Solutions to Problem Set 9

Problem 9-1. Stuffing the ballot box

Okay, so I don’t know why we made the special evil rule. However, we did, and I hope people followed it, and it was good.

There were several approaches to solving this problem, I tried to evaluate them fairly, and if I found no flaws in them, and they made sense, they got full credit. Two popular solutions include

- Create multiple admins, and have votes go through all of them (so there will be multiple signatures on each ballot). This is not a cryptographic solution, but it does ensure security as long as it is much less likely to have two corrupt admins. Maybe even creating a watchdog group to appoint admins and verify their work. This always reduces to trusting a small set of people however.

- Use a PKCS when signing, with every user having a well established public key. After the votes have all been submitted to the admin, the admin will publish ALL the \(<ID, e, s>\) triplets he has. It should be a fairly tedious but feasible job to make sure all signatures are valid. Then, if the count of triplets and final tally do not match, something is wrong. Unfortunately, this makes it fairly easy to sabotage the elections. Also, there is the possibility of reusing votes from previous elections (though this can be fixed by submitting a more complex vote which also encodes the current date into the signature).

Understanding the fundamental issues that lead to this problem, and explaining a solution which would work, while analyzing the potential downside of it, is what was looked for in a solution.