

All or Nothing


BY DENNIS E. SHASHA

Any message can be represented as a number. For example, the word “meet” in “Let’s meet at the corner of Constitution and Lake” would be represented in most computers by 109 101 101 116 in decimal, using the encoding known as ASCII.

Suppose you want to send a secret directive—perhaps a rendezvous time and location—via five couriers, but you fear that one or two will be caught. You therefore want to spread the message among the couriers such that any three of them can together reconstruct it but two or fewer cannot.

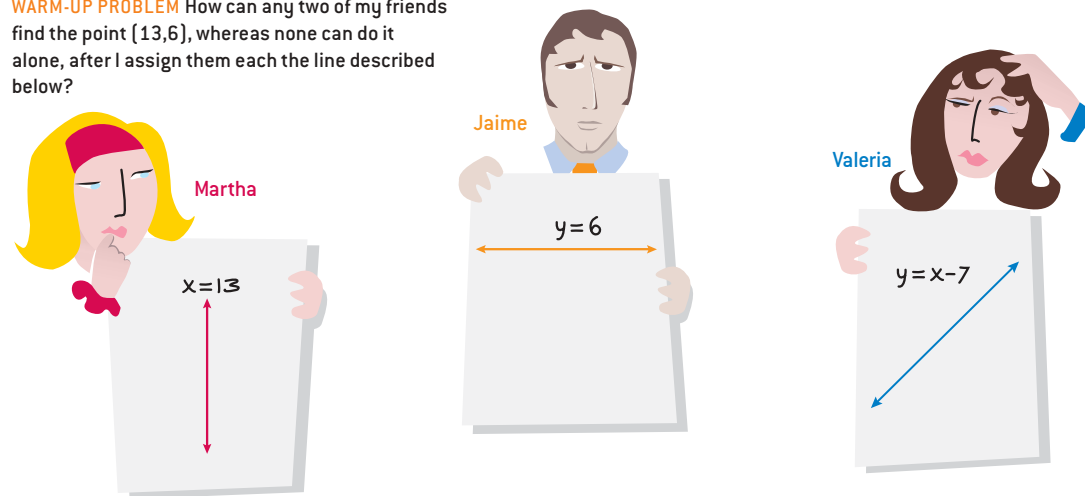
Because messages are encoded numbers, you could think of this problem as having the five couriers share the secret of a number. Intuitively, you might think it wise to give each of them part of the number, but that is not the most secure approach.

Instead you want to establish an information “cliff”: two couriers give you no useful information, but three give you the entire message. To reach that goal, you have to think of a cleverer plan.

To warm up, suppose I think of a point in a plane—say (13,6)—and ask three friends to identify that spot. I want any two of the three, but no single friend, to find it. As a clue, I give Martha the line $x = 13$, Jaime the line $y = 6$, and Valeria the line $y = x - 7$ [see illustration below]. How could my pals use that information? Can you see that two are necessary and sufficient? Similar reasoning will give you a solution to the five-courier problem. 

Dennis E. Shasha is professor of computer science at the Courant Institute of New York University.

WARM-UP PROBLEM How can any two of my friends find the point (13,6), whereas none can do it alone, after I assign them each the line described below?



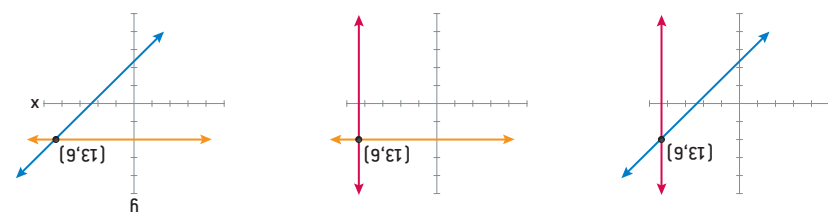
Answer to Last Month's Puzzle

Two tests are needed to verify the four-element circuit. In the first test, put 0 in inputs A, B and C and 1 in input D; output E should be 1. In the second test, put 1 in inputs A and C and 0 in inputs B and D; output E should be 0. If the circuit has four AND gates, three tests would be required, with the following inputs: 0111 (meaning input A is 0 and the others are 1), 1011 and 1110.

Only two circuits in the three-element configuration cannot be verified with one test: the circuit in which element 2 is an AND gate and the others are OR gates, and the circuit in which element 2 is an OR gate and the others are AND gates.

Web Solution

For a peek at the answer to this month's problem, visit www.sciam.com



ANSWER: With just one line, no friend has useful information: my point could be any one of the infinite points in the assigned line. But any two of my friends can find the point (13,6) instantly by determining where their lines intersect on a standard x,y grid. My pals go from facing infinite uncertainty to having precise knowledge.