SECRETLY SHARING PASSWORDS

Diane Donovan
Mathematics Department, The University of Queensland.

Secret Sharing

In our technological age the consequences of unauthorised access to computers can be grave. For example, bank safes are controlled by electronic locks, and nuclear powered nation use computers to fire missiles. For security reasons, it may be the case that the safe is unlocked when two bank employees enter individual sequences which are combined to from a password, or that the missiles are launched only after two generals each enter numbers which when summed form a password. The big question is "Do these systems provide enough security?" Greater security would be achieved by requiring a larger number of individuals to combine information to form the password. However, what happens if someone forgets their password, or one of the employees is sick, or one of the generals is killed in an air strike? Will it still be possible to open the safe or launch the missile? What is really required is a secure but flexible system. This can be achieved through a t–out–of–n *secret sharing scheme* in which the password K is divided into n secret bits, called *shares*, in such a way that

- any t of the shares can be used to reconstruct the password K, but
- less than t shares provides no useful information about the password.

The important thing is that t is less than n and so not all the shares are needed to reconstruct the password K, but in addition the password cannot be reconstructed from less than t shares.

The question is how can this be achieved? In this article I will illustrate how the equation to a straight line, $y = mx + c$, is being used to construct secret sharing schemes and thus improve computer security. This particular application of pure mathematics is ideal for presentation in schools as the notion of a computer password is easily grasped and the mathematical concepts, the equation to a straight line or a curve, are studied by the students. In addition, the student can be shown how pure mathematics is used to assess the security of such systems. A possible student worksheet has been included at the end of the article.

Two points fix a straight line

Intersecting lines in an XY–plane are being used to construct 2–out–of–n secret sharing schemes. For example, the password could be shared between n tellers (or generals) as follows:

S1 Choose two numbers r and s, so that together they form a password.

S2 Think of the password as a point (r, s) in an XY–plane.

S3 Choose a line L which passes through the point (r, s). The equation to this line is not secret and is broadcast to all individuals participating in the scheme, but remember the point (r, s) must be kept secret.

S4 Choose another line M, which intersects L at the point (r, s). The equation to this line must be kept secret.

S5 Finally, take n points (other than (r, s)), all of which lie on M, and give one point to each teller (or general) as his share. Each teller receives a different point and must keep it secret.

S6 To recover the password, two tellers enter their points into the computer. The computer uses both points to recover the equation to the line M and then intersects M with L, thus recovering the point (r, s) and thus the password.

An example

Assume that the password is to be divided between 6 tellers in such a way that any 2 can combine their shares and recover the password. (In this example the numbers are small for ease of computation. In practice these numbers are chosen to be very large.)

S1 Let's choose r to be 7 and s to be -4.

S2 We associate the password with the point $(7, -4)$.

S3 Let's choose L to be the line with equation $y = -x + 3$. Note that the point $(7, -4)$ is on this line. The equation to this line is given to all individuals who are participating in the scheme, but the point $(7, -4)$ is kept secret.

S4 Let's choose another line, M, equal to say $y = x - 11$. This line is to be kept secret.

S5 Take the points $(1, -10)$, $(22, 11)$, $(-1, -12)$, $(0, -11)$, $(13, 2)$, and $(5, -6)$, all of which are on M, and give one point to each of the six tellers participating in the scheme. Each teller must keep their point (share) secret.

S6 To recover the password the computer must receive two points, say $(-1, -12)$ and $(5, -6)$. Then it computes M as follows

$$\begin{aligned} y - (-12) &= \frac{(-12) - (-6)}{(-1) - 5}(x - (-1)) \\ y + 12 &= \frac{-6}{-6}(x + 1) \\ y + 12 &= x + 1 \\ y &= x - 11. \end{aligned}$$

Now solving the simultaneous equations

$$y = -x + 3 \quad (1)$$
$$y = x - 11 \quad (2)$$

by subtracting (1) from (2), gives,

$$\begin{aligned} 0 &= -x + 3 - (x - 11) \\ \rightarrow 2x &= 14 \\ \rightarrow x &= 7 \\ \rightarrow y &= -7 + 3 = -4. \end{aligned}$$

The point of intersection, that is the password, $(7, -4)$ is recovered.

Points to be noted

Before I finish this article I think the following points should be made.

- Secret sharing schemes are being used to improve computer security.
- Sometimes, students ask "Why not just give the value r to half the tellers and s to the other half?" This greatly reduces the security of the scheme. Individuals holding the value r know that the password is a point on the line $x = r$. Now if they know the equation to L they can quickly work out s. Such an idea also reduces the flexibility of the scheme, as not all pairs can combine their shares.
- The fact that the equation to a straight line can be written algebraically allows us to code these ideas and programme them on a computer.
- To assess the security of the scheme one must ask

  > "Can an individual guess the password given that he knows L and his share, the the point (u, v)"

  No, you need two points to fix the line M. There are many lines which intersect L and pass through (u, v). Here we should emphasise that pure mathematics can be used to check the security of the scheme. This is a very important part of the process.
- The password can be chosen to be a point on the y–axis. Thus the line L is $x = 0$. This does not affect the security of the scheme and in fact makes it easier to generalise the scheme.
- To construct a 3–out–of–n secret sharing scheme one can use the fact that 3 points fix a parabola. The password is chosen to be a point a_0 on the y axis and the line M is replaced by a parablola with equation $y = a_0 + a_1x + a_2x^2$. The shares in a_0 are points (distinct from $(0, a_0)$) on the parabola and when any three points are received they can be used in step **S6** to generate three equations in three unknowns. These will have a unique solution and hence a_0 can be recoved.
- To construct a t–out–of–n secret sharing scheme, choose the password to be a point a_0 on the y axis and the shares to be points on a curve with equation

  $$y = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_{t-1}x^{t-1}.$$

  Note the degree of this polynomial is $t - 1$ and so any t points on this curve can be used to generate t equations in t unknowns. These have a unique solution and so a_0 can be recoverd.

- In both the two previous examples it can be shown that $t-1$ shares cannot be used to recover a_0. For example, assume $t-1$ individuals collaborate, they know the password is the constant term of a polynomial of degree $t-1$ passing through their points. They use their shares to write down $t-1$ equations in t unknowns. To obtain a unique solution they must have another equation. However each of the points $(0, y_0)$ will provide another equation and hence a different solution. So they are no better off than if they had just guessed a_0.

The following references will provide extra information on secret sharing schemes.

References

[1] Diane Donovan, *Some interesting constructions for secret sharing schemes*, Australasian Journal of Combinatorics, **9**, (1994), 37–65.

[2] G.J. Simmons, *An introduction to shared secret and/or shared control schemes and their applications*, in Contemporary Cryptology, The Science of Information Integrity, IEEE Press, Piscataway, (1991), 441–497.

SECRETLY SHARING PASSWORDS
WORKSHEET PAGE 1

Divide the class into groups of six. Each groups executes the following tasks.

Q1 Pick a line in the XY plane. Name this line L. Write down the equation to your line and sketch it. The line you have chosen is not secret so you do not have to hide it.

> *HINT:* To choose your line, first decide where it should cut the Y axis. This point is called the $Yintercept$. (This intercept should not be $(0,0)$.) Next choose where it should cut the X axis. This point is called the $Xintercept$. The GRADIENT of your line is given by $m = \frac{Yintercept}{Xintercept}$ and the equation of your line is
>
> $$y = (GRADIENT)\ x\ +\ (Yintercept)$$
>
> or $y = mx + c$ where m is the GRADIENT and c is the $Yintercept$.

Q2 Choose your secret point. It must be a point (x_s, y_s) on the line L you selected in Q1. Write down your point but remember it must be kept secret.

> *HINT:* To choose your point (x_s, y_s) begin by taking the line $y = mx + c$ you chose in part Q1. Select any value for x_s, and substitute this value for x in the equation $y = mx + c$. The answer you get when you evaluate $mx_s + c$ is the value of y_s and (x_s, y_s) is your secret point on the line L.

Q3 Now you must evaluate shares in the secret point (x_s, y_s). These will be given to the members of one of the other groups.

To work out your shares first choose a line M which passes through your secret point (x_s, y_s) but which is different from the line L. Write down the equation to M and sketch it on the same graph as L. The equation to this line is secret.

> *HINT:* You need to find a line of the form $y = nx + d$ which passes through (x_s, y_s). Begin by choosing the point at which this new line will cut the Y-axis. This value is d in the equation $y = nx + d$. You want this line to pass through (x_s, y_s), so evaluate $y_s = nx_s + d$ to obtain n.

Q4 Next choose six points (x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4), (x_5, y_5), (x_6, y_6) on your new line M. Write down each of these points. For the moment these points are to be kept secret.

> *HINT:* If you have trouble finding these points go back to the hint in Q2.

Q5 Now you must distribute these shares (points) to the students in another group. So begin by selecting the group you are going to share your secret with. Next take a piece of paper and on it write the equation to the line L, you chose in Q1, and the point (x_1, y_1) you chose in Q4. Then on different pieces of paper repeat this process for each of the points (x_2, y_2), (x_3, y_3), (x_4, y_4), (x_5, y_5), (x_6, y_6). You should now have six pieces of paper each with the equation to the line L and one point on it.

These pieces of paper are the shares you distribute to the members of the other group. You must give one piece of paper to each person. The information on each piece of paper is *SECRET*.

Each student has been given a piece of paper and on this paper is written the equation to the line L and a point of the form (x_i, y_i). Each group should divide into pairs and execute the following proceedure.

Q5 In pairs, combine your points (x_i, y_i) and (x_j, y_j) to find the equation to the line M and write it down.

HINT: To find the line which passes through the points (x_i, y_i) and (x_j, y_j) use the formula

$$y - y_i = \frac{y_i - y_j}{x_i - x_j}(x - x_i).$$

Q6 Now you must find the point at which the two lines L and M intersect. This is the secret point (x_s, y_s) and thus the password.

HINT: To find the intersection of two lines L, $y = mx + c$, and M, $y = nx + d$, you solve the simultaneous equations. One way of doing this is to note that

$$\begin{aligned} & mx + c = nx + d \\ \rightarrow \quad & mx - nx = d - c \\ \rightarrow \quad & x(m - n) = d - c \\ \rightarrow \quad & x = \frac{d - c}{m - n}. \end{aligned}$$

At this point you have the value of x_s. Now substitute x_s in the equation $y = mx + c$ and you have the value of y_s.

Q7 Why do we need two students to work together to get the secret point? Why can't one student use the equation to L and the point (x_i, y_i), that they hold, to find the value of (x_s, y_s)? Explain your answer.