11.54 Algorithm Key generation for the DSA

SUMMARY: each entity creates a public key and corresponding private key.
Each entity A should do the following:

1. Select a prime number q such that $2^{159} < q < 2^{160}$.
2. Choose t so that $0 \leq t \leq 8$, and select a prime number p where $2^{511+64t} < p$ $2^{512+64t}$, with the property that q divides $(p-1)$.
3. (Select a generator α of the unique cyclic group of order q in $\mathbb{Z}_p^*$.)
   3.1 Select an element $g \in \mathbb{Z}_p^*$ and compute $\alpha = g^{(p-1)/q} \bmod p$.
   3.2 If $\alpha = 1$ then go to step 3.1.
4. Select a random integer a such that $1 \leq a \leq q-1$.
5. Compute $y = \alpha^a \bmod p$.
6. A's public key is (p, q, α, y); A's private key is a.