1. What is Fiestel structure in the context of block ciphers? Explain (5 points)

In each Fiestel round a 2n-bit block to be encrypted is split into two n-bit blocks – the right side block R and the left side block L. The operations in each Fiestel round are controlled by a round key K(i) and an F-block function F(). One of the primary motivation for using Fiestel structure is that the F-block need not be invertible.

Encryption:
\[ L(i) = R(i - 1) \]
\[ R(i - 1) = L(i - 1) \oplus F(R(i - 1), K(i)) \]

Decryption:
\[ R(i - 1) = L(i) \]
\[ L(i - 1) = R(i - 1) \oplus F(L(i), K(i)) \]

2. Illustrate how encryption and decryption are performed in CBC and CFB modes (5 points)
See slide 32 in acrypt.pdf

3. Explain the difference between pre-image resistance and collision resistance in the context of hash functions (5 points)
Pre-image resistance: Given x, y, where x = h(y), it is infeasible to find some y’ (other than y) such that x = h(y’).
Collision resistance: It is infeasible to find any x, y1, y2 such that x = h(y1) = h(y2).
The requirement of pre-image resistance is easier to meet. If we use n-bit hash function the brute force complexity for an attacker is of the order of \(2^n\). The requirement of collision resistance is harder to meet. For a n-bit hash function the brute force complexity for finding a collision is only \(2^{n/2}\).