Block Ciphers and DES

CIS-4040 Homework #2

Peter C. Chapin, Vermont Technical College

Due: Monday, June 12, 2017

Read Chapter 4. Review relevant class slides and resources.

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. Why not? 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.

2. In the context of cryptography, what is meant by the terms "confusion" and "diffusion?"

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

4. 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.