CS 435: Introduction to Cryptography **2012 Fall**

Homework 2

Professor Somesh Jha **Due:** October 12

1. (Problem 2.6) Let an encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ satisfy Definition 2.1 for all distributions over $\mathcal{M}$ *that assign non-zero probability to each* $m \in \mathcal{M}$ (as per the simplifying convention used in Chapter 2). Show that the scheme satisfies the definition for *all* distributions over $\mathcal{M}$ (i.e., including those that assign zero probability to some messages in $\mathcal{M}$). Conclude that the scheme is also perfectly secret for any message space $\mathcal{M}' \subseteq \mathcal{M}$.

2. Prove that the Vigenère cipher is not perfectly secret using Definition 2.4 of perfect secrecy.

   Hint. How do you deal with the fact that the adversary doesn't know how long the key is?

3. (Problem 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 $\Pr[C = c \wedge C' = c'] > 0$:

   $$\Pr[M = m \wedge M' = m' \mid C = c \wedge C' = c'] = \Pr[M = m \wedge M' = m'],$$

   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 $c = c'$.

4. (a) (Problem 2.10) 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 $\Pr[C = c \wedge C' = c'] > 0$:

   $$\Pr[M = m \wedge M' = m' \mid C = c \wedge C' = c'] = \Pr[M = m \wedge M' = m' \mid M \neq M'],$$

   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 in terms of the length of a message?

   Hint. The encryption scheme you propose need not be "efficient".

   (b) Formulate a similar definition of perfect secrecy for the encryption of $k > 1$ messages. Does your encryption scheme from part (a) satisfy this definition for all k?