Encryption

Daan Snoeken

July 2020

1 Encryption

Let's say we have a random string we want to encrypt:

```
Daan Snoeken
```

We can convert this into numbers according to the ASCII table and to make sure we always have 3 digits for each character, we add 101 to the value of each character. However, we may also pick larger numbers to add. Next we concatenate all the numbers we get in order. This will give us the following number:

$$a_0 = 169198198211133184211212202208202211. \tag{1}$$

Now consider the following first degree polynomial,

$$y = a_0 + a_1 x \tag{2}$$

and note that the value of a_0 is the same in eq. 2 as in eq. 1. Next, pick a random value for a_1 and find two points at e.g. $x = 1$ and $x = 2$ that lie on this line. These will be your encrypted numbers. Only somebody who knows both numbers can figure out what the original number a_0 was that you started with. This can of course be extended to higher order equations, e.g.

$$y = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n. \tag{3}$$

Note that for a polynomial of degree n, we need (at least) $n+1$ points to describe it. In all cases, a_0 needs to be the original number (eq. 1) and all the others can be picked at random. As was done with the linear equation, pick random x values for every point and solve equation 3 for each x value and save the output. Now you can store every number on a separate location and only when someone has all the numbers, will they be able to solve the original message. So, if you and your friend have a secret, you can do this and give one number to your friend. Then keep one number yourself. Now neither of you can decrypt the message on your own, but you can solve it when you are together.