1 Working with computational security

Recall the following definitions.

Definition 1. A function \( p : \mathbb{Z}^+ \rightarrow \mathbb{R}^+ \) is a polynomial (bounded) function if there exists \( k, N \in \mathbb{Z}^+ \) such that for all \( n > N \) it holds that \( p(n) \leq n^k \).\(^1\)

Definition 2. A function \( f : \mathbb{Z}^+ \rightarrow \mathbb{R}^+ \) is negligible function if for every positive polynomial \( p \) there is an \( N \) such that for all integers \( n > N \) it holds that \( f(n) < \frac{1}{p(n)} \).\(^2\)

a) 10 pts Show that the product, \( p \cdot q \) of two polynomial functions \( p, q \) is a polynomial function. (Your response should consider the \( N_p, N_q \) where this becomes true for each function \( p, q \).)

b) 10 pts Show that the sum, \( p + q \) of two polynomial functions, \( p, q \) is a polynomial function. (Your response should consider the \( N_p, N_q \) where this becomes true for each function \( p, q \).)

c) 10 pts Show that for any polynomial function \( p(n) \) and negligible function \( \epsilon(n) \) the function \( p(n)\epsilon(n) \) is a negligible function. (Your response should consider the \( N_p, N_{\epsilon} \) for each function.)

d) 10 pts Show that the sum, \( (\epsilon + \nu)(n) \), of two negligible functions, \( \epsilon(n), \nu(n) \) is negligible. (Your response should consider the \( N_\epsilon, N_\nu \) where this becomes true for each polynomial \( p \).)

e) 10 pts Consider a PPT \( A \) that makes invokes another PPT \( A' \) as a sub-routine.\(^3\) Show that the overall running time of \( A \) is polynomial time (even counting the running time \( A' \)). In this question \( A \) may make multiple calls to \( A' \).

**Hint:** What is the maximum number of times that \( A \) can invoke \( A' \)? You may use your answers from any previous part.

---

\(^1\)Here we are talking about a function that is bounded by a polynomial not an actual polynomial. For example \( p(n) = \sin(n) \) would satisfy our definition but this function is not a polynomial. For the purposes of this problem set we are concerned with polynomial time. In this setting, we care that the function is bounded above by a polynomial. That is what this definition guarantees.

\(^2\)This definition is equivalent to saying that \( p(n) \leq cn^k \) for some constant \( c > 0 \). The constant \( c \) can be avoided by increasing \( k \), so we remove it to simplify notation.

\(^3\)We did not explicitly define this behavior but you can think of this as a function call in a program language.
2 Computational Definitions of Security

Recall our definition of indistinguishable encryptions:

Definition 3 (Indistinguishable). An encryption scheme \((\mathcal{M}, K, \text{Enc}, \text{Dec})\) has indistinguishable encryptions if for all PPT \(A\) for every two messages \(m_1, m_2 \in \mathcal{M}\):

\[
| \Pr_{k \in K} [A(\text{Enc}_k(m_1)) = 1] - \Pr_{k \in K} [A(\text{Enc}_k(m_2)) = 1] | < \epsilon(n).
\]

for some negligible function \(\epsilon(n)\).

Consider the following alternative definition:

Definition 4 (Indistinguishable). An encryption scheme \((\mathcal{M}, K, \text{Enc}, \text{Dec})\) has IND encryptions if for all PPT \(A\) for every two messages \(m_1, m_2 \in \mathcal{M}\):

\[
\Pr_{k \in K, b \leftarrow \{1, 2\}} [A(\text{Enc}_k(m_b)) = b] \leq \frac{1}{2} + \epsilon(n).
\]

for some negligible function \(\epsilon(n)\).

a) (10 pts) Describe in words how the two definitions are different.

b) (20 pts) Show Definitions 3 and 4 are equivalent (show both directions of the implication).\(^3\) Also show the relationship between the two negligible functions.

c) (10 pts) In class we showed a version of semantic security for multiple messages. Present a definition of indistinguishable encryptions for multiple messages.

d) (10 pts) Does an encryption scheme with indistinguishable encryptions for a single message have indistinguishable encryptions for multiple messages? If yes, provide a proof, if not provide a counterexample.

\(^3\)You may want to refer to proof in class on the equivalence of semantic security and indistinguishable encryptions.