ENEE 457: Computer Systems Security
Written Homework I

1. What happens if the same IV (or ctr) is used twice—for two different encryptions—in CBC, OFB or CTR mode? What will happen if bad randomness (i.e. does not have sufficient entropy) is used for generating IV (or ctr) ?

2. Of the modes of operation that we saw (CBC, OFB, CTR), which ones allow for parallelized *encryption*? Which ones allow for parallelized *decryption*?

3. Modes of Operation do not provide authentication/integrity: Consider CBC, OFB, CTR mode. Show how an adversary can modify a ciphertext in such a way that it will be accepted by the receiver. Can the adversary do this in such a way so that the adversary knows the relationship between the sent and decrypted message (e.g. flipping a single bit of the message)?

4. Authenticated Encryption: Consider an authenticated encryption scheme that is constructed using the (insecure) Encrypt-and-Mac paradigm. Specifically, to an encrypt a message m it outputs a ciphertext consisting of (c,t) where:

$$c \leftarrow Enc_{k_E}(m) \qquad t \leftarrow Mac_{k_M}(m)$$

Show that if the Mac is deterministic, then the resulting encryption scheme cannot be CPA-secure.

5. Difference between a Mac and a Hash function. Hash functions are used in practice as a form of authentication. For example, when downloading a file, one can check for errors by computing the hash of the file (e.g. using SHA-2) and checking whether the output of the hash matches a pre-computed value that was published on the download page. However, the above usage does not provide the cryptographic guarantees that we expect from a message authentication code. Why not?
Specifically, let H be a hash function. Explain why $H(m)$ is not a secure Mac.