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. $C_1 \equiv E_{K_1}$
   iii. $C_1 \equiv (M + K_1) \mod 26$
   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,

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

   Where $K_3 \in \mathcal{K}$ and $K_3 = K_1 + K_2$. Therefore, resulting key of multiple encipherment is K_3.

□

   (b) *Proof.* Based on previous proof, superencipherment using shift cipher can be defined as follows

$$E_{K_i}(M) \equiv (M + \sum_{\substack{K_i \in \mathcal{K} \\ i=1}}^{n} K_i) \mod 26$$

   Where $M \in \mathcal{M}$, $K_i \in \mathcal{K}$, $n \in \mathbb{Z}$, and $i \geq 1, i \in \mathbb{Z}$.
   i. Base Case: let $n = 1$,

$$\begin{aligned} C &\equiv (M + \sum_{\substack{K_i \in \mathcal{K} \\ i=1}}^{1} K_i) \mod 26 \\ &\equiv (M + K_1) \mod 26 \end{aligned} \tag{1}$$

   ii. Induction hypothesis: Assume $n = m$, where $m \in \mathbb{Z}$. Therefore:

$$C \equiv (M + \sum_{\substack{K_i \in \mathcal{K} \\ i=1}}^{m} K_i) \mod 26$$

Let:

$$K^{'} = \sum_{\substack{K_i \in \mathcal{K} \\ i=1}}^{m} K_i$$
$$C \equiv (M + K^{'}) \mod 26 \tag{2}$$

Still results in a shift cipher, according to definition.

iii. Inductive case: According to induction hypothesis, we can show that $m+1$ holds true as well:

$$C \equiv (M + \sum_{\substack{K_i \in \mathcal{K} \\ i=1}}^{m+1} K_i) \mod 26$$
$$C \equiv (M + (\sum_{\substack{K_i \in \mathcal{K} \\ i=1}}^{m} K_i + \sum_{\substack{K_i \in \mathcal{K} \\ i=1}}^{1} K_i)) \mod 26$$
$$C \equiv (M + (\sum_{\substack{K_i \in \mathcal{K} \\ i=1}}^{m} K_i + K_1)) \mod 26$$
$$C \equiv (M + (K^{'} + K_1)) \mod 26$$
$$C \equiv (M + K^{"}) \mod 26$$

where K_1 is our base case (1) and $K^{'}$ is our induction hypothesis (2). Since $K_1 \in \mathcal{K}$ and $K^{'} \in \mathcal{K}$, therefore $K^{"} = K_1 + K^{'}, K^{"} \in \mathcal{K}$. Hence, the key of multiple encipherment is sum of all given keys.

□

2. *Proof.* Let $M \in \mathcal{M}$ be a plaintext of length $x \in \mathbb{Z}$. Let $p_0, p_1, p_2, ..., p_{x-1}$ be positions of letters in plaintext M. Given key $w_1 \in \mathcal{K}$ of length $m \in \mathbb{Z}$ and key $w_2 \in \mathcal{K}$ of length $n \in \mathbb{Z}$, let $k_0, k_1, k_2, ..., k_{m-1}$ be positions of letters in key w_1, and $l_0, l_1, l_2, ..., l_{n-1}$ be positions of letters in key w_2. To encrypt plaintext p_i, we use a key k_j, where i is letter position from 0 to $x-1$.

$$j \equiv i \pmod m$$

Let ciphertext C_i be ciphertext that corresponds to p_i

$$C_i \equiv p_i + k_j \pmod{26}$$

Where $k_j \equiv i \pmod m$.
Let ciphertext C_{2_i} be ciphertext that corresponds to C_i. Therefore, the second round of encryption, using the key w_2, results in following:

$$\begin{aligned} C_{2_i} &\equiv C_i + l_j && \pmod{26} \\ &\equiv (p_i + k_j) + l_z && \pmod{26} \\ &\equiv p_i + (k_j + l_z) && \pmod{26} \end{aligned}$$

Where $z \equiv i \pmod{n}$ and $l_z \equiv i \pmod{n}$. Therefore that ensures that length of resulting key will be x. $\square$

Problem 2 — Key size versus password size, 21 marks

Problem 3 — Equiprobability maximizes entropy for two outcomes, 12 marks