CSci 4554 Assignment 6

Due Monday, March 10th in class

Problem 1 (10 points). Solve the following system of linear equations using the Chinese Remainder Theorem:

$$\begin{aligned} x &\equiv 1 (\text{mod } 3) \\ x &\equiv 2 (\text{mod } 4) \\ x &\equiv 5 (\text{mod } 7) \end{aligned}$$

Problem 2 (5 points). Consider the idea of using a pseudo-random number generator with a 30-bit clock-based seed for generating a sequence of "random" bits for a one-time pad encryption. The generated sequence of bits can be arbitrarily long so it can accommodate any message length. Would this encryption scheme provide security equal to that of a one-time pad? Please explain your answer.

Problem 3 (10 points). The following message is the result of encryption using a 5-letter transposition cipher. Decrypt the message and find the encryption key. Explain how you found the solution.

```
RPTCYGAPORYSTHIERAHPTCECINSTADDOFUYIINHDIFOGNMTIRANO
```

Problem 4 (10 points). Consider a 5-letter key Vigenere cipher followed by a transposition cipher with a 5-letter block (the plaintext and the ciphertext both use English alphabet only).

Question 1. What is the size of the key space for the combined cipher? Show all your computations.

Question 2. Assume that the encrypted message is at least 500 characters long. What are the cipher's weaknesses? Suggest a strategy for breaking this cipher.