Block Ciphers

CIS-4040 Homework #2

Peter C. Chapin, Vermont Technical College

Due: Wednesday, September 25, 2019

Read in Chapter 2. This chapter covers cryptography. It applies for this assignment and for the next few assignments. You don't necessarily need to read the entire chapter now, but you should finish it during the next couple of weeks. Chapter 20 is more directly relevant to the material in this assignment. You should read most of that chapter over the next couple of weeks as well (you can skip the material on RC4).

1. A 128 bit key is infeasible to crack using brute force. However, the 56 bit key used by DES is now considered too small for serious security (particularly against an attacker with enough resources to build specialized, highly parallel DES decryption hardware). What is the minimum key size that you think would be currently secure against a brute force attack by all possible attackers? Justify your answer (show me some calculations). This question can't be answered precisely.

   For purposes of this question assume that specialized hardware can break an algorithm with a 56 bit key by brute force in "a few" hours. You will need to make a choice about how long you need to resist such an attack. Discuss why you made that choice.

2. Many block ciphers are structured as Feistel ciphers. What is the main advantage of this design that helps account for its popularity?

3. DES has the property that if you encrypt the bitwise complement of the plaintext using the bitwise complement of the key, the ciphertext is the bitwise complement of the original ciphertext. Why is this true? Hint: The bitwise complement of a 32-bit number, A, can be thought of as A XOR 0xFFFFFFFF. Trace through the action of the DES round function 'f' and the subkey generation steps with this in mind. Refer to slide #4 in my DES slide deck for a picture of the DES round function and subkey generation process.

   I'm looking for as specific an answer as you can find. What happens to the bit inversion as the bits are processed? Keep in mind that the S-boxes are highly non-linear. If the inputs to the S-boxes are inverted, the outputs will not be simply inverted.

4. Read about Output Feedback Mode (OFB) in Wikipedia [https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation]. Does it allow easy random access to the data? What are its error propagation characteristics? OFB mode has a security concern. What is it? HINT: What can an attacker who can modify the cipher text do?

5. Do Problem 20.12 in the text (on ciphertext stealing). The problem is on page 632 and refers to the first part of Figure 20.12 on the following page.