Cryptography: Using Mathematics to Secure the Digital World

What is cryptography?

Cryptography is the science of protecting information by converting it into a form that cannot be understood by third party readers. This is done by using mathematical algorithms and techniques. Cryptography works by converting readable information (known as plaintext) into a form that can only be understood by the intended readers (known as ciphertext) by using encryption. A key can be used to decrypt the ciphertext back into plaintext so that it can be understood. The mathematical techniques involved in cryptography include algebra, number theory, statistics and linear algebra.

Basic mathematical techniques involved in cryptography

Affine cipher and Caeser cipher

There are many mathematical techniques used in cryptography, one of the simplest being the Caesar cipher in which each character in the plaintext is shifted along the alphabet by a fixed number based on the position.

For example, APPLE having a shift of 3 places for each character would end up with DSSOH.

Another cipher method includes the Affine cipher where the equation [(ax+b) mod 26] is applied (mod 26 meaning the remainder after dividing the value by 26) in which each letter of the plaintext is converted to a number based on its position in the alphabet (for instance A would be 0, B would be 1 and Z would be 25). Then, this value would be substituted in for x in the equation. Next, any random values of a and b can be chosen but the same values must be used for each character in the plaintext. The equation is then applied and the product value would be divided by 26 and the remainder left over would be converted to the specific letter that lies in that position in the alphabet (for instance if the remainder is 4 then this would be converted to the letter E because the position of E in the alphabet is 4).

More complex mathematical operations involved in cryptography

RSA encryption (with an example)

Furthermore, many of these examples are no longer used for modern methods of protecting information in cryptography because they are highly vulnerable to online attacks as hackers can easily break them, however, one of the most practical operations includes RSA encryption which is still very popular today since it is far harder to break. This involves using 2 keys, including a public key that anyone can use for encryption and a private key that only the receiver can use to decrypt the ciphertext information. The public and private key can be generated from the product of 2 prime numbers.

The method involves picking 2 large prime numbers, p and q (for example 61 for p and 53 for q) and then calculating the product of these 2 prime numbers (which in this case would be n=3233) and setting n = the product of the primes. Next, the

variable ϕ(n) (Euler's totient function) is used to calculate the number of integers less than or equal to the value of n that are coprime to n, this is done by using the equation ϕ(n)=(p-1) (q-1) (which is 3120 in this example). After, a variable e is used to pick a random number that is coprime to the value of ϕ(n) (use 7 for the value of e in this case since 7 is coprime to 3120). The following step includes multiplying e with a value d in which the mod of this product with the value of ϕ(n) equals 1. So, the equation would be ed mod ϕ(n)=1 (7d mod 3120=1 in our example). To find the value for d, we can use the Extended Euclidean Algorithm method where the equation can be rearranged to get ed + ϕ(n)k = 1 (7d+3120k=1). Using the example, the next step would be to do 3120/7= 445 remainder 5, and 7/5= 1 remainder 2, and 5/2= 2 remainder 1. In the first step the value of ϕ(n) was divided by the value of e and the remainder was calculated, then e was divided by the remainder to get a new remainder, and the original remainder of the first equation was divided by the new remainder to get a remainder of 1. Essentially, this step involves continually dividing by the new remainder until a remainder of 1 is produced. The overall mathematics involved in this step would therefore be:

1. 61*53=3233 n=3233
2. ϕ(n)= 60*52 ϕ(n)=3120
3. e=7 (7 coprime to 3120)
4. ed mod ϕ(n)=1
5. 7d mod 3120k=1
6. 3120/7=445 remainder 5
7. 7/5=1 remainder 2
8. 5/2=2 remainder 1

The steps 6-8 can be rearranged to form these 3 equations:

1. 3120= 7*445 +5
2. 7= 5*1 +2
3. 5= 2*2 +1

After this, the method is to work backwards from 1 to eventually find the value of d. This step includes, by using the example again, rearranging the 3rd equation, 5=2*2 +1 to solve for 1 which would be 1= 5- 2*2.

The 2nd equation 7= 5*1 +2 can then be rearranged to solve for 2 which is 2= 7-5.

This value can then be substituted into one of the values for 2 in the 3rd equation 1= 5-2*2 to get 1= 5-2(7-5) and the brackets must then be expanded to get 1= 5-2*7+2*5 which can be simplified to 1= 3*5-2*7.

Next the 1st equation can also be rearranged to solve for 5 to get 5= 3120-7*445 which can then be substituted for the value of 5 in the equation 1= 3*5-2*7 to get 1= 3*(3120-7*445)-2*7 which simplifies to 1= 3*3120-1337*7.

Now, this expression is in the same form as the original needed to calculate the value of d which is 7d mod 3120=1, the general expression being ed mod ϕ(n)=1 from earlier. To solve for d, you must apply the mod 3120 to 3*3120-1337*7, however the value of 3*3120 would cancel out because the remainder when dividing any multiple of 3120 by 3120 would be 0. This therefore leaves 1= -1337*7 mod 3120. By comparing this to 1= ed mod ϕ(n) I can see that 7 correlates to the value of e and therefore d is -

1337. To get the positive value of d we can simply do $\phi(n)+(-1337) = 1783$ and 1783 is therefore the final value for d.

This method avoids using trial and error to calculate the value for d and instead using a mathematically rigorous method. The final steps involve using the equation $C=M^e \bmod n$, which is the equation for the public key encryption. In this equation M is the value of each character in the plaintext (for example if we were to use the letter A, this has the ASCII value 65 which would produce a value of 2790 for c which is the value of the cipher text) to produce ciphertext by using the equation. To decrypt the ciphertext back into plaintext the equation $M=C^d \bmod n$, is used (with the example $2790^{1783} \bmod 3233$ producing the original value of 65), to reverse the encryption and therefore convert back to plaintext.

This overall involves using a very secure method using complex keys to protect the information and is far safer since it is extremely difficult to reverse the processes that have just been completed by hackers which keeps sensitive information well protected.

ECC encryption

Another modern method of cryptography is the use of ECC (Elliptic curve cryptography) which uses points on an elliptic curve (curve that is symmetrical along the x axis containing points which satisfy the equation $y^2=x^3+ax+b \bmod p$) to generate a pair of public and private keys for encryption and decryption. In this method, a random and fixed coordinate is chosen (x, y) from the curve.

The private key is a random integer that is quick and easy to generate that shouldn't be told to anyone else that shouldn't understand the data (for example we can use k to represent any integer).

To get the public key, there is a more complex method involved in which we use the equation $Q=k*G$ where Q is the public key, k is the private key and G is the starting point on the curve. This method doesn't actively involve calculations however, instead we use the elliptic curve and start at a point G and then draw a tangent line and find where this intersects the elliptic curve and then reflect this point to add G back to itself and keep repeating this process until you have manually added G to itself k amount of times. This can be done via differentiation to get the formula for the gradient of an elliptic curve.

Firstly, if we use k as 2, use mod 17 and pick a random coordinate (5,1). $ is the slope.

Calculate the slope using the equation: $\$= [3x^2+a]/2 \bmod 17$.

Next, plug in the values: $\$=[3(5)^2+2]/2 \bmod 17$ to get $\$=77/2 \bmod 17$

To calculate the value of $ we use modular arithmetic, $\$=77*(2^{-1} \bmod 17)$ we must find a value such that $2*x \bmod 17 = 1$ (finding the inverse of 2 mod 17) which would be $x=9$ since $2*9=18$ and $18/17= 1$ remainder 1.

Multiply: $77*9 \pmod{17} = 13$

Next, we use the equation for the new value of x on the graph (new value for G) which is $x_n=\$^2-2x \pmod p$ where x_n is the new value for x on the curve.

Substitute values: $x_n=13^2-2(5) \bmod 17$

159 mod 17= 6= x_n

Then, we use the equation for the new value of y on the graph which is y_n=$(x- x_n)-y (mod p) where y_n is the new value for y on the curve.

Substitute values: y_n=$(5-6)-y (mod 17)

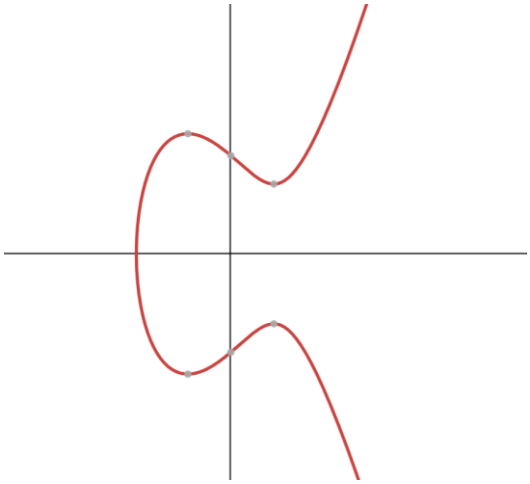
5-6=-1 and -1 mod 17=16

Multiply $ by the value: y_n=(13*16)-y (mod 17)

208 mod 17=4

Substitute y=1: y_n=4-1 so y_n=3

So overall the coordinate of the public key for the private key of k=2 is (6,3).



Finalising the safety in cryptography

Both RSA and ECC encryption methods are examples of one-way functions which are functions that are simple to calculate but very complex to reverse which makes them very essential in data security. A function is represented as y=f(x) and is normally one way in which an input value for x is used to determine a value for y however, given a value of y it is computationally difficult to determine the value for x. This overall makes these 2 methods along with many other methods very safe procedures in cryptography.