Cryptography – Homework 1

冯诗伟 161220039

1 Problem 1

Prove Lemma 2.6 :

Encryption scheme Π is perfectly secret if and only if it is perfectly indistinguishable.

Proof.

$$\mathsf{PrivK}^{\mathsf{eva}}_{\mathcal{A},\Pi}$$

I. Given that an encryption scheme Π is perfectly secret. Let's do the adversial indistinguishable experiment $\mathrm{PrivK}^{eva}_{\mathcal{A},\Pi}$. Now the adversary $\mathcal{A}$ knows the ciphertext c and he has to output a bit, 0 or 1. We have

$$\Pr[M = m_0] = \Pr[M = m_1] = \frac{1}{2}$$

Due to the perfectly secrecy,

$$\Pr[M = m_0|C = c] = \Pr[M = m_0] = \frac{1}{2}$$

$$\Pr[M = m_1|C = c] = \Pr[M = m_1] = \frac{1}{2}$$

Thus, it is obvious that

$$\Pr[\mathsf{PrivK}^{\mathsf{eva}}_{\mathcal{A},\Pi} = 1] = \frac{1}{2}$$

which means Π is perfectly indistinguishable.

II. Given that an encryption scheme Π is perfectly indistinguishable. It means that even if I know the ciphertext of one of the two plaintext, the probability of success is exactly $\frac{1}{2}$ which is the same as that of just guessing.

$$\Pr[M = m_0|C = c] = \Pr[M = m_1|C = c] = \frac{1}{2}$$

$$\therefore \Pr[M = m_i|C = c] = \Pr[M = m_i] = \frac{1}{2},\ i = 0, 1.$$

Therefore, Π is perfectly secret. □

2 Problem 2

Prove or refute: Every encryption scheme for which the size of the key space equals the size of the message space, and for which the key is chosen uniformly from the key space, is perfectly secret.

Proof. Refute. These restrictions only focus on the size and distribution and do not pay attention to matters about distinguishability. Imagine an encryption scheme where $\mathcal{K} = \mathcal{M} = \{0, 1\}^\ell$ and the key is uniformly chosen from $\mathcal{K}$ while $\mathsf{Enc}_K(m) = m$. This encryption scheme is not secret at all. □

3 Problem 3

(a) Solution:

$$
\begin{aligned}
Pr[\mathsf{PrivK}^{\mathsf{eva}}_{\mathcal{A},\Pi} = 1] &= \frac{1}{2}Pr[\mathsf{PrivK}^{\mathsf{eva}}_{\mathcal{A},\Pi} = 1|b = 0] + \frac{1}{2}Pr[\mathsf{PrivK}^{\mathsf{eva}}_{\mathcal{A},\Pi} = 1|b = 1] \\
&= \frac{1}{2}Pr[\mathcal{A}\,\text{output}\,0|b = 0] + \frac{1}{2}Pr[\mathcal{A}\,\text{output}\,1|b = 1] \\
&= \frac{1}{2}Pr[\mathcal{A}\,\text{output}\,0|b = 0] + \frac{1}{2}\Big(1 - Pr[\mathcal{A}\,\text{output}\,0|b = 1)\Big) \\
&= \frac{1}{2}\Big(\frac{1}{3}Pr[\mathcal{A}\,\text{output}\,0|b = 0,\, t = 1] + \frac{1}{3}Pr[\mathcal{A}\,\text{output}\,0|b = 0,\, t = 2] + \frac{1}{3}Pr[\mathcal{A}\,\text{output}\,0|b = 0,\, t = 3]\Big) \\
&+ \frac{1}{2}\Big(1 - (\frac{1}{3}Pr[\mathcal{A}\,\text{output}\,0|b = 1,\, t = 1] + \frac{1}{3}Pr[\mathcal{A}\,\text{output}\,0|b = 1,\, t = 2] + \frac{1}{3}Pr[\mathcal{A}\,\text{output}\,0|b = 1,\, t = 3])\Big) \\
&= \frac{1}{2}\Big(\frac{1}{3} \times 1 + \frac{1}{3} \times \frac{26}{26^2} + \frac{1}{3} \times \frac{26 \times 1 \times 26}{26^3}\Big) + \frac{1}{2}\Big(1 - (\frac{1}{3} \times 0 + \frac{1}{3} \times \frac{26}{26^2} + \frac{1}{3} \times \frac{26 \times 1 \times 26}{26^3})\Big) \\
&= \frac{2}{3}
\end{aligned}
$$

(b) Solution: Define $\mathcal{A}'$ as follows: $\mathcal{A}'$ output $m_0 = aa$ and $m_1 = ab$. When give a ciphertext $c = c_1c_2$, it outputs 0 if $c_1 = c_2$, and outputs 1 if $c_1 \neq_2$.

$$
\begin{aligned}
Pr[\mathsf{PrivK}^{\mathsf{eva}}_{\mathcal{A}',\Pi} = 1] &= \frac{1}{2}Pr[\mathsf{PrivK}^{\mathsf{eva}}_{\mathcal{A}',\Pi} = 1|b = 0] + \frac{1}{2}Pr[\mathsf{PrivK}^{\mathsf{eva}}_{\mathcal{A}',\Pi} = 1|b = 1] \\
&= \frac{1}{2}Pr[\mathcal{A}'\,\text{output}\,0|b = 0] + \frac{1}{2}Pr[\mathcal{A}'\,\text{output}\,1|b = 1] \\
&= \frac{1}{2}Pr[\mathcal{A}'\,\text{output}\,0|b = 0] + \frac{1}{2}\Big(1 - Pr[\mathcal{A}'\,\text{output}\,0|b = 1)\Big) \\
&= \frac{1}{2}\Big(\frac{1}{2}Pr[\mathcal{A}'\,\text{output}\,0|b = 0,\, t = 1] + \frac{1}{2}Pr[\mathcal{A}'\,\text{output}\,0|b = 0,\, t = 2]\Big) \\
&+ \frac{1}{2}\Big(1 - (\frac{1}{2}Pr[\mathcal{A}'\,\text{output}\,0|b = 1\, t = 1) + \frac{1}{2}Pr[\mathcal{A}'\,\text{output}\,0|b = 1\, t = 2))\Big) \\
&= \frac{1}{2}\Big(\frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{26}\Big) + \frac{1}{2}\Big(1 - (\frac{1}{3} \times 0 + \frac{1}{2} \times \frac{1}{26})\Big) \\
&= \frac{3}{4} > \frac{2}{3}
\end{aligned}
$$