Crypto and Comm Security	**Homework 1**
CS 6750 Fall 2009 (Pucella)	**Due: Sep 24, 2009**

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, 1.6) If an encryption function e_K is identical to the decryption function d_K, then the key K is said to be an *involutory key*. Find all involutory keys in the *Shift Cipher* over $\mathbb{Z}_{26}$.

(2) (Stinson, 1.21(a)–(b)) Below are given two examples of ciphertext, one obtained from a *Substitution Cipher*, the other from a *Vigenère Cipher*. In each case, the task is to determine the plaintext.

Give a clearly written description of the steps you followed to decrypt each ciphertext. This should include all statistical analysis and computations you performed.

The plaintexts were taken from "The Diary of Samuel Marchbanks", by Robertson Davies, Clarke Irwin, 1947.

(a) *Substitution Cipher*: (Hint: F decrypts to w)

```
EMGLOSUDCGDNCUSWYSFHNSFCYKDPUMLWGYICOXYSIPJCK
QPKUGKMGOLICGINCGACKSNISACYKZSCKXECJCKSHYSXCG
IODPKZCNKSHICGIWYGKKGKGOLDSILKGOIUSIGLEDSPWZU
GFZCCNDGYYSFUSZCNXEOJNCGYEOWEUPXEZGACGNFGLKNS
ACIGOIYCKXCJUCIUZCFZCCNDGYYSFEUEKUZCSOCFZCCNC
IACZEJNCSHFZEJZEGMXCYHCJUMGKUCY
```

(b) *Vigenère Cipher*:

```
KCCPKBGUFDPHQTYAVINRRTMVGRKDNBVFDETDGILTXRGUD
DKOTFMBPVGEGLTGCKQRACQCWDNAWCRXIZAKFTLEWRPTYC
QKYVXCHKFTPONCQQRHJVAJUWETMCMSPKQDYHJVDAHCTRL
SVSKCGCZQQDZXGSFRLSWCWSJTBHAFSIASPRJAHKJRJUMV
GKMITZHFPDISPZLVLGWTFPLKKEBDPGCEBSHCTJRWXBAFS
PEZQNRWXCVYCGAONWDDKACKAWBBIKFTIOVKCGGHJVLNHI
FFSQESVYCLACNVRWBBIREPBBVFEXOSCDYGZWPFDTKFQIY
CWHJVLNHIQIBTKHJVNPIST
```

Note: while I believe the above is correct, I cannot make any guarantees that I did not mess up copying the ciphertexts...

(3) Let n be a positive integer. A *Latin square* of order n is an $n \times n$ array L of the integers $1, \ldots, n$ such that every one of the n integers occurs exactly once in each row and each column of L. An example of a Latin square of order 3 is as follows:

1	2	3
3	1	2
2	3	1

Given any Latin square L of order n, we can define a related cryptosystem. Take $P = C = K = \{1, \ldots, n\}$. For $1 \leq i \leq n$, the encryption rule e_i is defined to be $e_i(j) = L(i, j)$, the entry of L at row i and column j. (Hence each row of L gives rise to one encryption rule.)

Give a complete proof that this *Latin Square Cryptosystem* achieves perfect secrecy provided that every key is used with equal probability.

(4) Show that if a cryptosystem has perfect secrecy and $|K| = |C| = |P|$, then every ciphertext is equally probable.