Background

In November 2013 it was widely reported that a man named James Howells had thrown away a hard drive containing the keys to bitcoins worth more than £4 million[1]. He had stored all the keys in his laptop which later broke when he accidentally spilled lemonade on it. Nevertheless he dismantled the laptop and kept the hard drive to gather dust in a drawer. Three years later while clearing out his drawer he threw away the hard drive without giving it much thought. At the end of that week he realised his mistake. He did not have a backup to the keys and therefore could not spend any of that money ever. That led him to a long and fruitless search for the hard drive in the local land fill. To date he has never found the hard drive and is not likely to.

For the purposes of this exploration, all that has is to be known about bit coins is that in order to spend this form of currency, one needs to know the keys to the coins. If not, the coins cannot be transacted. The keys are a 256-bit number[2],that is a 256 digits long number in base 2. In decimal, base 10 number it is 78 digits long. It is impossibly difficult to guess the key because of the enormous number. These unique numbers are required when the coins are transacted.

If James had a backup of all the keys to his coins, he could just spend the coins at any time. He could have placed all the keys in several computer hard drives or in a memory stick. In view of the relative ease of hackers to access a computer hard drive, this may not be a good idea. An intruder will most certainly have sufficient incentive to hack a computer and learn the keys because of the enormous value of the coins. Placing several copies of the keys in different locations only increases the chance that the hacker getting the keys.

An alternative would be to split individual keys into several parts and save them in different places. For this illustration let us take the secret key as "1234567890". The key can be split into "12", "34", "56", "78" and "90" and placed in five different places. The first share "12" can be written down on paper, the second share "34" could be stored in a thumb drive etc. etc. The major problem with this is that all the shares would be needed to recover the keys. If any one is missing, the whole key cannot be recovered at all. This does not make the situation any better because losing just one share will make the whole key irrecoverable. There is a higher chance of losing one share than losing the whole key without splitting it.

Furthermore, there is a security issue. If an intruder somehow manages to get four of the five shares, all he has to do is to guess the last two digits. It is known that the last two digits are base 10 and there are only two digits. Using this information the intruder knows that there are only 100 possibilities $\{00, 01, 02, 03 \ldots 98, 99\}$.He can try all hundred possibilities and may be able to discover the key. This is not as difficult as guessing the whole key. As such, by discovering more shares, it becomes easier for the intruder to guess the original key. Given enough time, the intruder has a higher chance of figuring out the key.

The Shamir Secret Sharing Scheme[3] is one solution. This scheme allows you to take a secret number and split the secret to several shares. A threshold number of shares can be set so that only if the

[1] Hern, A. (2013, November 27). Missing: Hard drive containing Bitcoins worth £4m in Newport landfill site. Retrieved March 27, 2016, from http://www.theguardian.com/technology/2013/nov/27/hard-drive-bitcoin-landfill-site

[2] Private key. (n.d.). Retrieved March 27, 2016, from https://en.bitcoin.it/wiki/Private_key

[3] Shamir, A. (1979). How to share a secret. *Communications of the ACM*, *22*(11), 612-613.

threshold number of shares is presented can the original secret be recovered. With less than the threshold number of shares, it is impossible to reveal any information about the secret. James can split his secret keys into several shares and place them in several locations. He can set a threshold number of shares that are needed to recover the original key so that even if he loses some of them, he can recover the keys. Furthermore, an intruder who somehow is able to gain access to some of the shares will be completely unable to find any information about the keys as long as he has less than the threshold number of shares. James can reduce the chance of an intruder getting the threshold number of shares by setting the threshold very high.

In a more mathematical notation, a secret number S can be split into n number of shares $\{S_1, S_2 \ldots\ldots S_n\}$. The properties of this scheme is as follows:

I. It is possible to easily compute the original secret if more than the threshold, t numbers of shares is presented.
II. No information about the secret S is revealed if any less than t number of shares are presented.

The idea behind the Shamir Secret Sharing Scheme

The basic scheme is based on the principle that a unique polynomial of order t can be recreated through interpolation only if there are $t + 1$ coordinates known. If there are too few coordinates known, the polynomial cannot be determined. For example, in order to recreate a first degree polynomial $N(x) = 2x + 1$, one would need at least two coordinates to determine the original equation. To define a second degree polynomial, a parabola, at least three coordinate points would be needed. In order to define a third degree polynomial, a hyperbola, at least four coordinates would be needed and so on.

To demonstrate the property, here is example showing the equation of a parabola.

Using the coordinates $(1, 7), (2, 6), (3, 9)$ from equation $M(x)$. From this information we can create three relationships.

$$a(1)^2 + b(1) + c = 7 \quad —①$$

$$a(2)^2 + b(2) + c = 6 \quad —②$$

$$a(3)^2 + b(2) + c = 9 \quad —③$$

This system of three equations can be solved to reveal the values of a, b and c to reveal the polynomial connecting the three points.

$$② - ①,$$

$$3a + b = -1 \quad —④$$

$$③ - ②,$$

$$5a + b = 3 \quad —⑤$$

$$⑤ - ④,$$

$$2a = 4$$

$$a = 2$$

$$Substituting\ a = 2\ into\ ④,$$

$$6 + b = -1$$

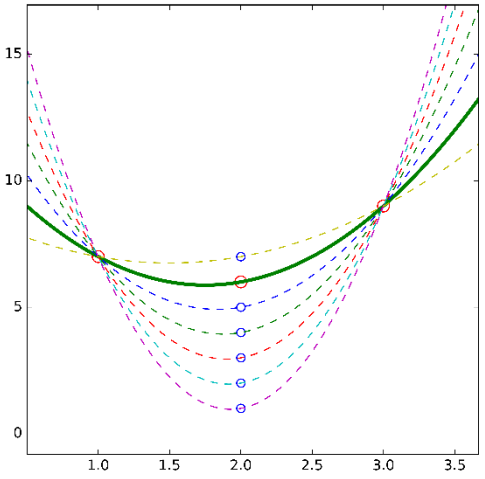
$$B = -7$$

$$Substituting\ a = 2,\ b = -7\ into\ ①,$$

$$2 - 7 + c = 7$$

$$C = 12$$

So the polynomial connecting the three points is $M(x) = 2x^2 - 7x + 12$ *Figure*



When forming a parabola, at least three coordinates are required. If only 2 out of 3 points are known, there is an infinite number of possible parabolas that can be formed, as illustrated in Figure 1.

In general, there are an infinite number of t order polynomials that pass through the points if less than $t + 1$ coordinate points are known.All these polynomials are equally likely to interpolate the $t + 1$ coordinate points.

An overview of the scheme

Using the Shamir secret sharing scheme the secret passcode will be the constant of a randomly generated coefficients of a polynomial of the order $t - 1$ where t is the threshold number of shares. From this polynomial, n number of coordinates can be distributed to shareholders. When a threshold number of shareholders reveal their shares to a dealer, he can interpolate all the shares and recover the constant of the polynomial which is the passcode.

The Method

These are the following numbers to be defined initially. A secret number, S, the number of shareholders, n and the threshold number,t .The conditions are such that $0 < t \leq n$

Creating the polynomial

A polynomial in the form $y = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_{t-1}x^{t-1}$ has to be created by a dealer such that the values of $a = \{a_1, a_2 \ldots a_{t-1}\}$ are positive integers and random values. The value of t is the threshold number of shares required to recombine the secret. The value of a_0 is the secret code S. To create the shares, random values of $x_k = \{x_0, x_1, x_2, \ldots, x_n\}$ are generated where $x_k \in Z^+$. The values in x_k are evaluated $f(x_k)$ to create the coordinates $(x_k, f(x_k))$. These coordinates which are the shares are distributed to shareholders for them to keep.

In order to recombine the shares to reveal the original secret, at least t number of shareholders have to present their shares to the dealer. The dealer uses the Lagrange interpolation polynomial to find

out the polynomial,$M(x)$ connecting all the points. Since the secret is the constant in the polynomial, the dealer evaluates $M(0)$ to reveal the secret.

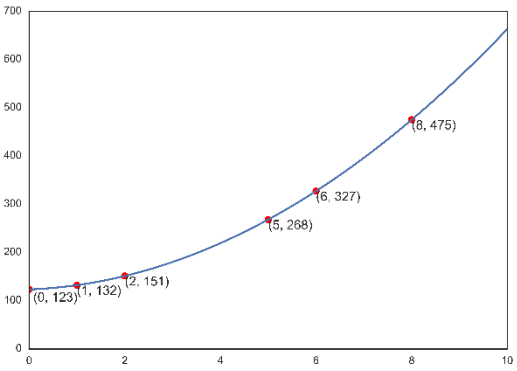
A real implementation

For this example the secret will be 123, there will be 5 shares created and a threshold of 3 shares to recreate the secret.

Creation of shares

In this case the randomly generated polynomial will be $f(x) = 123 + 4x + 5x^2$. Note that the constant is the secret. The randomly generated x_i values will be $\{5, 8, 1, 2, 6\}$. As the dealer I evaluate the values of $f(x_i)$ to create the shares. The shares are therefore (5,268), (8,475), (1,132), (2,151) and (6,372). These shares are distributed to share holders. The points have been plotted figure 2 for reference.

Figure



From James' point of view, he is both the dealer and the shareholder. He creates the shares and deposits the shares at different locations.

Recovery of secret

Let's say that three shareholders present their shares (8,475), (1,132) and (2,151) to a dealer. As the dealer I take the three shares and interpolate the points using the Lagrange interpolation polynomial. The Lagrange interpolation polynomial is a faster and better way of interpolating the points instead of manually manipulating a system of equations as done before. The Lagrange interpolation polynomial is as follows:[4]

$$M(x) = \sum_{i=1}^{n}\left(\prod_{j=1\ i\neq j}^{n}\frac{x-x_j}{x_i-x_j}\right)\bullet y_i$$

Where $(x_k, f(x_k)) = (x_k, y_k)$ and n is the number of coordinate points.

An explicit expansion of the polynomial is as follows:

$$M(x) = \left(\frac{x-x_2}{x_1-x_2}\times\frac{x-x_3}{x_1-x_3}\times\cdots\times\frac{x-x_n}{x_1-x_n}\right)\bullet y_1$$

$$+\left(\frac{x-x_1}{x_2-x_1}\times\frac{x-x_3}{x_2-x_3}\times\cdots\times\frac{x-x_n}{x_2-x_n}\right)\bullet y_2$$

$$\vdots$$

$$+\left(\frac{x-x_1}{x_n-x_1}\times\frac{x-x_2}{x_n-x_2}\times\cdots\times\frac{x-x_{n-1}}{x_n-x_{n-1}}\right)\bullet y_n$$

In this unique case here is the usage of the Lagrange polynomial to find the polynomial connecting the coordinates.

[4] Lagrange Interpolating Polynomial. (n.d.). Retrieved March 27, 2016, from http://mathworld.wolfram.com/LagrangeInterpolatingPolynomial.html

$$Z(x) = \left(\frac{x-x_2}{x_1-x_2} \times \frac{x-x_3}{x_1-x_3}\right) \bullet y_1 + \left(\frac{x-x_1}{x_2-x_1} \times \frac{x-x_3}{x_2-x_3}\right) \bullet y_2 + \left(\frac{x-x_1}{x_3-x_1} \times \frac{x-x_2}{x_3-x_2}\right) \bullet y_3$$

$$Z(x) = \left(\frac{x-1}{8-1} \times \frac{x-2}{8-2}\right) \cdot 475 + \left(\frac{x-8}{1-8} \times \frac{x-2}{1-2}\right) \cdot 132 + \left(\frac{x-8}{2-8} \times \frac{x-1}{2-1}\right) \cdot 151$$

$$Z(x) = 5x^2 + 4x + 123$$

This series of operations yields $Z(x)$ which the same as $f(x)$. The original secret,123,is the constant and can be readily calculated by evaluating $Z(0)$.

There is a major security problem with this method. The problem can be solved by limiting the values to a field p.

The security problem

The main issue is that the intruder is able to get a lot of information of the secret code with less than the threshold number of shares. Let's say an intruder manages to get his hands on two shares (8,475) and (1,132). It is publicly known that the threshold,t, is 3. From that he can deduce that the polynomial will take the form $Z(x) = a_0 + a_1 x + a_2 x^2$.

The intruder can fill $Z(x)$ with the values of (x_k, y_k):

$$Z(8) = a_0 + a_1(8) + a_2(8)^2 = 475 \text{ —①}$$

$$Z(1) = a_0 + a_1(1) + a_2(1)^2 = 132 \text{ — ②}$$

The intruder can remove one unknown,a_0, from the equation by ① − ② :

$$7a_1 + 63a_2 = 343$$

Which is also $a_1 = \frac{343-63a_2}{7}$

It is known that both $a_1$and a_2 are elements of Z^+ .The intuder can therefore replace a_2 with $\{1, 2, 3, 4\ldots\}$ until a_1 becomes negative. This method allows the intruder to find out all the possible values of a_1 and a_2.

$$a_2 = 1 \Rightarrow \frac{343-63(1)}{7} = a_1 = 40$$

$$a_2 = 2 \Rightarrow \frac{343-63(2)}{7} = a_1 = 31$$

$$\vdots$$

$$a_2 = 5 \Rightarrow \frac{343-63(5)}{7} = a_1 = 4$$

Replacing a_2 with any integer greater than 5 will make a_1 negetive, which is outside the conditions for a_1. He has now found a set of 5 possible values for a_1 and a_2, one of which will certainly be the right combination.

Using this set of values the intruder is able to limit the number of choices for the secret code.Substituting one pair of a_1 and a_2 values into ① allows the intruder to find the corresponding value of a_0:

$$Z(1) = a_0 + 40(1) + 1(1)^2 = 132$$

$$a_0 = 91$$

Now that the intruder has one value of a_0 that he can try and use it. In this case it is not the correct value of a_0.If it does not work, he can try another set of a_1 and a_2 values to eventually find out the actual secret number. This is a serious security issue.

In a more general perspective where there are more values of a, in other words, more coefficients for the polynomial, the intruder has more combinations of possible values of a that he can test. Given enough time and resources, the intruder is fully capable of trying all the combinations, thus revealing the secret.

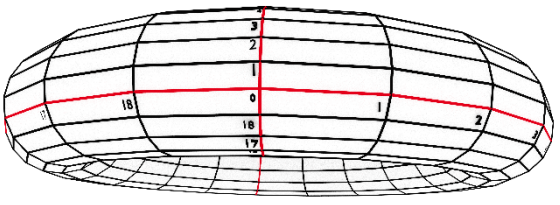
The Solution

The solution would be to limiting all the elements of the scheme to a finite field. The characteristic of the field should be a prime number p. As such, $t, n, S, a < p$



Finite fields can be understood to be similar to clock arithmetic. The number of hours in a 12 hour clock is limited to 12 hours. There are not more than 12 hours in a clock. The time 15 o clock does not exist. Instead, the equivalent time on the 12 hour clock is 3 o clock. In mathematical terms, 15 is congruent to 3 modulo 12. The notation for this relationship is $15 \equiv 3 \ mod \ 12$.

When utilising finite fields in two dimensions, it becomes a little more complicated. Clock arithmetic is limited to one single dimension because it requires only one coordinate to specify a point in the field. The Shamir secret sharing scheme requires a two dimensional plane that has both x and y values. Both the x and y values have to be limited to the field p. It is possible to visualise finite fields in two dimensions using a torus (see figure 3)[5]. In the figure, the Cartesian plane is wrapped around a torus. In this case, the x and y axis does not continue to infinity. Instead it goes back to zero when it reaches the last element in the field.



Figure

[5] Multiplicative inverses mod n. (2014, February 12). Retrieved January 10, 2016, from https://www.youtube.com/watch?v=_bRVA5b4sb4.Posted by user GVSUmath

In finite fields, the coordinates should be evaluated $\left(x_k, f\left(x_k\right) mod\, p\right)$ instead of $\left(x_k, f\left(x_k\right)\right)$.This limits the values of the coordinates to the field of size p.

The shares should be distributed as before to shareholders as $\left(x_k, f\left(x_k\right) mod\, p\right)$.

Unlike before, the dealer generates the shares from the equation $f(x) = 123 + 4x + 5x^2\, mod\, p$ using the x_i values $\{5, 8, 1, 2, 6\}$. The dealer selects a prime number p greater than S which is 313. The shares generated will then be $(5,\ 268)$, $(8,\ 162)$,$(1,\ 132)$, $(2,\ 151)$ and $(6,\ 14)$.

Now that all elements of the scheme are limited to a field, an intruder encounters a large obstacle in gaining information of the secret code despite knowing the values of a few shares. Let's say an intruder managers to get his hands on the shares $(8, 162)\ and\ (1, 132)$.

It is a fact that $p = 313$ and $t = 3$ are publically known. Using this information the intruder deduces that the polynomial will take the form $Z(x) = a_0 + a_1x + a_2x^2\, mod\, p \Rightarrow a_0 + a_1x + a_2x^2 - m_ip, m \in Z^+, p \in Prime$.He can substitute values from the shares he knows into the equation:

$$Z(8) = a_0 + a_1x + a_2x^2\, mod\, p = 162 \Rightarrow a_0 + 8a_1 + 64a_2 - m_1p = 162 \quad —①$$

$$Z(1) = a_0 + a_1x + a_2x^2\, mod\, p = 132 \Rightarrow a_0 + 1a_1x + 1a_2 - m_2p = 132 \quad —②$$

In the equations ① and ② there are total of 5 unknowns: a_0, a_1, a_2, m_1 and m_2.The only thing known about these unknowns is that they are all elements of Z^+ and are within the field p.

The intruder can attempt to remove one unknown a_0 as he would have done before by ① − ②.

This results in:

$$7a_1 + 63a_2 + p(m_2 - m_1) = 30$$

Which can also be expressed as:

$$a_1 = \frac{30 - 63a_2 - 313(m_2 - m_1)}{7}$$

If the intruder replaces a_2 with $\{1, 2, 3, 4 \ldots p\}$,he cannot stop because he does not know when $30 - 63a_2 - 313(m_2 - m_1)$ becomes negative.As such, the intuder finds nothing about the possible relationships between a_1 and a_2 so he does not gain any additional information by knowing less than the threshold number of shares.

Comments on the finite field

Finite fields remove the whole notion of the negative range. This is because any number that has a mathematical operation carried out on it will remain within the field of p,$\{1, 2, 3, 4 \ldots p\}$. As such, it is impossible to discriminate some combination of values of $\{a_1, a_2, a_3 \ldots a_{p-1}\}$ based on whether it is negative or not.

Things to take note of concerning p

The prime number p has to be large so that it is impossible to guess the values of $\{a_1, a_2 \dots a_{t-1}\}$ and the secret, S.It is known that $\{a_1, a_2 \dots a_{t-1}\}$ and the secret are all less than p.If the field p is small, all the intruder has to do is try and see which one of the values within the field p is the secret. Let's say that the secret is 123 and the characteristic of the field is 127(a prime). All the intruder has to do to find the secret is to try all 127 possible numbers$\{1, 2, 3 \dots 127\}$ and will be able to find the secret. It is not very difficult for an intruder to test such a small number of possibilities, especially if he as a computer to carry out the tests. It becomes a lot harder for the intruder if the size of field p is very huge. The larger the field p is, the wider the range of possibilities for the secret is. Even a computer may take too long to compute the different possibilities[6].

There is also a risk associated with using a field that is too big. If the size of field p is much greater than the values of $f(x)$, there is a high chance that $f(x)\ mod\ p\ =\ f(x)$. For example, if the value of p is 179426549 and the values of $f(x)$ are $\{10, 20, 30\}$,i.e. all within the range [1,100].Clearly, the value of p is much greater than $f(x)$. When evaluating the values of $f(x) mod\ p$, we find that the values are still $\{10, 20, 30\}$. Evaluating $f(x) mod\ p$ does not have any effect on the value of $f(x)$.The intruder can then assume that the values of m_i are zero so he removes it from the list of unknowns. Once again the intruder will be able to compute possible combinations of values for $\{a_1, a_2, a_3 \dots a_{t-1}\}$. This time the intruder knows that there is a high chance that one of the combinations is valid instead of being completely sure that one of the combinations will work.

Additional steps when recombining shares

The shares are recombined using the Lagrange interpolation polynomial that is done within the field. In practice, addition, subtraction, multiplication and division are done modulo p. The main difference from before is that division is not carried out. Instead the Modular multiplicative inverse of a number is multiplied. For example, when dividing a with b in a finite field, the Modular multiplicative inverse of b has to be found and then multiplied with a. Generally, the most efficient way of finding out the Modular multiplicative inverse would be to use the Extended Euclidian algorithm.

Interpolation techniques

When interpolating with the Lagrange polynomial within the finite field, all operations must also be done with modular arithmetic.

$$M(x) = \sum_{i=1}^{n} \left(\prod_{\substack{j=1 \\ i \neq j}}^{n} \frac{x - x_j}{x_i - x_j} \right) \cdot y_i$$

[6] Shamir Secret Sharing Scheme. (n.d.). Retrieved January 09, 2016, from https://en.wikipedia.org/wiki/Shamir's_Secret_Sharing

Note that instead of dividing $\left(x - x_j\right)$ with $\left(x_i - x_j\right)$, the multiplicative inverse of $\left(x_i - x_j\right)$ is found using the Extended Euclidean algorithm and multiplied with $\left(x - x_j\right)$. In addition, the coefficients of the recovered polynomial should be evaluated modulo p.

Recovering the secret in the finite field

Using the shares that were distributed, for this example, the shares $(1,\ 132)$, $(2,\ 151)$ and $(6,\ 14)$ will be used. The coordinates will be added to the lagrange interpolation polynomial to recover the polynomial connecting the three points. This time, all the mathematical operations will be done within the field $p = 313$. This time, for simplicity sake,the polynomial will be evaluated $f(0)$. The secret is only in the constant of the polynomial so it is unnecessary to find out the whole polynomial.

$$Z(0) = \left(\frac{0-2}{1-2} \times \frac{0-6}{1-6}\right)\cdot 132 + \left(\frac{0-1}{2-1} \times \frac{0-6}{2-6}\right)\cdot 151 + \left(\frac{0-1}{6-1} \times \frac{0-2}{6-2}\right)\cdot 14$$

$$Z(0) = \left(\frac{1584}{5}\right) + \left(\frac{906}{-4}\right) + \left(\frac{28}{20}\right)$$

In order to limit the whole equation to the field size p,the modular multiplicative inverse of the denominators 5,-4 and 20.

Finding the multiplicative inverse

For the sake of simple explanation, small numbers will be used to illustrate the steps for finding the multiplicative inverse of a number. Suppose we need to find the multiplicative inverse of $\frac{1}{8}$ in a field of 11.We are looking for a number that x that when multiplied by 8, will result in a number that is equal to 1 in a field of 11.When you multiply 8 by x and divide it by 11, the remainder is supposed to be equal to 1. One way to find out x will be to list out a list of products of a list of values of x and 8 and see which one will result in 1 in the field of 11. This is shown in the following table.

x	1	2	3	4	5	6	7	8	9	10
$(x\times 8)\ mod\ 11$	3	5	2	10	7	4	1	9	6	3

From the table we can see that the value $x = 7$ results in the value 1 in the field 11.

This method of listing out all possible values of will surely be too slow if the value of x is large. If x is more than 1000, it will take a very long time to try out all the values of x. There is a much quicker way of finding out the value of x, the multiplicative inverse.

Using the extended Euclidean algorithm

We will have to find the greatest common divisor of the two numbers 8 and 11 using the extended Euclidean algorithm. The multiplicative inverse can be found in the process of using the extended Euclidean algorithm.

In order to find the multiplicative inverse, the prime number,11, is divided by 8 and presented in the following manner:

		Quotient		Dividor		Remainder	
11	**=**	**1**	**×**	**8**	**+**	**3**	--Line 1

Then from line 1,I take the Dividor and divide it with the remainder from Line 1

		Quotient		Dividor		Remainder	
8	**=**	**2**	**×**	**3**	**+**	**2**	--Line 2

Then from line 2,I take the Dividor and divide it with the remainder from Line 2

		Quotient		Dividor		Remainder	
3	**=**	**1**	**×**	**2**	**+**	**1**	--Line 3

We now have to “work backwards”

We rearrange line 3:

$1 = 3 - 2\times1$ –(i)

We know that the value 2 in (i) is equal to $8 - 2\times3$ from line 2.

We substitute this into equation (i) to get:

$$1 = 3 - (8 - 2\times3) \times 1$$

Which is

$$1 = 3\times3 - 8 \quad -(ii)$$

We know that the value 3 in equation (ii) is equal to $11 - 8(1)$ from line 1.

We substitute this into equation (ii) to get

$$1 = 3(11 - 8\times 1) - 8$$

Which is

$$1 = 3\times11 - 8\times4 \quad -(iii)$$

We rearrange (iii) to form:

$$1 - 3\times11 = -8\times4$$

When we evaluate modulo 11 both sides of the equation,

$$(1 - 3\times11) mod\ 11 = (-4\times8)\ mod\ 11$$

$$1\ mod\ 11 = 7\times8\ mod\ 11$$

We have found that multiplying 8 with 7 within the field 11, we get the 1. The multiplicative inverse of 8 is 7. This has been confirmed in the table above.

In a similar manner,in order to recover the secret, I find the multiplicative inverse of the numbers $5, -4$ and 20 in the field of 313. The multiplicative inverses of $5, -4$ and 20 are $188, -235$ and 47 respectively.These values can be substituted into the polynomial $Z(0)$

$$Z(0) = (1584\times188) + (906\times -235) + (28\times47)$$

$$Z(0) = 86198\ mod\ 313$$

$$Z(0) = 123$$

As shown the original secret has been recovered.

Extensions of the Scheme

This whole exploration has exclusively dealt with integers. Imagine if James had a secret that was in text form, such as the name of the place where he has locked his money away, he will be unable implement the secret sharing scheme on his secret. This can be easily resolved if the text is converted to a numerical form. The easiest form will be in the widely used ASCII encoding format. Essentially, according to the ASCII standard, every letter in the alphabet has a binary code such as

1010101. James can covert the name of the place to the ASCII format. Most computer systems will readily be able to convert this binary code back to readable letters. The good thing about the binary codes is it can be manipulated as if it is number. The key difference here is that all the manipulations have to be carried out with a base 2 field instead of a base 10 field.

Other applications of the Scheme

The Shamir Secret Sharing Scheme can be utilised in many other areas.

For example, if a bank director want a minimum of 4 employees to cooperate to open the bank vault, he can give shares of the bank vault's passcode to all trusted employees. If and only if at least five employees present the shares can the bank vault's passcode be recovered. This prevents single or small groups of employees from cheating and misusing the vault while acting alone.

The additional benefit of the scheme is it can be applied in a hierarchical context. The bank director can distribute more shares to people of greater importance within the organisation, such as the board members and less shares to the low level employees. This allows less people from higher up in the organisation to be required in opening the vault. For example, board members with two shares each would need to cooperate with only one other board member. On the other hand, lowly clerks with one share each would need to cooperate with three others to meet the threshold of 4 shares to open the vault.

Another area would be in voting. On voting day, the votes of individuals is very crucial. Any exclusion of votes from the general tally could shift the balance in an election. Authorities usually transmit the votes to a central collation location through multiple channels. In order to prevent the loss of voting data due to transmission failure or interception by third parties, authorities can create a scheme where shares of this voter data are transmitted through multiple channels. Even if a few channels fail, the information can be transmitted.

Weaknesses of the Shamir Secret Sharing scheme

So far it has been proven to be utterly impossible to recover the secret if an intruder has less than the threshold number of shares. Following all the conditions for construction of the scheme will ensure that. This means that the coefficients of the polynomial must be truly random, all the calculations must be limited to the field and so on. The problem arises when some of these conditions are not met.

Introduction of fake shares

An intruder may introduce shares that are wrong when recovering the original secret. This is of particular importance if the secret is in binary form. There might be only two parties in a particular constituency so there can be only two possible votes. If the intruder changes some of the shares en route to the central collation location, it might cause the wrong value of the secret to be calculated. This might be a serious problem if it changes some of the votes in favour of one party. In general, the intruder is able to change the secret by introducing fake shares. There are a number of ways of

detecting fake shares that have been developed since, such as using Solomon-Reed error correcting codes.[7]

Issue of randomness

The question is how random are the coefficients of the polynomials? By definition, the random coefficients should be utterly unpredictable and must have absolutely no intelligible pattern or combination[8]. If the values of the coefficients can be predicted then it is not secure at all as an intruder has to just find the pattern linking the coefficients to find out the coefficients that he does not know. The randomness of coefficients is a cause for concern when generating the values of coefficients with a computer.

A conclusion

The Shamir Secret Sharing scheme is largely very secure as long as the initial conditions are strictly met. Failure of this scheme is only caused by incorrect implementation of the scheme. Perfect security of the scheme is guaranteed as long as the secret itself cannot be guessed or takes very long to try all possibilities. For additional security, the dealer may periodically regenerate new shares and distribute to all shareholders. In James's case, he can regenerate the shares and store them in different places every 6 months or so and destroy the old ones. An intruder cannot get his hand on anymore shares from the old set, and has to start all over again to collect the new set of shares.

[7] Harn, L., & Lin, C. (2009). Detection and identification of cheaters in (t, n) secret sharing scheme. *Designs, Codes and Cryptography*, *52*(1), 15-24.

[8] Randomness. (n.d.). Retrieved January 10, 2016, from https://en.wikipedia.org/wiki/Randomness

Bibliography

1. Hern, A. (2013, November 27). Missing: Hard drive containing Bitcoins worth £4m in Newport landfill site. Retrieved March 27, 2016, from http://www.theguardian.com/technology/2013/nov/27/hard-drive-bitcoin-landfill-site
2. Private key. (n.d.). Retrieved March 27, 2016, from https://en.bitcoin.it/wiki/Private_key
3. Shamir, A. (1979). How to share a secret. *Communications of the ACM*, *22*(11), 612-613.
4. Shamir Secret Sharing Scheme. (n.d.). Retrieved January 09, 2016, from https://en.wikipedia.org/wiki/Shamir's_Secret_Sharing
5. Lagrange Interpolating Polynomial. (n.d.). Retrieved March 27, 2016, from http://mathworld.wolfram.com/LagrangeInterpolatingPolynomial.html
6. Multiplicative inverses mod n. (2014, February 12). Retrieved January 10, 2016, from https://www.youtube.com/watch?v=_bRVA5b4sb4.Posted by user GVSUmath
7. Wagner, D. (n.d.). CS276,Lecture 4.14.04.,Spring 2004. Lecture. Retrieved December 30, 2015, from http://www.cs.berkeley.edu/~daw/teaching/cs276-s04/22.pdf
8. Harn, L., & Lin, C. (2009). Detection and identification of cheaters in (t, n) secret sharing scheme. Designs, Codes and Cryptography, 52(1), 15-24.
9. Randomness. (n.d.). Retrieved January 10, 2016, from https://en.wikipedia.org/wiki/Randomness

Image sources

1. Sienicki, T. (2010, January 2). Quartz watch ubt EXP 123. Retrieved March 28, 2016, from https://commons.wikimedia.org/wiki/File:Quartz_watch_ubt_EXP_123.JPG