Introduction to Cryptography

Midterm 2

December 19, 2006

1. Number Theory is a rich source of difficult problems that can be used in cryptographic protocols. List at least four such problems.

   (a) factoring large integers
   (b) solving the discrete log problem
   (c) computing $g^{ab} \bmod p$ from $g^a \bmod p$ and $g^b \bmod p$
   (d) computing square roots modulo composite integers
   (e) deciding whether an integer is a square modulo composite integers
   (f) finding a prime p with given $(\frac{a}{p})$ for many integers a

   Checking primality of large integers is not; neither are problems that can be solved using the Euclidean algorithm, Chinese remainder theorem, etc.

2. Consider the following cryptosystem: Alice and Bob agree on a large prime p and a primitive root g modulo p; Alice picks a random integer x coprime to $p-1$ and publishes $y \equiv g^x \bmod p$.

   In order to send Alice a message m, Bob picks a random integer k coprime to $p-1$, and sends Alice the pair $(m + g^k \bmod p, y^k \bmod p)$.

   Explain how Alice can retrieve the message m.

   Obviously Alice must compute $g^k \bmod p$ and subtract it from $m + g^k \bmod p$; this can be done as follows: compute an integer u with $xu \equiv 1 \bmod p-1$, and compute $y^u = g^{xu} \equiv g \bmod p$.

3. Let p and q be large primes with $p \equiv 1 \bmod q$. Let g be an element of order q in $(\mathbb{Z}/p\mathbb{Z})^\times$. Alice picks a random integer x coprimes to $p-1$ and publishes $y \equiv g^x \bmod p$.

   To send signed messages m, Alice picks a random integer $k \leq q-1$, computes r as the minimal positive integer $\equiv mg^k \bmod p$, and solves the

congruence $s \equiv -k - xr \bmod q$; the signed message consists of the pair $(r \bmod p, s \bmod q)$.

Show that Bob can retrieve the message by computing $ry^r g^s \bmod p$, and explain why he may conclude that the message was sent by Alice.

We have $ry^r g^s \equiv mg^k g^{xr} g^{-k-xr} \equiv m \bmod p$. Only Alice knows the integer x needed to compute s.

WARNING: it is not true that $g^r \equiv g^{mg^k} \bmod p$; this would only hold if we had $r \equiv mg^k \bmod q$, but this is false in general.

4. Explain how the Diffie-Hellman key exchange works.

   See the notes.

5. List the algorithms we have discussed for solving the discrete log problem in $(\mathbb{Z}/p\mathbb{Z})^\times$, and briefly explain for which primes they work best. Also give a more detailed description of *one* of these algorithms.

   (a) Pollard's rho method works for small primes since it takes $O(\sqrt{p})$ steps.

   (b) Shanks baby-step giant-step method also works for small primes; it also takes $O(\sqrt{p})$ steps.

   (c) Pohlig-Hellmann works if $p - 1$ is "smooth", i.e., only divisible by small primes, where small means small enough to apply Pollard's or Shanks' methods.

   (d) The index calculus works for larger primes.

   Note that algorithms that take $O(\sqrt{p})$ steps become useless for primes $p < 10^{20}$.

6. Explain the following (what does it mean? What is it good for?):

   (a) key exchange

   (b) authentication

   (c) zero knowledge proofs

   (d) secret sharing

   Here's what wikipedia says:

   (a) key exchange: a cryptographic protocol that allows two parties that have no prior knowledge of each other to establish a shared secret key over an insecure communications channel.

(b) authentication: verifying the identity of the sender of a communication.

(c) zero knowledge proof: a method for one party to prove to another that a statement is true, without revealing any information about the statement.

(d) secret sharing: method for distributing a secret amongst a group of participants, each of which is allocated a share of the secret. The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own.

7. The ElGamal Signature Protocol. Alice chooses a prime p, a primitive root $g \bmod p$, a random integer $a < p-1$, and computes $y \equiv g^a \bmod p$. Her public key is (p, g, y), her private key is a.

   To sign a message $m < p$, Alice picks a random $k < p-1$ and computes an integer $r < p$ with $r \equiv g^k \bmod p$, as well as $s \equiv k^{-1}(m - ar) \bmod p-1$. She then sends the triple (m, r, s) to Bob.

   (a) Which condition must k satsify so that Alice can compute s?

   The integer k must be coprime to $p-1$ for the inverse $k^{-1} \bmod p-1$ to exist.

   (b) Bob computes $u \equiv y^r r^s \bmod p$ and $v \equiv g^m \bmod p$; show that if the signature is valid, then $u = v$.

   $y^r r^s \equiv g^{ar}(g^k)^{k^{-1}(m-ar)} \equiv g^{ar+m-ar} \equiv g^m \bmod p$.

   (c) This protocol is vulnerable to existential forgery; this means that Malice can compute a triple (m, r, s) with a valid signature. In fact, she can choose integers u and v with v coprime to $p-1$, compute $r \equiv g^u y^v \bmod p$ and $s \equiv -rv^{-1} \bmod p-1$; verify that (r, s) is a valid signature for the message $m = us$.

   We find $y^r r^s \equiv y^r (g^u y^v)^s \equiv g^{us} y^r y^{-r} \equiv g^{us} \bmod p$, so (r, s) is the signature of the message $m = us$.

   (d) Replace the message m in the ElGamal signature protocol by $h(m)$, where h is a suitable hash function. Explain why existential forgery is now impossible.

   Here (r, s) is a valid signature if $y^r r^s \equiv g^{h(m)} \bmod p$. In order to find a message with signature (r, s), Malice now has to look for an m with $h(m) = us$; but this is next impossible for pre-image resistant hash functions.