Recall the 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 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

Elliptic Curve Digital Signature Algorithm

Key creation - Trusted Party

- Generate $E(\mathbb{F}_p) : Y^2 = X^3 + AX + B$ and $G \in E(\mathbb{F}_p)$ of large prime order q
- Publish (p, A, B, G, q)

Sam

- Choose secret key s where $0 < s < q - 1$
  Compute $V = sG \in E(\mathbb{F}_p)$
  Publish V as verification for all signatures

Sign message D - Sam

- Compute $d = \text{hash}(D)$
- Pick ephemeral e where $0 < e < q$
- Compute $eG \in E(\mathbb{F}_p)$

$$s_1 \equiv x(eG) \mod q$$
$$s_2 \equiv \left(d + s\, s_1\right) e^{-1} \mod q$$

- Send $(D, (s_1, s_2))$

Verify signature - Victor

- Compute

$$d = \text{hash}(D)$$
$$v_1 \equiv d\, s_2^{-1} \mod q$$
$$v_2 \equiv s_1\, s_2^{-1} \mod q$$
$$v = v_1 G + v_2 V \in E(\mathbb{F}_p)$$

- If $x(v) \equiv s_1 \mod q$ then valid
  Otherwise invalid

The Trusted Party Store publishes toy credentials

$(p, A, B, G, q) = (953, 13, 12, (375, 647), 113)$

1. Sam publishes $V = (45, 266)$ for use with her ECDSA signatures.
   Which, if any, of the following are valid ECDSA signatures?
   (a) $(D,\ (s_1, s_2)) =$ ("Whoever invented stew was a genius. I mean, it's got milk in it, but it still tastes good.", $(97, 52)$)
   (b) $(D,\ (s_1, s_2)) =$ ("Someone hit the big score. They figured it out, that we're gonna do it anyway, even if doesn't pay.", $(23, 105)$)

2. You want to use ECDSA to sign the message
   "Give him some space, and let him do his thing. Make him feel safe, and listen to him sing."
   (a) Use $s = 87$ to compute your value for V.
   (b) Use an ephemeral value of $e = 58$ to sign your message.