Problem 1. *Answer provided by YANG Mingwei*

The decryption algorithm is $\mathsf{Dec}(k, c) = k^{-1} \cdot c$.

To prove correctness, note that for every $m \in \mathcal{M}$ and $k \in \mathcal{K}$, we have

$$\mathsf{Dec}(k, \mathsf{Enc}(k, m)) = k^{-1} \cdot (k \cdot m) = m\,.$$

To prove perfect secrecy, as shown in the next problem, it is sufficient to show that for any $m_0, m_1 \in \mathcal{M}$ and $c \in \mathcal{C}$,

$$\Pr\left[\mathsf{Enc}\left(k, m_0\right) = c\right] = \Pr\left[\mathsf{Enc}\left(k, m_1\right) = c\right]\,.$$

The left-hand side of the equation equals

$$\Pr\left[\mathsf{Enc}\left(k, m_0\right) = c\right] = \Pr\left[k = c \cdot m^{-1}\right] = \frac{1}{|\mathcal{K}|}\,,$$

so is the right-hand side.

Problem 2.

Perfect secrecy implies perfect indistinguishability. Let M satisfies the uniform distribution over $\mathcal{M}$. For any $m \in \mathcal{M}$ and $c \in \mathcal{C}$, we have

$$\begin{aligned} \Pr[M=m|C=c] &= \frac{\Pr[M=m]\Pr[C=c|M=m]}{\Pr[C=c]} \\ &= \frac{\Pr[M=m]}{\Pr[C=c]} \cdot \Pr[\mathsf{Enc}(K,m)=c]. \end{aligned} \tag{1}$$

Prefect secrecy tells us that $\Pr[M=m|C=c]=\Pr[M=m]$, which implies that $\Pr[\mathsf{Enc}(K,m)=c]=\Pr[C=c]$. Thus for any $m_0, m_1 \in \mathcal{M}$, for any $c \in \mathcal{C}$,

$$\Pr\left[\mathsf{Enc}\left(K,m_0\right)=c\right]=\Pr[C=c]=\Pr\left[\mathsf{Enc}\left(K,m_1\right)=c\right].$$

Perfect indistinguishability implies perfect secrecy. Consider any distribution of the message. For arbitrary $c \in \mathcal{C}$ and $m \in \mathcal{M}$

$$\Pr[M=m|C=c]=\frac{\Pr[M=m \wedge C=c]}{\Pr[C=c]}.$$

Its numerator equals $\Pr[M=m]\Pr[\mathsf{Enc}(K,m)=c]$. Its denominator equals

$$\sum_{m' \in \mathcal{M}} \Pr[M=m' \wedge C=c] = \sum_{m' \in \mathcal{M}} \Pr[M=m'C=c]\Pr[\mathsf{Enc}(K,m')=c].$$

Due to prefect indistinguishability, we know $\Pr[\mathsf{Enc}(K,m')=c]=\Pr[\mathsf{Enc}(K,m)=c]$ for any m'. Therefore, perfect secrecy follows from

$$\begin{aligned} \Pr[M=m|C=c] &= \frac{\Pr[M=m \wedge C=c]}{\Pr[C=c]} \\ &= \frac{\Pr[M=m]\Pr[\mathsf{Enc}(K,m)=c]}{\sum_{m' \in \mathcal{M}} \Pr[M=m']\Pr[\mathsf{Enc}(K,m')=c]} \\ &= \frac{\Pr[M=m]}{\sum_{m' \in \mathcal{M}} \Pr[M=m']} = \Pr[M=m]. \end{aligned}$$

Problem 3. *Answer provided by GUO Chengzhi*

Part B. Proof of $I[X;Y;Z] = I[X;Y] - I[X;Y|Z]$.

$$\begin{aligned} I[X;Y;Z] &= H[X] + H[Y] + H[Z] - H[X,Y] - H[X,Z] - H[Y,Z] + H[X,Y,Z] \\ &= I[X;Y] + H[Z] - H[X,Z] - H[Y,Z] + H[X,Y,Z] \\ &= I[X;Y] - (H[X,Z] - H[Z]) - (H[Y,Z] - H[Z]) - (-H[X,Y,Z] + H[Z]) \\ &= I[X;Y] - H[X|Z] - H[Y|Z] + H[X,Y|Z] \\ &= I[X;Y] - I[X;Y|Z] \end{aligned}$$

Proof of $H[Z] \geq I[X;Y;Z] \geq -H[Z]$.

$$\begin{aligned} I[X;Y;Z] &= H[X] + H[Y] + H[Z] - H[X,Y] - H[X,Z] - H[Y,Z] + H[X,Y,Z] \\ &= (H[X] - H[Z,X]) + (H[Y] - H[X,Y]) + (H[Z] - H[Y,Z]) + H[X,Y,Z] \\ &= -H[Z|X] - H[X|Y] - H[Y|Z] + H[X,Y,Z] \\ &= -H[Z|X] - H[X|Y] - H[Y|Z] + H[Z] + H[Y|Z] + H[X|Y,Z] \\ &= -H[Z|X] - H[X|Y] + H[Z] + H[X|Y,Z] \end{aligned}$$

Since $H[X|Y,Z] - H[X|Y] \leq 0, -H[Z|X] \leq 0$, we have

$$I[X;Y;Z] = -H[Z|X] - H[X|Y] + H[Z] + H[X|Y,Z] \leq H[Z]$$

On the other hand, we have

$$\begin{gathered} H[Z] - H[Z|X] \geq 0 \\ H[X|Y,Z] - H[X|Y] = -I[X;Z|Y] \geq -H[Z|Y] \geq -H[Z], \end{gathered}$$

so we get

$$I[X;Y;Z] \geq -H[Z]$$

.

An example where $I[X;Y;Z] = H[Z] > 0$**.** Assume Z is taken uniformly from $\{0,1\}$ and $X = Y = Z$, then $I[X;Y;Z] = H[Z] = 1$.

An example where $I[X;Y;Z] = -H[Z] < 0$**.** Assume X, Y are taken uniformly from $\{0,1\}$ and $Z = X \oplus Y$, then $I[X;Y;Z] = -H[Z] = -1$.

Part C. Let random variable M, K, C denote the message, key, ciphertext during an encryption. The distribution of K is specified by Gen. The distribution of M will be specified later. First we have

$$I[C;M|K] = H[C|K] + H[M|K] - H[C,M|K]\,.$$

Since M and K are independent, we have

$$H[M|K] = H[M]\,.$$

Since M can be determined by C, K, we have $H[M|C,K] = 0$. So

$$H[C,M|K] = H[C|K] + H[M|C,K] = H[C|K]\,.$$

Problem 3 continued on next page…

Therefore

$$I[C; M|K] = H[M]$$

By perfect secrecy, we have $I[C; M] = 0$, so by Part B we have

$$I[C; M; K] = I[C; M] - I[C; M|K] = -H[M]$$
$$H[K] \geq -H[M] \geq -H[K]$$

Let M satisfy the uniform distribution over $\mathcal{M}$, then $H[M] = \log|\mathcal{M}|$. By inequality above we have $H[K] \geq \log|\mathcal{M}|$.

Problem 4.

Part A. $|\mathcal{K}| \geq |\mathcal{M}|$
Proof. Suppose not. Take arbitrary c_0. Since $|\{\mathsf{Dec}\,(k, c_0) : k \in \mathcal{K}\}| \leq |\mathcal{K}| < |\mathcal{M}|$, there must exist m such that $\Pr[M = m | C = c_0] = 0$. Then, for any distribution where $\Pr[M = m] > 1 - \varepsilon$, the condition $|\Pr[M = m|C = c_0] - \Pr[M = m]| \leq 1 - \varepsilon$ cannot hold. So $|\mathcal{K}| \geq |\mathcal{M}|$.

Part B. $|\mathcal{K}| \geq (1 - \varepsilon)|\mathcal{M}|$
Fix m_0 to be any message, sample m_1 uniformly at random. Consider the following distinguisher D.

$$\mathsf{D}(c) \text{ outputs } 1 \iff \exists k \in \mathcal{K} \text{ such that } \mathsf{Dec}(k, c) = m_1.$$

Since the scheme is perfectly correct, the distinguisher always outputs 1 when $b = 1$.
When $b = 0$, let $c = \mathsf{Enc}(K, m_0)$ be the ciphertext. The distinguisher outputs 1 if and only if there exists k such that $\mathsf{Dec}(k, c) = m_1$. In other words, the distinguisher outputs 1 if and only if

$$m_1 \in \Big\{\mathsf{Dec}(k, c) \;\Big|\; k \in \mathcal{K}\Big\}.$$

Note that m_1 is independent from k, c, so the probability m_1 falls in the above set is at most $|\mathcal{K}|/|\mathcal{M}|$.

$$\begin{aligned}
&\Pr_{\substack{k \leftarrow \mathsf{Gen} \\ b \leftarrow \{0,1\}}}\Big[\mathsf{D}(\mathsf{Enc}(K, m_b)) = b\Big] \\
&= \frac{1}{2}\Pr_{k\leftarrow \mathsf{Gen}}\Big[\mathsf{D}(\mathsf{Enc}(K, m_1)) = 1\Big] + \frac{1}{2}\Pr_{k\leftarrow \mathsf{Gen}}\Big[\mathsf{D}(\mathsf{Enc}(K, m_0)) \neq 1\Big] \\
&\geq \frac{1}{2}\Big(1 + 1 - \frac{|\mathcal{K}|}{|\mathcal{M}|}\Big).
\end{aligned}$$

Part C. $|\mathcal{K}| \geq (1 - \varepsilon)|\mathcal{M}|$
Proof. (The proof assumes algorithms $\mathsf{Enc}, \mathsf{Dec}$ to be deterministic. While it can be easily generated to the case where $\mathsf{Enc}, \mathsf{Dec}$ may be probabilistic.) Suppose not. Take the uniform distribution over $\mathcal{M}$. Fix arbitrary $c_0 \in \mathcal{C}$.
Since for all m,

$$\Pr[M = m|C = c_0] = \Pr[M = m] = \frac{1}{|M|}$$

we can compute

$$\begin{aligned}
\Pr_{k\leftarrow \mathsf{Gen}}[\mathsf{Enc}(m, k) = c_0] &= \Pr[C = c_0|M = m] \\
&= \Pr[M = m|C = c_0] \cdot \frac{\Pr[C = c_0]}{\Pr[M = m]} \\
&= \Pr[C = c_0]
\end{aligned}$$

Let $S_{c_0} = \{\mathsf{Dec}(k, c_0) : k \in \mathcal{K}\}$. We know

$$|S_{c_0}| \leq |\mathcal{K}| < (1 - \varepsilon)|\mathcal{M}|$$

Problem 4 continued on next page...

For $m \notin S_{c_0}$, if $\mathsf{Enc}(k, m) = c_0$, then $\mathsf{Dec}(k, \mathsf{Enc}(k, m)) \neq m$. Thus,

$$\begin{aligned}
& \Pr[\mathsf{Dec}(K, \mathsf{Enc}(K, M)) \neq M] \\
\geq\ & \Pr[M \notin S_{\mathsf{Enc}(K,M)}] \\
=\ & \sum_{c_0 \in \mathcal{C}} \Pr[M \notin S_{c_0}, C = c_0] \\
=\ & \sum_{c_0 \in \mathcal{C}} \sum_{m \notin S_{c_0}} \Pr[C = c_0, M = m] \\
=\ & \sum_{c_0 \in \mathcal{C}} \sum_{m \notin S_{c_0}} \Pr[C = c_0 | M = m] \Pr[M = m] \\
=\ & \frac{1}{|\mathcal{M}|} \sum_{c_0 \in \mathcal{C}} \sum_{m \notin S_{c_0}} \Pr_{k \leftarrow \mathsf{Gen}}[\mathsf{Enc}(m, k) = c_0] \\
=\ & \frac{1}{|\mathcal{M}|} \sum_{c_0 \in \mathcal{C}} \sum_{m \notin S_{c_0}} \Pr[C = c_0] \\
=\ & \frac{1}{|\mathcal{M}|} \sum_{c_0 \in \mathcal{C}} \Pr[C = c_0](|\mathcal{M}| - |S_{c_0}|) \\
>\ & \frac{\varepsilon|\mathcal{M}|}{|\mathcal{M}|} \sum_{c_0 \in \mathcal{C}} \Pr\left[C = c_0\right] \\
=\ & \varepsilon\,.
\end{aligned}$$

This also implies $\Pr[\mathsf{Dec}(K, \mathsf{Enc}(K, M)) = M] < 1 - \varepsilon$. But on the other hand,

$$\begin{aligned}
& \Pr[\mathsf{Dec}(K, \mathsf{Enc}(K, M)) = M] \\
=\ & \sum_{m \in \mathcal{M}} \Pr[\mathsf{Dec}(K, \mathsf{Enc}(K, M)) = M | M = m] \Pr[M = m] \\
=\ & \sum_{m \in \mathcal{M}} \Pr_{k \leftarrow \mathsf{Gen}}[\mathsf{Dec}(k, \mathsf{Enc}(k, m)) = m | M = m] \Pr[M = m] \\
\geq\ & (1 - \varepsilon) \sum_{m \in \mathcal{M}} \Pr[M = m] \\
=\ & 1 - \varepsilon\,.
\end{aligned}$$

This is a contradiction.

An Alternative Proof. Let random variable M be uniformly distributed over $\mathcal{M}$. Since the scheme is perfectly secure, by Problem 2, we know that for any $m_0, m_1 \in \mathcal{M}$, it holds that

$$\forall c \in \mathcal{C}, \Pr[\mathsf{Enc}(K, m_0) = c] = \Pr[\mathsf{Enc}(K, m_1) = c]$$

which implies that $\mathsf{Enc}(K, M)$ and M are independent. Define oracle $\mathrm{Eve}(m, c)$ for any $m \in \mathcal{M}, c \in \mathcal{C}$ as

$$\mathrm{Eve}(m, c) = [\exists k \in \mathcal{K}, \mathsf{Dec}(k, c) = m].$$

On one hand, we know that

$$\begin{aligned}
\Pr[\mathrm{Eve}(M, \mathsf{Enc}(K, M)) = 1] &= \Pr[\exists k \in \mathcal{K}, \mathsf{Dec}(k, \mathsf{Enc}(K, M)) = M] \\
&\geq \Pr[\mathsf{Dec}(K, \mathsf{Enc}(K, M)) = M] \\
&\geq 1 - \varepsilon
\end{aligned}$$

Problem 4 continued on next page...

On the other hand,

$$\Pr[\text{Eve}(M, \mathsf{Enc}(K, M)) = 1] \leq \sum_{k \in \mathcal{K}} \Pr[\mathsf{Dec}(k, \mathsf{Enc}(K, M)) = M] \leq \sum_{k \in \mathcal{K}} \frac{1}{|\mathcal{M}|} = \frac{|\mathcal{K}|}{|\mathcal{M}|}$$

where the second inequality is because M and $\mathsf{Enc}(K, M)$ are independent, and M is uniformly distributed. Therefore, it follows that

$$1 - \varepsilon \leq \frac{|\mathcal{K}|}{|\mathcal{M}|}$$

by which we obtain $|\mathcal{K}| \geq (1 - \varepsilon)|\mathcal{M}|$.