Network Security Technology Spring, 2021
Tutorial 2, Week 2 (March 2) LIU Zhen
Due Date: March 9

Questions:

1. **(50 points) Now you've learned the RC4 scheme (one of the stream cipher of symmetric key encryption). Denote $KeyGen(\lambda)$ as the key generation algorithm: pick a uniform $k \in \{0,1\}^{128}$, and output k. Denote m as a message of l bytes and c as the ciphertext. Please use your own words (or pesudocode) to describe the encoding algorithm $Enc(k, m)$ and decoding algorithm $Dec(k, c)$.**

   Hints: 1) The Enc determines the format of ciphertext output. 2) A stream cipher need synchronized information between encryption and decryption side (why?). Consider a real example: after A and B shared secret key k, A is going to send message m_1 to B in the first day and send message m_2 to B in the second day. In the meanwhile, A and B's computers running Enc/Dec may shut down or restart due to failure. Take a look at whether your algorithms can support this example safely and conveniently.

   (a) $Enc(k, m)$.

   (b) $Dec(k, c)$.

2. **(50 points) Suppose the key for a cipher is an l-bit binary string.**

   (a) What is the key space size of this cipher?

   (b) To find a key by exhaustive key search, how many keys does an attacker need to test on average?