The Digital Signature Algorithm

- KeyGen (1^n); choose a prime q and p s.t. $q \mid p-1$.

  choose $g \xleftarrow{\$} \mathbb{Z}_p^*$ and $y_1 = g^{\frac{p-1}{q}}$ $\quad$ ($y_1^q \equiv 1 \mod p$).

  choose a secret $s \xleftarrow{\$} \mathbb{Z}_p^*$ and $y_2 = y_1^s$ $\quad$ due to Pollig-Hellman attack.

  output $pk = (p, g, y_1, y_2)$ and $sk = (s)$

- Sign (sk, m); choose a random $0 < r < q-1$.

  compute $\sigma_1 = y_1^r \mod p \mod q$.

  $\sigma_2 = r^{-1}(m + s \cdot \sigma_1) \mod q$. $\rightarrow$ $m \equiv -s\sigma_1 + r\sigma_2 \mod q$.

  output (σ_1, σ_2).

  $\sigma_2^{-1} m \equiv -s\sigma_1\sigma_2^{-1} + r \mod q$.

  $\Rightarrow r \equiv \sigma_2^{-1} m + s\sigma_1\sigma_2^{-1} \mod q$.

  $\equiv u_1 + s u_2 \mod q$.

- Verify (pk, σ); parse σ as (σ_1, σ_2).

  compute $u_1 \equiv \sigma_2^{-1} m \mod q$

  $u_2 \equiv \sigma_2^{-1} \sigma_1 \mod q$.

  $v = y_1^{u_1} y_2^{u_2} \mod p \mod q$.

  if $v = \sigma_1$, output 1.

  if $v \neq \sigma_1$, output 0.

  $\underbrace{y_1^r}_{\sigma_1} = y_1^{u_1 + s u_2}$

  $= \underbrace{y_1^{u_1} \cdot y_2^{u_2}}_{v} \mod p \mod q$.

Think thing