MATH 3375 (Theory of Cryptology) – Fall 2013

Homework Assignment 6

Due: October 31, 2013

---

1. From Section 3.1 Exercise 1
2. From Section 3.2 Exercise 1a, 1d, 3a, 3b, 5, 10a, 15,
3. From Section 3.3 Exercise 1
4. The following questions concern Hill's original paper "Concerning certain linear transformation apparatus of cryptography". A link to a copy of this paper can be found on the class website. Using this paper, answer the following questions:
   (*a*) Which of the following sets are scales: $\mathbb{Z}, \mathbb{R}$, and $\mathbb{Z}_{26}$? Justify your answers.
   (*b*) Hill uses the notation $S(n)$. What is the modern notation? Repeat for $R\{n\}$.
   (*c*) Give an example of a regular element in $\mathbb{Z}_{26}$ and a signular element.
   (*d*) What term do we use for recipical?
   (*e*) Look on page 138. Have you seen the division property before? Where?
   (*f*) Look at Sections 11 and 12 (and the previous sections for any needed definitions and examples). Explain why what we did in class is a very special case of Hill's result? In particular, what does n and f correspond to from class?