META

Polynomials, Secret Sharing, Erasure Errors, General Errors, Self Reference

1 General Comments

1. Logistics
   - Let students know that not everything will be covered during section.
   - Also remind them to check the Piazza for solutions and walkthroughs!
2. RSA
   - Sections earlier in the week may not have strong RSA practice, so dont spend too much time if they arent very familiar with it
   - If you dont get to the RSA questions, briefly explain how it works on a high-level
   - Make sure they understand how RSA actually works the implementation questions test for that pretty well
   - Draw a picture! Ask what is public? What is private?
   - Coin tosses question is interesting. Tests if they actually understand why RSA works, rather than just how its implemented
   - Go over the proof from notes on how/why RSA works
3. Polynomials
   - Draw a graph to visualize why n+1 points are needed for an n-degree polynomial.
   - Make sure that the students are clear with the interpolation formula.
   - Question 1a: Have students convince themselves that it works for the first few polynomials.
   - Question 1b: Have students write out the first few polynomials to find a pattern with the degree.

4. Secret Sharing
   - Explain how polynomials are used for secret sharing. For example: what is the secret in terms of the polynomial? and what is shared among sharers?
   - Figure out which of the schemes to use (polynomial facts, erasure code or general error?) It's most likely that we have not cover general error yet but it's fine to have a quick introduction/leave an open question.
5. Erasure Errors
   - This should go fairly quickly.
   - The first 4 questions (before exercises) are meant to be the lesson plan. Go over this together with the students.
   - First exercise problem is purely algebraic (Group 2 (Thu/Fri) might want to skip).

2 Questions

2.1 Polynomials

1. **Polynomial Facts**
   - Draw a picture to cover the rules in the box
   - Good induction practice!!!

2.2 Erasure Errors

1. **Send N**
   - Second one is more: set up equation as (how many packets are sent)*(fraction packets not erased) = (number packets in original message)