COL759 Quiz 2

Anish

TOTAL POINTS

3 / 10

QUESTION 1

1 True/False 3 / 5

✓ **+ 2 pts** *Q1 Correct*

✓ **+ 1 pts** *Q2 correct*

+ 2 pts Q3 correct

QUESTION 2

2 Randomized encryption scheme 0 / 5

✓ **+ 0 pts** *Incorrect, the scheme is not semantically secure.*

+ 0 pts Insufficient explanation.

+ 5 pts Correct construction of G, and correct description of attack on encryption scheme.

Name: ANISH BANERJEE

2301-COL759 Quiz 2
Total marks: 10

Entry No: 2021CS10134

True/False Questions (5 marks)

Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be **any** secure pseudorandom generator (you should not assume anything extra about G). For each of the following questions, indicate whether the statement follows from the fact that G is a secure PRG. Write 'true' if the statement follows from the fact that G is a secure PRG, else write 'false'.

1. Given $y = G(x)$ for a uniformly random string $x \leftarrow \{0,1\}^n$, no **polynomial time** algorithm can find an $x' \in \{0,1\}^n$ such that $G(x') = y$ (with non-negligible probability).

   True

2. Given $y = G(x)$ for a uniformly random string $x \leftarrow \{0,1\}^n$, no **exponential time** algorithm can find an $x' \in \{0,1\}^n$ such that $G(x') = y$ (with non-negligible probability).

   False

3. Given $y = G(x)$ for a uniformly random string $x \leftarrow \{0,1\}^n$, no **polynomial time** algorithm can compute the first bit of x with probability greater than $3/4$.

   Because True

A randomized encryption scheme using PRGs (5 marks)

Let $G : \{0,1\}^{2n} \to \{0,1\}^{4n}$ be a secure pseudorandom generator. Consider the following encryption scheme $\mathcal{E}'_G$ with, key space $\{0,1\}^n$, message space $\{0,1\}^{4n}$ and ciphertext space $\{0,1\}^n \times \{0,1\}^{4n}$.

- $\mathsf{Enc}(k, m)$: Choose a uniformly random string $r \leftarrow \{0,1\}^n$, output $(r, m \oplus G(r \mid\mid k))$.
- $\mathsf{Dec}(k, \mathsf{ct} = (\mathsf{ct}_1, \mathsf{ct}_2))$: Output $\mathsf{ct}_2 \oplus G(\mathsf{ct}_1 \mid\mid k)$.

Is the above encryption scheme semantically secure?

If you think it is secure, give a high-level idea of the proof of security. For instance, you can give the intermediate hybrid experiments and discuss informally why the consecutive hybrids are indistinguishable.

If you think it is insecure, construct a PRG $G : \{0,1\}^{2n} \to \{0,1\}^{4n}$ such that G is a secure PRG, but $\mathcal{E}'_G$ is not a semantically secure encryption scheme. In order to construct G, you can use a secure PRG G' with domain $\{0,1\}^n$ and co-domain appropriately chosen. Discuss informally why G is a secure PRG (assuming G' is a secure PRG), and why $\mathcal{E}'_G$ is not semantically secure.

World 0 C $\xrightarrow{G(s)}$ B $\xleftarrow{m_0, m_1}$ A The PRG

$\longrightarrow$