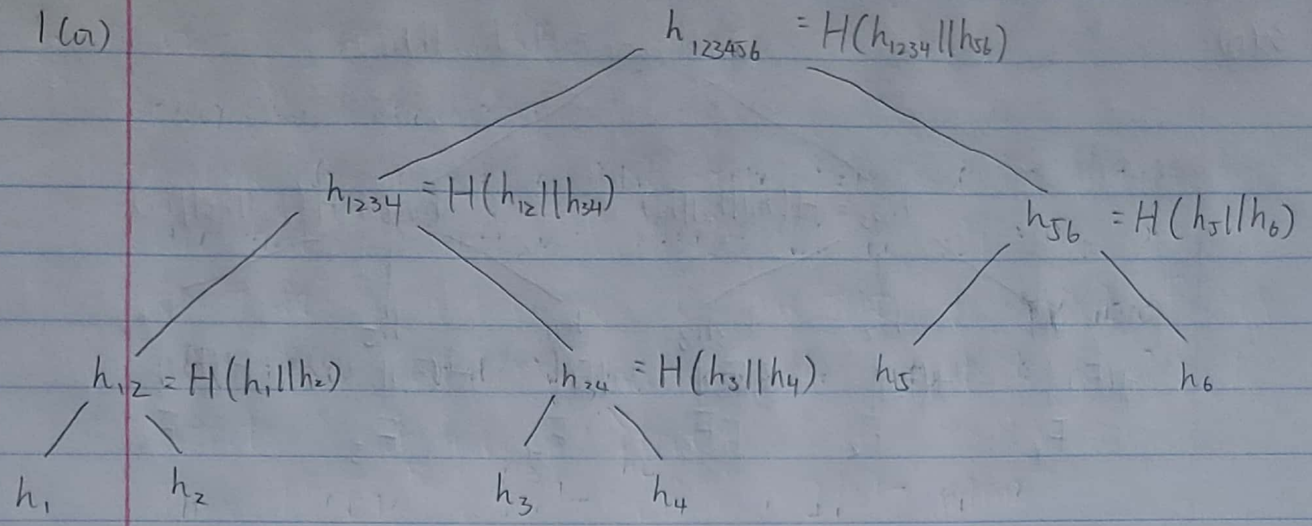
CS 435 Quiz 2
Zhaoyi Zhang
9079627627

1(a)



1(b) If Alice wants to retrieve file F_1, the server should send F_1', h_2', h_{34}' and h_{56}'.
Alice should compute $h_1' = H(F_1')$, $h_{12}' = H(h_1' \| h_2')$, $h_{1234}' = H(h_{12}' \| h_{34}')$, $h_{123456}' = H(h_{1234}' \| h_{56}')$ and verify if $h_{123456} = h_{123456}'$

1(c) The server can send a shorter proof which includes F_2', F_4', $h_1', h_{34}', h_3', h_{12}', h_{56}'$

2(a) Proof by contradiction

Assume $H \circ G$ is not collision resistant, then there exists $x \neq x'$, such that $H \circ G(x) = H \circ G(x')$. $(H(G(x)) = H(G(x')))$

Since G is collision resistant, $x \neq x'$, let $y = G(x)$ and $y' = G(x')$, we know $y \neq y'$

Since H is collision resistant, $y \neq y'$, but $H(y) = H(y')$, which gives a contradiction.

Therefore, if H and G are collision resistant, so does $H \circ G$

2(b) Proof by induction

Without loss of generality, let $H = G$ in the context of part (a)

Thus, we have the base case where $i = 1$, and $H(H(x))$ is collision resistant.

Inductive step: Assume H^i is collision resistant, prove H^{i+1} is collision resistant

Using the result proved in part (a), if H and H^i are collision resistant, $H \circ H^i = H^{i+1}$ is collision resistant.

By induction, H^i is collision resistant.

3. G_K is still a PRF
Proof by contradiction
Assume G is not a PRF, then there exists a distinguisher D such that $\left| Pr[D^{G_k(\cdot)}(1^n)=1] - Pr[D^{f(\cdot)}(1^n)=1] \right| \neq negl(n)$
Construit a distinguisher $\hat{D}$ such that it calls the oracle like this: $O(O(x))$ and pass the output to D. The $\hat{D}$ outputs 1 whenever D output 1.
Thus $\left| Pr[\hat{D}^{F_k(\cdot)}(1^n)=1] - Pr[\hat{D}^{\tilde{f}(\cdot)}(1^n)=1] \right| = 1 - negl(n)$
which contradicts that F is a PRF.
Thus G is a PRF.

4.(a) Let F be a PRF. Define $y_i := F_k(ctr+i)$
Encryption: $c_i := y_i \oplus m_i$
Decryption: $m_i := c_i \oplus F_k(ctr+i)$

4.(b) The encryption and decryption can be parallelizable. Since c_i does not rely on c_{i-1} and m_i does not rely on m_{i-1}. and $y_i := F_k(ctr+i)$ can be computed independently, parallelization is possible

4(c) CTR-MAC is not secure.
Construct an adversary A and assume A will use message of length n.

A choose two messages m_1 and m_2 such that $|m_1| = |m_2| = n$

A queries the oracle with these two messages and get tags C_1 and C_2.

A output $m_1 || m_2$ and $C_1 \oplus C_2$.

$C_1 := m_1 \oplus F_k(ctr+1)$, $C_2 := m_2 \oplus F_k(ctr+2)$

and encryption of $m_1 || m_2$ is $m_1 \oplus F_k(ctr+1) || m_2 \oplus F_k(ctr+2)$

which is $C_1 || C_2$.

$m_1 || m_2 \notin Q$

Thus A breaks the MAC and CTR-MAC is not secure.