

## Introduction to Cryptology ENEE459E/CMSC498R: Homework 5

Due by beginning of class on 3/8/2016.

1. What is the effect of a dropped ciphertext block (e.g., if the transmitted ciphertext  $c_1, c_2, c_3, \dots$  is received as  $c_1, c_3, \dots$ ) when using the CBC, OFB, and CTR modes of operation?
2. Say  $\Pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$  is a secure MAC, and for  $k \in \{0, 1\}^n$ , the tag-generation algorithm  $\text{Mac}_k$  always outputs tags of length  $t(n)$ . Prove that  $t$  must be super-logarithmic or, equivalently, that if  $t(n) = O(\log n)$  then  $\Pi$  cannot be a secure MAC.  
**Hint:** Consider the probability of randomly guessing a valid tag.
3. Assume secure MACs exist. Prove that there exists a MAC that is secure (by Definition 4.2) but is *not* strongly secure (by Definition 4.3).
4. Consider the following MAC for messages of length  $\ell(n) = 2n - 2$  using a pseudorandom function  $F$ : On input a message  $m_0 || m_1$  (with  $|m_0| = |m_1| = n - 1$ ) and key  $k \in \{0, 1\}^n$ , algorithm  $\text{Mac}$  outputs  $t = F_k(0 || m_0) || F_k(1 || m_1)$ . Algorithm  $\text{Vrfy}$  is defined in the natural way. Is  $(\text{Gen}, \text{Mac}, \text{Vrfy})$  secure? Prove your answer.
5. Let  $F$  be a pseudorandom function. Show that each of the following MACs is insecure, even if used to authenticated fixed-length messages. (In each case  $\text{Gen}$  outputs a uniform  $k \in \{0, 1\}^n$ . Let  $\langle i \rangle$  denote an  $n/2$ -bit encoding of the integer  $i$ .)
  - (a) To authenticate a message  $m = m_1, \dots, m_\ell$ , where  $m_i \in \{0, 1\}^n$ , compute  $t := F_k(m_1) \oplus \dots \oplus F_k(m_\ell)$ .
  - (b) To authenticate a message  $m = m_1, \dots, m_\ell$ , where  $m_i \in \{0, 1\}^{n/2}$ , compute  $t := F_k(\langle 1 \rangle || m_1) \oplus \dots \oplus F_k(\langle \ell \rangle || m_\ell)$ .