CS 601.442/642 – Modern Cryptography Instructor: Abhishek Jain

Homework 3

Deadline: October 22; 2017, 11:59 PM

1 Encryption

1. (15 Points) Let $\mathcal{E}_1 = (\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ and $\mathcal{E}_2 = (\mathsf{Gen}_2, \mathsf{Enc}_2, \mathsf{Dec}_2)$ be two public key encryption schemes such that only one of them is **IND-CPA** secure, but you don't know which one. Using only $\mathcal{E}_1$ and $\mathcal{E}_2$, construct an **IND-CPA** secure encryption scheme and prove its security.

2. (20 Points) Consider the following alternate definition of **IND-CPA** security for secret-key encryption, where the adversary also gets access to an encryption oracle. The oracle takes a message m as input and returns a ciphertext $c \leftarrow \mathsf{Enc}(\mathsf{m}, \mathsf{s})$:
(One-Message) IND-CPA$^+$ Security: A secret-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is one-message IND-CPA$^+$ secure if for all n.u. PPT adversaries $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ such that:

$$\Pr\left[\begin{array}{rl} & s \xleftarrow{\$} \mathsf{Gen}(1^n), \\ (m_0, m_1) \leftarrow \mathcal{A}^{\mathsf{Enc}(\mathsf{s},.)}(1^n), & : \mathcal{A}^{\mathsf{Enc}(\mathsf{s},.)}(\mathsf{Enc}(s, m_b)) = b \\ & b \xleftarrow{\$} \{0,1\}, \end{array}\right] \leq \frac{1}{2} + \mu(n)$$

Note that since the adversary is a polynomial time algorithm, it can only make polynomial number of queries to the oracle.

   (a) Show that for a stateless encryption scheme to be IND-CPA$^+$ secure, its Enc algorithm must be randomized.

   (b) Define multi-message IND-CPA$^+$ security and prove that one-message IND-CPA$^+$ security for secret-key encryption implies multi-message IND-CPA$^+$ security.

2 Authentication

1. (10 Points) Let $\mathcal{M}_1 = (\mathsf{Gen}_1, \mathsf{Sign}_1, \mathsf{Verify}_1)$ and $\mathcal{M}_2 = (\mathsf{Gen}_2, \mathsf{Sign}_2, \mathsf{Verify}_2)$ be two MAC schemes such that only one of them is **UF-CMA** secure, but you don't know which one. Using only $\mathcal{M}_1$ and $\mathcal{M}_2$, construct a **UF-CMA** secure MAC scheme and prove its security.

2. (15 Points) A one-time signature scheme $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify})$ is **strongly UF-CMA** secure if for all n.u. PPT adversaries $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ such that:

$$\Pr\left[\begin{array}{rl} (sk, pk) \leftarrow \mathsf{Gen}(1^n), & \\ m \leftarrow \mathcal{A}(1^n, pk), & \\ \sigma \leftarrow \mathsf{Sign}(sk, m), & \\ (m', \sigma') \leftarrow \mathcal{A}(1^n, pk, \sigma), & : ((m, \sigma) \neq (m', \sigma')) \wedge (\mathsf{Ver}_{pk}(m', \sigma')) = 1 \end{array}\right] \leq \mu(n)$$

Note that in **strongly UF-CMA** security, the adversary is allowed to output $m' = m$ as long as $\sigma' \neq \sigma$.
Prove that Lamport's signature scheme instantiated with an injective (one-to-one) one-way function is **strongly UF-CMA** secure.