CS 427/519: Homework 2

Due: Monday January 29, 10pm; **typed** and **submitted electronically**.

1. I used 2-out-of-10 Shamir secret sharing over $\mathbb{Z}_{11}$ to share a secret. Alice's share was $(4, 6)$ and Bob's was $(7, 3)$. Two shares should be enough to reconstruct the secret. So, what was the secret, and what were the other 8 shares? **Show your work.**

2. Suppose there are 9 people on an important committee: Alice, Bob, Carol, David, Eve, Frank, Gina, Harold, & Irene. Alice, Bob & Carol form a subcommittee; David, Eve & Frank form another subcommittee; and Gina, Harold & Irene form another subcommittee.

   Suggest how a dealer can share a secret so that it can only be opened when a *majority of each subcommittee* is present. Clearly describe how the Share and Reconstruct algorithms work (not necessarily using actual code). Describe why a 6-out-of-9 threshold secret-sharing scheme does **not** suffice.

3. Suppose f and g are negligible functions.

   (a) Use the definitions to show that $f + g$ is also negligible.

   (b) Give an example f and g which are both negligible (and nonzero), but where $f(\lambda)/g(\lambda)$ is not negligible.

grad. Prove that the two libraries are indistinguishable.

$\mathcal{L}_{\text{left}}$

$\textsc{avoid}(v \in \{0,1\}^\lambda)$:
  return null

$\textsc{samp}()$:
  $r \leftarrow \{0,1\}^\lambda$
  return r

$\mathcal{L}_{\text{right}}$

$\mathcal{V} := \emptyset$

$\textsc{avoid}(v \in \{0,1\}^\lambda)$:
  $\mathcal{V} := \mathcal{V} \cup \{v\}$
  return null

$\textsc{samp}()$:
  $r \leftarrow \{0,1\}^\lambda \setminus \mathcal{V}$
  return r

More precisely, show that if an adversary makes q_1 number of calls to $\textsc{avoid}$ and q_2 calls to $\textsc{samp}$, then its distinguishing advantage is at most $q_1 q_2 / 2^\lambda$. For a polynomial-time adversary, both q_1 and q_2 (and hence their product) are polynomial functions of the security parameter, so the advantage is negligible.