CS165 – Computer Security
Assignment 1 (Due November 8 2014)

1. The file book1.enc is an encrypted version of one of the books from Project Gutenberg (www.gutenberg.org). It was encrypted using a stream cipher whose key stream was taken from the output of a linear congruential random number generator. Specifically, each character of the plaintext (encoded using UTF-8) was converted into an integer, and then that integer was added with the corresponding output from the LCG. Each line of book1.enc contains the encrypted version of a single character from the plaintext. Decrypt book1.enc, and provide the parameters of the random number generator (including the seed).
2. The file book2.enc is also an encrypted version of one of the books from Project Gutenberg. This time, it was encrypted using a combination of two ciphers. The first was a mono-alphabetic substitution cipher. The second was a columnar transposition cipher. Decrypt book2.enc. Provide the number of columns that were used in the transposition cipher.
3. Prove: For all $n \geq 3$, $\varphi(n)$ is even.
4. Prove: If $m \perp n$, then $n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 \pmod{mn}$
5. Prove: If $a \perp n$, then $a^{\varphi(n-1)} + a^{\varphi(n-2)} + \ldots + a^2 + a + 1 \equiv 0 \pmod{n}$

For problems 1 and 2, provide a brief but complete (no longer than 1 page) description of the techniques that you used to break the cipher. You will be graded not only on your ability to correctly decrypt the documents, but also on your ability to explain how you were able to do so.

When you have completed the assignment, create a PDF containing your responses to all of the questions. Create a tar archive containing that PDF, along with any and all code you wrote to assist you with the assignment.

All code must be written in C/C++, and must be accompanied by a written description of its operation and structure. You may not use any libraries other than the standard language libraries. All code you write must be entirely your own work.