Problem 1: ElGamal FDH

Bob studied the RSA-FDH construction. He notices that RSA-FDH essentially does the following: To sign a message $m$, it decrypts $H(m)$ using textbook RSA, and to check a signature $\sigma$, it encrypts $\sigma$ and compares the result with $H(m)$.

This lead him to the following idea: Instead of textbook RSA, he uses ElGamal in the construction of FDH, because ElGamal is more secure (it is IND-CPA secure, after all).

Why is the resulting scheme “ElGamal-FDH” bad?

Problem 2: Random oracle model

Write down the definition of IND-CPA security in the random oracle model (for symmetric encryption schemes).

Problem 3: Security proof in the ROM [Bonus problem]

This is a bonus problem.

Fix a hash function $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$. We define the following block cipher with message and key space $\{0, 1\}^n$:

- **Encryption $E$**: To encrypt $m \in \{0, 1\}^n$ under key $k$, choose a random $r \in \{0, 1\}^n$ and return the ciphertext $c := (r, m \oplus H(k\|r))$.
- **Decryption $D$**: To decrypt $c = (r, c')$ with key $k$, compute and return $m := H(k\|r) \oplus c'$.

Below is a proof that this encryption scheme is $(\tau, q_E, q_H, \varepsilon)$-IND-CPA secure in the random oracle model. Fill in the gaps. (The length of the gaps is unrelated to the length of the text to be inserted.)

**Proof.** In the first game, we just restate the game from the IND-CPA security definition (in the random oracle model).

**Game 1.**

To show that the encryption scheme is $(\tau, q_E, q_H, \varepsilon)$-IND-CPA secure, we need to show that

$$\left| \Pr[b = b’ | Game 1] - \frac{1}{2} \right| \leq \varepsilon$$

(1)

$q_E$ is the number of encryption oracle queries, and $q_H$ the number of random oracle $H$ queries performed by $A$. 
As a first step, we replace the random oracle.

**Game 2.** Like Game 1 except that we define the random oracle $H$ differently:

We have $\Pr[b = b']_{\text{Game 1}} = \Pr[b = b']_{\text{Game 2}}$.

One can see that the adversary cannot guess the key $k$ (where $k$ is the key used for encryption in Game 2), more precisely, the following happens with probability $\leq q_H 2^n$:

“The adversary invokes $H(x)$ with $x = k \| r'$ for some $r'$.” (We omit the proof of this fact.)

Let $r_0$ denote the value $r$ that is chosen during the execution of $c \leftarrow E^H(k, m_b)$ in Game 2. Consider the following event: “Besides the query $H(k \| r_0)$ performed by $c \leftarrow E^H(k, m_b)$, there is another query $H(x)$ with $x = k \| r_0$ (performed by the adversary or by the oracle $E^H(k, \cdot)$.” This event occurs with probability $q_H 2^n + q_E 2^n$. Namely, the adversary make such $H(x)$ queries with probability $\leq q_H 2^n$ because $3$, and each invocation of the oracle $E^H(k, m_b)$ makes such an $H(x)$ query with probability $\leq 2^n$ because $4$.

Thus, the response of the $H(k \| r_0)$-query performed by $c \leftarrow E^H(k, m_b)$ is a random value that is used nowhere else (except with probability $\leq (q_H + q_E)2^n$). Thus, we can replace that value by some fresh random value.

**Game 3.** Like Game 2 except that we replace $c \leftarrow E^H(k, m_b)$ by $r_0 \overset{\$}{\leftarrow} \{0, 1\}^n$, $h^* \overset{\$}{\leftarrow} \{0, 1\}^n$, $c \leftarrow (r_0, m_b \oplus h^*)$.

We have that

$$|\Pr[b = b']_{\text{Game 2}} - \Pr[b = b']_{\text{Game 3}}| \leq (q_H + q_E)2^n = \varepsilon.$$

To get rid of $m_b$ in Game 3, we use the fact that $h^*$ is chosen uniformly at random and XORed on $m_b$. That is, we can replace $m_b \oplus h^*$ by $5$.

**Game 4.** Like Game 3 except that we replace $c \leftarrow (r_0, m_b \oplus h^*)$ by $6$.

We have that $\Pr[b = b']_{\text{Game 4}} = \Pr[b = b']_{\text{Game 3}}$. Notice that $b$ is not used in Game 4, thus we have that $\Pr[b = b']_{\text{Game 4}} = 7$.

Combining the equations we have gathered, (1) follows.