Chapter 02

Mingjia Huo

Problem 2.3. Refute: Assume $\mathcal{M} = \{0, 1\}$ with uniform distribution, define (Gen, Enc, Dec):

- Gen: $\varnothing \to \mathcal{K}$, where $\mathcal{K} = \{k_1k_2 \mid k_1 \in \{0,1\}, k_2 \in \{0,1,2\}\}, \Pr[K = k_1k_2] = \frac{1}{6}$.
- Enc: $\mathcal{K} \times \mathcal{M} \to \mathcal{C}$, where $\mathcal{C} = \{c_1c_2 \mid c_1, c_2 = 0, 1\}$. Here, $c_1 = k_1 \oplus m$, and

$$c_2 = \begin{cases} 0, & k_2 = 0, 1 \\ 1, & k_2 = 2 \end{cases}$$

- Dec: $\mathcal{K} \times \mathcal{C} \to \mathcal{M}$, where $m = c_1 \oplus k_1$.

In this construction, $\Pr[M = m \mid C = c] = \frac{1}{2} = \Pr[M = m]$. But

$$\Pr[C = 00] = \Pr[c_1 = 0] \times \Pr[c_2 = 0] = \frac{1}{3},$$

$$\Pr[C = 01] = \Pr[c_1 = 0] \times \Pr[c_2 = 1] = \frac{1}{6},$$

a contradiction.

Problem 2.11. Part 1:

Assume $\mid \mathcal{C} \mid=\mid \mathcal{M} \mid= n$, $\mid \mathcal{K} \mid= l$, there exists a encryption scheme (Gen,Enc,Dec). Let $\mathcal{M} = \{m_1, \cdots, m_n\}, \mathcal{K} = \{k_1, \cdots, k_l\}, \mathcal{C} = \{c_1, \cdots, c_n\}$, and

- Gen: $\{0,1\}^* \to \mathcal{K}$

$$\Pr[\text{Gen} = k_j] = \begin{cases} \frac{1}{n}, & j \in \{1, \cdots, l-1\} \\ \frac{n-l+1}{n}, & j = l \end{cases}$$

- Enc: $\mathcal{K} \times \mathcal{M} \to \mathcal{C}$

  For $j \in \{1, \cdots, l-1\}$, $\text{Enc}_{k_j}(m_i) = c_{(i+j \mod n)}$.

  For $j = l$, and $\forall t \in \{l, l+1, \cdots, n\}$, $\Pr[\text{Enc}_{k_l}(m_i) = c_{(i+t \mod n)}] = \frac{1}{n-l+1}$.

- Dec: $\mathcal{K} \times \mathcal{C} \to \mathcal{M}$

  For $j \in \{1, \cdots, l-1\}$, $\text{Dec}_{k_j}(c_i) = c_{(i-j \mod n)}$.

  For $j = l$, and $\forall t \in \{l, l+1, \cdots, n\}$, $\Pr[\text{Dec}_{k_l}(m_i) = c_{(i-t \mod n)}] = \frac{1}{n-l+1}$.

Then $\forall i, j \in [n], m_i \in \mathcal{M}$,

- when $j \in \{(i+1) \mod n, \cdots, (i+l-1) \mod n\}$:

$$\Pr[\mathrm{Enc}_K(m_i) = c_j] = \Pr[\mathrm{Enc}_{k_{(j-i \mod n)}}(m_i) = c_j] = \frac{1}{n};$$

- otherwise,

$$\Pr[\mathrm{Enc}_K(m_i) = c_j] = \Pr[\mathrm{Enc}_{k_l}(m_i) = c_j] \times \Pr[K = k_l] = \frac{1}{n-l+1} \frac{n-l+1}{n} = \frac{1}{n},$$

which means $\forall m, m' \in \mathcal{M}, c \in \mathcal{C}$,

$$\Pr[\mathrm{Enc}_K(m) = c] = \Pr[\mathrm{Enc}_K(m') = c] = \frac{1}{n}.$$

So the construction ensures perfect secrecy.

And for message m_i, when

1. $k \in \{k_1, \cdots, k_{l-1}\}$, then $\mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m$.
2. $k = k_l$, assume $C_m = \{c \mid c \in \mathcal{C}, \Pr[\mathrm{Enc}_{k_l}(m) = c] \neq 0\}$, then

$$\begin{aligned}\Pr[\mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m] &= \sum_{c \in C_m} \Pr[\mathrm{Enc}_{k_l}(m) = c] \Pr[\mathrm{Dec}_{k_l}(c) = m] \\ &= (n-l+1) \times \frac{1}{n-l+1} \times \frac{1}{n-l+1} \\ &= \frac{1}{n-l+1}.\end{aligned}$$

To sum up,

$$\begin{aligned}&\Pr[\mathrm{Dec}_K(\mathrm{Enc}_K(m)) = m] \\ =&\sum_{k=k_1}^{k_{l-1}} \Pr[K = k] \times \Pr[\mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m] + \Pr[K = k_l] \times \Pr[\mathrm{Dec}_{k_l}(\mathrm{Enc}_{k_l}(m)) = m] \\ =&(l-1) \times \frac{1}{n} + \frac{n-l+1}{n} \times \frac{1}{n-l+1} \\ =&\frac{l}{n}.\end{aligned}$$

Let $l = \lceil 2^{-t} n \rceil$, so when n is large enough, we have $l < n$, which means $\mid \mathcal{K} \mid < \mid \mathcal{M} \mid$. Then

$$\Pr[\mathrm{Dec}_K(\mathrm{Enc}_K(m)) = m] = \frac{\lceil 2^{-t} n \rceil}{n} \geq 2^{-t},$$

which satisfies the condition.

Part 2:

From **Part 1** we have $\mid \mathcal{K} \mid = l = \lceil 2^{-t} n \rceil$. Then we proof l must $\geq \lceil 2^{-t} n \rceil$.

By condition, $\Pr[\mathrm{Dec}_K(\mathrm{Enc}_K(m)) = m] \geq 2^{-t}$. So

$$\sum_m \Pr[\mathrm{Dec}_K(\mathrm{Enc}_K(m)) = m] \geq 2^{-t} n$$

. Let $C_{k,m} = \{c \mid \Pr[\mathrm{Enc}_k(m) = c] \neq 0\}$. Then we have

$$\begin{aligned}
&\sum_m \Pr[\mathrm{Dec}_K(\mathrm{Enc}_K(m)) = m] \\
=&\sum_m \sum_k \Pr[K = k] \Pr[\mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m] \\
=&\sum_{m,k} \Pr[K = k] \sum_{c \in C_{k,m}} \Pr[\mathrm{Enc}_k(m) = c] \times \Pr[\mathrm{Dec}_k(c) = m \mid \mathrm{Enc}_k(m) = c] \\
=&\sum_{m,k} \sum_{c \in C_{k,m}} \Pr[K = k] \Pr[\mathrm{Enc}_k(m) = c] \Pr[\mathrm{Dec}_k(c) = m \mid \mathrm{Enc}_k(m) = c]
\end{aligned}$$

When $\Pr[\mathrm{Enc}_k(m) = c] \neq 0$, $\Pr[\mathrm{Dec}_k(c) = m \mid \mathrm{Enc}_k(m) = c] = \Pr[\mathrm{Dec}_k(c) = m]$. And when $c \notin C_{k,m}$, we have $\Pr[\mathrm{Enc}_k(m) = c] = 0$. Thus,

$$\begin{aligned}
&2^{-t} n \\
\leq&\sum_m \Pr[\mathrm{Dec}_K(\mathrm{Enc}_K(m)) = m] \\
=&\sum_{m,k} \sum_{c \in C_{k,m}} \Pr[K = k] \Pr[\mathrm{Enc}_k(m) = c] \Pr[\mathrm{Dec}_k(c) = m \mid \mathrm{Enc}_k(m) = c] \\
=&\sum_{m,k} \sum_{c \in C_{k,m}} \Pr[K = k] \Pr[\mathrm{Enc}_k(m) = c] \Pr[\mathrm{Dec}_k(c) = m] \\
=&\sum_{m,k,c} \Pr[K = k] \Pr[\mathrm{Enc}_k(m) = c] \Pr[\mathrm{Dec}_k(c) = m]
\end{aligned}$$

On the other hand, by perfect secrecy,

$$\forall m, m' \in \mathcal{M}, \Pr[\mathrm{Enc}_K(m) = c] = \Pr[\mathrm{Enc}_K(m') = c] = \Pr[C = c].$$

Thus,

$$\sum_{c,m} \Pr[C = c] \Pr[\mathrm{Dec}_k(c) = m] = \sum_c \Pr[C = c] \times 1 = 1.$$

Obviously,

$$\forall m, \Pr[C = c] = \sum_{k' \in \mathcal{K}} \Pr[K = k'] \Pr[\mathrm{Enc}_{k'}(m) = c].$$

Then,

$$
\begin{aligned}
l =& \sum_{k \in \mathcal{K}} 1 \\
=& \sum_{k} \sum_{c,m} \Pr[C = c] \Pr[\mathrm{Dec}_k(c) = m] \\
=& \sum_{k,c,m} \sum_{k' \in \mathcal{K}} \Pr[K = k'] \Pr[\mathrm{Enc}_{k'}(m) = c] \Pr[\mathrm{Dec}_k(c) = m] \\
=& \sum_{k=k',c,m} \Pr[K = k'] \Pr[\mathrm{Enc}_{k'}(m) = c] \Pr[\mathrm{Dec}_k(c) = m] \\
& + \sum_{k,c,m} \sum_{k' \neq k} \Pr[K = k'] \Pr[\mathrm{Enc}_{k'}(m) = c] \Pr[\mathrm{Dec}_k(c) = m] \\
\geq& \sum_{k=k',c,m} \Pr[K = k'] \Pr[\mathrm{Enc}_{k'}(m) = c] \Pr[\mathrm{Dec}_k(c) = m] \\
=& \sum_{k,c,m} \Pr[K = k] \Pr[\mathrm{Enc}_{k}(m) = c] \Pr[\mathrm{Dec}_k(c) = m] \\
\geq& 2^{-t} n.
\end{aligned}
$$

So the lower bound is $\lceil 2^{-t} \mid \mathcal{M} \mid \rceil$.