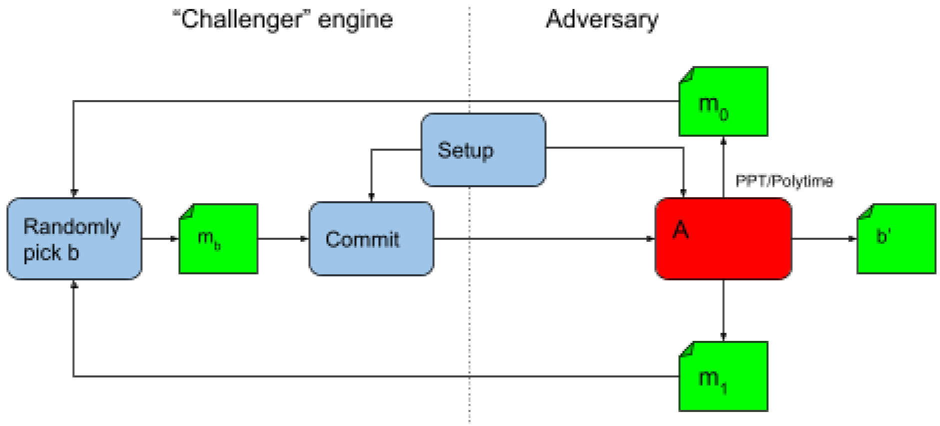
A0216695U Ng Jong Ray, Edward

Question 1



A commitment scheme Π has the hiding property if for all PPT adversary A, there exists a $negl$, s.t.

$$Pr[Hiding_{A,\Pi}(n) = 1] \leq negl(n) + \frac{1}{2}$$

Question 2

h_2 is not collision resistant. 2 messages m_0, m_1 where $m_0 = \{0, 1\}^n$ || 0 and $m_1 = \{0, 1\}^n$ || 0 where $m_0 \neq m_1$. This would result in the same hash under h_2. When the least significant bit b is 0, then the hashes will just be $\{0\}^{n+1}$. Thus both messages m_0, m_1 will collide with the same hash.

Question 3

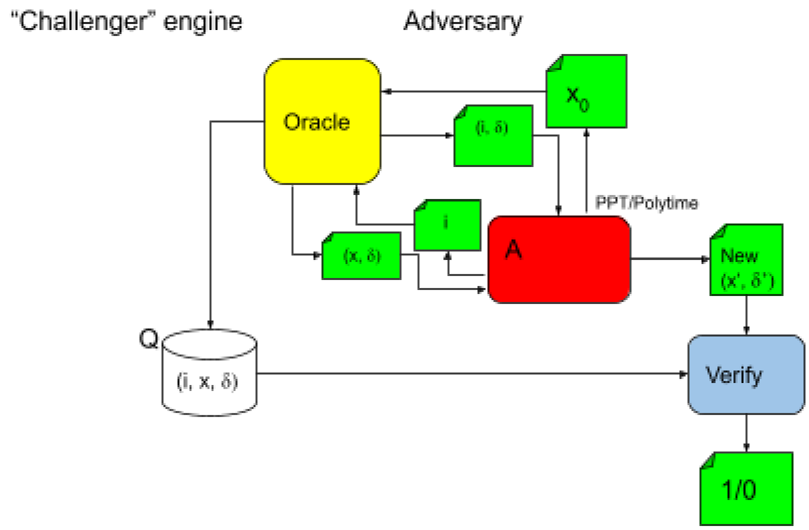
Assume that $H_1(x)$ is not collision resistant. This means that $y = H_1(x)$ is not collision resistant. Then $z = H_1(y)$, which is also equivalent to $H_1(H_1(x))$, is also not collision resistant. However, this contradicts with $H(x)$ being collision resistant, thus this proves that H_1 is collision resistant.

Question 4

$H_1^s(x)$ is collision resistant. Considering 2 inputs x, x' and $x \neq x'$, their resultant hashes will be $H_1^s(x) = Z_B$ || L and $H_1^s(x') = Z'_B$ || L'. To find a collision, both $Z_B = Z'_B$ and $L = L'$ has to be the same. For $L = L'$, both x and x' must be of the same length. For $Z_B = Z'_B$, this would mean that the hashes of x and x' are equal meaning that $x = x'$. However this would contradict that $x \neq x'$ proving that $H_1^s(x)$ is collision resistant.

Question 5

a) Fingerprinting Game



1) Adversary has an oracle access. The Adversary will create a file x_0 and $Put()$ the file into the Oracle. The Oracle will output $(i,\ \delta)$ which of the file x_0.
2) This will be stored in Q as $(i,\ x,\ \delta)$
3) The Oracle can also answer $Get()$ queries when the adversary inputs the index i, the Oracle will then return the $(x,\ \delta)$ corresponding file and fingerprint.
4) The Adversary now has to create a new file x' and the corresponding fingerprint δ' and $Verify()$.
5) The Adversary wins $(Verify() = 1)$ if it is able to find a new $(i,\ x',\ \delta')$ for a fingerprint that can match a file in the server.

b) The Π is unforgeable iff for any PPT Adversary A, there is a $negl$, s.t.

$$Pr[Fileforge_{A,\Pi}(n) = 1] \leq negl(n)$$

c) Definition of a Fingerprint Server:
Define Q as a storage which stores $(i,\ x,\ \delta)$ as a tuple.
Define $H(x)$ as a hash function which hashes the file x

$Put(x)$: With the input file x, $\delta := H(x)$, i will be the index of file x in Q
$Get(i)$: With the input index i, output $< x_i,\ \delta_i >$ from Q
$Vrfy(i,\ x_b,\ \delta_b)$: With the input $(i,\ x_b,\ \delta_b)$. First, verify $H(x_b) = \delta_b$. Next, compare $\delta_b = \delta_i$. Thus $Vrfy = 1$ or output 'ok', $\delta_i = \delta_b = H(x_b)$. Else $Vrfy = 0$.