ECE 543 Quiz 2

Alan Palayil
A20447935
Due Date: 2/17/2023

1. Alice can utilize CBC encryption along with CBC residue to provide both confidentiality and integrity. Alice creates a random initialization vector (IV) and uses the IV and CBC encryption to encrypt the message. By utilizing CBC and the same IV to encrypt the final block of the message, Alice calculates the CBC residue. Alice sends the recipient both the CBC-encrypted message and the CBC residue. The recipient checks the message's integrity after receiving it by recalculating the CBC residue and comparing it to the received value. The recipient uses CBC decryption using the received IV to recover the original plaintext message if the two values are identical.

2. Alice and Bob share the same key, say K_{AB}. To calculate the MAC, Alice can use a hash function like HMAC (Hash-based Message Authentication Code). The HMAC function generates a fixed-length output that can act as the MAC by taking the message and a secret key as inputs. Bob can use the same HMAC function to validate the MAC on his end when Alice shares the secret key with him. For Alice's messages to Bob, this offers both integrity protection and authentication.