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

Homework 5

Professor Somesh Jha **Due:** Nov 14

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. In LectureLet 21, we did the Merkle-Damgrad construction which took a hash function h that compresses by a factor of $1/2$ and constructs a hash function H by a factor of $1/3$. Repeat the construction to construct a hash function H that compresses by a factor of $1/5$. Also redo the proof of collision resistance that was done in the LectureLet.

3. Alice has six files $F_1, F_2, F_3, F_4, F_5, F_6$ 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 a Merkle hash tree for $F_1, F_2, F_3, F_4, F_5, F_6$ where the root is binary and the internal nodes are ternary. This shows that Merkle hash tree doesn't necessarily have to be binary.

   (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*.