Homework 1

Instructions: Submit typed solutions to these problems.

1. Stinson, 2.6: If an encryption function $e(k, p)$ is identical to the decryption function $d(k, c)$ for the same key k, then the key k is said to be an **involutory key**. Find all the involutory keys in the Shift Cipher over $\mathbb{Z}_{26}$.

2. Stinson, 2.26: We describe a special case of a **Permutation Cipher**. Let m, n be positive integers. Write out the plaintext, by rows, in $m \times n$ rectangles. For example, if $m = 3$, $n = 4$, then we would encrypt the plaintext `cryptography is intriguing` by forming the following rectangles:

   ```
   cryp    isin
   togr    trig
   aphy    uing
   ```

   The ciphertext would be formed by reading in columns: `ctaropyghpryitusriiinngg`.

   (a) Describe how Bob would decrypt a ciphertext string, given values for m and n.

   (b) Decrypt the following ciphertext, which was obtained by using this method of encryption (but the values of m and n are not given, nor do you know the number of rectangles, but the text fits into a whole number of rectangles without any letters left over):

   ```
   MYAMRARUYIQTENCTORAHROYWDSOYEOUARRGDERNOGW
   ```

3. This quotation was encrypted with a Substitution Cipher:

   ```
   AOFKW GOZLP OKLUQ KLGDO BGKCL BQGHL IOCPL GDLWG LZZCP GDOGS
   KONQB PLMFP GHCGH LIOCP LGDLW GLZZC PGDOG SKONQ BPIOB HLHLO GLB
   ```

   Carefully explain how you decoded the message. If you were unable to read the message, describe your attempts in detail. This table may be of some use:

   `https://pi.math.cornell.edu/~mec/2003-2004/cryptography/subs/frequencies.html`

4. Consider the congruence $9x \equiv 3 \pmod{12}$. If we multiply both sides by 2, we get $6x \equiv 6 \pmod{12}$, which has the solution $x \equiv 1$. But $x \equiv 1$ is not a solution to the original congruence.

   What happened? All we did was multiply both sides by the same amount! Identify the error in logic being exploited here.

5. Solve the congruence $653x \equiv 12705 \pmod{1287719}$ and show your work. You may use a CAS (Matlab, WolframAlpha, etc.) to assist with 'routine' calculations, but not for solving the congruence directly.

6. Write a formal definition (P, C, K, E, D) for the Affine Cipher.