now?
3. (1.5pts) Decrypt 10101010 01111111 10101010 11111111 using the key 1010101010 in counter mode. Assume the counter starts at 0 (i.e. 00000000, 00000001, and so on). Use the symbol ⊕ for XOR.
   1. What is the plaintext?
   2. If you were asked to encrypt the message (rather than decrypt it), will your answer in part (a) change? Why?

## Part2 (5pts): Hashing

Using the hash calculator at <http://www.fileformat.info/tool/hash.htm>, answer the following question:

Consider the following **Hex** message: F2. This message was sent from Bob to Alice. Along with the message, Alice received from Bob a MAC: 2BA3119C (represented in Hex as well). The MAC was calculated using the mechanism described in figure 2.5a in the book. The encryption mechanism used was the simplified DES in ECB mode and key 0001100110. The hash function used was CRC32. Is the signature of the message correct? Describe your steps clearly (use bullets to describe steps).

## Part3 (5pts): Password Cracking

Using “John the Ripper”, which is available in Kali, break the Linux shadow (password) file included with this assignment for users “root” , “john”, and “hackmeifyoucan”. You will need some dictionary files, which is also included. Describe how you broke the passwords and show a screen shot of the cracked password.

Explain the meaning of each field on both the password and shadow files. What are the differences between the different shells assigned to each user?

Which users are actually allowed to login from the console on the machine where this file resides (hint: look at the shells assigned to each account in the passwd file and what they mean)?