# Problem Set 5

This problem set is due on *Thursday, October 22, 1998* at the end of class. Late homeworks will *not* be accepted. You are to work on this problem set in groups of three to four people. Mark the top of each sheet with your names, 6.857, the problem set number and question, and the date. **Type up your solutions**, and be clear. Points may be deducted if your TA has problems understanding your solution. We strongly recommend you get started on this problem set early.

### Problem 5-1. ElGamal Signature Variant

Suppose we make a variant to the El Gamal signature scheme where $r$ is computed as $y^k$ instead of $g^k$, where $g$ is the standard public generator modulo $p$, $y$ is the signer's public key, and $k$ is chosen randomly.

**(a)** What corresponding modifications would you make to the computation of $s$?

**(b)** How is verification performed in the modified scheme?

**(c)** Compare the modified scheme to the original scheme. Is it also secure?

### Problem 5-2. DSA needs good random bits

Alice uses DSA to generate her digital signatures, but is lazy about generating good random bits. Her $i$-th digital signature needs a random 160-bit value, which we call $k_i$.

**(a)** Alice generates $k_1$ at random, but defines $k_{i+1}$ to be $k_i + 1 \bmod q$ for $i \geq 2$. Break her scheme; find her secret key!

**(b)** Same problem, except that $k_{i+1} = 2k_i \bmod q$ for $i \geq 2$. (Let's presume that 2 is known to be a generator modulo $q$, in case it matters.)

**(c)** Generalize. Suppose $k_i = ai + b \bmod q$ for a pair of values $a$, $b$ that Alice has picked at random modulo $q$.

**(d)** How can a smart card that Alice has purchased and loaded with her private DSA key intentionally leak her secret key to an accomplice by performing signatures for her in a certain way?

### Problem 5-3. Intentionally weak keys

Consider setting up a digital signature scheme for commerce. Bob is worried that some parties might intentionally choose "weak" signature keys (e.g. easy-to-factor RSA numbers, or easy-to-take-discrete-log numbers for DSA) so that later, they can announce that their signature key has been broken, when they want to repudiate a signature that they have made.

Discuss whether it is better to:

- Force users to prove initially that their signature keys are strong (without, of course, revealing their secret signature key).
- Require users to honor their signatures in any case.
- Something else (explain).

Please keep your answer to less than a page.