11.56 Algorithm DSA signature generation and verification

SUMMARY: entity A signs a binary message m of arbitrary length. Any entity B can this signature by using A's public key.

1. *Signature generation.* Entity A should do the following:
   (a) Select a random secret integer $k, 0 < k < q$.
   (b) Compute $r = (\alpha^k \bmod p) \bmod q$ (e.g., using Algorithm 2.143).
   (c) Compute $k^{-1} \bmod q$ (e.g., using Algorithm 2.142).
   (d) Compute $s = k^{-1}\{h(m) + ar\} \bmod q$.
   (e) A's signature for m is the pair (r, s).