CS 202 - Introduction to Applied Cryptography **Fall 2016**

HomeWork 1

October 12, 2016 *Liangjian Chen*

1. (Problem 1)

   1.1 As hint says, just consider about the case of $\ell = 1$

      a Yes, through $\mathcal{K}$, all messages get the same ciphertext set $\mathcal{C} = \mathcal{S}^2$.
      $P(\mathcal{C} = c|\mathcal{M} = m) = \frac{1}{4}$, which is a constant. So, $\forall m, P(\mathcal{C} = c|\mathcal{M} = m)$ are same.

      b No. because, $|\mathcal{K}| < |\mathcal{M}|$

      c No. $01 \oplus 10 = 11$, so $11 \in \mathcal{C}$. However there is not key k that $Enc_k(00) = 11$. Violet the Shannon's theorem.

   1.2 When $|\mathcal{K}| < |\mathcal{M}|$, which is in case(b), cipher could not be secure according to the **theorem 2.10** in the textbook. When $\mathcal{K} = \{0,1\}^\ell$, cipher is always secure, because no matter what message set is, as long as it is not empty, the ciphertext set $\mathcal{C}$ is always $\{0,1\}^\ell$ which makes $P(\mathcal{C} = c|\mathcal{M} = m) = 2^{-\ell}$.

2. (Problem 2)

   (a) $\forall m, P(\mathcal{C} = c|\mathcal{M} = m) = \frac{1}{26}$ is a constant, so they are all same.

   (b) let take a example, $m_0 = aa, m_1 = ab$ and $c = bb$. we can say $P(\mathcal{C} = c|\mathcal{M} = m_0) = \frac{1}{26}$ however $P(\mathcal{C} = c|\mathcal{M} = m_1) = 0$.

   (c) this means this cipher is not perfectly secrecy anymore. The prior distribution and posterior distribution of $\mathcal{M}$ are different.

   (d) the largest set of A is $\mathcal{K}$.
   Proof:
   (1)First, I want to argue that if $\mathcal{M} = \mathcal{K} = A$, then $\forall m \in \mathcal{M}, A = \{Enc_k(m)|\forall k \in \mathcal{K}\}$,as well as the mapping $\forall m \in \mathcal{M}, \mathcal{F} : \mathcal{K} \to \{Enc_k(m)|\forall k \in \mathcal{K}\}$ is bijection.
   The proof is easy if aware that A is a permutation group. Since A is a subgroup of A, for any element m, its coset is A. Thus $A = \{Enc_k(m)|\forall k \in \mathcal{K}\}$ holds. Also because of coset, the mapping is bijection
   Now, two condition of Shannon's theorem are met. So it is a perfect cipher.

   (2)According to Shannon's theorem, $|\mathcal{M}| \leq |\mathcal{K}|$. The size of any possible set is less or equal to the size of $\mathcal{K}$.

   Base on (1),(2), A is a largest perfect cipher.

3. (Problem 3)

   An example, $m_0 = 00, m_1 = 01$ and $c = 00$. Then $P(\mathcal{C} = c|\mathcal{M} = m_0) = \frac{1}{2}$, $P(\mathcal{C} = c|\mathcal{M} = m_1) = 0$.

4. (Problem 4)

2.11 Let $\mathcal{M}$ be the set of all possible messages that are possible decode of c, that is,

$$\mathcal{M}(c) = \{m | m = \text{Dec}_k(c) \text{ for someone } k \in \mathcal{K}\}$$

Because for every different k, there are at most 2^t different choice about m, so $|\mathcal{M}(c)| \leq 2^t|\mathcal{K}|$. Thus $|\mathcal{K}| \geq 2^{-t}|\mathcal{M}(c)|$

2.12 The idea is first filling some elements into set $\mathcal{K}$ to make its size equal to $\mathcal{M}$ and cipher is "perfect", then calculate the probability and subtract these elements out.

Consider following encryption algorithm III. Let $|\mathcal{K}| = |\mathcal{M}|$, and a special attack rule in adversarial experiment is that there is a special key set $K_{valid} \in \mathcal{K}$. When Gen generate a key which is **not** in this set, adversary win directly. Then, it leads following probability:

$$Pr[\text{Privk}^{eav}_{\mathcal{A},\text{III}} = 1] = \frac{M-K}{M} + \frac{1}{2} * \frac{K}{M}$$

here, $M = |\mathcal{M}|, K = |K_{valid}|$. Now, we take other elements away and only keep the set K_{valid} as $\mathcal{K}$. Still, we can see that new game is the same as previous one and the probability is not change. Which leads:

$$\begin{aligned} Pr[\text{Privk}^{eav}_{\mathcal{A},\text{III}} = 1] &\leq \frac{1}{2} + \epsilon \\ \frac{K}{M} + \frac{1}{2} * \frac{M-K}{M} &\leq \frac{1}{2} + \epsilon \\ K &\geq (1-2\epsilon)M \end{aligned}$$

Thus, the bound is $K \geq (1-2\epsilon)M$.