Elliptic Curve Digital Signature Algorithm
Trusted party publishes $E(\mathbb{F}_p)$ and $G \in E(\mathbb{F}_p)$ where $q = \text{ord}(G)$ is large prime

- **Samantha – Sign message** D
- Picks secret key s where $1 < s < q - 1$
- Publishes $V = sG \in E(\mathbb{F}_p)$
- Hashes D to value d where $0 < d < q$
- Chooses ephemeral $e < q$ Computes

$$s_1 = x(eG) \mod q$$
$$s_2 = (d + ss_1)e^{-1} \mod q$$

Sends $(D, (s_1, s_2))$

- **Victor – Verify Signature**
- Computes

$$v_1 \equiv ds_2^{-1} \mod q$$
$$v_2 \equiv s_1 s_2^{-1} \mod q$$

$$v = v_1 G + v_2 V \in E(\mathbb{F}_p)$$

- Signature valid if $x(v) \equiv s_1 \mod q$