CSE 590 YA: Practical Aspects of Modern Cryptography
Winter 2002

Assignment #8 (revised)

Due in class: Tuesday, March 5

1. Suppose that two users each share a (weak) password with a server. Describe a protocol that the three can engage in to allow the two users to communicate securely with each other assuming that the passwords are not discovered by an adversary before the protocol is complete. It may be possible for the server to eavesdrop or impersonate one of the users, but no outsider should be able to do so. Try to keep your protocol efficient.

2. Most of the computational requirements of a DSA signature can be performed without the message. Specifically, a random 160-bit value k is selected, and $r = (g^k \bmod p) \bmod q$ can be computed without a message M. Thus, a large amount of precomputation is possible. This computation can be sped up further by storing values that will be repeatedly used rather than computing them freshly each time. Suppose that you are going to be generating many DSA signatures with a 1024-bit prime p and have 20KB of cache storage available (enough to hold 160 1024-bit values). Describe how to use this storage to significantly speed up your computation of $r = (g^k \bmod p) \bmod q$ for a random k that will be chosen later. Suppose that your cache is increased to 75KB and describe how another substantial computational speed up can be achieved by re-blocking the exponent k so that as many as four of the previous modulo p multiplications can be achieved with a single modulo p multiplication.

3. Contrast RSA and DSA for digital signatures in each of the following scenarios.

   (a) The signer is a client with lots of free cycles and the verifier is a busy server that can become occasionally saturated.

   (b) The signer is a busy server that can become occasionally saturated and the verifier is a client with lots of free cycles.

4. The integer 561 is a kind of "false" prime since for most of the 560 integers a in the range $0 < a < 561$, it is true that $a^{560} \bmod 561 = 1$. Characterize which of these integers a satisfy the equation. How many are there? Hint: factor 561 and use Fermat's Little Theorem to see what happens to a^{561} modulo each factor of 561. You do not need a computer (or even a calculator) to do this — just use the facts you proved in assignment #2.

5. Suppose that a sieve is used as part of a prime generation procedure that works as follows. A random n-bit integer N is selected, and a sieve is used to find all candidate primes in the range N to $N + 999$. Each surviving candidate prime (starting with the smallest on the list) is successively tested for primality using the Miller-Rabin test until one is found that passes the test. If no primes are found in the range, select a new random n-bit integer and repeat.

   Are all n-bit primes roughly equally likely to be selected by this procedure or are some n-bit primes more likely to be selected than others? Explain. (You should discount the "edge" effects caused by N being chosen extremely close to a power of two.)