reduced modulo the smaller prime q). Finally, Alice finds an integer s such that $sk \equiv h + xr \pmod q$. Her signature is then the pair (r, s) of integers modulo q.

To verify the signature, the recipient Bob computes $u_1 = s^{-1}h \pmod q$ and $u_2 = s^{-1}r \pmod q$. He then computes $g^{u_1}y^{u_2} \pmod p$. If the result agrees modulo q with r, he is satisfied. (Note that $g^{u_1}y^{u_2} = g^{s^{-1}(h+xr)} = g^k \pmod p$.)

This signature scheme has the advantage that signatures are fairly short, consisting of two 160-bit numbers (the magnitude of q). On the other hand, the security of the system seems to depend upon intractability of the discrete log problem in the multiplicative group of the rather large field $\mathbf{F}_p$. Although to break the system it would suffice to find discrete logs in the smaller subgroup generated by g, in practice this seems to be no easier than finding arbitrary discrete logarithms in $\mathbf{F}_p^*$. Thus, the DSS seems to have attained a fairly high level of security without sacrificing small signature storage and implementation time.

Algorithms for finding discrete logs in finite fields. We first suppose that all of the prime factors of $q-1$ are small. In this case we sometimes say that $q-1$ is "smooth." With this assumption there is a fast algorithm for finding the discrete log of an element $y \in \mathbf{F}_q^*$ to the base b. For simplicity, we shall suppose that b is a generator of $\mathbf{F}_q^*$. We now describe this algorithm, which is due to Silver, Pohlig and Hellman.

First, for each prime p dividing $q-1$, we compute the p-th roots of unity $r_{p,j} = b^{j(q-1)/p}$ for $j = 0, 1, \ldots, p-1$. (As usual, we use the repeated squaring method to raise b to a large power.) With our table of $\{r_{p,j}\}$ we are ready to compute the discrete log of any $y \in \mathbf{F}_q^*$. (Note that, if b is fixed, this first computation needs only be done once, after which the same table is used for any y.)

Our object is to find x, $0 \le x < q-1$, such that $b^x = y$. If $q-1 = \prod_p p^\alpha$ is the prime factorization of $q-1$, then it suffices to find $x \bmod p^\alpha$ for each p dividing $q-1$; from this x is uniquely determined using the algorithm in the proof of the Chinese Remainder Theorem (Proposition I.3.3). So we now fix a prime p dividing $q-1$, and show how to determine $x \bmod p^\alpha$.

Suppose that $x \equiv x_0 + x_1 p + \cdots + x_{\alpha-1}p^{\alpha-1} \pmod{p^\alpha}$ with $0 \le x_i < p$. To find x_0 we compute $y^{(q-1)/p}$. We get a p-th root of 1, since $y^{q-1} = 1$. Since $y = b^x$, it follows that $y^{(q-1)/p} = b^{x(q-1)/p} = b^{x_0(q-1)/p} = r_{p,x_0}$. Thus, we compare $y^{(q-1)/p}$ with the $\{r_{p,j}\}_{0\le j<p}$ and set x_0 equal to the value of j for which $y^{(q-1)/p} = r_{p,j}$.

Next, to find x_1, we replace y by $y_1 = y/b^{x_0}$. Then y_1 has discrete log $x - x_0 \equiv x_1 p + \cdots x_{\alpha-1}p^{\alpha-1} \pmod{p^\alpha}$. Since y_1 is a p-th power, we have $y_1^{(q-1)/p} = 1$ and $y_1^{(q-1)/p^2} = b^{(x-x_0)(q-1)/p^2} = b^{(x_1+x_2p+\cdots)(q-1)/p} = b^{x_1(q-1)/p} = r_{p,x_1}$. So we can compare $y_1^{(q-1)/p^2}$ with $\{r_{p,j}\}$ and set x_1 equal to the value of j for which $y_1^{(q-1)/p^2} = r_{p,j}$.

It should now be clear how we can proceed inductively to find all $x_0, x_1,$