DSA (Digital Signature Algorithm)

The set of messages $\mathcal{M} = \mathbb{F}_p^*$, the set of signatures – $\mathcal{P} = \mathbb{F}_q \times \mathbb{F}_q$, where p is prime and q is a prime divisor of $p-1$.

The private key: $K_{pr} = \langle a \rangle,\ 0 < a < q-1$.

The public key: $K_{pb} = \langle p, q, \alpha, \beta \rangle$, $\alpha \in \mathbb{F}_p$ is an element of order q, i.e. $\alpha^q \equiv 1 \pmod{p}$. $\beta \equiv \alpha^a \pmod{p}$.

Signing: choose $k \in \mathbb{F}_q^*$ an compute: $sig(x|K_{pr}) = \langle \gamma, \delta \rangle$,

$$\gamma \equiv \alpha^k (\text{mod } p) \pmod{q},\ \delta \equiv (x + a\gamma)k^{-1} \pmod{q}.$$

The condition $(\delta, q) = 1$ must be fulfilled.

Verification of signature: signature is accepted if and only if

$$\begin{aligned} &\alpha^{e_1}\beta^{e_2}(\text{mod } p) \equiv \gamma \pmod{q}, \\ &e_1 \equiv x\delta^{-1} \pmod{q}, e_2 \equiv \gamma\delta^{-1} \pmod{q}. \end{aligned}$$

Gouillou-Quisquater digital signature

Choose two different big primes p, q and compute $n = pq$.

Choose $e, (e, \phi(n)) = 1$ and encode your ID as some number $I, 1 < I < n, (I, n) = 1$.

Find a number a such that $I \cdot a^e \equiv 1 \pmod{n}$.

You can compute this number like this:

$$d \equiv e^{-1} \pmod{\phi(n)}, \quad a \equiv I^{-d} \pmod{n}.$$

The private key: $K_{pr} = \langle a \rangle$.

The public key: $K_{pb} = \langle n, e, I \rangle$.

Signing. The messages which can be signed are represented by natural numbers, $\mathbb{N} = \{1, 2, \ldots\}$.

The hash-function $h : \mathbb{N} \to \mathbb{Z}_n$ should be used, take, for example

$$h(m) = (n-m)^2 + m \ (\text{mod} n).$$

Use this function for two arguments as $h(m_1, m_2) = h(m_1 + m_2)$.

Signature of the message x:

1. choose a random k and compute $r \equiv k^e \pmod{n}$;
2. find $l = h(x, r)$;
3. compute $s \equiv ka^l \pmod{n}$;
4. $sig(x|K_{pr}) = \langle s, l \rangle$

Verification:

1. compute $u \equiv s^e I^l \pmod{n}$ and $l' = h(x+u)$;
2. accept the signature if $l = l'$.

ESIGN (Efficient Digital signature)

Choose two prime numbers $p, q, p > q$, compute $n = p^2 q$, choose an integer $k \geqslant 4$.

The private key: $K_{pr} = \langle p, q \rangle$.

The public key: $K_{pub} = \langle n, k \rangle$.

The messages which can be signed are represented by natural numbers, $\mathbb{N} = \{1, 2, \ldots\}$.

The hash-function $h : \mathbb{N} \to \mathbb{Z}_n$ is required, take, for example,

$$h(m) = (n-m)^2 + m \ (\mathrm{mod} n).$$

Signature of the message x:

1. compute $v = h(x)$;
2. chosse a random number $r, 1 < r < p$;
3. compute $w = \lceil ((v - r^k)(\mathrm{mod}\ n))/(pq) \rceil, \quad y \equiv w \cdot (kr^{k-1})^{-1} (\mathrm{mod}\ p)$
4. compute $s \equiv r + ypq (\mathrm{mod}\ n)$;
5. $sig(x|K_{pr}) = s$.

Verification:

1. compute $u \equiv s^k \pmod{n}$ and $z = h(x)$;
2. accept the signature if $z \leqslant u \leqslant 2^{\lceil \frac{2}{3} \log_2 n \rceil}$.