Atentos a la situación, una persona A, llamemosla Alice quiere mandarle un mensaje a una persona B, dígamosle Bob, y pasa que Alice no se fía y piensa que alguien puede estar espiándolos, y efectivamente a medio camino está Eva.

Si Alice manda algo a Bob, Eva lo va a interceptar y su privacidad no estará a salvo. ¿Que puede hacer Alice para mantener en secreto su mensaje? Es necesario que Alice lo modifique para que solo Bob y ella puedan entenderlo, es decir, tiene que encriptarlo.

Hay muchas formas de hacerlo, desde desplazar las letras en el alfabeto **(Cifrado Cesar)**, hasta incluso usar física cuántica, pero esta vez vamos a hablar de uno de los más seguros y usados, el método RSA.

Con este, si Alice quiere mandarle algo a Bob, Bob le da una caja para la cual sólo él tiene la llave, ella mete su mensaje ahí y se lo manda. Esta caja es lo que se conoce como una clave pública, mientras que la llave es una clave privada.

Pero, ¿Cómo es que se crean estas claves?

Para eso tomamos 2 números primos, en este ejemplo van a ser 5 y 11, pero normalmente suelen usarse números de cientos de dígitos de longitud. llamaremos “p” al 5, y “q” al 11.

Luego los multiplicamos y al resultado lo llamamos “n”, en este caso, vale 55, porque 5 por 11 son 55.

Ahora necesitamos saber cuántos números enteros positivos menores o iguales a “n” son coprimos con este, es decir en los que el máximo común divisor es 1. Para eso usamos la función fi de Euler, la cual dice que tenemos que restarle 1 a “p” y a “q” y multiplicar los resultados entre sí. En este ejemplo, esto da 40, un número al cual llamaremos “fi”.

Lo siguiente es conseguir un número entero menor a “fi” que sea coprimo con este, 7 nos sirve, y a partir de ahora lo vamos a llamar “e”.

Lo que sigue es crear las claves, la primera es la pública, que se forma con “n” y “e”, colocando esos números así: **(n,e)**, que en este caso sería: **(55,7).**

Ahora toca hacer la privada, y para eso usamos la fórmula ,
donde “k” es un número entero cuyo valor aumenta en 1 con cada ciclo, es decir, que primero vale 1, luego 2, después 3 y así va hasta que el resultado sea un entero. En este caso, el valor de k debe ser 4, lo cual hace que el resultado sea 23.

Finalmente, para formarla, usamos “n” y “d”, colocando los números así: **(n,d)**

Estas van a ser las claves de Bob **(mostrar “pública=(55,7), privada=(55,23)”)**

Ahora regresemos al ejemplo del principio, Alice quiere enviarle algo a Bob, una “c”, por ejemplo.

Primero toma esa “c” y le asigna un número, por comodidad 3, que es su posición en el alfabeto.

Luego toma ese número y lo usa para aplicar la siguiente fórmula $a = c^{e} \, mod \, n$ , dónde módulo es el residuo de dividir $C^{e}/n$ , en este caso se vería algo así $3^{7} mod \, 55$ , lo cual da como resultado 42, este número es lo que se conoce como un valor encriptado.

Este valor encriptado es básicamente el mensaje de Alice luego de meterlo a la caja que Bob le dió.

Luego, si Bob quiere recuperar el mensaje original, simplemente tiene que usar esta otra fórmula $b = a^{d} \, mod \, n$ , con lo que va a conseguir el 3 que Alice le quería enviar.

Supongo que alguno de ustedes pensarán, ¿Pero no es fácil para una compu simplemente probar un montón de números hasta encontrar el que es y así conseguir la información?
Pues resulta que no, ya que para eso tendría que descifrar “p” y “q”, números que normalmente suelen tener 617 dígitos cada uno.

Cada número tiene $10^{617}$ combinaciones posibles, y considerando que son dos números con la misma cantidad de dígitos se puede deducir que $10^{617^{2}} = 10^{1234}$ es la cantidad de combinaciones posibles, un número absurdamente grande incluso para una computadora, y lo peor de todo...es que solo una de esas combinaciones es la correcta.

Así que aún si Eva tuviera una computadora 10000 veces más potente que una de escritorio común y corriente, de todas formas le tomaría miles de millones de años conseguir la clave correcta...y para ese momento, pues para qué si Alice y Bob...y Eva, habrán muerto hace mucho

¿Pero qué tal si Eva consigue una computadora que sea capaz de descifrar esos números rápidamente? pues fácil, ¡Los hacemos más grandes y listo!

Con incrementar la cantidad de dígitos de cada número a los 1233, las combinaciones subirían a los $10^{2466}$ , lo cual es miles de millones de veces más difícil de descifrar...y puede que me esté quedando corto.

No importa qué tan buena sea la computadora de Eva, siempre habrán números más grandes que se puedan usar. Y eso es algo completamente comprobable al resolver esta integral

$$\operatorname{Li}(x) = \int_2^x \frac{dt}{\ln t}$$

cuyos pasos están disponibles en el siguiente link :https://docs.google.com/document/d/1Jr_67kOkyIaNa9XsiDo1WsrSlke1Kf7Px0Z1B48cNAM/edit?usp=sharing

Y bueno, hemos llegado al final de este vídeo, si te gustó, porfa haz click en el botón ...oh, plataforma equivocada XD