Exercise 6 – Introduction to Cryptography 89-656

Due Date: January 13, 2019

December 30, 2018

Exercise 1: Assume the RSA problem is hard. Show that the plain RSA signature scheme satisfies the following weak definition of security: an attacker is given the public key (N, e) and a uniform message $m \in \mathbb{Z}_N^*$. The adversary succeeds if it can output a valid signature on m without making any signing queries. Formally define the notion of security and prove the claim.

Exercise 2: Provide a full detailed proof that the following scheme is a secure message authentication code:

1. Gen: Run genRSA to obtain (N, e, d) and choose a random $k \leftarrow \{0,1\}^n$ for a pseudorandom function F with domain $\mathbb{Z}_N$. The MAC key is (N, e, d, k).
2. Mac: Upon input $m \in \{0,1\}^*$ and key (N, e, d, k) compute $t = (F_k(m))^d \bmod N$.
3. Vrfy: Upon input m, t and key (N, e, d, k) output 1 if and only if $F_k(m) = t^e \bmod N$.

You may rely on the proof of RSA-FDH in your proof (i.e., reduce the security of the MAC to RSA-FDH). Your proof should rely only on the assumption that F is a pseudorandom function and that the RSA inversion problem is hard.

Exercise 3: Analyze the following proposals for digital signatures:

1. *El-Gamal signatures:* Run $\mathcal{G}(1^n)$ to obtain $(\mathbb{G}, q, g)$ and choose $x \leftarrow \mathbb{Z}_q$. The public key is $h = g^x$ and the private key is x. In order to sign on a message $m \in \mathbb{Z}_q$, compute $u = g^m$ and $v = u^x$. The signature is the pair (u, v).
2. *Random Oracle El-Gamal signatures:* Exactly as above, but compute $u = g^{H(m)}$, where H is modeled as a random oracle with range $\mathbb{Z}_q$.

Exercise 4:

1. Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme for encrypting a single bit. Consider a new scheme for encrypting messages of arbitrary length by encrypting each bit separately. In class, we stated that if $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is CPA-secure then the new scheme described above is CPA-secure. If $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is CCA-secure, then is the new scheme also CCA secure? Prove your answer.
2. Let $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ be a secure signature scheme for signing on a single bit. Consider a new scheme for signing messages of arbitrary length by signing each bit separately. Is the new scheme a secure signature scheme? Prove your answer.

3. Let $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Vrfy})$ be a secure signature scheme for signing on a single bit. Consider a new scheme for signing messages of arbitrary length by signing each bit separately and then signing on a cryptography hash of the message. Specifically, to sign on a message m of length L, sign on each bit of the string $m \| H(m)$ where H is a collision-resistant hash function.

   Is the new scheme a secure signature scheme? Is it secure assuming that H is a random oracle? Prove your answer.

Exercise 5: Consider the following proposal for a scheme for signing on a single bit:

- $\mathsf{Gen}(1^n)$: run $\mathsf{GenRSA}(1^n)$ to get (N, e, d). Choose two random strings $x_0, x_1 \in \mathbb{Z}_N$. The public verification key is $vk = (N, e, x_0, x_1)$; the private signing key is $sk = (N, d, x_0, x_1)$.
- $\mathsf{Sign}(sk, b)$ for $b \in \{0, 1\}$: output $\sigma = (x_b)^d \bmod N$.
- $\mathsf{Vrfy}(vk, b, \sigma)$: output 1 if and only if $\sigma^e = x_b \bmod N$.

Is the scheme secure? Prove your answer.