Math 2240	Poor Man's Cryptography	Project #2

DUE: Wednesday, September 24^{th} at the **beginning** of class.

Section 2.5 in your textbook describes a poor man's cryptosystem. *Warning:* If, for example, `BillCooksBigDiscounts.com` uses this form of cryptography and you placed an order with them, you'll soon be a "poor man" too – this system is *very* easy to break! But you'll make some hacker happy and isn't that more important than your financial security? Anyway...

- Write up problems: #16 (encoding), #22 (decoding), and #24 (breaking).
- Consider the 3 by 3 elementary matrix associated with the operation: "Swap Row 1 and Row 3". What will this matrix do to each block of 3 symbols?
- Make an 5 by 5 encoding matrix which reverses each 5 symbol block in a message. Also, give an example of encoding and decoding a short message with this matrix.
- Discuss the relationship between elementary matrices and encoding matrices which "scramble" messages (i.e. rearrange the order of symbols).

Now that you've had some practice, I want you to make up your own encoding matrix and message. But first, notice that so far each encoding matrix has integer entries and the corresponding decoding matrix has integer entries as well. I want you to make sure that this is the case for your matrix.

- Think about the algorithm for finding the (multiplicative) inverse of a square matrix. Which operation(s) can introduce fractions?
- Create (an interesting) 3 by 3 encoding matrix and use it to encode and decode a short message. *Hint:* To make your encoding matrix start with the 3 by 3 identity and perform acceptible row operations on it.
- Write your encoding and decoding matrices as products of elementary matrices. Discuss which kinds of elementary matrices appear in your factorization.