CS655: Cryptography **Spring 2007**

Homework #3

Due date & time: 10:30am on February 13, 2007. Hand in at the beginning of class (preferred), or email to the instructor (ninghui@cs.purdue.edu) by the due time.

Late Policy: Late homework will not be accepted.

Additional Instructions: (1) The submitted homework must be typed. Using Latex is recommended, but not required.

Problem 1 (5 pts) *An equivalent formulation of perfect secrecy*

Prove that a symmetric cipher has perfect secrecy if and only if it satisfies the following condition:

$$\forall_{M_0 \in \mathcal{M}} \forall_{M_1 \in \mathcal{M}} \forall_{C_0 \in \mathcal{C}} \ (\mathsf{Pr}\left[\mathsf{CT} = C_0 \mid \mathsf{PT} = M_0\right] = \mathsf{Pr}\left[\mathsf{CT} = C_0 \mid \mathsf{PT} = M_1\right])$$

Hint: I ran the proofs quickly in my mind. It seems to work, but I am not certain. So if you find any direction of the implication is not true, give a counter example.

Problem 2 (10 pts) *Problem 3.3.*

Given a PRF $F : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$, construct a PRF $G : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^{2n}$. Prove the security of your construction.

Hint: Consider the construction Qihua gave in class: $G_K(x) = F_K\left(F_K(x)\right) \| F_K\left(\overline{F_K(x)}\right)$. What happens when we replace F with the family of all functions? You may need to bound advantage of attackers based on the number of queries made.

Problem 3 (10 pts) *Problem 4.2.*

Consider the following notion of indistinguishability of an encryption scheme $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$:

$$\mathbf{Adv}^{\mathsf{ind0\text{-}cpa}}_{\mathcal{SE}}(A) = \mathsf{Pr}\left[K \xleftarrow{\$} \mathcal{K} : A^{\mathcal{E}_K(\cdot)} = 1\right] - \mathsf{Pr}\left[K \xleftarrow{\$} \mathcal{K} : A^{\mathcal{E}_K(0^{|\cdot|})} = 1\right].$$

That is, a scheme is IND0-CPA secure if the encryption of every string looks like the encryption of a string of zeros of equal length. Prove that this notion of security is equivalent to IND-CPA security, carefully stating a pair of theorems and proving them.

Problem 4 (5 pts) *Problem 4.5.*

The CBC-Chain mode of operation is a CBC variant in which the IV that is used for the very first message to be encrypted in random, while the IV used for each subsequent message is the last block of ciphertext that was generated. The scheme is probabilistic and stateful. Show that CBC-Chain is insecure by giving a simple and efficient adversary that breaks it in the IND-CPA sense.