Quiz I

Full Marks: 20, **Time**: 1 hour (+ 15 minutes)

Roll Number: ____________________ **Name:** ____________________

1. Answer each question on a new page of the answer booklet.
2. Do not use pencils. Pens only!

Problem 1: [5 marks]

Let q elements $y_1, y_2, \ldots, y_q$ be chosen uniformly and independently at random from a set of size N, then show that:

$$\text{coll}(q, N) = \Pr[\exists i \neq j \text{ s.t. } y_i = y_j] \leq \frac{q^2}{2N}$$

Problem 2: [7 marks (3+4)]

1. Assume we require only that an encryption scheme $(\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$ with message space $\mathcal{M}$ satisfy the following: For all $m \in \mathcal{M}$, we have $\mathbb{P}[\texttt{Dec}_K(\texttt{Enc}_K(m)) = m] \geq 2^{-t}$. (This probability is taken over the choice of the key as well as any randomness used during encryption.) Show that perfect secrecy can be achieved with $|\mathcal{K}| < |\mathcal{M}|$ when $t \geq 1$. Prove a lower bound on the size of $\mathcal{K}$ in terms of t.

2. Let $\epsilon \geq 0$ be a constant. Say an encryption scheme is ϵ-*perfectly secret* if for every adversary $\mathcal{A}$ it holds that
$$\mathbb{P}[\texttt{Priv}^{\texttt{eav}}_{\mathcal{A},\Pi} = 1] \leq \frac{1}{2} + \epsilon.$$
Show that for ϵ-perfectly secure encryption (with $\epsilon > 0$), $|\mathcal{K}| \geq (1 - \epsilon) \cdot |\mathcal{M}|$.

Problem 3: [8 marks (2+2+2)+2 (for correct reasons)]

Let $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ be a pseudorandom generator (PRG), with $\ell(n) > 2n$. In each case below, answer whether G' is a PRG or not. If yes, give a proof; if not, show a counterexample.

1. $G'(s) \stackrel{\text{def}}{=} G(s_1 \cdots s_{\lfloor n/2 \rfloor})$, where $s = s_1 \cdots s_n$.

2. $G'(s) \stackrel{\text{def}}{=} G(0^{|s|}||s)$, where $||$ means concatenation.

3. $G'(s) \stackrel{\text{def}}{=} G(s)||G(s+1)$.

Problem 4 (bonus): [4 marks]

Here is how we defined *pseudorandom ciphertext security*, which intuitively says that no efficient adversary can distinguish an encryption of a chosen message from a random ciphertext. Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme defined over key space $\mathcal{K}$, message space $\mathcal{M}$, and ciphertext space $\mathcal{C}$. Assume that one can generate ciphertext from $\mathcal{C}$ at random. We define the following game between an adversary Eve^{prcs} and challenger:

- Eve^{prcs} selects $m \in \mathcal{M}$ and sends it to the challenger.
- The challenger picks $b \in_R \{0,1\}$, $k \leftarrow \mathsf{Gen}(1^n)$. It then computes $c_0 \leftarrow \mathsf{Enc}(k, m)$, picks $c_1 \in_R \mathcal{C}$, and sends c_b to Eve^{prcs}.
- Eve^{prcs} outputs a bit b'.

The game $\mathsf{PRCS}_{\mathsf{Eve}^{prcs},\Pi}$ above outputs 1 if $b' = b$ (i.e., Eve^{prcs} wins), and 0, otherwise.

Π satisfies **pseudorandom ciphertext security** if for every PPT Eve^{prcs}, there exists a negligible function negl such that

$$\Pr[\mathsf{PRCS}_{\mathsf{Eve}^{prcs},\Pi}(n) = 1] \leq 1/2 + \mathsf{negl}(n)$$

Prove that if Π is pseudorandom ciphertext secure, then Π satisfies computational indistinguishability against an eavesdropper (as we defined in class).