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 `XDMBRU`?

   (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.

Solution:

(a) We first convert the letters of the plaintext and the one-time pad into numbers and then XOR them modulo 26:

Plaintext M	S	E	C	U	R	E
	10010	00100	00010	10100	10001	00100
One-time pad K	K	T	X	M	L	U
	01010	10011	10111	01100	01011	10100
$M \oplus K$	11000	10111	10101	11000	11010	10000
Ciphertext C	**Y**	**X**	**V**	**Y**	**,**	**Q**

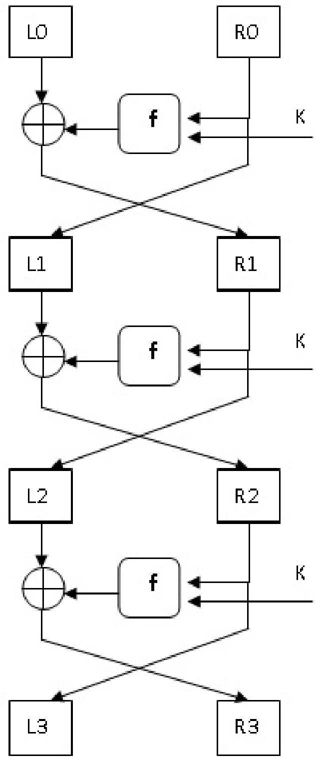
(b) Decrypting the ciphertext using the one-time pad `TQURI` yields the following:

Ciphertext C	Y	X	V	Y	A	Q
	11000	10111	10101	11000	11010	10000
One-time pad K	X	D	M	B	R	U
	10111	00011	01100	00001	10001	10100
$C \oplus K$	01111	10100	11001	11001	01011	00100
Plaintext M	**P**	**U**	**Z**	**Z**	**L**	**E**

Because both decryptions yield an intelligible English word, an adversary cannot know which one is the correct one. It is in fact possible to "decrypt" the ciphertext into any message with the same number of letters by simply using a different key.

(c) The one-time pad is defined as $C = M \oplus K$, with C the ciphertext, M the message and K the key. If we encrypt two messages with the same key and XOR their ciphertext, we get: $C_1 \oplus C_2 = (M_1 \oplus K) \oplus (M_2 \oplus K) = M_1 \oplus M_2$. If a key is re-used an adversary can thus learn the XOR of the two plaintexts.

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).



Solution:

$$
\begin{aligned}
& R_2 = L_3 \\
& L_2 = f(L_3, K) \oplus R_3 \\
\Rightarrow\ & R_1 = L_2 = f(L_3, K) \oplus R_3 \\
& L_1 = f(L_2, K) \oplus R_2 \\
& \quad = f(f(L_3, K) \oplus R_3, K) \oplus L_3 \\
\Rightarrow\ & R_0 = L_1 = f(f(L_3, K) \oplus R_3, K) \oplus L_3 \\
& L_0 = f(L_1, K) \oplus R_1 \\
& \quad = f(f(f(L_3, K) \oplus R_3, K) \oplus L_3, K) \oplus f(L_3, K) \oplus R_3
\end{aligned}
$$

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

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

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 $K_1 = K_2$?

Solution:

(a) This is the expected number of keys we need to try. The length of K is $|K| = |K_1| + |K_2| = 56 + 56 = 112$. Suppose that we always try from $00\cdots 00$. If the key is $K = 00\cdots 0$, we only need to try 1 key. If $K = 00\cdots 1$, we need to try 2 keys. $\cdots$. If $K = 11\cdots 1$, we need to try 2^{112} keys. Since the key K is a random 112-bit string, the probability that K is equal to a particular value is exactly $1/2^{112}$. So the expected number of keys we need to try is $\frac{1}{2^{112}} \times 1 + \cdots + \frac{1}{2^{112}} \times 2^{112} \approx 2^{111}$.

(b) If $K_1 = K_2$, then

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

which is the original DES encryption. This is called **backward compatibility**.

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

Solution: P = IAMBOB = 1000 0000 1100 0001 1110 0001, which consists of 6 blocks of size 4. Since $k = 2$, the encryption of X, $E_k(X)$, where X is any letter, simply is the second letter after X.

$$\begin{aligned}
C_0 &= E_k(IV \oplus P_0) = E_k(0010 \oplus 1000) = E_k(1010) = E_k(\mathrm{K}) = \mathrm{M}(1100) \\
C_1 &= E_k(C_0 \oplus P_1) = E_k(1100 \oplus 0000) = E_k(1100) = E_k(\mathrm{M}) = \mathrm{O}(1110) \\
C_2 &= E_k(C_1 \oplus P_2) = E_k(1110 \oplus 1100) = E_k(0010) = E_k(\mathrm{C}) = \mathrm{E}(0100) \\
C_3 &= E_k(C_2 \oplus P_3) = E_k(0100 \oplus 0001) = E_k(0101) = E_k(\mathrm{F}) = \mathrm{H}(0111) \\
C_4 &= E_k(C_3 \oplus P_4) = E_k(0111 \oplus 1110) = E_k(1001) = E_k(\mathrm{J}) = \mathrm{L}(1011) \\
C_5 &= E_k(C_4 \oplus P_5) = E_k(1011 \oplus 0001) = E_k(1010) = E_k(\mathrm{K}) = \mathrm{M}(1100)
\end{aligned}$$

Therefore, the ciphertext is MOEHLM.

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.
Solution:

(a) IV is the nonce in CTR Mode. Since the IV is chosen randomly and uniformly and k is different in two encryptions, he doesn't need do worry for that case.

(b) Since the length of IV is 64 in DES, it's almost impossible that $IV + I$ equals to IV for some large i. Therefore, he doesn't need to worry for that.