Recall: The 160-bit Digital Signature Algorithm

Alice – Key Generation

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

Recall: The 160-bit Digital Signature Algorithm

Alice – Sign message x

- Choose ephemeral $0 < k_E < q$ and compute
- Compute

$$r \equiv \left(\alpha^{k_E} \mod p\right) \mod q$$
$$s \equiv (\mathrm{SHA}(x) + dr)\, k_E^{-1} \mod q$$

- Send $(x, (r, s))$

Bob – Verify signature using public (p, q, α, β)

$$w \equiv s^{-1} \mod q$$
$$u_1 \equiv w \cdot \mathrm{SHA}(x) \mod q$$
$$u_2 \equiv w \cdot r \mod q$$

$$v \equiv (\alpha^{u_1} \beta^{u_2} \mod p) \mod q$$

If $v \equiv r \mod q$ then valid