Network Security Technology Spring, 2019
Tutorial 1, Week 2 (March 6) LIU Zhen
Due Date: March 20

Questions:

1. **One-Time Pad (20 points)**:

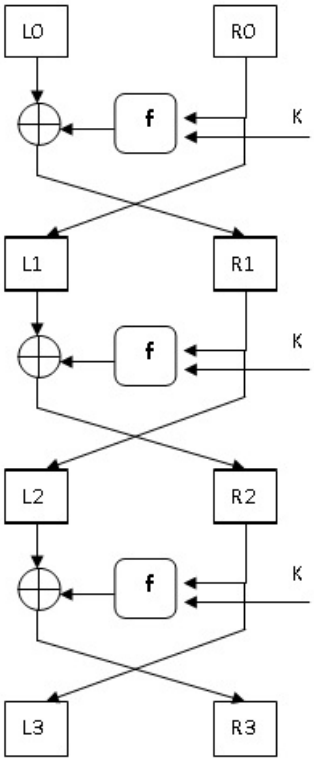
   (a) Alice wants to send the message `SECURE` to Bob using a one-time pad with the value `KTXMLU`. What is the ciphertext?
   Hint: First convert the letters into numbers (with binary form) using the table below. Note that all letters should have the same binary length.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Q	R	S	T	U	V	W	X	Y	Z	,	.	?	!	%	#
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

   (b) What is the plaintext you get if you decrypt the ciphertext from 1a with the key `XDMBRO`?

   (c) Assume a key K is used twice for encrypting two different plaintexts M_1 and M_2. Show what information about the plaintexts an adversary can gain just by looking at the two cipertexts C_1 and C_2.

2. **DES(20 points)**: Consider a simplified DES with only 3 rounds. Suppose that you are given the key K and a ciphertext (L_3, R_3). Show how to compute the plaintext (L_0, R_0).



3. **3DES (20 points)**: Consider 3DES:

$$C = \text{DES}_{K_1}(\text{DES}^{-1}_{K_2}(\text{DES}_{K_1}(M)))$$

where C, M are the ciphertext and plaintext, respectively, and $K = (K_1, K_2)$ is the key.

(a) How many keys on average do we have to try in a brute force attack?

(b) What's the effect if $K_1 = K_2$?

4. **Block Cipher Modes (20 points)**: Suppose that we have a **shift cipher** with plaintext/message space specified in the table below. In other words, the space has 16 letters.

Suppose that the shift cipher is used as a block cipher which has 4-bit input and 4-bit output with the conversion between the letters and binary strings given in the table below.

Let the key be $k = 2$. Encrypt the plaintext $P =$ IAMBOB using CBC mode with IV = 0010.

A	B	C	D	E	F	G	H
0000	0001	0010	0011	0100	0101	0110	0111
I	J	K	L	M	N	O	P
1000	1001	1010	1011	1100	1101	1110	1111

5. **CTR Mode (20 points)**: Suppose a user with secret key K runs DES with CTR mode to encrypt data. (1) Discuss whether he need to worry that two IV's, say IV_1 and IV_2, in two encryptions are too close so that $IV_2 = IV_1 + j$ for some j. (2) Discuss whether he needs to worry $IV + i$ equals to IV for some large i.

Hint: Note that IV is chosen randomly and uniformly.