Cryptography: Homework 2

(Deadline: 11:59am, 2019/10/02)

1. (20 points) Let $\mathcal{K} = \{k_1, k_2, k_3, k_4, k_5\}, \mathcal{M} = \{a, b\}$, and let $\mathcal{C} = \{1, 2, 3, 4, 5\}$. Let $\Pi = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec}) + \mathcal{M}$ be a private-key encryption scheme with key space $\mathcal{K}$, plaintext space $\mathcal{M}$ and ciphertext space $\mathcal{C}$, where the algorithms are defined as follows:

   - $k \leftarrow \mathbf{Gen}$: Randomly choose the secret key k from $\mathcal{K}$ such that $\Pr[k = k_1] = \Pr[k = k_2] = \Pr[k = k_3] = 1/9$ and $\Pr[k = k_4] = \Pr[k = k_5] = 1/3$. Output k.
   - $c \leftarrow \mathbf{Enc}(k, m)$: For $k \in \mathcal{K}$ and $m \in \mathcal{M}$, define the ciphertext c as the (k, m)-entry of the following table

	a	b
k_1	1	2
k_2	2	3
k_3	3	1
k_4	4	5
k_5	5	4

     i.e., the entry at row k and column m. Output c.
   - $m \leftarrow \mathbf{Dec}(k, c)$: For $k \in \mathcal{K}$ and $c \in \mathcal{C}$, define the plaintext m as the element of $\mathcal{M}$ such that the (k, m)-entry of the above table is equal to c. Output m.

   Show that the private-key encryption scheme Π is perfectly secret.

2. (30 points) Let Π be the Vigenère cipher where the message space consists of all 3-character strings (i.e., $\mathcal{M} = \{\mathrm{a}, \mathrm{b}, \ldots, \mathrm{z}\}^3$), and the key is generated by first choosing the key length t uniformly from $\{1, 2, 3\}$ and then choosing the secret key k uniformly from the set $\{\mathrm{a}, \mathrm{b}, \ldots, \mathrm{z}\}^t$. Construct an adversary $\mathcal{A}$ such that $\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] > 0.5$.

   Grading Policy: The highest score s for your adversary $\mathcal{A}$ is defined as follows:

$$s = \begin{cases} 0 \text{ points}, & \text{if } \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] \leq 0.5; \\ 15 \text{ points}, & \text{if } 0.5 < \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] \leq 0.6; \\ 20 \text{ points}, & \text{if } 0.6 < \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] \leq 0.7; \\ 25 \text{ points}, & \text{if } 0.7 < \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] \leq 0.8; \\ 30 \text{ points}, & \text{if } \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] > 0.8. \end{cases}$$