Homework 2

Task 1 - Negligible Functions (10 points)

(a)

The function $f(k)$ is negligible.

Proof. For all $d \geq 1$, we want to find k_0 such that for all $k > k_0$, we have $k^{-log^2(k)} < k^{-d}$. We take logarithms to the base two of both sides, we get $k^{-log^2(k)} < k^{-d}$ is equivalent to:

$$log^2(k) > d$$

If we take for example $k_0 = 2^d$, then for all $k > k0$ we have:

$$log^2(k) > log^2(k_0) = log^2(2^d) > d$$

The first inequality follows from the fact that $k \mapsto log^2(k)$ grows monotonically, the last inequality follows from the fact that $log^2(2^d) = d^2 > d$ for all $d \geq 1$.

(b)

(i) Since $f(k)$ and $g(k)$ are both negligible, by the definition of negligible functions, we know there exists k_f and k_g such that for all $k > k_f$ and $k > k_g$:

$$f(k) < k^{-d} \text{ and } g(k) < k^{-d}$$

We can take $k_1 = \max(k_f, k_g, 3)$, then for all $k > k_1$ we have:

$$h_1(k) = f(k) + g(k) < 2k^{-d} < 2k^{-d-1} < k \cdot k^{-d-1} < k^{-d}$$

Therefore, by definition, $h_1(k)$ is negligible.

(ii) Assume $d' = d + c$, since $d \geq 1$ and $c > 0$, we know $d' > 1$. Since $f(k)$ is negligible, by the definition of negligible functions, we know for all $d' > 1$ there exists k_f such that for all $k > k_f$:

$$f(k) < k^{-d'}$$

We can take $k_2 = k_f$, then for all $k > k_2$ we have:

$$h_2(k) = k^c \cdot f(k) < k^c \cdot k^{-d'} = k^{-d'+c} = k^{-(d+c)+c} = k^{-d}$$

Therefore, by definition, $h_2(k)$ is negligible.

Task 2 - Block Ciphers (10 points)

(a)

Since Υ_0 and Υ_1 are evaluated using the same key, we know once we find a key that satisfies $E(K', 0^n) = \Upsilon_0$, we can use the same key to satisfy $E(K', 1^n) = \Upsilon_1$.
We can see that the distinguisher only returns 1 when it finds a K' that satisfy the condition above in the entire key space. Since the key for evaluating the block cipher is chosen uniformly at random and the distinguisher is searching through the entire key space, we have:

$$Pr[D^{KF[E]} \Rightarrow 1] = |K'| \times Pr[E(K', 0^n) = \Upsilon_0] = |K'| \times \Pr_{K \xleftarrow{\$} \{0,1\}^n}[K = K'] = 2^n \times \frac{1}{2^n} = 1$$

(b)

For some $K' \in \{0, 1\}^n$, we have:

$$\begin{aligned} &Pr[E(K', 0^n) = \Upsilon_0 \text{ and } E(K', 1^n) = \Upsilon_1] \\ =&Pr[E(K', 0^n) = \Upsilon_0] \times Pr[E(K', 1^n) = \Upsilon_1 \mid E(K', 0^n) = \Upsilon_0] \\ =&\frac{1}{2^n} \times \frac{1}{2^n - 1} = \frac{1}{2^{2n} - 2^n} \end{aligned}$$

Since distinguisher D search through the entire key space, we have **the upper bound probability that D outputs 1 is**:

$$Pr[D^{RP[n]} \Rightarrow 1] = |K'| \times Pr[E(K', 0^n) = \Upsilon_0 \text{ and } E(K', 1^n) = \Upsilon_1] = 2^n \times \frac{1}{2^{2n} - 2^n} = \frac{1}{2^n - 1}$$

Therefore we know:

$$\mathsf{Adv}^{\mathsf{prp}}_{\mathsf{E}}(D) = |Pr[D^{KF[E]} \Rightarrow 1] - Pr[D^{RP[n] \Rightarrow 1}]| = |1 - \frac{1}{2^n - 1}| = \frac{2^n - 2}{2^n - 1}$$

(c)

The distinguisher doesn't contradict the existence of secure pseudorandom permutations because the distinguisher runs in exponential time (since it searches through the entire key space which grows exponentially as the key length grows). The security of pseudorandom permutations is defined on distinguishers that runs in polynomial time, since in the real world we don't have a computer that has virtually unlimited computational power to efficiently run the $O(2^n)$ algorithm in the distinguisher above on a large enough key space.

Task 3 - IND-CPA Security (9 points)

(a)

distinguisher $D^{\mathsf{LR}_{b[\Pi]}}$:
$C_1 \leftarrow \mathsf{LR}_{b[\Pi]}.\mathsf{Encrypt}(0^n, 0^n)$
$C_2 \leftarrow \mathsf{LR}_{b[\Pi]}.\mathsf{Encrypt}(0^n, 1^n)$
if $C_1 = C_2$ **then**
  return 1
return 0

Since Enc is deterministic, we know for some $K \xleftarrow{\$} Kg()$:

$$Pr[D^{\mathsf{LR}_{0[\Pi]}} \Rightarrow 1] = Pr[\mathsf{Enc}(K, 0^n) = \mathsf{Enc}(K, 0^n)] = 1$$

$$Pr[D^{\mathsf{LR}_{1[\Pi]}} \Rightarrow 1] = Pr[\mathsf{Enc}(K, 0^n) = \mathsf{Enc}(K, 1^n)] = 0$$

Therefore, we know that Π cannot be IND-CPA secure, since:

$$\mathsf{Adv}_{\Pi}^{\mathsf{ind\text{-}cpa}}(D) = |Pr[D^{\mathsf{LR}_{0[\Pi]}} \Rightarrow 1] - Pr[D^{\mathsf{LR}_{1[\Pi]}} \Rightarrow 1]| = |1 - 0| = 1$$

(b)

(c)

Task 4 - More IND-CPA Security (8 points)

(a)

(b)

Task 5 - Pseudorandom Functions (8 points)

(a)

(b)