Crypto and Comm Security	Homework 6
CS 6750 Fall 2009 (Pucella)	Due: Nov 12, 2008

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, Question 5.15) This exercise exhibits what is called a *protocol failure*. It provides an example where ciphertext can be decrypted by an opponent, without determining the key, if a cryptosystem is used in a careless way. The moral is that it is not sufficient to use a "secure" cryptosystem in order to guarantee "secure" communication.

Suppose Bob has an *RSA Cryptosystem* with a large modulus n for which the factorization cannot be found in a reasonable amount of time. Suppose Alice sends a message to Bob by representing each alphabetic character as an integer between 0 and 25 (where A is 0, B is 1, C is 2, etc.), and then encrypting each residue modulo 26 as a separate plaintext character.

(a) Describe how Oscar can easily decrypt a message which is encrypted in this way.

(b) Illustrate this attack by decrypting the following ciphertext (which was encrypted using an *RSA Cryptosystem* with $n = 18721$ and $b = 25$) without factoring the modulus:

$$365, 0, 4845, 14930, 2608, 2608, 0.$$

(2) Alice and Bob have fallen in love, via the internet. Bob wishes to mail Alice a ring. Unfortunately, they live in a country where anything sent through the mail will be stolen unless it is enclosed in a box with a padlock through the latch. Alice and Bob each have plenty of padlocks, each with its own key to unlock it. Unfortunately, they do not have a single padlock for which they both have a key. Given all of this, can Bob get the ring safely into Alice's hands (using the mail, of course), and if so, how?