Cryptography Engineering Midterm (revised)

April 2021

0713309 徐宜蓉

Problem 1

In the following let p be a prime. The set $Z_p = \{\, x \text{ integer}, \text{ such that } 0 \le x < p\}$ is a group with respect to addition modulo p (i.e. every element x in Z_p has an inverse $-x \in Z_p$ such that $x + (-x) = 0 \; mod \; p$. The set $Z_p^* = \{\, x \text{ integer}, \text{ such that } 0 < x < p\}$ is a group with respect to multiplication modulo p (i.e. every element x in Z_p^* has an inverse $x^{-1} \in Z_p^*$ such that $xx^{-1} = 1 \; mod \; p$.

(1) Another cipher with perfect secrecy. Consider the following cipher.
Let Z_p^* be the message space, the key space and the ciphertext space.
Alice and Bob share a key $k \in Z_p^*$ uniformly chosen at random. To send a message $m \in Z_p^*$ to Bob, Alice computes the ciphertext $c = mk \; mod \; p$.
Prove that this cipher provides perfect secrecy using the criterium we proved in class.

$c = mk \;\; mod \;\; p$

A cipher (E, D) over (K, M, C) has perfect secrecy if

$\forall m_0, m_1 \in M, len(m_0) = len(m_1) \;\; and$

$\forall c \in C, \Pr[E(k, m_0) = c] = \Pr[E(k, m_1) = c]$ where k is uniform in K

proof:

$Z_p^* = \{\text{integer } \; x, s.t. 0 < x < p\}$

$xx^{-1} \equiv 1 \;\; (mod \;\; p)$

$\rightarrow xx^{-1} = pn + 1, n \in Z_0^+$

Ex. $p = 13$

$pn + 1 = \{1, 14, 27, 40, 53, 66, 79, 92, 105, 118, 131, 144, 157, \ldots\}$

$Z_p^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

$mk \;\; mod \;\; p$ values:

m\k	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	6	8	10	12	1	3	5	7	9	11
3	3	6	9	12	2	5	8	11	1	4	7	10
4	4	8	12	3	7	11	2	6	10	1	5	9
5	5	10	2	7	12	4	9	1	6	11	3	8
6	6	12	5	11	4	10	3	9	2	8	1	7
7	7	1	8	2	9	3	10	4	11	5	12	6
8	8	3	11	6	1	9	4	12	7	2	10	5

9	9	5	1	10	6	2	11	7	3	12	8	4
10	10	7	4	1	11	8	5	2	12	9	6	3
11	11	9	7	5	3	1	12	10	8	6	4	2
12	12	11	10	9	8	7	6	5	4	3	2	1

Observe that for each c, the probabilities of m and k (which produces them) are all the same.

So, it satisfies prefect secrecy.

How to prove that $Z_p^* = \{1, 2, 3, \ldots, p-1\}$ (In other words, there is exact one "1" in each row and column)？

Consider that we're using the above (tabling) method to calculate $mk\ \ mod\ \ p$.

In the same row,

$$\text{value of next column} = (\text{value of current column} + m)\ \ mod\ \ p$$

If there are two "1"s in one row:

$$1 = \left(1 + m * col_{dif}\right)\ \ mod\ \ p$$

$$\because m < p \ \text{ and } \ col_{dif} < p - 1, \text{and} \ p \ \text{ is prime}$$

$$\therefore \left(m * col_{dif}\right)\ \ mod\ \ p \neq 0 \rightarrow \left(1 + m * col_{dif}\right)\ \ mod\ \ p \neq 1$$

contradicts→there can not be two "1"s in one row.

If there are no "1"s in one row,

there must be at least two same number $num < p$ in that row:

$$num = \left(num + m * col_{dif}\right)\ \ mod\ \ p$$

$$\because m < p \ \text{ and } \ col_{dif} < p - 1, \text{and} \ p \ \text{ is prime}$$

$$\therefore (m * col_{dif})\ \ mod\ \ p \neq 0 \rightarrow \left(num + m * col_{dif}\right)\ \ mod\ \ p \neq num$$

contradicts→there can not be no "1"s in one row.

So far, we proved that there must be exact one "1" in the $(\mathrm{p}-1) * (\mathrm{p}-1)$ table.

$$\leftrightarrow Z_p^* = \{1, 2, 3, \ldots, p-1\}$$

Using the same method, we can show that there must be exact one "1 to p-1" in each row and column. In other words, the cipher text has the same probabilities to be produced from every m and k in Z_p^*.

Therefore, the cipher provides perfect secrecy.

(To satisfy $\forall m_0, m_1 \in M, len(m_0) = len(m_1)$, one should pad the shorter messages with zero)

Problem 2

Predicting generators. Consider the following *congruential generator*. It uses constants $a, b \in Z_p^*$. The seed is a value $x_0 \in Z_p^*$. The i^{th} value generated is computed as

$$x_i = ax_{i-1} + b \bmod p$$

The sequence output by the generator is $S = x_0, x_1, x_2, \ldots$ Assume that an attacker knows p and witness the sequence. Prove that after a short prefix (i.e. a few of the values x_i's) the attacker is able to predict the rest of the sequence (i.e. the rest of the x_j's).

What does this say about the security of using the congruential generator as the keystream generator for a stream cipher?

Assume that the attacker witnesses $\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3$, and knows p:

$x_2 = (ax_1 + b) mod\ \ p$ -> $ax_1 + b = pl + x_2$

$x_3 = (ax_2 + b) mod\ \ p$ -> $ax_2 + b = pm + x_3$

$x_4 = (ax_3 + b) mod\ \ p$ -> $ax_3 + b = pn + x_4$

$$\mathrm{a} = \frac{p(l-m) + (x_2 - x_3)}{(x_1 - x_2)} = \frac{p(l-n) + (x_2 - x_4)}{(x_1 - x_3)} = \frac{p(m-n) + (x_3 - x_4)}{(x_2 - x_3)}$$

Solve $\begin{cases} \frac{p(l-m)+(x_2-x_3)}{(x_1-x_2)} = \frac{p(l-n)+(x_2-x_4)}{(x_1-x_3)} \\ \frac{p(l-m)+(x_2-x_3)}{(x_1-x_2)} = \frac{p(m-n)+(x_3-x_4)}{(x_2-x_3)} \\ \frac{p(l-n)+(x_2-x_4)}{(x_1-x_3)} = \frac{p(m-n)+(x_3-x_4)}{(x_2-x_3)} \end{cases}$ to get the value of $\mathrm{l, m, n}$ -> get $\mathrm{a, b}$

Now, the attacker can predict the rest of the sequence using $\mathrm{a, b}$ and p.

LCG is not secure.

Problem 3

Non-linear Composition of LFSRs. Consider the follow LFSR-based generator G. It is composed by three LFSR's R_1, R_2, R_3. Let $x_i(t)$ be the output of register R_i at clock pulse t. Then

$$G(t) = \left(x_1(t) AND x_2(t)\right) \oplus \left(\bar{x}_1(t) AND x_3(t)\right)$$

where $\bar{x}$ denotes the complement of bit x. Prove that

$$Prob[G(t) = x_1(t)] = \frac{1}{2}$$

$$Prob[G(t) = x_2(t)] = \frac{3}{4}$$

By listing all possibilities,

$x_1(t)$	$x_2(t)$	$x_3(t)$	$x_1(t)$ & $x_2(t)$	$\overline{x_1}(t)$ & $x_3(t)$	G(t)	= $x_1(t)$?	= $x_2(t)$?
0	0	0	0	0	0	Y	Y
0	0	1	0	1	1	N	N
0	1	0	0	0	0	Y	N
0	1	1	0	1	1	N	Y
1	0	0	0	0	0	N	Y
1	0	1	0	0	0	N	Y
1	1	0	1	0	1	Y	Y
1	1	1	1	0	1	Y	Y

we can show that

$$P[G(t) = x_1(t)] = \frac{1}{2}$$

$$P[G(t) = x_2(t)] = \frac{3}{4}$$

Another way:

$$P[G(t) = x_1(t)]$$

$$= P[G(t) = 0 \;\; AND \;\; x_1(t) = 0] + P[G(t) = 1 \;\; AND \;\; x_1(t) = 1]$$

$$= \frac{1}{2} P[G(t) = 0 \;|\; x_1(t) = 0] + \frac{1}{2} P[G(t) = 1 \;|\; x_1(t) = 1]$$

$$= \frac{1}{2}\left(P\left[\left(0 \;\; AND \;\; x_2(t)\right) \oplus \left(1 \;\; AND \;\; x_3(t)\right) = 0\right] + P\left[\left(1 \;\; AND \;\; x_2(t)\right) \oplus \left(0 \;\; AND \;\; x_3(t)\right) = 1\right]\right)$$

$$= \frac{1}{2}\left(P[0 \oplus x_3(t) = 0] + P[x_2(t) \oplus 0 = 1]\right)$$

$$= \frac{1}{2}\left(P[x_3(t) = 0] + P[x_2(t) = 1]\right)$$

$$= \frac{1}{2}\left(\frac{1}{2} + \frac{1}{2}\right)$$

$$= \frac{1}{2}$$

$$P[G(t) = x_2(t)]$$

$$= P[G(t) = 0 \;\; AND \;\; x_2(t) = 0] + P[G(t) = 1 \;\; AND \;\; x_2(t) = 1]$$

$$= \frac{1}{2} P[G(t) = 0 \mid x_2(t) = 0] + \frac{1}{2} P[G(t) = 1 \mid x_2(t) = 1]$$

$$= \frac{1}{2}\left(P\left[(x_1(t) \;\; AND \;\; 0) \oplus \left(\overline{x_1}(t) \;\; AND \;\; x_3(t)\right) = 0\right] + P\left[(x_1(t) \;\; AND \;\; 1) \oplus \left(\overline{x_1}(t) \;\; AND \;\; x_3(t)\right) = 1\right]\right)$$

$$= \frac{1}{2}\left(P\left[0 \oplus \left(\overline{x_1}(t) \;\; AND \;\; x_3(t)\right) = 0\right] + P\left[x_1(t) \oplus \left(\overline{x_1}(t) \;\; AND \;\; x_3(t)\right) = 1\right]\right)$$

$$= \frac{1}{2}\left(P[\overline{x_1}(t) \;\; AND \;\; x_3(t) = 0] + P\left[x_1(t) \oplus \left(\overline{x_1}(t) \;\; AND \;\; x_3(t)\right) = 1\right]\right)$$

$$= \frac{1}{2}\left(\frac{3}{4} + \frac{1}{2}\left(P[0 \oplus x_3(t) = 1] + P[1 \oplus 0 = 1]\right)\right)$$

$$= \frac{1}{2}\left(\frac{3}{4} + \frac{1}{2}\left(\frac{1}{2} + 1\right)\right)$$

$$= \frac{3}{4}$$

Problem 4

Passwords with insecure keyboard

Consider the following scenario: Alice wants to login on a computer system. In order to gain access, she has to communicate her password to the system.

However, the keyboard (and the cable connection between the keyboard and the system) cannot be trusted since there may be a passive adversary recording the key strokes or tapping the line.

Conversely, let us assume that the display used by Alice (and the connection between the system and the display) is secure, meaning it cannot be monitored by an adversary.

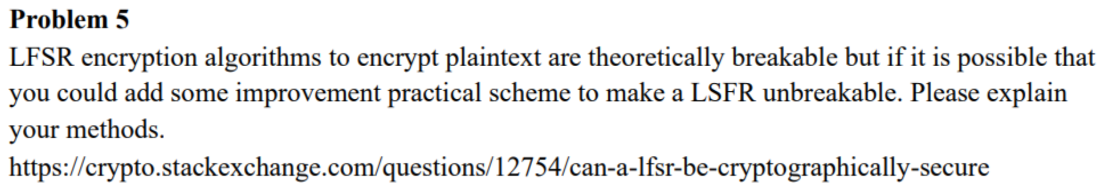
Devise a password protocol that will allow Alice to access the system without disclosing her password to the adversary.

老師上課提到的解決方法：
使用觸控面板、設計一次一密演算法。

我自己想到的解決方法：

1. 語音輸入。
2. 虛擬鍵盤：可用滑鼠點擊的鍵盤。
3. 自定義鍵盤按鍵：把實體鍵盤的按鍵 map 到不同虛擬按鍵上，這樣既可使用鍵盤打字，而又不會被竊聽到真實的內容，但這種方法會需要 一次一密 或 至少打多少字後必須更換 mapping 才安全，可能會常常需要熟悉新的配置。
4. 刻意在明文中穿插很多無意義字詞，以鍵盤輸入後，再以滑鼠選取並刪除。(adversary 看不到滑鼠選取位置，只會看到很多 backspace 被按下)

但以上方法都有輸入效率會降低的缺點。



Problem 5

LFSR encryption algorithms to encrypt plaintext are theoretically breakable but if it is possible that you could add some improvement practical scheme to make a LSFR unbreakable. Please explain your methods.

https://crypto.stackexchange.com/questions/12754/can-a-lfsr-be-cryptographically-secure

1. Alternating Step Generator (ASG):

Use 3 LFSRs(LFSR0, LFSR1, LFSR2). LFSR2 decides which of the other two should be used. For example, if LFSR2 outputs 0 -> lock LFSR0, and if LFSR2 outputs 1 -> lock LFSR1. The output of ASG is the XOR of the last bit produced by LFSR0 and LFSR1.

From the concept of 1., I came up with Rotor Machine mentioned in the class. Combining these two, we can use $2^n + \mathrm{n}$ LSFRs (n for deciding which of the other 2^n LFSRs should be locked) to make it more unbreakable.

2. Reseeding after several $(< 2\mathrm{n})$ times of output.

3. Do not output bits continuously. Skip random number of bits each time. For example, we can use another LFSR to decide whether to skip current bit or not.