

## CAS CS 538. Problem Set 5

**Problem 1.** Let  $w(\text{Gen}, \text{Enc}, \text{Dec})$  be a polynomially secure public-key cryptosystem. It is intuitively obvious that it should be hard to compute SK from the PK. Yet if you think about it, you can see that security of SK may not be sufficient for the security of the scheme. We'll now prove these intuitions formally:

(a) Assuming  $(\text{Gen}, \text{Enc}, \text{Dec})$  is secure, give a formal proof that it's hard to compute SK from PK. More formally, show that no polynomial-time algorithm  $R$  has a better than negligible in  $k$  chance of computing SK after being input  $(1^k, \text{PK})$ , where PK, SK are produced by  $\text{Gen}(1^k)$ .

(b) Give an example of an insecure public-key cryptosystem where it is provably hard to compute SK from PK. Extra points are given for cryptosystems where it is provably hard to compute any  $\text{SK}' \neq \text{SK}$ , such that  $\text{Dec}_{\text{SK}}(c) = \text{Dec}_{\text{SK}'}(c)$  for all (most) ciphertexts  $c$ .

**Problem 2.** Let  $f$  be a one-way function. Let  $g(x) = f(x) \circ f(x)$  (i.e.,  $f(x)$  concatenated with itself). Show by reduction that  $g$  is also a one-way function.

**Problem 3.** Show that composition of one-way functions is not necessarily one-way. In other words, show that if  $g$  and  $h$  are one-way, then  $f(x) = g(h(x))$  is not necessarily one-way. Of course, you need to assume that one-way functions exist in order for this statement to be true. (Hint: take two one-way functions and modify them as follows. Make the first one work in some invertible way on inputs of a certain rare form. Make the second make outputs of that rare form. Show that both remain one-way, but their composition does not. Use Problem 2.)

**Problem 4.**

*Extra credit:* Show how to factor  $n$  (in polynomial time) given  $(n, e, d)$  where  $ed \equiv 1 \pmod{\phi(n)}$ . (Thus, it is insecure to re-use the same modulus  $n$  for different RSA instances.)

**Problem 5.** Suppose you have a device (smart card, computer, etc.) that is performing an RSA signature (computing  $b = a^d \pmod{n}$  for some  $a$ , possibly randomly padded, so it is not chosen by adversary) using CRT: separately computing  $b_p = a^d \pmod{p}$  and  $b_q = a^d \pmod{q}$  and then combining. Suppose you can hit the device with just enough radiation to cause exactly one of the two CRT computations to compute an incorrect value,  $b'_p \neq b_p$ , thus causing the output to be some  $b' \neq b$ . Show how to break the scheme: compute the secret key  $\text{SK} = (d, n)$ . (To do so, factor  $n$  given  $a$  and  $b'$  in addition to the RSA public key  $\text{PK} = (n, e)$ ).

This is an actual attack that can be carried out on certain smart cards.