Noter qu'on a deux structures de groupes sous-jacentes:

$\mathbb{Z}_p^*$ d'ordre $\sim 2^{1024}$. (1024 bits)

Sous-groupe $\mathbb{Z}_q^*$ d'ordre 2^{160} (160 bits).

→ Comme EL GAMAL, $sig(x) = (r, s)$ d'un message x, est un couple où $|r|_2 = |p|_2 = 160$, soit 360 bits.

Signature DSA (noté Sig_{DSA})

1. choisir k_E clé Ephémère, $0 < k_E < q$
2. Calculer $r \equiv (\alpha^{k_E} \bmod p) \pmod q$.
3. Calculer $s \equiv (SHA(x) + d \cdot r) \cdot k_E^{-1} \pmod q$

SHA est une fonction de hachage; DSA utilise SHA1 qui en regessant x message, ressort une empreinte de taille 16 bits. (voir § hachage)

Vérification Signature DSA noté Ver_{DSA}.

1. Calculer $w \equiv s^{-1} \pmod q$
2. Calculer $u_1 \equiv w \cdot SHA(x) \pmod q$
3. Calculer $u_2 \equiv w \cdot r \pmod q$
4. Calculer $v \equiv (\alpha^{u_1} \cdot \beta^{u_2} \bmod p) \pmod q$
5. Vérifier: $ver_{k_{pub}}(x, (r, s))$:

$$\begin{cases} v \equiv r \bmod q \Rightarrow \text{valide} \\ v \not\equiv r \bmod q \Rightarrow \text{invalide} \end{cases}$$