T-79.5502 Advanced Course in Cryptology
Exam
December 16, 2011

Exam policy: Select any three problems, but not more than three.

1. Consider the CPA indistinguishability experiment $\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n)$ for a private-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.

   - A key k is generated by running $\mathsf{Gen}(1^n)$.
   - The adversary $\mathcal{A}$ is given input 1^n and oracle access $\mathsf{Enc}_k(\cdot)$. Then it outputs a pair of messages m_0, m_1 of the same length.
   - A random bit $b \leftarrow \{0,1\}$ is chosen. A ciphertext $c \leftarrow \mathsf{Enc}_k(m_b)$ is computed and given to $\mathcal{A}$. We call c the challenge ciphertext.
   - $\mathcal{A}$ continues to have access to oracle $\mathsf{Enc}_k(\cdot)$. Eventually, $\mathcal{A}$ outputs a bit b'. We denote $b' = \mathsf{output}(\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n, b))$.
   - The result of the experiment is defined to be 1 if $b' = b$, and 0 otherwise. We write $\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n) = 1$ if the result is 1 and in this case we say that $\mathcal{A}$ succeeded.

   Show that the following two conditions are equivalent

   (i) there exists a negligble function negl such that

   $$\Pr[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathsf{negl}(n),$$

   (ii) there exists a negligble function negl such that

   $$|\Pr[\mathsf{output}(\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n, 0)) = 1] - \Pr[\mathsf{output}(\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n, 1)) = 1]| \leq \mathsf{negl}(n).$$

2. Suppose that $\Pi_{\mathsf{E}} = (\mathsf{Gen}_{\mathsf{E}}, \mathsf{Enc}, \mathsf{Dec})$ is a private-key encryption scheme and $\Pi_{\mathsf{M}} = (\mathsf{Gen}_{\mathsf{M}}, \mathsf{Mac}, \mathsf{Vrfy})$ is a message authentication code. Give a construction of a private-key encryption scheme that can be proven to have indistiguishable encryptions under a chosen-ciphertext attack. What security assumptions about Π_{E} and Π_{M} are made to achieve a proof of CCA-security? (You do not need to give the security proof.)

3. Let $\mathcal{G}$ be a polynomial time algorithm that, on input 1^n outputs a description of a cyclic group $\mathbb{G}$, its order q, with $\|q\| = n$, and a generator g in $\mathbb{G}$. Prove that if the discrete logarithm problem is hard relative to $\mathcal{G}$, then there exists a collision-resistant fixed-length hash function (Gen, H).

4. Suppose that $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a public-key encryption scheme and $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ is a private-key encryption scheme. Give a construction of the Hybrid encryption scheme. Formulate the statement on the security of this construction and outline its proof "by transitivity".