

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 $E_K(M) \equiv (M + K) \pmod{26}$. 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. $E_{K_1}(M) \equiv (M + K_1) \pmod{26}$
- ii. $C_1 \equiv E_{K_1}(M)$
- iii. $C_1 \equiv (M + K_1) \pmod{26}$
- iv. Let $C_2 = E_{K_2}(C_1)$, where $E_{K_2}(C_1) \equiv (C_1 + K_2) \pmod{26}$
- v. Therefore, by substituting C_1 ,

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

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

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

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 $n = 1$,

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

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

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

Let:

$$K' = \sum_{\substack{K_i \in \mathcal{K} \\ i=1}}^m K_i \quad (2)$$

$$C \equiv (M + K') \pmod{26}$$

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:

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

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

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

$$C \equiv (M + (K' + K_1)) \pmod{26}$$

$$C \equiv (M + K'') \pmod{26}$$

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 $p_0, p_1, p_2, \dots, p_{x-1}$ be positions of letters in plaintext M . Given key w_1 of length m , let $k_0, k_1, k_2, \dots, k_{m-1}$ be positions of letters in key w_1 .

□

Problem 2 — Key size versus password size, 21 marks

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