

CAS CS 538. Problem Set 5

Due 5pm Friday, October 24, 2008, either by email to reyzin@bu.edu or under the door of MCS 287.

Problem 1. (30 points) Suppose G that expands its k -bit input to a $2k$ -bit output is a PRG. Show that it is also a one-way function.

Problem 2. (30 points) Suppose you have a device (smart card, computer, etc.) that is performing an RSA secret-key operation (computing $m = c^d \bmod n$ for some c) using CRT: separately computing $m_p = c^d \bmod p$ and $m_q = c^d \bmod q$ and then combining. Suppose you can hit the device with just enough radiation to cause exactly one of the two modular exponentiations to compute an incorrect value, $m'_p \neq m_p$, while the other modular exponentiation computes the correct m_q , thus causing the output to be some $m' \neq m$. Show how to factor n given c and m' (and, of course, the RSA public key (n, e)). This is an actual attack that can be carried out on certain smart cards. (Hint: it may be easier to first figure out first how to factor n given m , m' , and the public key (n, e) .)

Problem 3. (40 points) So far, we have considered only passive adversaries for encryption: our adversaries have been limited to observing ciphertexts. A stronger adversary is one endowed with the power to obtain decryptions of some ciphertexts. Notice that this stronger adversary is quite realistic: for example, when someone sends you email, you often include whatever was sent in your reply. So if you use encrypted email, the adversary could send you a ciphertext and wait for the reply to find out what the plaintext was. This is known as a “chosen ciphertext attack.”

There are two types of chosen ciphertext attack. In the first one, the adversary gets to ask for decryptions of ciphertexts *before* she gets the challenge ciphertext c (which is an encryption of m_0 or m_1). In the second one, she also gets to ask *after* seeing c (but, of course, she doesn't get to ask for a decryption of c — that would be impossible to protect against; however, she may ask for ciphertexts related to c if she wants). There are denoted CCA1 and CCA2, respectively. (CCA1 is also sometimes referred to as “lunchtime” attack, because, presumably, adversary just gets to you use your computer for a while when you are out to lunch. CCA2 is sometimes called a “midnight” attack, for reasons that I don't comprehend.) While CCA1 is hard to protect against and CCA2 is even harder, there exist cryptosystems secure against CCA1 and CCA2 under reasonable assumptions.

In this problem, you will show that the cryptosystems we studied fail under CCA attacks.

(a) (15 points) Recall that the last bit is hardcore for RSA. Specifically, the statement is as follows. Suppose you have an oracle A that outputs $x \bmod 2$ after seeing $x^e \bmod n$. Then there exists a PPT algorithm B that uses A (as an oracle, perhaps multiple times on different inputs) to compute a when given $a^e \bmod n$.

Use this fact to show that single-bit RSA is not secure under CCA2. That is, demonstrate the existence an adversary that given encryption of c a bit m , asks for single-bit decryptions of some ciphertexts (not equal to c), and then computes m .

(b) (15 points) Because the same last bit is also hardcore for Rabin, your attack from the part (a) also applies to the bit-by-bit Rabin. Show to modify it into a CCA1 attack. Why doesn't the same modification work to turn your attack on RSA into a CCA1 attack?

(c) (10 points) Show a CCA2 attack on ElGamal encryption (hint: modify the challenge ciphertext c and ask for its decryption; then “undo” the modification).