

PROBLEM

Alice, Bob, and Charlie play the following card game. Charlie has seven cards, numbered 1–7. He shuffles (honestly) and deals 3 cards each to Alice and Bob, leaving one for himself. Can Alice and Bob speak to each other, with Charlie present, in such a way that Alice learns what cards Bob has, Bob learns what cards Alice has, but for any card other than his own, Charlie cannot determine who holds that card? (Assume Charlie has unlimited computational power, so cryptographic methods like Diffie-Hellman key exchange are out of the question.)

Source: Mathematical Intelligencer, 2001

SOLUTION

We present a solution that uses modular arithmetic. (Google this term if you are not familiar with it.) Note that all of the cards together add up to $0 \pmod 7$; to see this, you can form pairs (1,6), (2,5), (3,4) that each add up to $0 \pmod 7$ and the remaining 7 card is $0 \pmod 7$. For what remains, we will let $x \equiv y$ mean that x equals $y \pmod 7$.

Let a be the sum of Alice's cards mod 7, b be the sum of Bob's cards mod 7, let c be Charlie's card, and note that $a + b + c \equiv 0$. From this, Bob can determine Charlie's card, since $c \equiv -a - b$. Bob responds, "Charlie has c ." That's all they have to say.

Bob will know what cards Alice has by elimination, since he knows his own cards and Charlie's card. Similarly, since Alice learns Charlie's card from Bob, she can determine what cards Bob has.

What's trickier is showing that Charlie cannot determine, for any card other than c , whether Alice or Bob has that card. The details are more tedious than they are tricky; the following terse argument makes it look harder than it really is.

Claim 1: Given any set F with 5 of the 7 cards, and any k , you can get form a pair in F that sums to k . Proof: $4k + 4k \equiv 8k \equiv k$, so the pairs $(4k + 1, 4k - 1)$, $(4k + 2, 4k - 2)$, and $(4k + 3, 4k - 3)$ each sum to k ; if you are missing only 2 cards, you will be able to form at least one of these pairs.

Claim 2: With F as above and any k , you can get 3 cards in F that sum to k . Proof: Let s be the sum of the cards in F . By the previous claim, you can form a pair that sums to $s - k$; the remaining 3 cards then must sum to $s - (s - k) \equiv k$.

Now, let d be any card other than Charlie's, and let F be the 5 cards other than c and d . We must show that Charlie cannot determine who holds d . By Claim 1, there is a pair of cards e_1, e_2 in F that sum to $a - d$. By Claim 2, there are three cards f_1, f_2, f_3 in F (not necessarily distinct from e_1 and e_2) that sum to a . Alice might have cards d, e_1 , and e_2 , since these sum to a ; or, Alice might have cards f_1, f_2, f_3 , since these also sum to a . In short, it is possible that Alice has d , and it is possible that Alice does not have d . So, Charlie cannot determine who holds d .