Digital Signature Algorithm, 160-bit

Key creation - Alice

- Find 1024-bit prime p,
  160-bit prime q where q divides $p-1$
- Find $\alpha \in \mathbb{Z}_p^*$ where $\text{ord}(\alpha) = q$
- Choose private d where $0 < d < q$
  Compute $\beta \equiv \alpha^d \mod p$
- Publish (p, q, α, β)

Sign message x - Alice

- Choose ephemeral k_E where $0 < k_E < q$
- Compute
  $$r \equiv \left(\alpha^{k_E} \mod p\right) \mod q$$
  $$s \equiv \left(\text{SHA}(x) + dr\right) k_E^{-1} \mod q$$
- Send $(x, (r, s))$

Verify signature - Bob

- Compute
  $$w \equiv s^{-1} \mod q$$
  $$u_1 \equiv w \cdot \text{SHA}(x) \mod q$$
  $$u_2 \equiv w \cdot r \mod q$$
  $$v \equiv \left(\alpha^{u_1}\beta^{u_2} \mod p\right) \mod q$$
- If $v = r$ then valid
  If $v \neq r$ then invalid

Use Hash[x,"SHA3-256"] for the hash function in our small DSA

1. Alice publishes $(p, q, \alpha, \beta) = (241\,553\,623, 13\,033, 52\,824, 238\,101\,207)$
   (a) Verify that p, q and α are reasonable choices for our small version of DSA.

   (b) Which, if any, of the following are valid DSA signatures?
      (i) $(x,\ (r, s)) = (\text{"Argybargy"}, (5105, 11\,671))$

      (ii) $(x,\ (r, s)) = (\text{"Pleased to Meet Me"}, (9543, 3174))$

2. You want to use our small version of DSA to sign the message

   "My cabbages!"

   using values of $p = 2\,738\,078\,869, \quad q = 65\,323, \quad$ and $\alpha = 11\,208$

   (a) Verify that p, q and α are reasonable choices for our small DSA.

   (b) Use $d = 17\,132$ to compute your value for β.

   (c) Use a value of $k_E = 41\,821$ to sign your message.