COMP4140 Cryptography Assignment 3 Written Component

1)

For security param n, consider the MAC for messages of length n using a pseudorandom function $F:\{0,1\}^n \times \{0,1\}^n \Rightarrow \{0,1\}$ defined as follows: On input k and message $m=m_1 m_2 \ldots m_n$, the algorithm $MAC_k(\cdot)$ is defined by $MAC_k(m)=F_k(1\|m_1 m_2 \ldots m_{n-1}) \oplus F_k(0\|m_2 m_3 \ldots m_n)$.

The algorithm Vrfy can be defined using canonical verification.

Is this a secure MAC?

This is not a secure MAC. Prove that there exists a PPT adversary such that for any negligible function negl the following does not hold: $Pr[Mac-forge_{A,\Pi}(n)=1] \leq negl(n)$.

Let A be an adversary that selects any string $x \in \{0,1\}^{n-2}$ and outputs messages $m_1=0\|x\|0$, $m_2=0\|x\|1$, and $m_3=1\|x\|0$. It uses the oracle $MAC_k(\cdot)$ to generate the following tags:

$$t_1=MAC_k(m_1)=F_k(1\|0\|x) \oplus F_k(0\|x\|0)$$

$$t_2=MAC_k(m_2)=F_k(1\|0\|x) \oplus F_k(0\|x\|1)$$

$$t_3=MAC_k(m_3)=F_k(1\|1\|x) \oplus F_k(0\|x\|0)$$

Let $A=F_k(1\|0\|x)$, $B=F_k(0\|x\|0)$, $C=F_k(0\|x\|1)$, and $D=F_k(1\|1\|x)$.

A outputs the pair $(m=1\|x\|1, t=t_1 \oplus t_2 \oplus t_3)$.

How often is the adversary correct?

$$t=MAC_k(m)=F_k(1\|1\|x) \oplus F_k(0\|x\|1)=D \oplus C$$

$$t_1 \oplus t_2 \oplus t_3=(A \oplus B) \oplus (A \oplus C) \oplus (D \oplus B)=A \oplus A \oplus B \oplus B \oplus D \oplus C=D \oplus C$$

Therefore the adversary is always correct, and $Pr[Mac-forge_{A,\Pi}(n)=1]=1>negl(n)$.

Therefore this MAC is not secure.

2)

Prove that CBC-MAC is not secure if it outputs every generated t instead of just the last.

For any security parameter n, let A be an adversary that picks any $m_1 = a \| 0^n$ where $a \in \{0,1\}^n$. The adversary uses the oracle to generate the m_1 tags $t_1^1 = F_k(0^n \oplus a) = A$ and $t_2^1 = F_k(A \oplus 0^n) = B$. Let $m_2 = B \| 0^n$. The adversary uses the oracle to generate the m_2 tags $t_1^2 = F_k(0^n \oplus B) = C$ and $t_2 = F_k(C \oplus 0^n) = D$. The adversary then outputs $(m = A \| 0^n, t = (B, C))$.

How often is the adversary correct?

The tags for $m = A \| 0^n$ are:

$$t = F_k(0^n \oplus A) = B$$

$$t = F_k(B \oplus 0^n) = C$$

Since this MAC outputs all generated tags, the complete tag for m is (B, C).

Therefore the adversary is always right, and $Pr[Mac-forge_{A,\Pi}(n) = 1] = 1 > negl(n)$ and the modified CBC-MAC is not secure.