An Introduction to The Threshold Secret Sharing Scheme in Entry Level Mathematics Courses

Hisa Tsutsui
Department of Mathematics, Box 1002
Millersville University
Millersville, Pennsylvania 17551
Hisaya.Tsutsui@millersville.edu

1. *Introduction*

In this article, we present material to be used for one or two class periods in an entry level mathematics course. The subject we introduce is known as The Threshold Secret Sharing Scheme. While the deeper end of the subject is highly sophisticated and widely used in modern society, the basic mathematical idea behind it is surprisingly simple: simple enough to be fully accessible to students in a College Algebra level class. It is the purpose of this article to introduce the subject as a possible enhancement for an entry level college course.

2. *A Classroom Presentation to Introduce the Subject*

What follows is a "transcript" of a classroom presentation with additional comments for the instructor. Homework problems that we have assigned are also supplied.

Suppose that you have been keeping a diary in a computer that has been giving you problems lately and you are afraid that you might lose the diary file someday. What would you do? Perhaps make a copy on a diskette? But are you safe then? What if you have a cat who loves to destroy your diskettes? How about making some extra copies then? Sounds good... but you must be careful. You do not want any one else to read your diary and the more copies you make, the higher possibility that someone might find a copy and intentionally or not, read it and find out everything about you!

There is an interesting secret sharing scheme that would nicely solve this type of problem. To make it simpler, let's use a number S as your secret instead of using an entry in your diary.

Choose a positive integer n and another positive integer k less than n. A stunning conclusion is that it is possible to make n pieces of information about your secret number S in such a way that S can still be recovered even if $n-k$ of the information pieces are destroyed. Not only that, but anyone's attempt to collect less than k of any of the n information pieces reveals absolutely no information about S. This method of concealing information is called the **Simple $<\mathbf{k,n}>$ Threshold Scheme** and it is based on the elementary fact that given k points in the 2-dimensional plane (x_1, y_1), (x_2, y_2), ... , (x_k, y_k), there is at most one polynomial $f(x)$ of degree $k-1$ such that $f(x_i)=y_i$ for all i (See for example, Runborg [5]). How this is possible may be best explained by showing a few simple examples.

EXAMPLE 1: Simple $<2,3>$ Threshold Scheme

Here we have, $k=2$ and $n=3$. This means: we shall create 3 different pieces of information; A, B, and C about the secret number S in such a way that we only need any two out of the three to know the number S. And yet, knowing only one of A, B, or C reveals absolutely no information about the number S.

The geometric idea behind this is very intuitive: there are infinitely many lines that pass through a single point but if two points are given, there is only a single line that passes through the points. A demonstration of one way to implement such a scheme follows:

Plot the secret number S on the y-axis. For example, if the secret number S is 5, then plot (0, 5). Then sketch any straight line that goes through the point, and choose A, B, and C to be any three distinct points on the line that are not S as shown in Figure A. Now you see easily that if someone knows any two out of the three points A, B, and C, then all he or she must do to find the number S is to connect the two known points and extend the line to find the point on the y-axis. Since two points determine the unique line, the third point is not needed. On the other hand, Figure B shows that it is not possible to determine S knowing only one point out of the three.

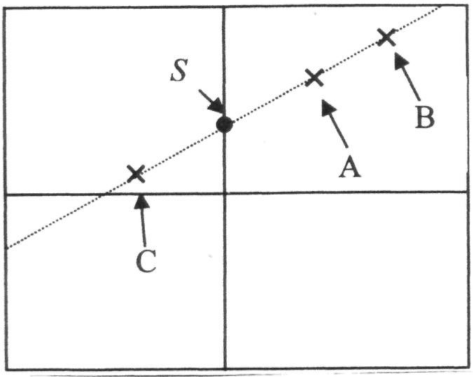

Figure A

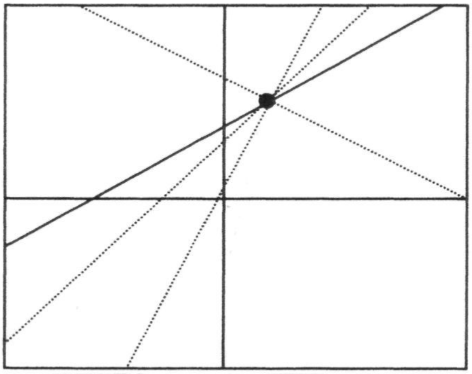

Figure B

After presenting the example, we give the following exercise problem: Using Simple $<2,5>$ Threshold Scheme, a secret number *S* is secured on the *y*-axis as was demonstrated in Example 1. Suppose that you found two out of the five secret coordinates; A= (1, 2), and B= (3, 4). Find *S*.

Students are asked to follow Example 1 and find *S* graphically. That is, we let students plot the points A and B on a graph paper, connect the two points and extend to find the *y*-intercept. After a few minutes, most students normally find the *y*-intercept (0, 1) easily by looking at their sketch, and they seem to feel a better grasp of the example. We then continue to ask "But how do you know *S* is 1? Could it be 0.95?" If this material is presented in a Precalculus or College Algebra class where students have learned about an equation of a straight line, then it is an elementary algebraic exercise for them to find an equation and its *y*-intercept of a straight line passing through two points. Otherwise, it would be a good motivation for them to learn the material.

EXAMPLE 2: Simple $<3,6>$ Threshold Scheme

This time $k=3$, and $n=6$. That means: we shall construct 6 different information pieces A, B, C, D, E, and F about the secret number *S* in such a way that we only need any three out of six to know the number *S*. And yet, knowing two or less out of the six information pieces reveals absolutely no information about the number.

To implement such a scheme, we again start by plotting *S* on the *y*-axis. This time, you sketch a graph of a polynomial function of degree 2 that passes through *S*. Then, choose A, B, C, D, E, and F to be any six distinct points on the curve that are not *S* as shown in Figure C. Since any three points with different *x*-coordinate have at most one second-degree polynomial passing through them, the scheme will work perfectly as it did in the previous example.

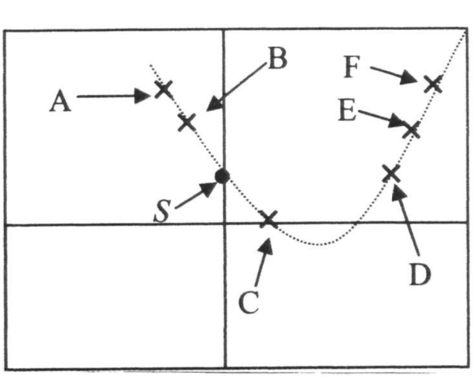

Figure C

Depending on the level of the class, we normally adjust the time we spent on this example. For example, in a liberal art mathematics course for non-science majors, we only spend a few minutes to explain that we can expand the idea of Example 1 using a polynomial of a higher order. In a precalculus or an entry level discrete mathematics course, we present the following problem after explaining the example:

Using Simple $<3,7>$ Threshold Scheme, a secret number S is secured on the y-axis as demonstrated in Example 2. Suppose that you found three out of the seven secret coordinates; A=$(1,3)$, B=$(2, 0)$, and C=$(3,-1)$. Find S.

We begin by writing a general equation of a graph of a quadratic polynomial as $y=ax^2+bx+S$. With an appropriate hint or guidance, students will soon be convinced for the need of solving the system of linear equations below to find the solution $S=8$, and realize why "S" was used instead of "c" in the general equation above.

$$a+b+S=3$$

$$4a+2b+S=0$$

$$9a+3b+S=-1$$

EXAMPLE 3: Do you trust mathematicians?

Suppose 5 CIA agents and 15 mathematicians are working together under you. You want to give each member a secret code (or codes) to access your computer. Using a Simple $<k,n>$ Threshold Scheme, you want to distribute a minimum number of codes so that:

1. In order for a mathematician to access your computer without the attendance of CIA agents, he or she must be together with at least three other mathematicians (i.e., at least four mathematicians must get together to access your computer).
2. In order for a CIA agent to access your computer without the attendance of mathematicians, he or she must be together with at least one other agent (i.e., at least two CIA agents must get together to access your computer).

You must treat each mathematician equally. That is, the same number of code(s) must be distributed for each mathematician. You must also distribute the same number of code(s) among CIA members. What should k and n represent in this situation, and what values should you choose?

Solution

Here n is the total number of secret codes you use, and k is the number needed to access the computer. To fulfill the first condition, you need to choose k so that any mathematicians' attempt to access your computer with less than three other mathematicians will be blocked. If you choose $k=4$ and distribute one secret code to each mathematician, the condition will be fulfilled. But then how can two CIA agents together gain access to your computer so that the second condition will also be fulfilled? A simple solution for that is to distribute two secret codes to each CIA members. Therefore, all together, you need $1\times15+2\times5=25$ secret codes, or $n=25$.

Regardless of the level of the class, this example might not be as easily digested as previous ones at first. However, through choosing different values for the number of mathematicians and CIA agents, an open classroom discussion normally convinces a few students fairly quickly, and they in turn try to convince others. After several minutes of discussion, the following questions are useful to better assess the understanding of the class: Can one mathematician and one CIA agent access your computer together? How about two mathematicians and one CIA agent?

HOMEWORK PROBLEMS (solutions follow)

1. Using Simple $<2,5>$ Threshold Scheme, a secret number S is secured on the y-axis. Suppose that you found two out of the five secret coordinates; A=(1, 2), and B=(2, 3).

(a) Find S.

(b) Which of the following coordinates (perhaps only one) are possibly amongst the others?

a. $(-2, -3)$ b. $(-1, -2)$ c. (2.5, 3.5) d. (3, 4) e. (4, 5)

2. Using Simple $<3,5>$ Threshold Scheme, a secret number S is secured on the Y-axis.

(a) At least how many secret coordinates do you need in order to find S?

(b) Three secret coordinates have been found: A=(1, 6), B=(2, 11), and C=$(-1, 2)$. Find S.

3. Using Simple $<3,8>$ Threshold Scheme, a secret number S is secured. If you found two secret coordinates A=(1, 1), and B=(2, 4), can you find S ?

4. Suppose 7 FBI agents and 25 former KGB agents are working together on a project to eliminate a war. For security reasons, each agent has a secret password (or passwords) to operate the computer. Using a Simple $<k,n>$ Threshold Scheme, it was set so that in order for FBI agents to use the computer, at least 5 agents must sign in simultaneously; but, for KGB agents, only 2 of them are required to sign in together. Each FBI agent has the same number of passwords, and each KGB agent has the same number of passwords. Assume that the minimum possible numbers of passwords were distributed.

(a) What values are used for k and n?

(b) Can one KGB and two FBI agents sign-in together?

(c) Can one KGB agent and one FBI agent sign-in together?

5. Suppose 14 FBI agents and 14 former KGB agents are working together on a project to eliminate a war. For security reasons, each agent has a secret password (or passwords) to operate the computer. Using a Simple $<k,n>$

Threshold Scheme, it was set so that in order for FBI agents to use the computer, at least 4 members must sign in simultaneously; but, for KGB agents, only 3 members are required to sign in together. Each FBI agent has the same number of passwords, and each KGB agent has the same number of passwords. Assume that the minimum possible numbers of passwords were distributed.

(a) What values are used for k and n? (Be careful: $k = 4$ does not work.)
(b) Can one KGB and two FBI agents sign in together?
(c) How about one FBI agent and one KGB agent?

Solutions to problems 1 - 5 above
1. (a) 1 (b) c, d, e **2.** (a) 3 (b) 3 **3.** No **4.** (a) k=5, n=82 (b) Yes (c) No
5. (a) k=7 or 8, n=70 (b) Yes for k=7, and No for k=8 (c) No

3. *Conclusion*

Our interest here was to present material for the improvement of classroom effectiveness in the first years of college. However, interested readers can easily develop this material further for use in a slightly higher level class. Perhaps, one can introduce the subject in an entry level abstract algebra or number theory class when integers mod p is introduced, or in an elementary linear algebra class where systems of linear equations are studied intensively.

While this material was prepared for the use in a college algebra level class, it may also be used for a lecture in a developmental mathematics course. Perhaps, it would be a good experience for the students in such a class to see an application of a simple geometric concept that two distinct points determine a unique line. For this level of students, Example 1 and the exercise which follows may be used to familiarize the x-y coordinate system; and Example 2 should be omitted or be explained very briefly.

Introduction to this material in our elementary mathematics courses has seemed to get the students' attention. It has been our experience that the material in fact stimulates students in such classes and has helped in creating a lively classroom atmosphere. A sophisticated PowerPoint presentation that we have used is available for further enhancement of a classroom presentation, and we would be glad to share upon request for any interested readers. (Hisaya.Tsutsui@millersville.edu)

References

1. Aho A., Hopcroft J., and Ullman J. (1974). *The Design and Analysis of Computer Algorithm*, Addison-Wesley, Reading, MA.
2. Blakley G. R. (1979). *Safeguarding cryptographic key*, Proc. AFIPS NCC, 48, 313-317.
3. Gottesman D. (2002). *Uncloneable Encryption*, Proc. QCMC 2002, Rinton Press, Princton, NJ.
4. Liu C. L. (1968). *Introduction to Combinatorial Mathematics*, McGraw-Hill, New York, NY.
5. Runborg O. (2003). *Notes on Polynomial Interpolation,* www.nada.kth.se/kurser/kth/2D1250/ tilnum2- 03/interp.pdf.

Copyright of Mathematics & Computer Education is the property of MATYC Journal, Inc. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.