POIS Quiz 1 **29 January 2024**

1. Prove or disprove the negligibility of the following functions:
   (a) $\frac{2^{-1000}}{n}$
   (b) $\frac{1}{(logn)!}$
   (c) $\frac{1}{(\log \log n)!}$
   (d) $2^{\frac{-n}{1000}}$

   [10]

2. Using your experience in security definitions, provide a definition for perfect pseudorandom generators $G : \{0,1\}^n \to \{0,1\}^{n+1}$. Furthermore, prove that such perfect PRGs do not exist. [10]

3. Assuming that DLP is hard in Z_{17}^* (of course, it isn't really), using 4-bits to represent each of its elements, design a corresponding PRG $G : \{0,1\}^4 \to \{0,1\}^*$, and output the first six bits if seed is set to be the last 4 bits of your choice (say, the last 4 bits of the last 2 digits of your roll number). [10]

4. Prove that the shift cipher is perfectly secret as long as only one character in $[a, \ldots, z]$ is encrypted. [10]