Problem 1. [5 points] Alice and Bob want to write encrypted messages to a diary so that after decrypting the message they will know who wrote which message. They decide on the following method:

1. all messages of Alice will start with $n$ 0s, whereas
2. all messages of Bob will end with all 0s; and
3. no one will write the message where everything is all 0.

So if Alice wants to write a message $m$ to the diary, she will encrypt the message $0^n \| m$ where $0^n$ is a string of $n$ 0s, and $\|$ denotes concatenation.

Likewise, Bob’s messages will be of the form $m \| 0^n$. Assume that $m$ is also of length $n$ and $m \neq 0^n$. Note that with this encoding, each string that Alice and Bob write in the diary is of length $2n$ and it is never all 0.

To encrypt the message Alice and Bob agree to use one-time pad and jointly select a random key $k$ of length $2n$ which they will use to encrypt and write their strings to the diary.

Show how to decrypt all the messages in the diary without knowing the key $k$ as soon as both Alice and Bob written one string each in the diary. Also, show how to recover the key $k$.

Problem 2. [15 points] Give an example of a function $\nu : \mathbb{N} \rightarrow \mathbb{R}$ which is neither negligible nor non-negligible.

Problem 3. Suppose that $f : \{0,1\}^n \rightarrow \{0,1\}^n$ is a function such that $f(x) = 011\|0^{n-3}$.

- [5 points] Show that $f$ is not a one-way function (OWF).
- [5 points] Show that the last bit of $x$ is a hard-core bit for $f$ (even though $f$ is not a OWF).

Problem 4. [40 points] For any two functions $h$ and $g$, $h \circ g$ denotes their composition function, defined as follows$^1$:

$$(h \circ g)(x) = h(g(x)).$$

Let $f : \{0,1\}^n \rightarrow \{0,1\}^n$ be a OWF from $n$-bit strings to $n$-bit strings. Construct a new function $F$ using $f$ such that $F$ is also a OWF but $F \circ F$ is not a OWF. Support your answer by giving a proof that (a) $F$ is one-way, and (b) showing an attack against $F \circ F$.

$^1$Assume that the range of function $g$ is a subset of the domain of function $f$. 
Problem 5. This question highlights the difference between a one-way permutation (OWP) and a one-way function (OWF). Suppose that \( g : \{0,1\}^n \rightarrow \{0,1\}^n \) is a permutation. This means that for every \( y \in \{0,1\}^n \) there exists a unique \( x \in \{0,1\}^n \) such that \( g(x) = y \). (Note: do not assume that \( g \) is one-way).

- **[15 points]** Prove that if \( g \) has a hardcore predicate \( h \), then \( g \) is also one-way.

  *Hint 1:* Prove by contradiction. Assume that an efficient adversary \( A \) can invert \( g \) with noticeable probability. Then use \( A \) to prove that \( h \) is not a hardcore predicate for \( g \) by guessing \( h(x) \) with more than \( 1/2 \) probability.

  *Hint 2:* When using \( A \) to guess \( h(x) \) (given \( g(x) \) for a random \( x \)), if \( A \) fails to invert \( g \), you can always make a random guess for \( h(x) \) and be correct with probability \( 1/2 \).

  *Hint 3:* Do you notice the difference between this problem and Problem 3?

- **[5 points]** Prove that the composition function \( G = g \circ g \) is also a permutation.

- **[10 points]** Prove that if \( g \) is one-way then \( G = g \circ g \) define above is also one-way.

  *Hint 3:* Do you notice the difference between this problem and Problem 4?