CS 5840 Spring 2018 Problem Set #1

Jialiang Wang (01/30)

---

1. Question 1

   (a) Part A

   Let $a_1$ = a mod n, $b_1$ = b mod n, then $a = k_1 \cdot n + a_1$ and $b = k_2 \cdot n + b_1$, where $k_1$ and $k_2$ are integer.

   Let $C = (a + b)$ mod n, then there is an integer $k_3$, st. $(a + b) = k_3 \cdot n + C$

   LHS = $a_1 + b_1 = (a - k_1 \cdot n) + (b - k_2 \cdot n) = (a + b) - (k_1 + k_2) \cdot n$

   RHS = $(a + b) - k_3 \cdot n.$

   Since $k_1, k_2, k_3$ is arbitrary integers, so we can select $k_1 + k_2 = k_3$, then LHS = RHS.

   (b) Part B

   Let $a_1$ = a mod n, $b_1$ = b mod n, then $a = k_1 \cdot n + a_1$ and $b = k_2 \cdot n + b_1$, where $k_1$ and $k_2$ are integer.

   Let $C = (a \cdot b)$ mod n, then there is an integer $k_3$, st. $(a \cdot b) = k_3 \cdot n + C$

   LHS = $a_1 \cdot b_1 = (a - k_1 \cdot n) \cdot (b - k_2 \cdot n) = a \cdot b - (b \cdot k_1 + a \cdot k_2 - k_1 \cdot k_2 \cdot n) \cdot n$

   RHS = $(a \cdot b) - k_3 \cdot n$

   Because $k_1, k_2, k_3$ are arbitrary integer, we can select $k_3 = (b \cdot k_1 + a \cdot k_2 - k_1 \cdot k_2 \cdot n)$, then LHS = RHS.

   (c) Part C

   Let P(Y) be the probability Bob eat yellow, and P(O) be the one Bob eat other. We have

   $$0.2 \cdot P(Y) + 0.8 \cdot P(O) = 0.85$$

   with constrains: $0 \leq P(Y) \leq 1$ and $0 \leq P(O) \leq 1$ So, P(Y) = $4.25 - 4 \cdot P(O)$. Setting P(O) = 1, P(Y) = 0.25, Setting P(O) = 0, P(Y) = 4.25, but with upper bond of 1. Therefore,

   $$0.25 \leq P(Y) \leq 1$$

2. Question 2

   (a) Part A

   Define scheme (M, K, Gen, Enc, Dec):
   M = $\{0,1\}^n$, K = $\{0,1\}^n$ and cipher-text C = $\{0,1\}^n$, with $m_i$ denotes i-th character of M, $k_i$ denotes i-th character of K, and $c_i$ denotes i-th character of C.

   For each character, we have $c_{10 \cdot i} = m_i \oplus k_i$, followed by $c_{(10 \cdot i)+j} = j \oplus k_i$ for j from 1 to 9

   This is perfect-secure encryption scheme because any message pair $(m_1, m_2)$ with $K \leftarrow Gen$ with either message goes to given cipher-text is same. (XOR is perfect-secure with one-time pad, and this key space is 10 times the message space even through 90 percentage is useless.

   (b) Part B

   By definition, perfect secrecy with tuple (M, K, Gen, Enc, Dec), there is

   $$Pr[k \leftarrow Gen : Enck(m_1) = c] = Pr[k \leftarrow Gen : Enck(m_2) = c].$$

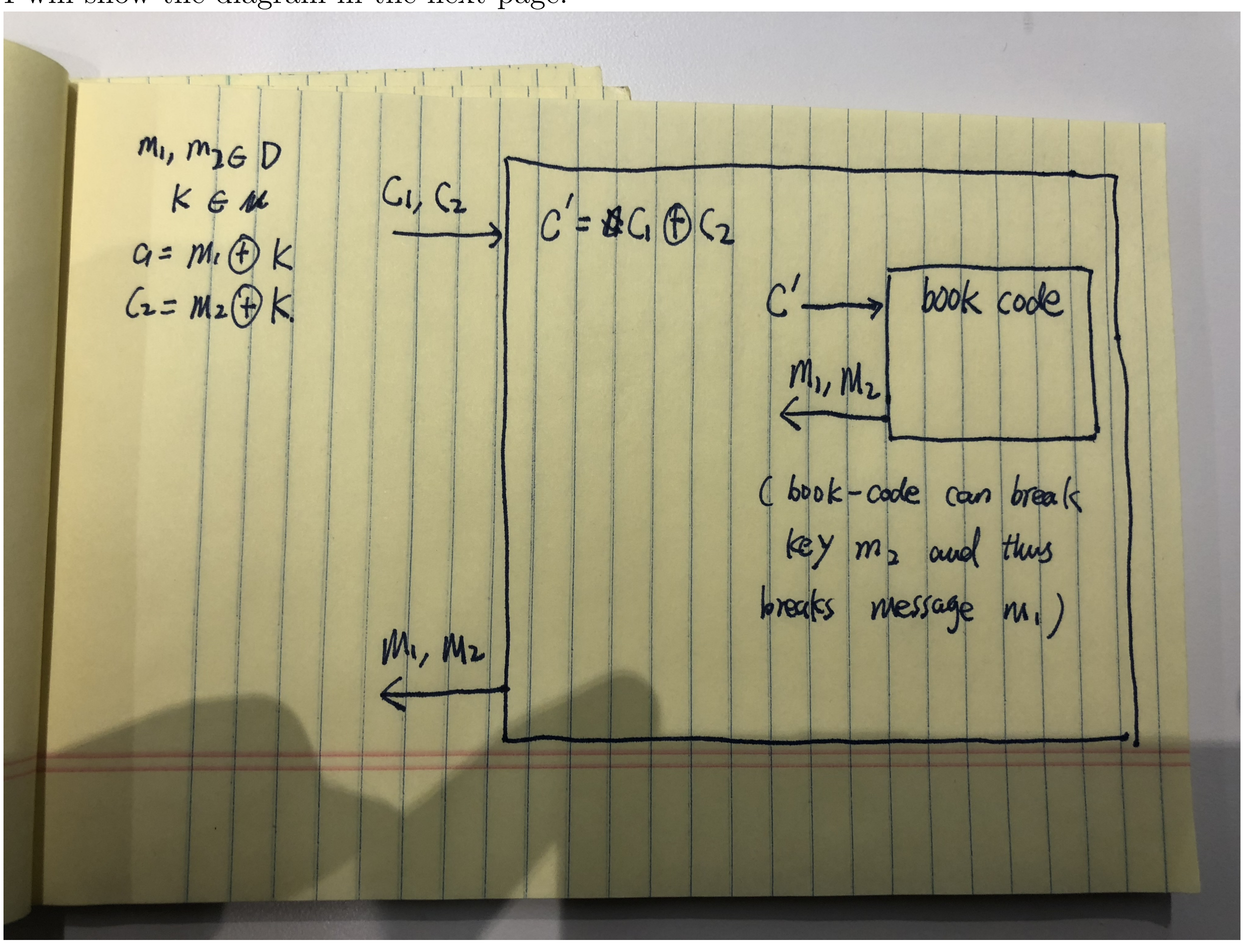
   Which means encrypted message cannot leak any information of original message, however, it reveals.
   proof: A schema is perfect secrecy if and only if it is Shannon secrecy, which indicates $Pr[m = m' | Enc_k(m) = c] = Pr[m = m']$. However, by revealing 10% of information, some message $m_i$ has $Pr[m = m_i] = 2^{-0.9 \cdot n}$, while other message $m_j$ has $Pr[m = m_j] = 0$, which contradict the assumption, therefore, it is not Shannon secrecy, and thus not perfect secrecy.

3. Question 3

   (a) Part A

   A $schema_1$ (M, K, Gen, Enc, Dec), with one-time pad key K to encrypt two messages $m_1, m_2$, with $e_1 = Enc(K, m_1), e_2 = Enc(K, m2)$, and a $scheme_2$ (M', K', Gen, Enc, Dec) with given distribution D over M' and K', and assume we have attacker A can break scheme2.

   For $e_1$ and $e_2$, since $e_1 = m_1 \oplus k$ and $e_2 = m_1 \oplus k$. we can do operation according to Enc (like XOR) to eliminate key K, $e_1 \oplus e2 = m_1 \oplus m_2$. Now, our new message is $m_1$ and new key is $m_2$ with encrypted message is $e_1 \oplus e_2$, with both $m_1$ and $m_2$ comes from distribution D. We then put this encrypted message into the black-box ($scheme_2$).
   I will show the diagram in the next page.



(b) Part B

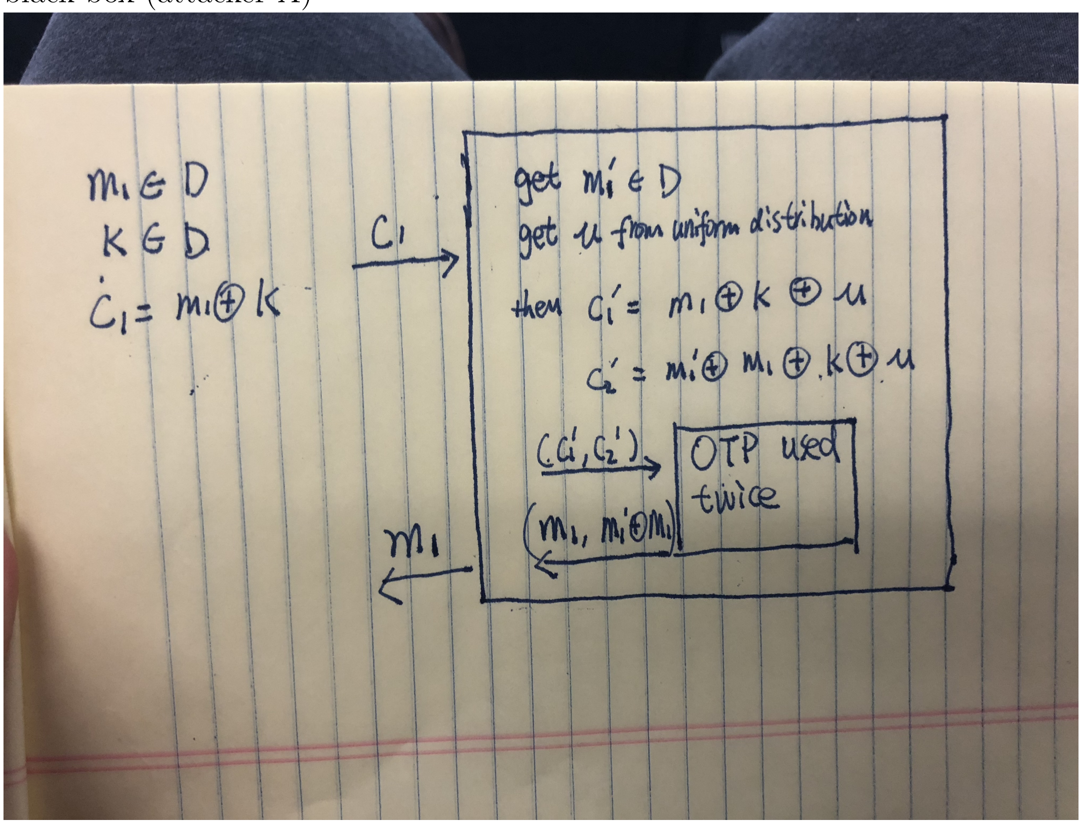
A *schema*$_1$ (M, K, Gen, Enc, Dec), with one-time pad key K to encrypt two messages $m_1, m_2$, with $e_1 = Enc(K, m_1), e_2 = Enc(K, m2)$, and a *scheme*$_2$ (M', K', Gen, Enc, Dec) with given distribution D over M' and K', and assume we have attacker A can break scheme1.

$e_1 = m_1 \oplus K$. First, randomly select message m' from distribution D and $\mu$ from uniform distribution. Then we construct cipher-text

$$c_1' = c_1 \oplus \mu = m_1 \oplus K \oplus \mu$$

$$c_2' = m_1' \oplus c_1 \oplus \mu = m_1' \oplus m_1 \oplus K \oplus \mu$$

Because $\mu$ is uniformly random selected, then $K \oplus \mu$ is in uniformly random distribution, and $m_1'$ is selected from distribution D, and thus $m_1' \oplus m_1$ is in distribution D. We can re-write cipher-text $c_1$ and $c_2$ in the format $c_1 = m_1 \oplus K'$ and $c_2 = m_1' \oplus K'$, where $m_1$ and $m_1'$ are selected from distribution D, and key $K'$ is in uniformly random distribution. Then feed cipher-text $c_1$ and $c_2$ in to the black-box (attacker A)



4. Question 4

   (a) Part A
   See HW1-gwriter-part1-gwriter.py

   (b) Part B
   Solution shows in part2 directory