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*?

The following two questions ask about modifications to CBC-MAC that render it insecure. Both modifications correspond to features of CBC-ENC that are not used in CBC-MAC. Specifically, in the first modification we output the intermediate blocks in CBC-MAC. In the second modification, we use a randomly chosen IV.

Let F be a length-preserving pseudorandom function. Show that each of the following message authentication codes is insecure. (In each case the shared key is a random $k \in \{0,1\}^n$.)

3. To authenticate a message $m = m_1||m_2$, where $m_1, m_2 \in \{0,1\}^n$, compute $t := F_k(m_1)||F_k\big(m_2 \oplus F_k(m_1)\big)$.

4. To authenticate a message $m = m_1||m_2$, where $m_i \in \{0,1\}^n$, choose $r \in \{0,1\}^n$ at random and compute $t := r||F_k(m_2 \oplus F_k(m_1 \oplus r))$.

Public Key Cryptography

5. Describe in detail a man-in-the-middle attack on the Diffie-Hellman key-exchange protocol whereby the adversary ends up sharing a key k_A with Alice and a different key k_B with Bob, and Alice and Bob cannot detect that anything has gone wrong. What happens if Alice and Bob try to detect the presence of a man-in-the-middle adversary by sending each other (encrypted) questions that only the other party would know how to answer?

6. Let (N, e) be the public key for "textbook" RSA, where $N = 3 \cdot 11 = 33$ and $e = 3$. Find the corresponding secret key (N, d). Then encrypt the message $m = 16$, obtaining some ciphertext c. Decrypt c to recover m. Do the computations by hand and show your work.