- Say we have a secret $S$ that we wish to distribute, with a threshold of $n$. We can create a polynomial of degree $n-1$:

$$P(x) = S + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1},$$

  and distribute the values $P(x_1), P(x_2), P(x_3), \ldots$
- To reconstruct $S$, $n$ shares must be combined, and the interpolation formula used to evaluate $P(0)$.
- It is *impossible* to recover the polynomial without $n$ points, so the secret is safe without $n$ shares.
- If a few shares are missing, the operation will still work, as we can use *any* $n$ points.