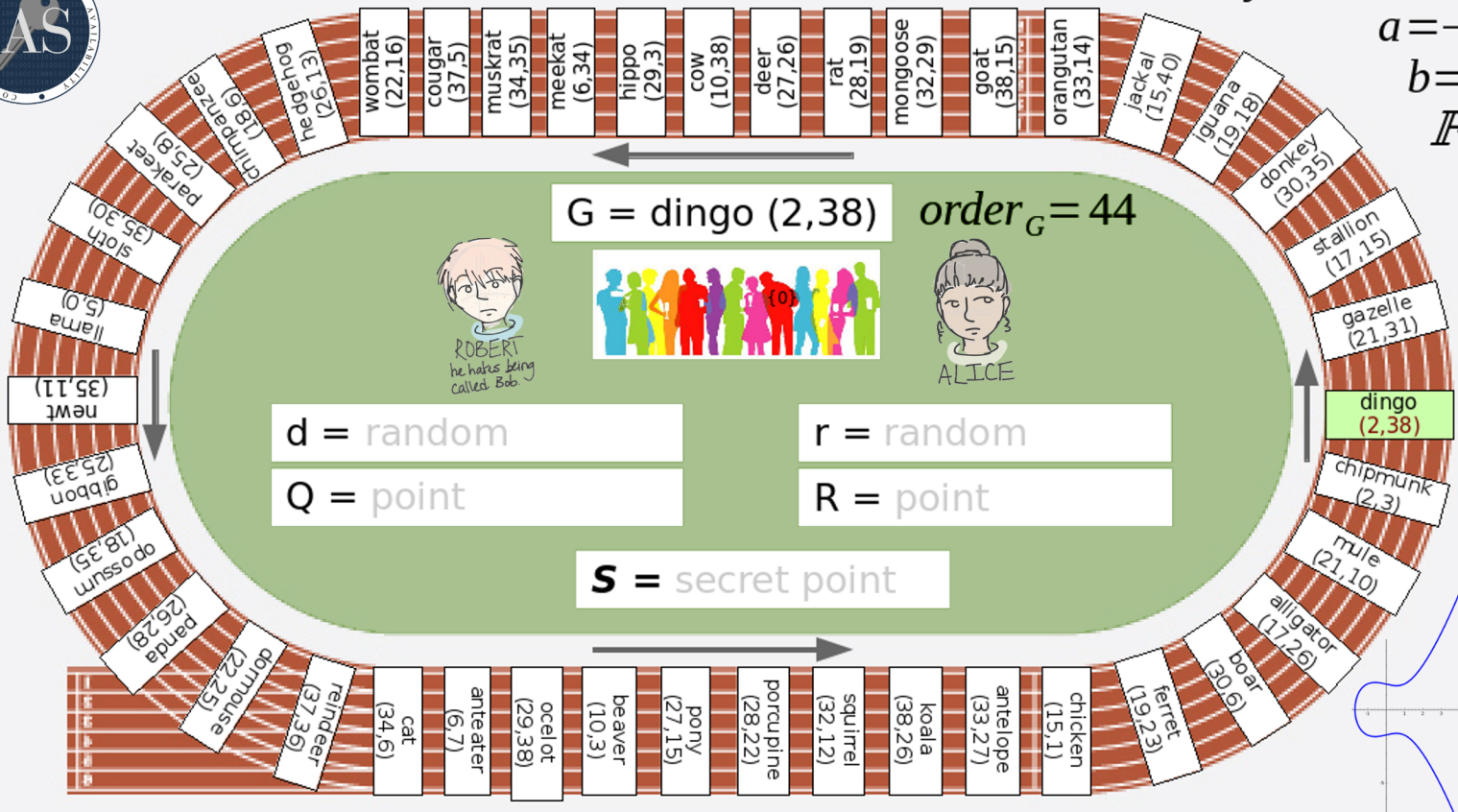


$$y^2 = x^3 + ax + b$$

$$a = -1$$

$$b = 3$$

$$\mathbb{F}_{41}$$

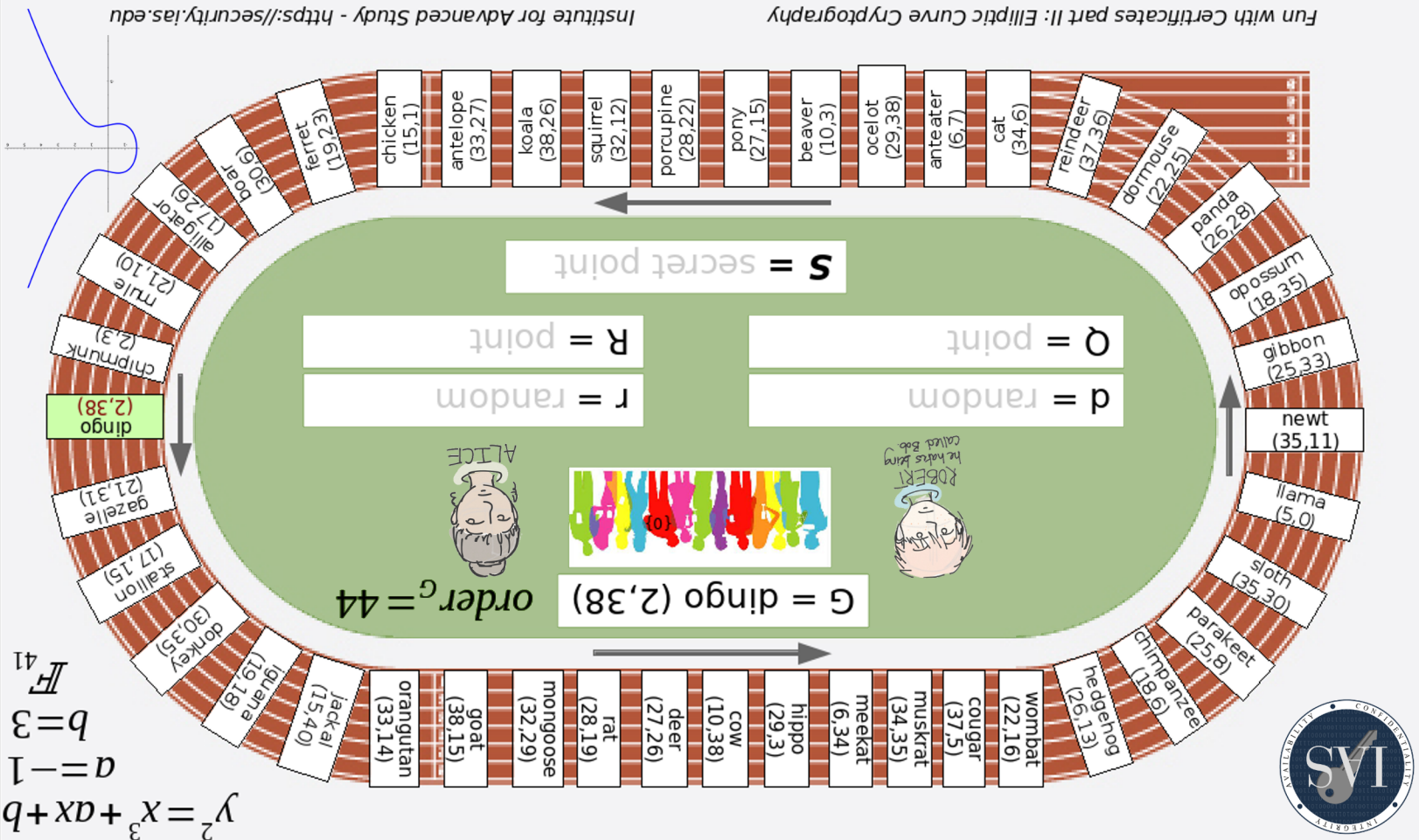


Fun with Certificates part II: Elliptic Curve Cryptography

Institute for Advanced Study - <https://security.ias.edu>

Institute for Advanced Study - <https://security.ias.edu>

Fun with Certificates part II: Elliptic Curve Cryptography



$$y^2 = x^3 + ax + b$$

$$a = -1$$

$$b = 3$$

$$\mathbb{F}_{41}$$



