Activity 16

Sharing secrets—*Information hiding protocols*

Age group	Middle elementary and up.
Abilities assumed	Adding three digit numbers competently; understanding the concept of *average* and how to calculate it.
Time	About 5 minutes.
Size of group	At least three children, preferably more.

Focus

Calculating an average.

Random numbers.

Cooperative tasks.

Summary

Cryptographic techniques enable us to share information with other people, yet still maintain a surprisingly high level of privacy. This activity illustrates a situation where information is shared, and yet none of it is revealed: a group of children will calculate their average age without anyone having to reveal to anyone else what their age is.

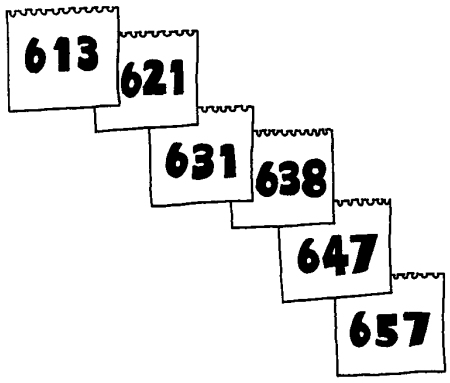

Figure 16.1: Pages of the pad used for finding the average age of five children

Technical terms

Computer security, cryptography, cryptographic protocol, averaging.

Materials

Each group of children will need:

a small pad of paper, and

a pen.

What to do

This activity involves finding the average age of a group of children, without anyone having to reveal what their age is. Alternatively, one could work out the average income (allowance) of the children in the group, or some similar personal detail. Calculating these statistics works particularly well with adults, because older people can be more sensitive about details like age and income. You will need at least three children in the group.

1. Explain to the group that you would like to work out their average age, without anyone telling anyone else what their age is. Ask for suggestions about how this might be done, or even whether they believe it can be done.

2. Select about six to ten children to work with. Give the pad and pen to the first child, and ask them to secretly write down a randomly chosen three-digit number on the top sheet of paper. In the example in Figure 16.1, 613 has been chosen as the random number.

3. Have the first child tear off the first page, add their age to the random number, and write it on the second sheet on the pad. In Figure 16.1, the first child's age is 8, so the second sheet shows 621. They should keep the page that was torn off (and not show it to anyone.)

4. The pad is then passed to the second child, who adds their age to the number on the top, tears off the page, and writes the total on the next page. In the example, the second child is 10 years old.

5. Continue this process having a child tear off the top page and add their age to the number on it, until all the children have had the pad.

6. Return the pad to the first child. Have that child subtract their original random number from the number on the pad. In the example, the pad has been around five children, and the final number, 657, has the original number, 613, subtracted from it, giving the number 44. This number is the sum of the children's ages, and the average can be calculated by dividing by the number of children; thus the average age of our example group is 8.8 years old.

7. Point out to the children that so long as everyone destroys their piece of paper, no-one can work out an individual's age unless two people decide to cooperate.

Variations and extensions

This system could be adapted to allow secret voting by having each person add one if they are voting yes, and zero if they are voting no. Of course, if someone adds more than one (or less than zero) then the voting would be unfair, although they would be running the risk of arousing suspicion if everyone voted yes, since the number of yes votes would be more than the number of people.

What's it all about?

Computers store a lot of personal information about us: our bank balance, how much tax we owe, how long we have held a driver's license, our credit history, examination results, medical records, and so on. Privacy is very important! But we do need to be able to share some of this information with other people. For example, when paying for goods at a store using a bank card, we recognize that the store needs to verify that we have the funds available.

Often we end up providing more information than is really necessary. For example, if we perform an electronic transaction at a store, they will probably discover who we bank with, what our account number is, and what our name is. Furthermore, the bank finds out where we have done our shopping. In principle, a bank could create a profile of someone by monitoring things like where they buy gas or groceries, how much they spend on these items each day, and when these places are visited. If we had paid by cash then none of this information would have been revealed. Most people wouldn't worry too much about this information being shared, but there is the potential for it to be abused, whether for targeted marketing (for example, sending travel advertisements to people who spend a lot on air tickets), discrimination (such as offering better service to someone whose bank usually only takes on wealthy clients), or even blackmail (such as threatening to reveal the details of an embarrassing transaction). If nothing else, people might change the way they shop if they think that someone might be monitoring them.

This loss of privacy is fairly widely accepted, yet cryptographic protocols exist that allow us to make electronic financial transactions with the same level of privacy as we would get with cash. It might be hard to believe that money can be transferred from your bank account to a store's account without anyone knowing where the money was coming from or going to. This activity makes such a transaction seem a little more plausible: both situations involve limited sharing of information, and this can be made possible by a clever protocol.

Further reading

David Chaum has written a paper with the provocative title "Security without identification: transaction systems to make Big Brother obsolete." The paper is quite readable, and gives simple examples of information hiding protocols, including how completely private transactions can be made using "electronic cash." It can be found in *Communications of the ACM*, October 1985.