Mathematics and Cryptography.

Mathematics and cryptography, which is the encoding and decoding of secure information, are an inseparable pair. In this essay, I will explain modular arithmetic, and how it ties into the Diffie Hellman key exchange and end to end encryption used by secure messaging services such as 'Signal Messenger.'

To explain modular arithmetic, I will start by explaining it mathematically. It is looking at the remainder from the addition required to get to the given fixed quantity, for example '9 + 6 = 12 remainder 3 meaning 9 + 6 = 3 mod12'.

Another way of explaining it would be by imagining a 12-hour analogue clock. From nine O'clock to three O'clock you would add six hours. Therefore '9+6 = 3 mod 12'. To summarise in modular arithmetic the number wraps around the given fixed quantity (in my example 12 but it can be replaced with any number).

Another necessary explanation for the Diffie Hellman key exchange, which is later in the essay, is co primes of the given fixed quantity as well as primitive roots. These are necessary for explaining the Diffie Hellman key exchange later in the essay. Let's suppose you were to choose modular 5. The co primes are numbers that are only divisible by one or themselves in that set so: 2 and 3 as 4 is divisible by 2 and is therefore not prime. As for the primitive roots, the number 'α' is a primitive root of a prime number or 'p' if α^1 to α^{p-1} are distinct or evenly distributed. For example, two is a primitive root of 5 as the products are evenly distributed as: 2, 4, 3 and 1. Comparatively, one is not a primitive root of 5 as it is not evenly distributed, and all the numbers are 1.

In the introduction, I mentioned end to end encryption. I am going to clarify what that is before continuing to the mathematics of the Diffie Hellman key exchange.

Suppose you wanted to send a message with sensitive information, such as credit card information or details of a location you want to meet a friend. You wouldn't want your message to be looked at by anyone, especially not a criminal (or even worse a member of the Government) who wants your information or to attack you.

This issue arises, when you send an email it is encrypted and then decrypted at the server and then encrypted again and then it gets to the recipient. This has the clear security flaw of the decrypted information being available outside of the hands of those directly involved in the communication.

So, with end-to-end encryption, you can have a key (something that is used to encrypt and decrypt) and your friend can have a key meaning only you can access your messages (no pesky criminals or Government officials getting involved in your affairs). But this leads to the issue: how do you get your keys to each other? And this is where the Diffie Hellman key exchange gets involved.

The Diffie Hellman key exchange as a short explanation is, when you have two public items in a domain the modular number or 'n' and a small co prime or 'g.' Then two people (let's name them Alice and Bob) have their own private keys (let's name them a and b). Alice and Bob would then combine their private keys with g to produce ag and bg. They would then send those to each other, at which point they would combine their private key with either ag or bg producing two lots of abg. This then gives them access to their private key without other people getting into their business.

To explain the Maths, I will re-visit some of the terms used in the previous paragraph. In the public domain, which means potential hackers can see the information, there are two pieces of information 'modular: N' or just 'N' (which would be a huge prime number in the real world but for simplicity's sake I am going to call mod11) and there would be a small primitive root (which in our case for simplicity's sake we will call 7). Then in the private domain, you and a friend or an acquaintance would pick a random number from the group privately, so the only person who knows your number is you – not even your friend knows it and vice versa. Let's call those two numbers a (your number) and b (your friend's number). For explanation's sake, we will say your number (a) is 2 and your friend's (b) is 4, but it is important to remember the only person who knows your number is you.

You would then take g (in our case 7) and raise it to the power of your secret number with your friend doing the same so now you have on your side, g^amod11 (7^2) and on your friend's g^bmod11 (7^4). Which then leaves you with 5mod11 on your side and 3mod11 on your friend's side. You would then send your friend 5mod11 and you would receive 3mod11. You would then raise your received information (3mod11) to the power of your private number: amodn. Your friend would do the same so you both end up with g^{ab}modn. In our case this would result in you getting the product 9. That way you both end up with the same key without having to transfer the key itself.

The reason this is so secure, even in our simplified example if a potential attacker, let's call her Eve, wanted to figure out what a and b are, she would have to identify the numbers that result in 5mod11 and 3mod11, respectively. To do this she would have to list the numbers, which is incredibly slow. In a real scenario where modN is an incredibly large number it would take so long that you, your friend, and Eve would probably be dead before she determined your secret numbers.

This is also difficult for computers to do due to something called the discrete logarithmic problem. Which means the Diffie Hellman key exchange is secure even when attempted to be broken by a computer.

To conclude, maths and cryptography, in our case modular arithmetic and the Diffie Hellman key exchange, however there are many more examples, work together. By understanding maths you can understand cryptography. This allows you to understand how your information is protected and gives you an insight into how the digital world around you works, which is truly remarkable.