Homework 24, due October 30

(1) Alice, Bob, and Eve use a public key cryptosystem; they have keys k_A, k_B, k_E respectively. (Thus Alice has encryption and decryptions functions E_{k_A} and D_{k_A}, etc.) Alice proposes that to send messages, they use the following protocol for user X to send message M to user Y (messages are of the form (sender's name, text, receiver's name), and $M|X$ is the concatenation of the strings M and X):

- X sends Y the message $(X, E_{k_Y}(M|X), Y)$.
- Y's computer decrypts $M|X$ by applying D_{k_Y}, and acknowledges receipt by automatically sending X the message $(Y, E_{k_X}(M|Y), X)$.

Eve claims that this protocol is too complicated, and that it would be easier to do the following:

- X sends Y $(X, E_{k_Y}(M), Y)$.
- Y acknowledges receipt by sending X $(Y, E_{k_X}(M), X)$.

If Eve can intercept Alice and Bob's encrypted messages, how could she use this simplified protocol to read a message M that Alice has previously sent (encrypted) to Bob?

(2) Let $p = 37$. Evaluate $L_2(24)$.

(3) (Page 215, problem 8) Suppose you have a random 500-digit prime p. Some people want to store passwords, written as numbers. If x is the password, then the number $2^x \pmod p$ is stored in a file. When y is given as a password, the number $2^y \pmod p$ is compared with the entry for the user in the file. Suppose someone gains access to the file. Why is it hard to deduce the passwords? If instead p is chosen to be a five digit prime, why would the system not be secure?