E0 235 : Cryptography	**Question Set**
Tutorial 6	
Instructor: Arpita Patra	*Feb 10, 2017*

Question 1

Consider the following MAC for messages of length $l(n) = 2n - 2$ 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 Mac outputs $t = F_k(0||m_0)||F_k(1||m_1)$. Algorithm Vrfy is defined in the natural way. Is $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ secure? Prove your answer.

Question 2

Let F be a pseudorandom function. Show that each of the following MACs is insecure, even if used to authenticate fixed-length messages. (In each case 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 $m = m_1, \cdots, m_l$, where $m_i \in \{0,1\}^n$, compute $t := F_k(m_1) \oplus \cdots \oplus F_k(m_l)$.

(b) To authenticate a message $m = m_1, \cdots, m_l$, where $m_i \in \{0,1\}^{n/2}$, compute $t := F_k(\langle 1 \rangle ||m_1) \oplus \cdots \oplus F_k(\langle l \rangle ||m_l)$.

Question 3

Let F be a pseudorandom function. Show that the following MAC for messages of length $2n$ is insecure: Gen outputs a uniform $k \in \{0,1\}^n$. To authenticate a message $m_1||m_2$ with $|m_1| = |m_2| = n$, compute the tag $F_k(m_1)||F_k(F_k(m_2))$.

Question 4

Prove that the following modifications of basic CBC-MAC do not yield a secure MAC (even for fixed-length messages):

A random initial block is used each time a message is authenticated. That is, choose uniform $t_0 \in \{0,1\}^n$, run basic CBC-MAC over the "message" $t_0, m_1, \cdots, m_l$, and output the tag $\langle t_0, t_l \rangle$. Verification is done in the natural way.

References

1. Jonathan Katz, Yehuda Lindell : Introduction to Modern Cryptography, Second Edition