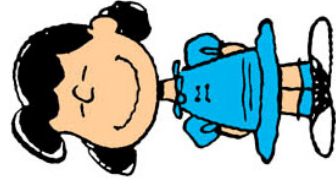


$$y = g^x$$

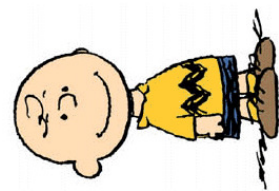


$$\beta \stackrel{\leftarrow u}{\mathbb{Z}_q}$$

$$g^\gamma = g^{k\beta x} \stackrel{?}{=} \alpha y^\beta$$

$$\begin{array}{c} \xrightarrow{\alpha = g^k} \\ \xrightarrow{\gamma = k + \beta x} \\ \xrightarrow{\hspace{1cm}} \end{array}$$

$$x \in \mathbb{Z}_q$$



$$k \stackrel{\leftarrow u}{\mathbb{Z}_q}$$