CPSC 418 / MATH 318 — Introduction to Cryptography
ASSIGNMENT 1

Name: Artem Golovin
Student ID: 30018900

Problem 1 — Superencipherment for substitution ciphers, 12 marks

1. (a) *Proof.* Encryption using Shift cipher is given by $E_K(M) \equiv (M + K) \mod 26$. Given $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$, $K_1, K_2 \in \mathcal{K}$ and $M \in \mathcal{M}$:
   Let $C_1 \in \mathcal{C}$ be a ciphertext that results from encrypting plaintext M with a key K_1:
   i. $E_{K_1}(M) \equiv (M + K_1) \mod 26$
   ii. $C_1 = E_{K_1}$
   iii. $C_1 = (M + K_1) \mod 26$
   iv. Let $C_2 = E_{K_2}(C_1)$, where $E_{K_2}(C_1) \equiv (C_1 + K_2) \mod 26$
   v. Therefore, by substituting C_1,

$$\begin{aligned} C_2 &= (C_1 + K_2) \mod 26 \\ &= ((M + K_1) + K_2) \mod 26 \\ &= (M + K_3) \mod 26 \end{aligned} \tag{1}$$

   Where $K_3 \in \mathcal{K}$ and $K_3 = K_1 + K_2$. Finally, according to definition, C_2 results in shift cipher.

□

   (b)

2.