

CAS CS 538. Problem Set 6

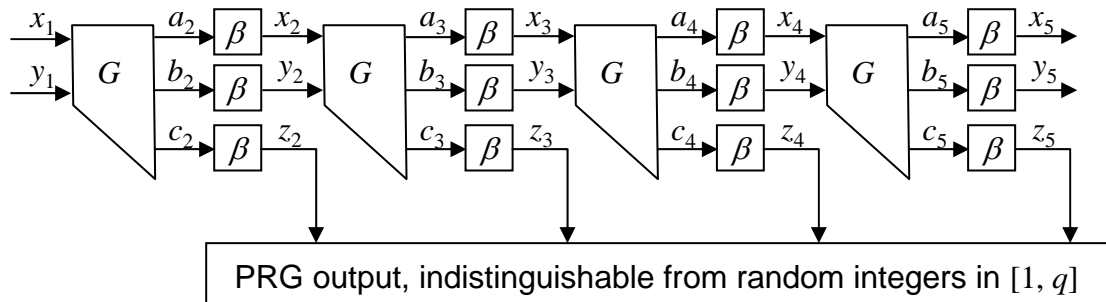
Due 5pm Friday, October 31, 2008, by email to reyzin@bu.edu or under the door of MCS 287.

Problem 1. (30 points) Let $(\text{Gen}, \text{Enc}, \text{Dec})$ be a secure public-key cryptosystem. Show 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 $\text{Gen}(1^k)$. (You may assume, if you need to, that given PK and a string s , it is easy to test whether $s = \text{SK}$ or not.)

Fact (you need not prove anything for this, it's just for your information): because SK is hard to compute from PK, and because our definition of security talks only about security of messages that the adversary can output when given PK, our security notion says nothing about encrypting SK with its own PK. Encrypting SK with its own PK may be insecure even if the cryptosystem satisfies semantic security! (Of course, it's unclear why you'd ever want to do this, since you'd need SK to decrypt SK.)

Problem 2. (30 points) Lamport's signatures for a message space of size 2^ℓ have 2ℓ values in the secret key (and, therefore, also in the public key). A signature consists of a particular message-dependent subset of those values. For simplicity, we will focus on $\ell = 3$: thus, the secret key consists of 6 values and the message space has size 8. Show how to generalize Lamport's scheme to allow for signatures on the message space of size 20 while keeping the key size at 6 values.

Problem 3. (40 points) One reason people consider the Decisional Diffie-Hellman assumption to be very strong is that it makes it too easy to build a PRG: in a sense, it already assumes a PRG. We will build a PRG out of DDH in this problem, as described in the following picture.



For simplicity, our PRG will not output bit strings that are indistinguishable from random, but rather sequences of integers between 1 and q that are indistinguishable from random.

Let q be a Sophie Germain prime, $p = 2q + 1$, and g be a generator of QR_p . Assume that p and g are public (or, alternatively, are part of the seed to our PRG). Assume DDH hold in QR_p .

(a) (20 points) Show how, based on the DDH assumption, to build a PRG G that takes two integers x_1, y_1 from $[1, q]$ and outputs three elements a_2, b_2, c_2 of QR_p that look indistinguishable from random.

(b) (20 points) Now that you have three elements of QR_p , you'd like to map them back to three elements of $[1, q]$. Show that the following function is a bijection from QR_p and $[1, q]$ that is efficiently

computable both ways: $\beta(a) = \{a \text{ if } a \leq q, \text{ and } p - a \text{ otherwise}\}$. Hint: use the fact that $p \equiv 3 \pmod{4}$ (but first show why that's the case).

Now the final PRG is built as follows (you don't need to prove anything for this paragraph; the proof would be a hybrid argument): start with two random elements from $[1, q]$, apply G , and apply β to each of the three elements of QR_p that result from G . Now you have three elements from $[1, q]$ that look random. Output one of them, and use the other two as an input to G again. Iterate as many times as needed.