Schnorr Protocol.

Ex. (Proof of Knowledge for Discrete Logarithm)

Let p be a DL-secure prime and $g \xleftarrow{\$} \mathbb{Z}_p^*$. | Prover and Verifier know g and y.

Let $y = g^x \bmod p$. | but only prover knows x s.t. $y = g^x$

Prover claims to know a discrete logarithm of y. i.e, $x = \log_g y$.

P ⇒ V i) [announcement]

- chooses $r \xleftarrow{\$} \mathbb{Z}_p^*$.
- compute $a = g^r \bmod p$ and sends a to Verifier.

V ⇒ P ii) [challenge]

- chooses $c \xleftarrow{\$} \mathbb{Z}_p^*$. and sends c to Prover.

P ⇒ V iii) [response]

- computes $s = r + cx \bmod p-1$ and sends s to Verifier.

iv) [verification]

- if $g^s = a \cdot y^c \bmod p$, then Verifier accepts.
  otherwise, Verifier rejects.

Ex. (Proof of Equality of Discrete Logarithm over Different Groups).

Prover and Verifier know $g_1 \in \mathbb{Z}_p^*$. $g_2 \in \mathbb{Z}_p^*$. $y_1 = g_1^x$ and $y_2 = g_2^x$

However, only Prover knows such x.

P ⇒ V i) [announcement]

- chooses $r \xleftarrow{\$} \mathbb{Z}_p^*$
- computes $a = g_1^r \bmod p$ and $b = g_2^r \bmod p$ and sends a and b to Verifier.

V ⇒ P ii) [challenge]

- chooses $c \xleftarrow{\$} \mathbb{Z}_p^*$ and sends c to Prover.

P ⇒ V iii) [response]

- computes $s = r + cx \bmod p-1$ and sends s to verifier.

iv) [verification]

- if $g_1^r = a \cdot y_1^c$ and $g_2^r = b \cdot y_2^c$, then Verifier accepts.
  otherwise, Verifier rejects.

Think thing