CS 120/CSCI E-177: Introduction to Cryptography

Problem Set 7

Assigned: Nov. 17, 2006 Due: FRIDAY, Dec. 1, 2006 (1:10 PM)

Justify all of your answers. See the syllabus for collaboration and lateness policies. You can submit by email to `ciocan@eecs` (please include source files) or by hardcopy to Carol Harlow in MD 343.

Problem 1. (Attacks on "Plain" Public-Key Schemes)

1. Suppose you see the encryption of messages m, $m+1$, and $m+2$ under plain RSA encryption with exponent 3. Show how to recover m in polynomial time.

2. Suppose Alice wants to invite 2 friends to a party and decides to encrypt the invitation m using plain Rabin encryption. Assume her friends use two different public keys, N_1, N_2. Show that if the uninvited Eve sees the 2 different encryptions sent to Alice's friends, $E_{N_1}(m), E_{N_2}(m)$, she can efficiently recover m and crash the party. (Hint: use the Chinese Remainder Theorem.)

3. Recall that, for efficiency reasons, public-key encryption schemes (G^1, E^1, D^1) are often used in conjunction with a private-key encryption scheme (G^2, E^2, D^2) to obtain a 'hybrid encryption' scheme that works as follows. The public and secret keys are generated as $(pk, sk) \leftarrow G^1(1^n)$, and $E_{pk}(m)$ is defined as follows: Choose a random key $k \stackrel{R}{\leftarrow} G^2(1^n)$, let $c^1 \stackrel{R}{\leftarrow} E^1_{pk}(k)$, let $c^2 \stackrel{R}{\leftarrow} E^2_k(m)$, and output (c^1, c^2). (The gain in efficiency is because typically $|m| \gg |k|$ and E^2 is more efficient than E^1.) In KL §9.4, it is shown that if both initial schemes have indistinguishable encryptions, then so does the hybrid scheme.

   Show that the hybrid encryption scheme is not necessarily secure if we use a plain trapdoor permutation for the public-key scheme. That is, show how to modify any collection of trapdoor permutations and secure private-key encryption scheme so that when "hybridized," the result is completely insecure.

4. Explain why such attacks could not work if we used public-key encryption schemes that have indistinguishable encryptions (i.e. are semantically secure).

Problem 2. (Paillier Encryption) Assume Alice is using a Paillier encryption scheme as described in class, where an encryption of a message m with random help value r is $E_N(m, r) = (1+N)^m r^N \mod N^2$, using her public Paillier key N.

1. We showed in class that Alice can prove to a third party that $c_1 = E_N(m, r_1)$ and $c_2 = E_N(m, r_2)$ are encryptions of the same value m without revealing any information about m by calculating $c_1/c_2 \bmod N^2 = E_N(m - m = 0, r_1/r_2 \bmod N^2)$ and revealing the random help value $r = r_1/r_2 \bmod N^2$. (The third party verifies $c_1/c_2 \equiv (r_1/r_2)^N \pmod{N^2}$.)

Assuming the Decisional Composite Residuosity Assumption, prove that this method indeed yields no information about m to a polynomial-time adversary. That is, show that for every $m, m' \in \mathbb{Z}_N$

$$(E_N(m, R_1), E_N(m, R_2), R_1/R_2) \stackrel{c}{\equiv} \left(E_N(m', R_1), E_N(m', R_2), R_1/R_2\right).$$

2. We also showed in class how Alice can prove, given public ciphertexts $c_1 = E_N(m_1, r_1)$ and $c_2 = E_N(m_2, r_2)$, that $m_1 \geq m_1$ without revealing any additional information about m_1 or m_2 (except an upper bound 2^t on their values). Show how Alice, given c_1 and c_2, can prove the strict inequality $m_1 > m_2$. (Hint: reduce proving a strict inequality to proving a weak inequality using the homomorphic properties of Paillier encryption.)

Problem 3. (Variants of CBC-MAC) Recall that for a pseudorandom function family $\mathcal{F}_n = \{f_k : \{0,1\}^n \to \{0,1\}^n\}$, the CBC-MAC is defined to be

$$M_k(m) = f_k\left(m_\ell \oplus f_k\left(m_{\ell-1} \oplus \cdots f_k\left(m_2 \oplus f_k\left(m_1\right)\right)\right)\right),$$

where $m_1 m_2 \cdots m_\ell$ is a partition of m into blocks of length n. It is shown in Katz–Lindell that this MAC is secure for message space $\{0,1\}^{\ell \cdot n}$, for any fixed value of ℓ.

1. Note that, unlike the CBC Encryption Mode for block ciphers, we do not output the intermediate pseudorandom function values $f_k(m_1), f_k(m_2 \oplus f_k(m_1)), \ldots$ Show that if we did so, the resulting MAC would be insecure.

2. Extra credit: In class, we saw a general method for transforming a secure MAC for short messages into a secure MAC for long messages. It is natural to ask whether the CBC construction can be used instead. That is, if $\mathcal{F}_n = \{f_k : \{0,1\}^n \to \{0,1\}^n\}$ is *any* secure MAC for message space $\{0,1\}^n$ (without necessarily being a pseudorandom function family), does it follow that CBC-MAC constructed using $\mathcal{F}_n$ is a secure MAC for message space $\{0,1\}^{\ell \cdot n}$? Show that the answer is no, i.e. there are secure MACs $\mathcal{F}_n$ for which the resulting CBC-MAC is insecure.