IS309: Network Security Technology
Tutorial 1, Week 1 (February 23)
Due Date: March 2

Chunyu Xue 518021910698

1 Problem 1

Describe the details of Caesars Cipher (50 points):

(a) Message space M.

Answer: The message space of Caesars Cipher is:

$$M = \{m \mid m \text{ is any string consists of 26 English letters with the length of } n\}$$

(b) Key-generation algorithm $KeyGen$.

Answer: The key-generation algorithm of Caesars Cipher is:

$$KeyGen(\lambda) = \{k \mid k \in \mathbb{N} \text{ and } k \text{ is randomly chosen in the range of } [0, 25] \text{ according to some probabilistic distribution}\}$$

(c) Encryption algorithm Enc.

Answer: The encryption algorithm of Caesars Cipher is:

$$Enc(k, m) = \{c \mid c[i] = (m[i] + k) \bmod 26,\ i \in [1, n]\},$$

which means c is the string that operates k ($k \in \mathbb{N}$ and $k \in [0, 25]$) shifts from original message m.

(d) Decryption algorithm Dec.

Answer: The decryption algorithm of Caesars Cipher is:

$$Dec(k, c) = \{m \mid m[i] = (c[i] - k) \bmod 26,\ i \in [1, n]\},$$

which means m is the string that operates k ($k \in \mathbb{N}$ and $k \in [0, 25]$) shifts (the direction is opposite to the Enc algorithm) from ciphertext c.

(e) Key space K.

Answer: The key space of Caesars Cipher is:

$$K = \{k \mid k = 0, 1, 2, ..., 25\},$$

which means that $|K| = 26$.

(f) Ciphertext space C.

Answer: The ciphertext space of Caesars Cipher is:

$C = \{c \mid c$ is the string that operates k ($k \in \mathbb{N}$ and $k \in [0, 25]$) shifts from original message m, which is also any string consists of 26 English letters with the length of $n\}$

2 Problem 2

Describe the details of Simple Substitution Cipher (50 points):

(a) Message space M.

Answer: The message space of Simple Substitution Cipher is:

$M = \{m \mid m$ is any string consists of 26 English letters with the length of $n\}$

(b) Key-generation algorithm $KeyGen$.

Answer: The key-generation algorithm of Simple Substitution Cipher is:

$KeyGen(\lambda) = \{k \mid k[i] \in \mathbb{N}$ and k is a random permutation of $1, 2, ..., 26$ according to some probabilistic distribution$\}$

(c) Encryption algorithm Enc.

Answer: The encryption algorithm of Simple Substitution Cipher is:

$$Enc(k, m) = \{c \mid c[i] = k[m[i]],\ i \in [1, n]\},$$

which means c is the string that operates hash mapping from original message m according to k.

(d) Decryption algorithm Dec.

Answer: The decryption algorithm of Simple Substitution Cipher is:

$$Dec(k, c) = \{m \mid m[i] = k^{-1}[c[i]],\ i \in [1, n]\},$$

which means m is the string that operates anti-hash mapping from ciphertext c according to k.

(e) Key space K.

Answer: The key space of Simple Substitution Cipher is:

$$K = \{k \mid k = permutation(1,\ 26)\},$$

which means that k is a random permutation of $1, 2, ..., 26$ and $|K| = 26!$.

(f) Ciphertext space C.

Answer: The ciphertext space of Simple Substitution Cipher is:

$C = \{c \mid c$ is the string that operates hash mapping from original message m according to k, which is also any string consists of 26 English letters with the length of $n\}$