Secret Sharing

- Objective
  - Divide data $D$ into $n$ pieces $D_1, \ldots, D_n$ in such a way that
    - Knowledge of any $k$ or more $D_i$ pieces makes $D$ easy to compute,
    - Knowledge of any $k-1$ or fewer $D_i$ pieces leaves $D$ completely
      undetermined.
  - Such a scheme is called a $(k, n)$ threshold scheme.

- Useful when no single entity can be trusted with the secret
  - Management of cryptographic keys

Shamir’s Secret Sharing

- Underlying fact
  - Based on polynomial interpolation.
  - Given $k$ points in the 2-d plane $(x_1, y_1), \ldots, (x_k, y_k)$
    with distinct $x_i$’s,
  - there is one and only one polynomial $q(x)$ of degree $k-1$ such that
    $q(x_i)=y_i$ for all $i$. 
Shamir’s Secret Sharing (Cont’d)

• Split the secret D
  – To divide D into pieces $D_i$…
  – Pick a random $k - 1$ degree polynomial
    $$q(x) = a_0 + a_1x + \cdots + a_{k-1}x^{k-1}$$
    in which $a_0 = D$.
  – Evaluate $D_1 = q(1), D_2 = q(2), \ldots, D_n = q(n)$.
  – The secret shares represent distinct points on the polynomial.

Shamir’s Secret Sharing (Cont’d)

• Reconstruction
  – Given any subset of $k$ of these $D_i$ values (with their identifying indices)
    • Find the coefficients of $q(x)$ by interpolation,
    • Evaluate $D = q(0)$.
  – Given just $k - 1$ of these values,
    • $D$ could be any value
    • In other words, $D$ being any value will give one and only one possible polynomial
  • Alternatively, view these as linear equations.