1. Confusion and Diffusion?
2. What is difference between a block-cipher and a stream-cipher? Can a block cipher be converted to a stream cipher?
3. What is a Fiestel Structure? Why is it useful?
4. What are the different modes of block cipher operation? Why do we need them? What are some characteristics of each mode? (ECB, CTR), (CBC, CFB), (OFB)
5. What is the difference between a good cipher and a strong cipher? How can we convert a good cipher into a strong cipher? Is DES a good cipher? A strong cipher?
6. Is multiple encryption useful in all ciphers? Why or why not?
7. What is meet-in-the-middle attack
8. Explain the need for the sequence C=E.D.E(P) instead of C=E.E.E(P) in triple DES.
9. What is the difference between a hash function and a compression function?
10. What is Merkle-Damagard construction in the context of hash functions?
11. What is a HMAC? How are HMACs computed?