Exercise_03

1.

(1) Yes, because the random cipher can achieve truly unbreakable system.

(2) Yes.

$$\begin{aligned} P(plaintext|ciphertext) &= P(D(ciphertext)|ciphertext) \\ &= P(key|ciphertext) \\ &= P(key) \end{aligned}$$

$$\begin{aligned} P(plainttext) &= \sum_y P(plaintext|ciphertext = y)P(ciphertext = y) \\ &= P(key)\sum_y P(ciphertext = c) \\ &= P(key) \end{aligned}$$

so we have

$$P(plaintext|ciphertext) = P(plaintext)$$

which means a strongly ideal cipher can achieve perfect secrecy.

(3) Yes, the ciphertext of one time pad contains no information of the key.

$$\begin{aligned} P(key|ciphertext) &= P(plaintext = key \oplus ciphertext|ciphertext) \\ &= P(plaintext) \\ P(key) &= P(plaintext) \end{aligned}$$

so we have

$$P(key) = P(key|ciphertext)$$

2.

- Turing machine complexity is uniform. It can only be used to prove average complexity of breaking a cryptosystem.
- Gate complexity is non uniform. It defined a lower bound of the complexity so it can be used to prove if a system is provably secure.