Cryptography Comprehension Questions (part 1)

Question 1

Block ciphers can operate in either ECB mode or CBC mode.

a) Explain the difference between these two modes of operation. What extra information is required for CBC which isn't required for ECB?
CBC performs an XOR operation with the output of the previous step before encryption, as such it requires an initialisation vector. ECB encrypts block by block.
b) Construct a scenario which demonstrates the weakness of ECB mode.
ECB doesn't mask patterns, as such any constructed scenario which exploits this is an acceptable solution.
Imagine you have a text file with encrypted text in it which has salary information, if you identify a single salary, and it repeats – you know that salary for multiple people. If you happen to know which block is the salary, you could also replace that with another one.

Question 2

What are the three properties which make a hash function a cryptographic hash function, and why are they important?

All hash functions must be deterministic: The same input using the same hash function always provides the same hash value. This means the same input results in same hash so we can check integrity of data.
To be a cryptographic hash function it needs to additionally be pre-image resistant, second image resistant, and collision resistant.

Pre-image resistant: This means that given a random input, it is computationally infeasible to determine the input from the hash value alone. This effectively is a one-way function. This means it is difficult for an attacker to determine original input.
second image resistant: Given a hash value h1 it should be computationally infeasible to find a different input message which results in the same hash value h1 This means attacker can't easily find a version of input which results in the same output, hence would pass integrity check but data has been altered*
collision resistant: It should not be feasible to produce two inputs which have the same hash value as output.

Question 3

a) What form of attack can a MAC help mitigate?
Altering encrypted data in a block cipher

b) How does a MAC mitigate this?
It provides a way of checking the integrity of the data by making use of cryptographic hash functions based on secret keys and appended to the message, only those with the secret key can calculate the hash value, so if data is changed the attacker shouldn't be able to predict the altered hash value
c) Why can't we simply append a hash value to the end of the encrypted data to mitigate the attack?
Because this too could be altered to match the altered data. See the class material on MACs for further detail.

Question 4

a) Compare and contrast p-boxes and s-boxes
p-boxes provide permutation of bits, whilst s-boxes replace bits with a different set of bits. Permutation boxes can be of three different types, and the permutation box provides diffusion. Diffusion a property which means that when one bit of the plaintext changes, many bits of the ciphertext change. It obscures the relationship between the plaintext and ciphertext. S-boxes provide confusion, where each bit of ciphertext relies on multiple bits in the key. This obscures the relationship between the ciphertext and the key.

b) How does AES use p-boxes and s-boxes?
AES has several rounds which include rounds of substitution (SubBytes) and permutation (shift rows and mix columns).

Cryptography Scenario-based Questions

Question 5

Design a cipher which uses a Fiestel structure. Note it need not meet the formal requirements of a secure cipher.

This question aims to develop your understanding of the Fiestel structure. Any solution which uses the structure for encryption and defines a number of rounds, a block size (even is easiest) and a function f is acceptable. One possibility is 16 rounds, 16 bit blocks, and XOR as the function.