CS 435: Introduction to Cryptography **Spring 2020**

Homework 5

Professor Somesh Jha **Due: April 21**

1. **Exercise 4.8**

   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 $F_k(m_1) \| F_k(F_k(m_2))$.

2. **Exercise 4.1**

   Say $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ is a secure MAC, and for $k \in \{0,1\}^n$ the tag-generation algorithm Mac_k always outputs tags of length $t(n)$. Prove that t must be super-logarithmic or, equivalently, that if $t(n) = \mathcal{O}(\log n)$ then Π cannot be a secure MAC.

   Note. Super-logarithmic means not of the form $\mathcal{O}(\log n)$.

   Note. Super-logarithmic means not of the form $\mathcal{O}(\log n)$, i.e. it is not the case that $t(n) \leq C \log n$ for large n and some fixed $C > 0$.

   Hint: Consider the probability of randomly guessing a valid tag.

3. Alice has five files F_1, F_2, F_3, F_4, F_5 that she wants to store on Bob's computer (Bob just purchased a new server that has a gigantic hard disk). However, Alice is worried that Bob might corrupt or modify the files. Answer the following:

   (a) Show the Merkle hash tree for F_1, F_2, F_3, F_4, F_5.

   (b) What is stored on Alice's computer?

4. Now Alice wants to retrieve file F_3 from Bob's computer.

   (a) What does Bob send to Alice? Recall that Bob needs to "prove" to Alice that the file has not been modified.

   (b) Show that it is "hard" for Bob to generate a "proof" for Alice for a file F_3' different from F_3. We of course assume that hash functions that the Merkle hash tree is constructed from is *collision resistant*.