CS 127/CSCI E-127: Introduction to Cryptography

Problem Set 8

Assigned: Nov. 1, 2013 Due: Nov. 8, 2013 (5:00 PM)

Justify all of your answers. See the syllabus for collaboration and lateness policies. Submit solutions by email to `mbun@seas` (and please put the string "CS127PS8" somewhere in your subject line).

Problem 1. (Low exponent attack) Suppose you see the encryption of messages m, $m+1$, and $m+2$ under textbook RSA with exponent 3. Show that you can recover m in polynomial time. Can there be such an attack on an public-key encryption scheme with indistinguishable encryptions?

Problem 2. (Combining encryption schemes) Let $\Pi_1 = (\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ and $\Pi_2 = (\mathsf{Gen}_2, \mathsf{Enc}_2, \mathsf{Dec}_2)$ be two public-key encryption schemes for which it is known that at least one has indistinguishable encryptions. The problem is that you don't know which one is secure and which is not. Show how to construct an encryption scheme Π that is guaranteed to have indistinguishable encryptions as long as at least one of Π_1 or Π_2 has indistinguishable encryptions. Try to provide a full proof of your answer. (Hint: Generate two plaintext messages from the original plaintext so that knowledge of either one of the parts reveals nothing about the plaintext, but knowledge of both does yield the original plaintext.)

Problem 3. (When CPA security is not enough) Consider the following protocol for two parties A and B to flip a fair coin: (1) an incorruptible trusted party T publishes her public key pk; (2) A chooses a random bit b_A, encrypts it using pk, and announces the ciphertext c_A to B and T; (3) next B acts symmetrically, and announces a ciphertext $c_B \neq c_A$; (4) T decrypts both c_A and c_B, and XORs the results to obtain the value of the coin. (More complicated versions of this, which eliminate the need for a trusted party, might be used for Internet gambling.)

a) Argue that even if A is dishonest (but B is honest), the final value of the coin is uniformly distributed.

b) Show that CPA security for the encryption scheme is not sufficient to ensure security of the coin-flipping protocol against a dishonest PPT B. Specifically, show that using one of the candidate CPA-secure schemes from class (or one that you construct based on a plausible assumption), a PPT B can force the coin to be a particular value.

c) Extra credit: Show that if we use an encryption scheme that is secure against chosen *ciphertext* attack (see KL1e §10.6 for precise definition), a PPT B cannot bias the coin by a non-negligible amount.

Problem 4. (MACs Secure against Verification Queries) Consider an extension of the definition of secure message authentication where the adversary is provided with both a Mac and a Vrfy oracle.

a) Provide a formal definition of security for this case.

b) Let Π be a deterministic MAC using canonical verification (namely, $\mathsf{Vrfy}_k(m,t)$ accepts iff $\mathsf{Mac}_k(m) = t$) that is existentially unforgeable under an adaptive chosen-message attack. Prove that Π also satisfies your definition from Part (a).

c) Let $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ be a MAC that is existentially unforgeable under an adaptive chosen-message attack and has fixed-length tags (e.g. length n on security parameter n). Consider a new verification algorithm Vrfy' where $\mathsf{Vrfy}'_k(m, t\|t')$ accepts iff $\mathsf{Vrfy}_k(m,t)$ accepts *and* either $|t'| = 0$ or the $|t'|$'th bit of the key k is 1. Show that $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy}')$ is existentially unforgeable under chosen-message attack, but does not satisfy your definition from Part (a).