SPCS CRYPTOGRAPHY
HOMEWORK 11 (EXTREMELY OPTIONAL)

Spend time on your project first - think about these problems only if you are bored, perhaps. You are strongly encouraged to work in groups, but you have to write up the solution on your own.

1. Write down a quadratic polynomial whose graph passes through $(2, 4), (4, 7), (8, 1)$.

2. Consider a card game played on a deck of 9 cards (cards 1 through 9). Alice, Bob and Eve are the players. Each player is dealt three cards.
   (a) Find an algorithm for Alice and Bob to secretly decide upon a bit (1 or 0) using only public communication, using the cards in their hand.
   (b) Compare your algorithm with Diffie-Hellman. What's the difference?

3. Zelda has a secret to share with Alice, Bob, Carol, Donna, Edgar (yes, not Eve), Frank, and George (abbreviated A,B,C,D,E,F,G) so that
   - ABCDE can determine the secret.
   - AF can determine the secret.
   - BF can determine the secret.
   - CF can determine the secret.
   - AG can determine the secret.
   - BG can determine the secret.
   - CG can determine the secret.
   - DG can determine the secret.
   - EG can determine the secret.
   - FG can determine the secret.
   - No proper subset of the above can determine the secret.

   Can you figure out a way to do it?

4. Alice solved a Sudoku puzzle just now. Bob does not believe her. Help Alice come up with a zero-knowledge proof to Bob.