

SECRET SHARING

AN APPLICATION OF LINEAR ALGEBRA

Consider the following problem: you have a group of 10 people who are responsible for taking care of a bank account. If you give each of these access to the account, one of them might transfer money to his own account. If you demand that a transfer is only possible if all 10 of these people agree, then you will get nothing done because it rarely happens that all 10 are around at the same time.

What you would like to have is a procedure that allows any three of them to access the account. The problem is to split up the password in such a way that any three of them can reconstruct it. Linear algebra to the rescue!

In fact, assume that your password for the day is a number N , say $N = 3141$. Now you compute ten linear equations in three unknowns that all have solutions $(x, y, z) = (N, *, *)$, where the $*$ are arbitrary numbers, and you make sure that any three of these equations are linear independent. You hand out one equation to each person. As soon as three of them are together, they can solve the linear system and find $x = N$.

Here's an example: Take $N = 3141$ as above, and compute linear equations $ax + by + cz = d$ with the property that $(x, y, z) = (3141, 2011, 473)$ is a solution

person	a	b	c	d
1	3	2	-15	6350
2	-2	4	-7	-1549
3	3	-7	2	-3708
\vdots				\vdots
10	6	-9	-1	274

(I picked a, b, c "at random" and computed d from the solution (x, y, z)). Now each of these equations is given to exactly one person. If 1, 3 and 10 meet, they set up the linear system

$$\left(\begin{array}{ccc|c} 3 & 2 & -15 & 6350 \\ 3 & -7 & 2 & -3708 \\ 6 & -9 & -1 & 274 \end{array} \right)$$

Performing the usual row operations we get

$$\begin{aligned} \left(\begin{array}{ccc|c} 3 & 2 & -15 & 6350 \\ 0 & -9 & 17 & -10058 \\ 0 & -13 & 29 & -12426 \end{array} \right) &\longrightarrow \left(\begin{array}{ccc|c} 3 & 2 & -15 & 6350 \\ 0 & 1 & -17/9 & 10058/9 \\ 0 & 1 & -29/13 & 12426/13 \end{array} \right) \longrightarrow \\ \left(\begin{array}{ccc|c} 3 & 2 & -15 & 6350 \\ 0 & 1 & -17/9 & 10058/9 \\ 0 & 0 & -40/117 & -18920/117 \end{array} \right) &\longrightarrow \left(\begin{array}{ccc|c} 3 & 2 & -15 & 6350 \\ 0 & 1 & -17/9 & 10058/9 \\ 0 & 0 & 1 & 473 \end{array} \right) \longrightarrow \\ \left(\begin{array}{ccc|c} 3 & 2 & -15 & 6350 \\ 0 & 1 & 0 & 2011 \\ 0 & 0 & 1 & 473 \end{array} \right) &\longrightarrow \left(\begin{array}{ccc|c} 1 & 0 & 0 & 3141 \\ 0 & 1 & 0 & 2011 \\ 0 & 0 & 1 & 473 \end{array} \right) \end{aligned}$$

and now they can read off the password $N = 3141$.

What happens when only two out of the ten people meet? For example, 1 and 2 can set up the system

$$\left(\begin{array}{ccc|c} 3 & 2 & -15 & 6350 \\ -2 & 4 & -7 & -1549 \end{array} \right)$$

Adding the second line to the first and then proceeding as usual gives

$$\left(\begin{array}{ccc|c} 1 & 6 & -22 & 4801 \\ -2 & 4 & -7 & -1549 \end{array} \right) \longrightarrow \left(\begin{array}{ccc|c} 1 & 6 & -22 & 4801 \\ 0 & 16 & -51 & 8053 \end{array} \right)$$

Putting $x_3 = s$, the general solution is given by $x_2 = \frac{1}{16}(8053 + 51s)$ and $x_1 = 4801 + 22s - 6x_2 = \frac{1}{8}(23s + 14249)$.

If one of these two has a background in number theory, then he will see that if x_1 is an integer, s must be chosen in the form $8n + 1$. For $n = 1, 2, 3 \dots$ we now get the following possible values of N :

n	1	2	...	59
s	9	17	...	473
N	1807	1830	...	3141

What this means is that there are way too many possibilities for the right answer (what's more, n might be negative as well); guessing will not help, in particular if the password in real-life examples is a lot bigger.