CS381 Exercise 3

Name: Zhang Yupeng

Student ID: 5130309468

1. Can the random cipher achieve perfect secrecy?

Yes. Because through random cipher plaintext and ciphertext are statistically independent.

Can a strongly ideal cipher achieve perfect secrecy?

Yes.

Is one-time-pad a strongly ideal cipher?

Yes.

2. What are the differences between Turing-machine complexity and gate complexity?

Turing-Machine Complexity is uniform and symptotic, however, the gate complexity is non-uniform.

3. Prove that the complexity of key-search is 2^{k-1} (hint : define a random variable and compute the average.)

Proof: When do exhaustive key search, for given $x_0, y_0 = E(x_0, k_0)$, try each possible k until $E(x_0, k) = y_0$.

We define a random variable $X(E(x_0, k) = y_0)$, the probability $p_1(E(x_0, k) = y_0) = 1/2^k$, which means doing the search operation once and get the answer, we can similiarly get $p_2, p_3, \ldots p_n$

So, the average number of key-search operation is equal to the expectation of X, which is:

$$\sum_{i=1}^{i=2^k} p_i * x_i = 1 * 1/2^k + 2 * (1 - 1/2^k) * (1/2^{k-1}) + \ldots + 2^k * (1/2^k) = 2^{k-1}$$