Cryptography ENEE/CMSC/MATH 456: Homework 2

Due by beginning of class on 2/13/2019.

1. Prove that, by redefining the key space, we may assume the key-generation algorithm Gen chooses a key uniformly at random, without changing $\Pr[C = c|M = m]$ for any m, c.

   Hint: Define the key space to be the set of all possible random tapes for the randomized algorithm Gen.

2. Let $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over message space $\mathcal{M}$ with keyspace $\mathcal{K}$ and ciphertext space $\mathcal{C}$ be an encryption scheme that achieves perfect secrecy. Let $\mathcal{M}_1 \subseteq \mathcal{M}, \mathcal{M}_2 = \mathcal{M} \setminus \mathcal{M}_1$ be two subsets of $\mathcal{M}$ such that $|\mathcal{M}_1| \geq 1, |\mathcal{M}_2| \geq 1$. Furthermore, let $\mathcal{D}_1$ be the uniform distribution over $\mathcal{M}_1$, $\mathcal{D}_2$ be the uniform distribution over $\mathcal{M}_2$.
   Finally, let C_1 (resp. C_2) be the random variable corresponding to the distribution over ciphertexts when messages are sampled from $\mathcal{D}_1$ (resp. $\mathcal{D}_2$) and keys are sampled by Gen.

   Is it possible that there is a ciphertext $c \in \mathcal{C}$ such that $\Pr[C_1 = c] = 0$ and $\Pr[C_2 = c] > 0$? If yes, give an example of a specific encryption scheme that is perfectly secret and for which the above holds. If not, prove that for any encryption scheme that is perfectly secret, the above cannot hold.

3. In this problem we consider definitions of perfect secrecy for the encryption of two messages (using the same key). Here we consider distributions over pairs of messages from the message space $\mathcal{M}$; we let M_1, M_2 be random variables denoting the first and second message, respectively. We generate a (single) key k, sample messages (m_1, m_2) according to the given distribution, and then compute ciphertexts $c_1 \leftarrow \mathsf{Enc}_k(m_1)$ and $c_2 \leftarrow \mathsf{Enc}_k(m_2)$; this induces a distribution over pairs of ciphertexts and we let C_1, C_2 be the corresponding random variables.

   (a) Say encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is perfectly secret for two messages if for all distributions over $\mathcal{M} \times \mathcal{M}$, all $m_1, m_2 \in \mathcal{M}$, and all ciphertexts $c_1, c_2 \in \mathcal{C}$ with $\Pr[C_1 = c_1 \wedge C_2 = c_2] > 0$: $\Pr[M_1 = m_1 \wedge M_2 = m_2 | C1 = c_1 \wedge C_2 = c_2] = \Pr[M_1 = m_1 \wedge M_2 = m_2]$. Prove that no encryption scheme can satisfy this definition.
   Hint: Take $m_1 \neq m_2$ but $c_1 = c_2$.

   (b) Say encryption scheme $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is perfectly secret for two distinct messages if for all distributions over $\mathcal{M} \times \mathcal{M}$ where the first and second messages are guaranteed to be different (i.e., distributions over pairs of distinct messages), all $m_1, m_2 \in \mathcal{M}$, and all $c_1, c_2 \in \mathcal{C}$ with $\Pr[C_1 = c_1 \wedge C_2 = c_2] > 0$: $\Pr[M_1 = m_1 \wedge M_2 = m_2 | C1 = c_1 \wedge C_2 = c_2] = \Pr[M_1 = m_1 \wedge M_2 = m_2]$. Show an encryption scheme that provably satisfies this definition.
   Hint: The encryption scheme you propose need not be efficient, though an efficient solution is possible.

4. When using the one-time pad with the key $k = 0^\ell$, we have $\mathsf{Enc}_k(m) = k \oplus m = m$ and the message is sent in the clear! It has therefore been suggested to modify the one-time pad by only encrypting with $k \neq 0^\ell$ (i.e., to have Gen choose k uniformly at random from the set of non-zero keys of length ℓ). Is this modified scheme still perfectly secret? Explain.

5. For each of the following encryption schemes, state whether the scheme achieves perfect secrecy. Justify your answer using Definition 2.3, Lemma 2.4, Theorem 2.10 and/or Theorem 2.11.

   - Message space $\mathcal{M} = \{1, \ldots, 6\}$. Key space $\mathcal{K} = \{1, ..., 6\}$. $\mathsf{Gen}()$ chooses a key k at random from $\mathcal{K}$. Let k' be such that $k \cdot k' \equiv 1 \mod 7$ (e.g. for $k = 5$, we have $k' = 3$ since $(5 \cdot 3) \mod 7 \equiv (15) \mod 7 = 1 \mod 7$). $\mathsf{Enc}_k(m)$ returns $m \cdot k \mod 7$. $\mathsf{Dec}_k(c)$ returns $c \cdot k' \mod 7$.

   - What happens when we use the same scheme as above except with $\mathcal{M} = \{1, \ldots, 8\}$ and $\mathcal{K} = \{1, \ldots, 8\}$? I.e. $\mathsf{Gen}()$ chooses a key k at random from $\mathcal{K}$ and $\mathsf{Enc}_k(m)$ returns $m \cdot k \mod 9$.