We begin with the topic of a Vandermonde determinant:

Let $a_1, a_2, \ldots, a_n$ be real numbers. The **Vandermonde determinant** with respect to the coefficients $a_1, a_2, \ldots, a_n$, denoted $V(a_1, a_2, \ldots, a_n)$, is the determinant whose i-th column consists of the first n members of the geometric series with quotient a_i, i.e., the Vandermonde determinant is the determinant

$$V(a_1, a_2, \ldots, a_n) = det \begin{pmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_n \\ a_1^2 & a_2^2 & \ldots & a_n^2 \\ \ldots & \ldots & \ldots & \ldots \\ a_1^{n-1} & a_2^{n-1} & \ldots & a_n^{n-1} \end{pmatrix}$$

(sometimes the Vandermonde determinant is the determinant of the transpose of the above matrix, but the transpose has the same determinant).

The most important fact about the Vandermonde determinant is that it is different from zero if and only if all the coefficients $a_1, a_2, \ldots, a_n$ are distinct. This follows from the following theorem:

$$V(a_1, a_2, \ldots, a_n) = \Pi_{1 \leq i < j \leq n}(a_j - a_i),$$

which is not terribly hard to prove.

Thus, $V(a_1, a_2, \ldots, a_n) = 0$ if and only if $a_j - a_i = 0$ for some $j \neq i$ which is equivalent to at least two of the coefficients being equal.

This observation about the Vandermonde determinant implies several important facts:

1. for every $n \geq 1$, and every set of n distinct real numbers $a_1, a_2, \ldots, a_n$, the vectors

   $$(1, a_1, a_1^2, \ldots, a_1^{n-1}), (1, a_2, a_2^2, \ldots, a_2^{n-1}), \ldots, (1, a_n, a_n^2, \ldots, a_n^{n-1})$$

   are linearly independent

2. for every $n \geq 1$, every set of n distinct real numbers $a_1, a_2, \ldots, a_n$, and every sequence of reals $b_1, b_2, \ldots, b_n$, the homogeneous system of equations

   $$\begin{array}{ccccccccccc} 1x_1 & + & 1x_2 & + & \ldots & + & 1x_n & = & b_1 \\ a_1x_1 & + & a_2x_2 & + & \ldots & + & a_nx_n & = & b_2 \\ a_1^2x_1 & + & a_2^2x_2 & + & \ldots & + & a_n^2x_n & = & b_3 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_1^{n-1}x_1 & + & a_2^{n-1}x_2 & + & \ldots & + & a_n^{n-1}x_n & = & b_n \end{array}$$

   has a unique solution (follows from the Kramer's rule, since the determinant of the system, $V(a_1, a_2, \ldots, a_n)$, is non-zero).

On the other hand,

1. the system

   $$\begin{array}{ccccccccccc} 1x_1 & + & 1x_2 & + & \ldots & + & 1x_n & = & b_1 \\ a_1x_1 & + & a_2x_2 & + & \ldots & + & a_nx_n & = & b_2 \\ a_1^2x_1 & + & a_2^2x_2 & + & \ldots & + & a_n^2x_n & = & b_3 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_1^{n-1}x_1 & + & a_2^{n-1}x_2 & + & \ldots & + & a_n^{n-1}x_n & = & b_n \\ a_1^nx_1 & + & a_2^nx_2 & + & \ldots & + & a_n^nx_n & = & b_{n+1} \end{array}$$

   is usually inconsistent (has no solution), unless b_{n+1} is selected to be an appropriate combination of the numbers $b_1, b_2, \ldots, b_n$

2. while, for every $k < n$, the 'smaller' system

   $$\begin{array}{ccccccccccc} 1x_1 & + & 1x_2 & + & \ldots & + & 1x_n & = & b_1 \\ a_1x_1 & + & a_2x_2 & + & \ldots & + & a_nx_n & = & b_2 \\ a_1^2x_1 & + & a_2^2x_2 & + & \ldots & + & a_n^2x_n & = & b_3 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_1^{k-1}x_1 & + & a_2^{k-1}x_2 & + & \ldots & + & a_n^{k-1}x_n & = & b_k \end{array}$$

   has *infinitely many solutions*, as it is consistent (being a subsystem of a consistent system), but has more equations than variables. Hence, any smaller system has at least one free variable, and therefore infinitely many solutions.

Next, we move to the idea of secret sharing. It is quite simple. To consider the smallest example, imagine that we have a key combination (to open a safe) that needs to be shared by two people, who together should be able to open the safe, but neither one alone should be able to do it. This is easy to achieve. If the key is a sequence of six digits $a_1, a_2, a_3, a_4, a_5, a_6$, the first user can receive the first three digits, the second the second three, and they can only open the safe if they cooperate. But this still has a drawback. Namely, either one of the users already possesses half of the secret. As a consequence, either one only has to try 10^3 combinations for the other half to determine the key. This, compared to the 10^6 combinations either one would have to try if he had no idea about the key, would be a considerable saving in the time needed to open the safe without the partner (namely, one thousands of the time).

This can be avoided by the following idea: Instead of receiving half of the secret key, namely the sequence a_1, a_2, a_3, the first user receives a random sequence $b_1, b_2, b_3, b_4, b_5, b_6$ and the second user receives the sequence $a_1 - b_1, a_2 - b_2, a_3 - b_3, a_4 - b_4, a_5 - b_5, a_6 - b_6$. To put together the secret key, the two users simply need to add their two sequences. However, neither one has the slightest clue about the secret key without the other.

This idea can be generalized as follows:

An (n, k)**-secret sharing scheme** or an (n, k)**-threshold scheme**, $n \geq k$, is a protocol for distributing a secret key K among n-users so that any k of them can recover the key, but no fewer than k can do that, and moreover, no fewer than k gain any extra information that would limit the number of possible keys they have to try.

As hard as it sounds to achieve, a secret sharing scheme is possible:

Given $n \geq k > 1$, let $K \in \mathbb{N}$ be the secret key. Choose $b_1, b_2, \ldots, b_{k-1} \in \mathbb{N}$ at random, and form the polynomial

$$p(x) = K + b_1 x + b_2 x^2 + \ldots + b_{k-1} x^{k-1}.$$

Then select at random n distinct numbers $a_1, a_2, \ldots, a_n$, and give to each of the n users one of the pairs $(a_i, p(a_i))$ (distinct users receive distinct pairs).

1. Any k users can recover the secret key K:

   Suppose k users get together and put together their k keys $(a_{i_1}, p(a_{i_1})), (a_{i_2}, p(a_{i_2})), \ldots, (a_{i_k}, p(a_{i_k}))$. They can then set up the following system of k equations:

$$\begin{array}{ccccccccccccc}
1K & + & b_1 a_{i_1} & + & b_2 a_{i_1}^2 & + & \ldots & + & b_{k-1} a_{i_1}^{k-1} & = & p(a_{i_1}) \\
1K & + & b_1 a_{i_2} & + & b_2 a_{i_2}^2 & + & \ldots & + & b_{k-1} a_{i_2}^{k-1} & = & p(a_{i_2}) \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \\
1K & + & b_1 a_{i_k} & + & b_2 a_{i_k}^2 & + & \ldots & + & b_{k-1} a_{i_k}^{k-1} & = & p(a_{i_k})
\end{array}$$

   This is a system of k equations in k unknown, namely, the numbers K, $b_1, b_2, \ldots, b_{k-1}$ are the unknowns (while the powers of the numbers a_{i_j} can be calculated), where the coefficients are the coefficients from the Vandermonde determinant $V(a_{i_1}, a_{i_2}, \ldots, a_{i_k})$, with all the coefficients by definition selected distinct. Hence, it is a system with exactly one solution. Since we only care about the secret key K, we can use the Kramer's rule to recover the key:

$$K = \frac{det\mathbb{A}}{V(a_{i_1}, a_{i_2}, \ldots, a_{i_k})}$$

   where

$$\mathbb{A} = \begin{pmatrix}
p(a_{i_1}) & p(a_{i_2}) & \ldots & p(a_{i_k}) \\
a_{i_1} & a_{i_2} & \ldots & a_{i_k} \\
a_{i_1}^2 & a_{i_2}^2 & \ldots & a_{i_k}^2 \\
\ldots & \ldots & \ldots & \ldots \\
a_{i_1}^{k-1} & a_{i_2}^{k-1} & \ldots & a_{i_k}^{k-1}
\end{pmatrix}$$

   (note that even though $det\mathbb{A}$ is not a Vandermonde determinant, it can still be computed by expanding the first row, which then leads to k Vandermonde determinants; with the first term being for example $p(a_{i_1}) \cdot V(a_{i_2}, a_{i_3}, \ldots, a_{i_k})$).

2. No fewer than k users can recover the secret, and in fact, no fewer than k users can gain any insight, as any 'smaller' system has infinitely many solutions as stated in the first part about the Vandermonde determinants.