Quiz 10 Solutions

written by Alvin Wan . alvinwan.com/cs70

Thursday, February 25, 2016

This quiz does not count towards your grade. It exists to simply gauge your understanding. Treat this as though it were a portion of your midterm or final exam. In this quiz, we will walk through creating schemes for secret sharing.

1 Dog-mania

In this problem we have two groups of dogs, A for Australian Terriers, and B for Beagles. There are n dog breeds, $\{D_1, D_2, ...D_{n-1}\}$

1. Develop a scheme that requires x_1 dogs from A and x_2 dogs from B.

   Solution: Create a polynomial of degree $x_1 - 1$ for A and a second polynomial of degree $x_2 - 1$ for B. Use the roots of both polynomials to create a third polynomial of degree 1.

2. Develop a scheme that requires x_i from each of the n dog breeds.

   Solution: Create a n polynomials with degree $x_i - 1$ for the ith group. Use the roots of all n polynomials to create an $n + 1$th polynomial of degree $n - 1$.

3. Now, each dog breed elects o_i officials for a canine government. Construct a scheme that requires a_i officials from each breed; however, any 10 non-official dogs can get together to take the place of an official.

   Solution: Create a polynomial of degree $10a_i - 1$, and give each of the a_i officials 10 points each. Then, give each common dog 1 point each. Use the roots of all n polynomials to create an $n + 1$th polynomial of degree $n - 1$.

   Explanation: Since each official has 10 times the number of packets for the same polynomial, any 10 common dogs can "merge" to become a single official.

   Trick: "Re-weight" the packets given to each person.