CS6111: Foundations of Cryptography	Oct 24, 2017
Homework 3	
Instructor: Shweta Agrawal	*Due: Oct 31*

Notation. We let || denote the concatenation operator.

Problem 1: Digital Signatures

A strong one-time signature scheme satisfies the following (informally): given a signature σ on a message m, it is infeasible to output $(m', \sigma') \neq (m, \sigma)$ for which σ' is a valid signature on m' (note that $m = m'$ is now allowed, as long as $\sigma' \neq \sigma$).

Assuming the existence of one-way functions, show a one-way function f for which Lamport's scheme is not a strong one-time signature scheme.

Problem 2: One time signatures

In class, we saw Lamport's construction of a one time signature. In this problem, we will extend it to build a two-time signature. Let $f : X \to Y$. Assume that the messages to be signed are ℓ bits long. Let $L = 2^\ell$ and interpret m as a number in $\{1, \ldots, L\}$.

Let $\Sigma_n = \{1, \ldots, n\}$ and let $S_1, \ldots, S_L \subset \Sigma_n$ be subsets of Σ_n. The sets $S_1, \ldots, S_L$ are fixed and known to everyone. Consider the following signature scheme. Algorithm KeyGen picks random $x_1, \ldots, x_n \leftarrow X$ and outputs $\mathsf{PK} = \big(f(x_1), \ldots, f(x_n)\big)$ and $\mathsf{SK} = \big(x_1, \ldots, x_n\big)$.

We define

$$\sigma = \mathsf{Sign}(m, \mathsf{SK}) = \{\text{all } x_i \text{ where } i \in S_m\}$$

a. Explain how $\mathsf{Verify}(m, \sigma, \mathsf{PK})$ works. What is the worst case length of the resulting signature?

b. We say that the sets $S_1, \ldots, S_L$ are cover free if for all $1 \leq i \neq j \leq L$ we have $S_i \not\subseteq S_j$. Briefly explain why if $S_1, \ldots, S_L$ are cover free then the signature scheme is a secure one time signature scheme.

c. Let us assume that ℓ is a power of 2 and let $n = \ell + 1 + \log \ell$. For a message $m \in \{0,1\}^\ell$ let c be the number of 0s in m. Let $\hat{m} = m||c \in \{0,1\}^n$ and let $\hat{m}_1, \ldots, \hat{m}_n \in \{0,1\}$ be the n bits of $\hat{m}$. Define the set S_m as:

$$S_m = \{1 \leq i \leq n \text{ where } \hat{m}_i = 1\} \subseteq \Sigma_n$$

Prove that the sets $(S_1, \ldots, S_L)$ are cover free. What is the length of the resulting signatures as a function of ℓ?

d. We say that the sets $(S_1, \ldots, S_L)$ are 2-cover free if for all $1 \leq i, j, k \leq L$ where $i \neq j, k$ we have that $S_i \not\subseteq S_j \cup S_k$. Briefly explain why if $(S_1, \ldots, S_L)$ are 2-cover free the the signature scheme is a **two time** secure signature scheme (i.e. it remains secure as long as SK is not used to sign more than two messages).

e. **(extra credit)** Construct L sets $(S_1, \ldots, S_L) \subseteq \Sigma_n$ that are 2 cover free where $n = O(\ell^2)$. Note that $n = O(\ell)$ is possible.

Problem 3: More on Digital Signatures

Prove that the existence of secure digital signature schemes implies the existence of one-way functions.

Problem 4: PRF from MAC

Recall that a PRF is a MAC. In this problem, we will construct a PRF from a MAC.

a. Recall that we can compute a hardcore bit of a one-way function $f(x)$ using $\langle x, r\rangle$ where r is a random string and: $\langle y, r\rangle = \sum_{i=1}^{k} y_i r_i \mod 2$. Suppose g is a secure MAC for $\{0,1\}^k \times \{0,1\}^n \to \{0,1\}^m$. Let $f' : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}$ and $f'(s,x) = \langle g(s,x), r\rangle$ where $r \leftarrow \{0,1\}^m$. Give a contrived example to show that f' is not a PRF.

b. We fix the above function by keeping r secret as follows $h(s,r,x) = \langle g(s,x), r\rangle$. Prove that h is a PRF.

Hint 1: How can an adversary $\mathcal{A}$ that distinguishes between h and a truly random function be used to learn a value of h on an input without explicitly querying for it?

Hint 2: Recall that given a value r and a good prediction for $\langle z, r\rangle$ one can learn a value of z.

Hint 3: Use the above to break security of $g(s,x)$.

c. The output of h is a single bit. Propose a construction based on h that outputs more than one bit. Argue that your construction is a PRF.

Problem 5: Commitment Scheme

A commitment scheme enables Alice to commit a value x to Bob. The scheme is *hiding* if the commitment does not reveal to Bob any information about the committed value x. At a later time Alice may *open* the commitment and convince Bob that the committed value is x. The commitment is *binding* if Alice cannot convince Bob that the committed value is some $x' \neq x$. Here is an example commitment scheme:

- **Public Values:** (1) a 1024 bit prime p (2) two elements g and h of $\mathbb{Z}_p^*$ of prime order q.
- **Commit:** To commit an integer $x \in [1, q-1]$ Alice picks a random $r \in [1, q-1]$ and computes $b = g^x \cdot h^r \mod p$. She sends b to Bob as her commitment to x.
- **Open:** To open the commitment, Alice sends (x, r) to Bob. He verifies that $b = g^x \cdot h^r \mod p$.

Show that this scheme is both hiding and binding. For hiding, show that given b the committed value can be any $x' \in [1, q-1]$. To show binding, prove that if Alice can open her commitment to some (x', r') where $x' \neq x$, then she can find the discrete log of h base g.

Problem 6: Symmetric Key Encryption (Optional/Extra Credit).

In class we defined security against chosen-plaintext attacks (CPA security). A weaker notion of security is multi-message indistinguishability, which means that the adversary outputs two vectors of messages $(m_1^0, \ldots, m_k^0)$ and $(m_1^1, \ldots, m_k^1)$ and gets to see an encryption of one of these vectors. He cannot make any ciphertext queries for messages of his choice though. The attacker wins if he can guess which of the two vectors was encrypted in the challenge with probability non-negligibly better than 1/2.

Show that the notion of multi-message indistinguishability is strictly weaker than CPA security. To do so, construct a private-key encryption scheme that is secure in the sense of multi-message indistinguishability, but is not secure against chosen-plaintext attacks.