- **Assignment 1: Task 3**
- Deadline: 12th Feb. (Submit at the beginning of the class. You lose 4 point per day for late submissions.)

There are 4 questions for a total of 24 points.

---

(6) 1. We define the following new notion of security for PRGs:

Definition 1 (odd-even security). *Consider a PRG* $G : \{0,1\}^k \rightarrow \{0,1\}^{l(k)}$*. Let* $e_1, o_1, e_2, o_2, ...$ *denote the output bits of the PRG. G is considered odd-even secure if for every PPT algorithm A, we have:*

$$\forall i, \mathbf{Pr}[A(o_1, o_2, ...) = e_i] \leq 1/2 + negl(k), \text{ and}$$
$$\forall i, \mathbf{Pr}[A(e_1, e_2, ...) = o_i] \leq 1/2 + negl(k).$$

Show that if G is a secure PRG (w.r.t. indistinguishability[1]), then G is also odd-even secure.

(6) 2. Suppose we have a secure PRF $F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ (key, input, output are of equal length). The following PRG using F was suggested in the class:
$G(s)$

- Parse s as (K, x) such that $|K| = |x| = n$.
- Output $F_K(x)||F_K(F_K(x))||F_K(F_K(F_K(x)))||...||\underbrace{F_K(...F_K(x))}_{q \text{ terms}}$ of length qn bits.

Is G a secure PRG? Discuss. The more rigorous your answer is, the more points you will get.

(6) 3. We said in class that for one-time encryption schemes, message-indistinguishability is a strong notion of security that implies most other security notions. We saw some examples of this fact but still the message indistinguishability is slightly non-intuitive. Here is the formal definition os message-indistinguishability:

Definition 2 (Message Indistinguishability). *A one-time encryption scheme* (E, D) *is said to be secure with respect to message-indistinguishability if for every PPT adversary A and every pair of messages* m_0 *and* m_1 *of equal size, there exists a negligible function negl such that:*

$$|\mathbf{Pr}[A(E_K(m_0)) = 1] - \mathbf{Pr}[A(E_K(m_1)) = 1]| \leq negl(k)$$

where the probabilities are over choice of the key K and internal randomness of A (and the internal randomness of the encryption algorithm in case the algorithm is randomized.)

It came out during the discussion that a more intuitive strong security notion would be that given any *auxiliary* information about the message distribution[2], the ability of a bounded adversary in computing a function of the message should not increase when it has access to the cipher text corresponding to the message. This is known as *Semantic Security*. We formally define this security notion for one-time encryption schemes below:

Definition 3 (Semantic security). *A one-time encryption scheme* (E, D) *is said to to be semantically secure if for every PPT adversary A, there is a PPT adversary* A' *such that for all efficiently* sampleable

[1] recall that this is our standard notion of security for PRGs

[2] Note that we were able to break the substitution cipher because we had this auxiliary information that messages were typical english write-ups.

distributions $(X_1, X_2 ...,)$ [3] *and all polynomial time computable functions* I *and* f*, there exists a negligible function* $negl$ *such that*

$$|\mathbf{Pr}[A(I(m), E_K(m)) = f(m)] - \mathbf{Pr}[A'(I(m)) = f(m)]| \leq negl(k)$$

where m *is chosen according to distribution* X_k*, and the probabilities are taken over the choices of* m*, key* K*, and internal randomness of* A *and* A' *(and the internal randomness of the encryption algorithm in case the algorithm is randomized.).*

Show that the one-time encryption scheme is secure (w.r.t. message-indistinguishability) if and only if it is satisfies semantic security.

(6) 4. Later in the course, we will show that PRGs exist if One Way Functions (OWFs) exist. Someone asked if we can base existence of OWFs on the assumption that $\mathbf{P} \neq \mathbf{NP}$. This is unlikely, though unresolved. However, we can easily show that if $\mathbf{P} = \mathbf{NP}$, then secure OWFs cannot exist. This is precisely what you are asked to do in this question. For this, first we have to define what OWFs are.

Definition 4 (One Way Function). *A function* $f : \{0,1\}^* \rightarrow \{0,1\}^*$ *is called a one way function if the following two conditions hold:*

1. *(Easy to compute:) There exists a polynomial-time algorithm* M_f *computing* f*; that is,* $M_f(x) = f(x)$ *for all* x*.*
2. *(Hard to invert:) For every PPT algorithm* A*, there exists a negligible function* $negl$ *such that*

$$\mathbf{Pr}[Invert_{A,f}(n) = 1] \leq negl(n)$$

Where $Invert_{A,f}(n)$ *denotes the following experiment:*
$Invert_{A,f}(n)$

- *Choose input* $x \leftarrow \{0,1\}^n$*. Compute* $y = f(x)$*.*
- *Execute* A *with inputs* 1^n *and* y*. Let* x' *be the output of* A*.*
- *The output of the experiment is defined to be 1 if* $f(x') = y$*, and 0 otherwise.*

Show that if $\mathbf{P} = \mathbf{NP}$, then one way functions do not exist.

[3] This gives us the freedom of having different distributions for different values of the security parameter (here the key length k). Efficiently sampleable distribution means that there is a randomized algorithm that runs in time polynomial in k (you may assume that this algorithm takes 1^k as input) and outputs elements of the message space such that the output distribution is X_k.