Crypto and Comm Security	Homework 5
CS 6750 Fall 2009 (Pucella)	Due: Nov 5, 2009

Note on integrity: You may discuss problems with fellow students, but all written work must be entirely your own, and should not be from any other course, present or past. If you use a solution from another source you must cite it, including from other people who help you.

Questions

(1) (Stinson, exercise 13.1) Write a computer program to compute the key for the Shamir (t,w)-Threshold Scheme implemented in $\mathbb{Z}_p$. That is, given t public x-coordinates $x_1, x_2, \ldots, x_t$ and t y-coordinates $y_1, y_2, \ldots, y_t$, compute the resulting key using the Lagrange interpolation formula.

(a) Test your program if $p = 31847$, $t = 5$, and $w = 10$, with the following shares:

x_1	=	413	y_1	=	25439
x_2	=	432	y_2	=	14847
x_3	=	451	y_3	=	24780
x_4	=	470	y_4	=	5910
x_5	=	489	y_5	=	12734
x_6	=	508	y_6	=	12492
x_7	=	527	y_7	=	12555
x_8	=	546	y_8	=	28578
x_9	=	565	y_9	=	20806
x_{10}	=	584	y_{10}	=	21462

Verify that the same key is computed by using several different subsets of five shares.

(b) Having determined the key, compute the share that would be given to a participant with x-coordinate equal to 10000. (Note that this can be done without computing the whole secret polynomial $a(x)$.)

(2) Let $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5, P_6\}$. Set up a secret sharing scheme, such that exactly the groups $\{P_1, P_2\}$, $\{Q \subseteq P : |Q| \geq 3, P_1 \in Q\}$ and $\{Q \subseteq P : |Q| \geq 4, P_2 \in Q\}$ are authorized subsets, where $|Q|$ is the number of parties in the set Q. You may want to refer to Stinson section 13.2 for this one.