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

Quiz April 22, 2020

Professor Somesh Jha April 22, 2020

1. **(40 points):** Alice has six files $F_1, F_2, F_3, F_4, F_5, F_6$ that she wants to store on a remote server S.
   Part (a): Show the Merkle hash tree for the six files. What does Alice store on her computer?
   Part (b): Suppose Alice wants retrieve file F_1 from the server S. What should the server S send along with the file to convince Alice that the file has not been modified?
   Part (c): Show that the server S cannot convince Alice that some other file F_1' (not equal to F_1) is the "legitimate" file. This is similar to the proof we did in a Lecturelet.
   Part (d): Suppose Alice wants to retrieve two files F_2 and F_4. Can the server send a shorter proof? The obvious way is to send to separate proofs for F_2 and F_4.

2. **(30 points):** Let H and G be a collision resistant hash functions. Answer the following:
   Part (a): Is $H \circ G$ a collision-resistant hash function? Please justify your answer. $\circ$ denotes composition (e.g. $H \circ G(x) = H(G(x))$ *Part (b):* Prove that H^i (H^i is H composed with itself i times. $H^2(x) = H(H(x))$).
   Hint: Use part (a) and induction.

3. **(30 points):** Let F be a PRF where all the relevant sizes are n-bits (i.e key size, input, and output sizes). Recall that we proved that the MAC scheme that computes the tag as $t = F_k(m)$ is secure (assume that the key size is a random n-bit string). However, that scheme can only handle n-bit messages. Consider the following schemes for domain extension (i.e. handling larger messages). Prove that all of them are insecure.
   Part (a): To authenticate message $m = m_1 \cdots m_l$ (each message block m_i is of size $\frac{n}{2}$ bits), compute $t = F_k(\langle 1 \rangle \| m_1) \oplus \cdots \oplus F_k(\langle l \rangle || m_l)$. Let $\langle i \rangle$ denote the $\frac{n}{2}$-bit encoding of integer i.
   Part (b): To authenticate message $m = m_1 \cdots m_l$ (each message block m_i is of size $\frac{n}{2}$ bits), compute $t = F_k(r) \oplus F_k(\langle 1 \rangle \| m_1) \oplus \cdots \oplus F_k(\langle l \rangle || m_l)$. For each message $r \leftarrow \{0,1\}^n$ is chosen randomly. Recall that the random number r is sent by the sender along with the tags t_i (otherwise the MAC cannot be verified at the other end).