$\Rightarrow$ $s_1 - s_2 \equiv (x_1 - x_2) \cdot k_E^{-1} \pmod{p-1}$

$\Rightarrow$ $k_E \equiv \dfrac{x_1 - x_2}{s_1 - s_2} \pmod{p-1}$,

si $\text{pgcd}(s_1 - s_2, p-1) \neq 1$, plusieurs solutions k_E.

et $d \equiv \dfrac{x_1 - s_1 k_E}{r} \cdot \pmod{p-1}$

Conclusion : changer les k_E assez souvent.

→ Exercice : Comme RSA, si Oscar peut forger une signature en utilisant un message aléatoire.

§4.3. Algorithme DSA (Digital signature Algorithm)

Utilisé en pratique, plus que ELGAMAL ; la taille de la signature est 320 bits.

§§4.3.1. Algorithme DSA.

Génération de clés DSA : SETUP.

1. Générer p premier $2^{1023} < p < 2^{1024}$.
2. Trouver un diviseur premier q de $p-1$, $2^{159} < q < 2^{160}$.
3. Trouver α avec $\text{ord}(\alpha) = q$
4. Choisir un entier aléatoire d, $0 < d < q$
5. Calculer $\beta \equiv \alpha^d \bmod p$.

Les clefs sont $k_{pub} = (p, q, \alpha, \beta)$

$k_{pr} = (d)$