Deniz Aytemiz

## ECE 5560-Assignment 2

1. **Multiple Choice**
    a. **B**
    b. **B**
    c. **C**
    d. **C**
2.

` **I.** Phone call over wireless channels requires speed and security. The mode of encryion we should select should not propagate the error when it happens since the wireless communications are very prone to single byte errors. In order not to corrupt the whole block of data the error should not propagate. Also since it is a phone call it should work fast too. So instead of a block cipher a stream should be used. Then we can use the counter mode and AES 128. Counter mode works in parallel hence is fast and secure since it is encrypted with random blocks. However an error in plaintext can propagate. Therefore one can use the OFB mode 128 bit AES too. The error will not propagate hence it will be secure, also it is a stream cipher too. But it can be slower with respect to counter mode.

**II.** Generating random numbers requires considerable processing power. Small IoT devices have generally low processing power since they are designed for single tasks in general such as sensors etc. Hence their processing power may not be enough to undergo the process of random bit generation in many cases.