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

Quiz November 18, 2020

Professor Somesh Jha November 18, 2020

1. **(30 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 where all the nodes are binary. 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): 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. **(20 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 is collision resistant (H^i is H composed with itself i times. $H^2(x) = H(H(x))$).
   Hint: Use part (a) and induction.

3. **(20 points):** Let F_k be a PRF. Define a new PRF G_k as $F_k \circ F_k$ (i.e. $G_k(x) = F_k(F_k(x))$). Is G_k a PRF? Justify your answer.

4. **(30 points)** This question is regarding the CTR mode of operation.
   Part (a): Describe the encryption and decryption of the CTR mode of operation.
   Part (b): Are encryption and decryption steps of CTR mode parallelizable? Justify your answer.
   Part (c): Define $CTR - MAC(m)$ as follows: (1) set CTR to 0 and let $c_1, \cdots, c_k$ be the cipher blocks of when m is encrypted using the CTR-mode (we assume $m_1 \cdots m_k$ are the blocks of m) (2) define the MAC tag as $c_1 \oplus \cdots \oplus c_k$ (tag is the "xor" of the cipherblocks). Is $CTR - MAC$ a secure MAC?