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:

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

(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 $K \xleftarrow{\$} \mathsf{Kg}()$:

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

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

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

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

(b)

Assume we have some arbitrary plaintexts $M_0, M_1 \in \mathcal{M}$.

For an arbitrary distinguisher, we know $Pr[D^{\mathsf{LR}_{0[\Pi]}} \Rightarrow 1]$ and $Pr[D^{\mathsf{LR}_{1[\Pi]}} \Rightarrow 1]$ only differ by the single query allowed on $\mathsf{LR}_{0[\Pi]}.\mathsf{Encrypt}(M_0, M_1)$ and $\mathsf{LR}_{1[\Pi]}.\mathsf{Encrypt}(M_0, M_1)$ respectively.

By perfect secrecy, we know for all ciphertexts $C \in \mathcal{C}$:

$$\underset{K \overset{\$}{\leftarrow} \mathsf{Kg}()}{Pr}[\mathsf{Enc}(K, M_0) = C] = \underset{K \overset{\$}{\leftarrow} \mathsf{Kg}()}{Pr}[\mathsf{Enc}(K, M_1) = C]$$

Therefore, by the definition of $\mathsf{LR}_{b[\Pi]}$, we know for all $M_0, M_1 \in \mathcal{M}, C \in \mathcal{C}$:

$$Pr[\mathsf{LR}_{0[\Pi]}.\mathsf{Encrypt}(M_0, M_1) = C] = \underset{K \overset{\$}{\leftarrow} \mathsf{Kg}()}{Pr}[\mathsf{Enc}(K, M_0) = C]$$
$$= \underset{K \overset{\$}{\leftarrow} \mathsf{Kg}()}{Pr}[\mathsf{Enc}(K, M_1) = C] = Pr[\mathsf{LR}_{1[\Pi]}.\mathsf{Encrypt}(M_0, M_1) = C]$$

Since now the only difference between $Pr[D^{\mathsf{LR}_{0[\Pi]}} \Rightarrow 1]$ and $Pr[D^{\mathsf{LR}_{1[\Pi]}} \Rightarrow 1]$ are shown to have equal probability, we know:

$$Pr[D^{\mathsf{LR}_{0[\Pi]}} \Rightarrow 1] = Pr[D^{\mathsf{LR}_{1[\Pi]}} \Rightarrow 1]$$

Therefore:

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

(c)

The one-time pad is deterministic, but its security comes from the randomness of the one-time key In a), the deterministic nature of one-time pad was exploitable because the same key was used for multiple encryptions, which allows patterns of the ciphertext to be leaked. In b), since we restrict the distinguisher to have only one query, which allowed the one-time pad to preserve its security properties by only allowing one key to be used once. b) does not contradict a), instead the combination of them shows that the one-time pad is (1,0)-IND-CPA secure.

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

(a)

```
procedure Dec'($K, C'$) :
$C \leftarrow$ ($C'$ with the last occurrence of 0 removed)
return Dec($K, C$)
```

(b)

For some arbitrary plaintexts $M_0, M_1 \in \mathcal{M}$:

Let D be an arbitrary distinguisher for Π'. D queries $\mathsf{LR}_{b[\Pi']}$.Encrypt(M_0, M_1) (i.e. Enc'(K, M_0) or Enc'(K, M_1)) to get some ciphertext C'. Then D does some computation to produce an output.

Let D' be a distinguisher for Π that queries $\mathsf{LR}_{b[\Pi]}$.Encrypt(M_0, M_1) (i.e. Enc(K, M_0) or Enc(K, M_1)) to get some ciphertext C. D' then appends 0 to C to get C', and sends C' to D. D' then outputs whatever D outputs based on the C'.

By the definition above, we can see that for any distinguisher D there's a unique corresponding D' that appends 0 to some C to get C' and sends C' to D. Since appending 0 to some arbitrary text is $O(1)$ function, D' is still polynomial time if D is polynomial time.

Since C' in Π' is just C in Π with an additional 0 at the end, the advantage of D' in distinguishing between Enc(K, M_0) and Enc(K, M_1) is the same as the advantage of D in distinguishing between Enc'(K, M_0) and Enc'(K, M_1) (i.e. $\mathsf{Adv}_{\Pi}^{\text{ind-cpa}}(D') = \mathsf{Adv}_{\Pi'}^{\text{ind-cpa}}(D)$.

Therefore, we know given that Π is IND-CPA secure, Π' is also IND-CPA secure.

Task 5 - Pseudorandom Functions (8 points)

(a)

For $\mathsf{H}(K_1||K_2, x_1||x_2||x_3) = \mathsf{H}(K_1||K_2, x'_1||x'_2||x'_3)$, one strategy is to let:
$\mathsf{E}(K_1, x_1) = \mathsf{E}(K_1, x'_1)$ and $\mathsf{E}(K_2, x_1 \oplus x_2 \oplus x_3) = \mathsf{E}(K_2, x'_3)$ and $\mathsf{E}(K_2, x_3) = \mathsf{E}(K_2, x'_1 \oplus x'_2 \oplus x'_3)$.

Since E is a PRF, we know:

- $\mathsf{E}(K_1, x_1) = \mathsf{E}(K_1, x'_1)$ implies $x_1 = x'_1$
- $\mathsf{E}(K_2, x_1 \oplus x_2 \oplus x_3) = \mathsf{E}(K_2, x'_3)$ implies $x_1 \oplus x_2 \oplus x_3 = x'_3$
- $\mathsf{E}(K_2, x_3) = \mathsf{E}(K_2, x'_1 \oplus x'_2 \oplus x'_3)$ implies $x_3 = x'_1 \oplus x'_2 \oplus x'_3$

Therefore, for some $x_1, x_2, x_3 \in \{0,1\}^n$ where $x_1 \oplus x_2 \oplus x_3 \neq x_3$, we have: (x'_1, x'_2, x'_3) where $x'_1 = x_1, x'_2 = x_2, x'_3 = x_1 \oplus x_2 \oplus x_3$ satisfy that:
for all $K_1, K_2 \in \{0,1\}^n$: $(x_1, x_2, x_3) \neq (x'_1, x'_2, x'_3)$ such that $\mathsf{H}(K_1||K_2, x_1||x_2||x_3) = \mathsf{H}(K_1||K_2, x'_1||x'_2||x'_3)$.

One example can be:

- $(x_1, x_2, x_3) = (\{1\}^n, \{0\}^n, \{1\}^n)$
- $(x'_1, x'_2, x'_3) = (\{1\}^n, \{0\}^n, \{0\}^n)$
- $\mathsf{H}(K_1||K_2, x_1||x_2||x_3) = \mathsf{E}(K_1, \{1\}^n) \oplus \mathsf{E}(K_2, \{1\}^n \oplus \{0\}^n \oplus \{1\}^n) \oplus \mathsf{E}(K_2, \{1\}^n) = \mathsf{E}(K_1, \{1\}^n) \oplus \mathsf{E}(K_2, \{0\}^n) \oplus \mathsf{E}(K_2, \{1\}^n)$
- $\mathsf{H}(K_1||K_2, x'_1||x'_2||x'_3) = \mathsf{E}(K_1, \{1\}^n) \oplus \mathsf{E}(K_2, \{1\}^n \oplus \{0\}^n \oplus \{0\}^n) \oplus \mathsf{E}(K_2, \{0\}^n) = \mathsf{E}(K_1, \{1\}^n) \oplus \mathsf{E}(K_2, \{1\}^n) \oplus \mathsf{E}(K_2, \{0\}^n) = \mathsf{E}(K_1, \{1\}^n) \oplus \mathsf{E}(K_2, \{0\}^n) \oplus \mathsf{E}(K_2, \{1\}^n)$
- So $\mathsf{H}(K_1||K_2, x_1||x_2||x_3) = \mathsf{H}(K_1||K_2, x'_1||x'_2||x'_3)$

(b)

We define following oracles and distinguisher:

```
oracle KF[H]:

private procedure Init():
$K_1 \xleftarrow{\$} \{0,1\}^k$
$K_2 \xleftarrow{\$} \{0,1\}^k$
public procedure Eval($X$):
return H($K_1||K_2, X$)
```

```
oracle RF[$m, n$]:

private procedure Init():
$T \leftarrow$ empty dictionary
public procedure Eval($X$):
if $T[X] = \perp$ then $T[X] \xleftarrow{\$} \{0,1\}^n$
return $T[X]$
```

```
distinguisher $D^{\mathsf{O}}$:
$(x_1, x_2, x_3) \xleftarrow{\$} (\{0,1\}^n, \{0,1\}^n, \{0,1\}^n)$
$(x_1', x_2', x_3') \leftarrow (x_1, x_2, x_1 \oplus x_2 \oplus x_3)$
$C \leftarrow$ O.Eval($x_1||x_2||x_3$)
$C' \leftarrow$ O.Eval($x_1'||x_2'||x_3$)
if $C = C'$ then
    return 1
return 0
```

Since we have from a) that $\mathsf{H}(K_1||K_2, x_1||x_2||x_3) = \mathsf{H}(K_1||K_2, x_1'||x_2'||x_3')$, we know $Pr[D^{KF[H]} \Rightarrow 1]$ since the distinguisher D is just checking if the oracle returns the same value for $(x_1||x_2||x_3)$ and $(x_1'||x_2'||x_3')$.

Therefore, we have: $\mathsf{Adv}^{\mathsf{prf}}_{\mathsf{H}}(D) = |Pr[D^{KF[H]} \Rightarrow 1] - Pr[D^{RF[m,n]} \Rightarrow 1]| = |1 - \frac{1}{2^n}|$
Since $\frac{1}{2^n}$ shrinks exponentially as n grows, we know that $\mathsf{Adv}^{\mathsf{prf}}_{\mathsf{H}}(D)$ is large.