University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

Problem Set 2

Due at the *beginning* of class on Sept. 21

1. Prove that a private-key encryption scheme is perfectly secret if and only if it is perfectly indistinguishable in the sense we defined in class (i.e., Definition 2.4). (This is Proposition 2.5 in the book. Remember to prove both directions.)

2. (Exercise 2.2.) Prove or refute: For every encryption scheme that is perfectly secret it holds that for every distribution over the message space $\mathcal{M}$, every $m, m' \in \mathcal{M}$, and every $c \in \mathcal{C}$:
$$\Pr[M = m \mid C = c] = \Pr[M = m' \mid C = c].$$

3. (Exercise 2.4.) In this exercise, we study conditions under which the shift, mono-alphabetic substitution, and Vigenére ciphers are perfectly secret:

   (a) Prove that if only a single character is encrypted, then the shift cipher is perfectly secret.

   (b) What is the largest plaintext space $\mathcal{M}$ you can find for which the mono-alphabetic substitution cipher provides perfect secrecy? (Note: $\mathcal{M}$ need not contain only valid English words.)

   (c) Show how to use the Vigenére cipher to encrypt any word of length t so that perfect secrecy is obtained (note: you can choose the length of the key). Prove your answer.

   Reconcile this with the attacks that were shown in class.

4. (Exercise 2.9.) Consider the following definition of perfect secrecy for the encryption of *two* messages. An encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{M}$ is *perfectly-secret for two messages* if for all distributions over $\mathcal{M}$, all $m, m' \in \mathcal{M}$, and all $c, c' \in \mathcal{C}$ with $\Pr[C = c \wedge C' = c'] > 0$:
$$\Pr\left[M = m \wedge M' = m' \mid C = c \wedge C' = c'\right] = \Pr[M = m \wedge M' = m'],$$
   where m and m' are sampled independently from the same distribution over $\mathcal{M}$. Prove that *no* encryption scheme satisfies this definition. (*Hint:* Take $m \neq m'$ but $c = c'$.)

5. (Exercise 2.10.) Consider the following definition of perfect secrecy for the encryption of two messages. Encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{M}$ is *perfectly-secret for two messages* if for all distributions over $\mathcal{M}$, all $m, m' \in \mathcal{M}$ with $m \neq m'$, and all $c, c' \in \mathcal{C}$ with $c \neq c'$ and $\Pr[C = c \wedge C' = c'] > 0$:
$$\Pr[M = m \wedge M' = m' \mid C = c \wedge C' = c'] = \Pr[M = m \wedge M' = m' \mid M \neq M'],$$

where m and m' are sampled independently from the same distribution over $\mathcal{M}$. Show an encryption scheme that provably satisfies this definition. How long are the keys compared to the length of a message? (*Hint:* The encryption scheme you propose need not be "efficient".)

6. Show *directly* that if an encryption scheme is perfectly indistinguishable (in the sense we defined in class, i.e., Definition 2.4) then $|\mathcal{K}| \geq |\mathcal{M}|$. You should *not* use the fact that perfect indistinguishability and perfect secrecy are equivalent, but should instead proceed directly via the following steps:

   (a) Construct a specific adversary $\mathcal{A}$ for the experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$. You need to specify the messages it will output in the first step, and how it determines its output in the third step.

   (b) Compute $\Pr\left[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1\right]$, and show that it is not equal to $1/2$.

7. Prove that if ϵ_1, ϵ_2 are both negligible functions, then their sum ϵ (defined by $\epsilon(n) = \epsilon_1(n) + \epsilon_2(n)$) is also negligible.