THE DIGITAL SIGNATURE ALGORITHM

Invented by NIST (National Institute for Standards and Technology) in 1991 and adapted as a standard (Digital Signature Standard) in Dec. 1994.

Variation of El Gamal signatures — similar security characteristics.

Let H be a cryptographically secure hash function that maps bit strings to $\mathbb{Z}_q$ for some integer q. The DSS specifies that SHA-1 be used.

A produces her public and private keys as follows:

(1) Selects a 512-bit prime p and a 160-bit prime q such that $q \mid p-1$.
(2) Selects g, a primitive root modulo p
(3) Computes $h \equiv g^{(p-1)/q} \pmod{p}$, $0 < h < p$. Note that $h^q \equiv 1 \pmod{p}$, and if $a \equiv b \pmod{q}$, then $h^a \equiv h^b \pmod{p}$.
(4) Randomly selects $x \in \mathbb{Z}$ with $0 < x < q$ and computes $y \equiv h^x \pmod{p}$

Public key: $\{p, q, h, y\}$
Private key: $\{x\}$

A signs message M as follows:

(1) A selects a random integer k with $0 < k < q$.
(2) A computes $r \equiv (h^k \bmod p) \pmod{q}$, $0 < r < q$.
(3) A computes $s \equiv k^{-1}(H(M) + xr) \pmod{q}$.
(4) A's signature is the pair $\{r, s\}$ (320 bits)

B verifies A's signature as follows:

(1) B obtains A's authentic public key $\{p, q, h, y\}$.
(2) B computes $u_1 \equiv H(M)s^{-1} \pmod{q}$, $u_2 \equiv rs^{-1} \pmod{q}$, and $v \equiv (h^{u_1} y^{u_2} \bmod p) \pmod{q}$, $0 < v < q$.
(3) B accepts if and only if $v = r$.

Proof of Correctness. We note that $k \equiv s^{-1}(H(M) + xr) \pmod{q}$ and

$$\begin{aligned} h^{u_1} y^{u_2} &\equiv h^{H(M)s^{-1}} y^{rs^{-1}} \pmod{p} \\ &\equiv h^{H(M)s^{-1}} h^{xrs^{-1}} \pmod{p} \\ &\equiv h^{s^{-1}(H(M)+xr)} \pmod{p} \\ &\equiv h^k \pmod{p} \end{aligned}$$

Hence $(h^{u_1} h^{u_2} \bmod p) \equiv r \pmod{q}$ and $v = r$. □

Note. We have a small signature (320 bits) but computations are done modulo a 512-bit prime. Security is based on the belief that solving the DLP in $\langle [h] \rangle \subset \mathbb{F}_p^*$ is hard.

Security:

- based on the belief that solving the DLP in $\langle [h] \rangle \subset \mathbb{F}_p^*$ is hard (seems reasonable)
- proof of GMR-security does *not* hold, because $H(M)$ is signed as opposed to $H(M, r)$ (reduction requires that the forger be forced to use the same r for two signatures)

More information: "Another look at provable security" (Koblitz and Menezes, J. Cryptology 2007)