23 ELECTRONIC DIGITAL SIGNATURE DSA

A few more details need to be fixed up to get a functional digital signature scheme. As before, bad choices of p and g can weaken the algorithm. We will also want to hash the message M using a hash function so that we can sign messages of arbitrary length, and so that an opponent can't use the algorithm's algebraic structure to forge signatures on messages that were never signed. Having attended to these details and applied one or two optimisations, we get the *Digital Signature Algorithm* (DSA) which is a US standard and widely used in government applications.

DSA (also known as DSS, for Digital Signature Standard) assumes a prime p of typically 1024 bits, a prime q of 160 bits dividing $(p-1)$, an element g of order q in the integers modulo p, a secret signing key x and a public verification key $y = g^x$. The signature on a message M, $Sig_x(M)$, is (r, s) where

$$r \equiv (g^k \pmod p) \pmod q$$

$$s \equiv (h(M) - xr)/k \pmod q$$

The hash function used here is SHA1.

DSA is the classic example of a randomized digital signature scheme without message recovery. The standard has changed somewhat with faster computers, as variants of the algorithm used to factor large numbers can also be used to compute discrete logarithms modulo bases of similar size[4]. Initially the prime p could be in the range 512–1024 bits, but this was changed to 1023–1024 bits in 2001 [941]; the proposed third-generation standard will allow primes p in the range 1024–3072 bits and q in the range 160–256 bits [942]. Further tweaks to the standard are also foreseeable after a new hash function standard is adopted.

Digital signature

$$r \equiv \left(G^K \bmod P\right) \bmod q, \tag{1}$$

$$s \equiv \frac{m + r \times X}{K} \bmod q. \tag{2}$$

The receiver calculates the value

$$w \equiv \frac{1}{s} \bmod q, \tag{3}$$

hash value

$$m' = h(M), \tag{4}$$

as well as numbers

$$u_1 \equiv (m' \times w) \bmod q, \tag{5}$$

$$u_2 \equiv (r \times w) \bmod q. \tag{6}$$

$$r' \equiv \left(\left(G^{u_1} \times Y^{u_2} \right) \bmod P \right) \bmod q. \tag{7}$$

and checks that $r' \equiv r$.