Math/CS 103	Professor: Padraic Bartlett

Homework 16: Cryptography and Latin Squares

Due Friday, week 9 — *UCSB 2014*

Homework Problems.

Pick **two** of the following **four** problems to solve!

1. Take a $n \times n$ Latin square L filled with the symbols $\{s_1, \ldots s_n\}$, such that its first row and first column consist of the symbols $s_1, \ldots s_n$ in order. For example,

$$\begin{bmatrix} s_1 & s_2 & s_3 \\ s_2 & s_3 & s_1 \\ s_3 & s_1 & s_2 \end{bmatrix}$$

   is a Latin square in the desired form.

   Use L to define an operation $\cdot$ on the set $\{s_1, \ldots s_n\}$ as follows: define $s_i \cdot s_j$ to be whatever symbol is in cell (i, j). Does this define a group? If so, prove this claim; if not, construct an example that disproves the claim.

2. Consider the following method of turning a set of $n \times n$ mutually orthogonal Latin squares into a cryptographic scheme:

   - For two parties A, B to communicate, we ask that they pick a pair of mutually orthogonal Latin square L_1, L_2 from our set of orthogonal squares.
   - Now, suppose that A wants to send some plaintext message of the form (i, j), where $i, j \in \{1, \ldots n\}$.
   - To do this, have A send instead the pair (α, β), where α is the symbol in cell $L_1(i, j)$ and β is the symbol in cell $L_2(i, j)$.

   Prove that B can always decode this received signal (α, β) uniquely.

3. Create two Latin squares, one of order 4 and another of order 5. For each, find a minimal critical set. Prove that your sets are indeed minimal and critical.

4. Construct a (t, k)- secret sharing system, where both $t, k \geq 4$.