Colegio Inmaculado corazón
de María (Portaceli).

1ª EDICIÓN GROW-LAB EC2CE

PROYECTO: END

De cifras a secretos

Un viaje por la historia de la criptografía. Desde sus comienzos más primitivos, pasando por la complejidad del sistema RSA hasta la tecnología más innovadora.

Componentes:

Alfaro de Prado Martín, Antonio
Marín Maqueda, Antonio
Suarez Toribio, Juan
Zambrano Salas, Elena

Tutor:

Jiménez Ruiz, Juan José

Área de participación:
Matemáticas aplicadas

1 INTRODUCCIÓN

1.1 ¿Quiénes somos?

Somos un grupo de cuatro alumnos del colegio Portaceli en las ramas de salud y tecnología. El colegio nos seleccionó como uno de los grupos participantes en este proyecto ofrecido por la empresa ec2ce. Hemos estado trabajando unidos en el proyecto durante el curso. Dividimos el trabajo según nuestras preferencias y facultades, y la parte importante, hemos compartido todo lo aprendido unos con otros con el fin de sacar a la luz este resultado que aquí presentamos.

1.2 Presentación

Había algo especial en ese tema. No teníamos muy claro de qué se trataba y sin embargo había algo en él que llamaba nuestra atención. Quizás fue lo poco que conocíamos acerca de él o quizás fue el reto de enfrentarnos a un proyecto tan complicado. Lo que está claro es que, cuando aquel martes a las 15:20 de la tarde, nuestro tutor sugirió la criptografía como uno de los posibles temas del concurso en el que todos aquellos “frikis” aspirábamos a participar, no dudamos en solicitarlo como primera opción.

Unas semanas más tarde nos enteramos de que habíamos sido elegidos para participar, y no solo eso, sino que también nos habían cedido el proyecto que habíamos pedido.

Con la ilusión aún en nuestros ojos nos pusimos manos a la obra y comenzamos a informarnos de qué iba todo aquello. En los meses siguientes nos reunimos una y otra vez y nos empapamos de toda la información a la que pudimos acceder: libros, artículos, vídeos, proyectos, preguntamos a profesores acerca de las dudas que no éramos capaces de resolver e incluso acabamos asistiendo a conferencias sobre el tema algún que otro viernes por la tarde.
Muchos hubiesen considerado esto un auténtico suplicio, pero lo cierto es que nosotros lo disfrutamos como críos. Es verdad que no todo fue un camino de rosas, hubo muchas cosas que se nos atascaron y problemas que parecían imposibles de solucionar, pero con dedicación y mucho, mucho esfuerzo conseguimos hacerle frente a todos y cada uno de ellos.

A fin de cuentas, es cierto que el trabajo nos ha llevado mucha dedicación y momentos de frustración, pero sin duda la satisfacción de solucionar los problemas que tantos dolores de cabeza nos han provocado, todo lo que hemos aprendido sobre la materia así como el reto de enfrentarnos a un proyecto de esta magnitud nosotros solos y los momentos que hemos compartido hacen que todo el esfuerzo valga la pena.

Esperemos que disfruten nuestro trabajo y ¿quién sabe? Tal vez puedan aprender algo. Puede que nunca lleguemos a saberlo todo, pero pensamos que siempre es un placer seguir aprendiendo y que, como muy bien se dice, nunca es tarde si la dicha es buena.

1.3 Objetivos

➤Aprender y dar a conocer la evolución de la criptografía a lo largo de la historia así como la gran importancia que tiene.

➤Estudiar el código RSA, las matemáticas de la teoría de números en las que se basa junto con las cualidades de los números primos y su obtención así como los algoritmos utilizados en la generación de claves, cifrado, y descifrado de mensajes.

➤Crear una simulación computerizada mediante algoritmos que generen claves gracias a los procesos utilizados en RSA con el fin de ejemplificar la materia estudiada generando las claves, cifrando mensajes y descifrándolos.

➤Exponer métodos futuros ya no tan lejanos con los que se podría revolucionar increíblemente la criptografía gracias al desarrollo de la tecnología y a los ordenadores cuánticos.

➤Desarrollar nuestras capacidades tanto individuales como grupales en el campo de las matemáticas y sobre todo en la capacidad de cooperación y coordinación para la realización del proyecto.

2 HISTORIA

2.1 Introducción histórica

Desde los albores de la civilización, el ser humano se agrupa para sobrevivir, pero debido a la imposibilidad de que toda la humanidad se juntase en una misma congregación surgen corporaciones diferenciadas en creencias, culturas y, por tanto, objetivos. Debido a la incompatibilidad de muchas metas llega un punto en el que solo una sociedad puede alcanzarlas, estallando la guerra. La cooperación es la base del éxito, y es imposible cooperar sin comunicación. Sin embargo, no resulta productivo emitir un mensaje de vital importancia que el enemigo sea capaz de interceptar e interpretar. De hecho, resultaría aún más interesante que el adversario creyese que esa información no ha podido ser transmitida.

Solo era cuestión de tiempo que se empezasen a desarrollar métodos para mantener a salvo la información secreta. Surgió así la criptología. La criptología es la ciencia que engloba todas aquellas técnicas dirigidas a la protección y a la encriptación de datos, así como al interceptado y decodificado de los mismos. Para esto se vale de cuatro disciplinas que van de la mano dos a dos, de tal forma que dos de ellas lucharán por la privacidad de la información en contra de las otras dos, que intentarán hacerse con ella.

Por un lado, la esteganografía y el estegoanálisis se encargan de ocultar la información y descubrir la información oculta, respectivamente. Por otro lado, están la criptografía y el criptoanálisis. La criptografía es una disciplina que estudia métodos, sistemas y algoritmos con el fin de modificar una determinada información para que no pueda ser interpretada. Por el contrario, el criptoanálisis tendrá la misión de descifrar la información anterior para su posterior interpretación, es decir, encontrar los puntos débiles de los sistemas criptográficos para romper el código.

A continuación vamos a hacer un breve viaje por toda la historia de la criptología, desde sus comienzos en la grecia antigua hasta la Alemania de la segunda guerra mundial.

2.2 El arte de ocultar información

Como ya hemos explicado, el primer método usado para evitar que los enemigos fisgoneasen las comunicaciones privadas era evitar que supieran siquiera que un mensaje estaba siendo enviado. Para ocultarlo, utilizan diferentes métodos, como los que aparecen en “Las historias” de Herodoto. En este relato se explican algunos de los primeros métodos esteganográficos. Uno de ellos, por ejemplo, consistía, en lugar de escribir un mensaje en una tablilla convencional (de modo

que cualquiera pudiese leerlo), rayar la cera que la cubría y grabar el mensaje por debajo de esta. De esta forma, al cubrirla de nuevo con cera, en apariencia el mensajero solo transportaría una tablilla en blanco.

2.3 Escítala

Los primeros indicios que tenemos del uso de criptografía, sin embargo, datan del siglo V a.C. A este primer sistema de comunicación encriptada se le conocía por el nombre de escítala, y era usado por los espartanos para mandar mensajes secretos. La escítala consistía en un rollo de papiro o cuero estrecho que contenía el mensaje encriptado. Éste se enrollaba en espiral en una vara de un grosor determinado, cuyo diámetro conocían solo el emisor y el receptor del mensaje. Tras enrollar el papiro en blanco alrededor de la vara, se escribía el mensaje, de modo que al desenrollar el papiro se obtenían una serie de letras sin sentido aparente. Para descifrar el mensaje era necesario revertir el proceso volviéndolo a enrollar en una vara del mismo grosor. Sin embargo, si el grosor era diferente al de origen, el mensaje resultaba una sucesión ilegible de letras.

2.4 Polibio

	A	B	C	D	E
A	a	b	c	d	e
B	f	g	h	i	j
C	k	l	m	n	o
D	p	r	s	t	u
E	v	w	x	y	z

Más adelante surgió en el siglo II a.C un método para transmitir la información de un modo más eficaz. Es por eso que muchos no lo consideran como un verdadero sistema criptográfico, sin embargo, es de vital importancia ya que conforma la base de muchos métodos posteriores. Nos referimos al método de Polibio, el primer sistema de sustitución de la historia. Este método asignaba a cada letra del alfabeto dos letras o números diferentes, recogidos en la tabla de la derecha.
Siguiendo esta tabla, el mensaje en claro “POLIBIO” quedaría como: “DACECBBDABBDCE”.

2.5 Bacon

Varios siglos más tarde un filósofo inglés propuso un método similar que asociaba a cada letra del alfabeto un conjunto de cinco caracteres formado únicamente por A y B. Este sistema es el antecesor del código binario, sistema utilizado por todos los ordenadores actuales, el cuál sustituye A y B por unos y ceros.

2.6 Julio César

Uno de los personajes más famosos de la historia de la humanidad, y uno de los métodos de criptografía más conocidos y usados por los amateurs y aficionados.

a	b	c	d	e	f	g	h	i	j	k	l	m
D	E	F	G	H	I	J	K	L	M	N	O	P

n	o	p	q	r	s	t	u	v	w	x	y	z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

El método del gran general y cabeza del imperio romano fue usado no solo por él, sino por un gran número de peces gordos en Roma. Este método es una de las principales bases de la criptografía, y hoy en día permite introducir a un gran número de conceptos, como la aritmética modular. El método consiste en mover el abecedario tres letras hacia la derecha, (tal y como se puede ver en la tabla) y sustituir cada letra del mensaje original por la correspondiente del nuevo alfabeto. De éste modo, el mensaje visible era indescifrable para todos aquellos que desconocían su método.

2.7 Análisis de frecuencias

El análisis de frecuencias aparece en la Edad Media, y destroza todos lo avances que se habían hecho en criptografía hasta el momento. Este método criptoanalítico consistía en conseguir la frecuencia con la que aparece cada letra del abecedario, en el idioma en el que supuestamente estaba escrito el mensaje, y sustituir los símbolos que aparecen en el mensaje encriptado en consecuencia.
De esta forma, si en español la letra “e” aparece con una frecuencia de 13'68% y en mi texto la letra “h” aparece con esta frecuencia, podemos inferir que la h sustituye a la e a lo largo del texto.
Como usted comprenderá este método es fácil de burlar, y de esto ya se dieron cuenta los maestros criptográficos de la época. Para evitarlo, empezaron a hacer uso de ruido intencionado, pero este sistema no duró demasiado tiempo, pues poco ruido deja entrever el mensaje, pero demasiado lo hace difícil de hacer.
El ruido en criptografía se refiere a caracteres nulos, es decir, que no quieren decir nada, caracteres que sustituyen a ciertos espacios en blanco o caracteres homófonos. Por ejemplo, podemos hacer un código en el que la letra “a” equivalga a tres símbolos distintos y usarlos de forma alterna, confundiendo así al criptoanalista y a su tabla de frecuencias. Pero, como ya dijimos antes, mucho ruido pierde a cualquiera, y los mensajes se hacían cada vez más complicados de leer.

2.8 Revolución polialfabética

Leon Battista Alberti tuvo una genial idea a prueba de ciptoanálisis de frecuencias. Se le ocurrió crear un sistema que fuese cambiando el alfabeto a medida que avanzaba el mensaje. De esta forma, la frecuencia con la que aparecen la letras se altera, impidiendo su desencriptado.
Surgieron una grandísima cantidad de variantes, pero la más significativa es la que debe su nombre a Blaise de Vigenère, diplomático, químico y criptógrafo francés. El cifrado de Vigenère funciona de la misma forma que el método César, pero utilizando una palabra clave inicial. Si ponemos como palabra clave “JUAN”, la primera letra se encriptará como si el alfabeto empezara por la J, la segunda como si éste empezara por la U, etcétera, así que si el mensaje es la palabra “PROYECTO”, la “p” se sustituiría por una “z” (clave J), la r por una m (clave U), etc.

Hasta el siglo XX, con la aparición de la revolucionaria y famosísima máquina Enigma, se usaron variantes de este método, a veces usando pares de letras, o teniendo un número determinado de saltos de alfabeto.

2.9 Enigma

Aterrizamos en el siglo XX, Segunda Guerra Mundial, año 1939. 21 años antes se patentó la máquina Enigma, un aparato electrónico comercial que sirve para encriptar mensajes con un método digno de la calidad alemana.
La máquina consistía en un teclado estándar de máquina de escribir, tres rotores conectados una vez entre ellos, con 26 letras cada uno, y a veces un reflector, que servía para descifrar un mensaje con la misma clave.
El cifrar un mensaje es sencillo cuando se ve simplificado. Se introduce la letra “a” en el teclado, y la corriente eléctrica pasa por la letra “a” del primer rotor. De aquí pasa a la letra del segundo rotor acorde con la conexión que tenga con el primero. Si el primer rotor está conectado al segundo de la letra “a” a la “j”, las letras se cambiarán de acuerdo con esa clave. Y lo mismo sucede con el tercer rotor. La gracia está en que cada vez que se escribe una letra, la posición del primer rotor gira una vez, y cuando llega a la “a” otra vez, rota el segundo rotor, que cuando gira hasta la “a”, hace girar el tercer rotor.
Esta mecánica, que a grandes rasgos parece sencilla, se mantuvo vigente durante la segunda guerra mundial. Los alemanes utilizaban esta máquina para encriptar sus mensajes y comunicarse así con sus aliados de forma que solo ellos, que contaban con otras máquinas Enigma similares, pudiesen descifrarlos. El descifrado se llevaba a cabo de la misma forma que el cifrado, con la única condición de ajustar los rotores de la misma manera.

Los polacos sospechaban de los alemanes antes de la guerra, así que el Despacho de Inteligencia polaco contrató a tres matemáticos, entre ellos Marian Rejewski, el cuál consiguió descifrar la máquina Enigma. Luego los alemanes añadieron un par más de rotores, y, pasando su trabajo a los ingleses, Alan Turing terminó los cálculos de Rejewski acabando así la máquina con los algoritmos que consiguió acortar varios años la guerra.

3 ENTREMOS EN MATERIA: BASE MATEMÁTICA PARA RSA

Como habrán podido comprobar, desde los comienzos de las civilizaciones se produjo una competición entre aquellos que querían mantener oculta la información y aquellos que querían conocerla. Esta carrera fue dejando a su paso sistemas cada vez más complejos de criptografía y de criptoanálisis. Más tarde, la llegada de la era electrónica supuso un enorme cambio en la forma de comunicarnos, situación que el bando de los criptógrafos supo aprovechar para ponerse en cabeza en la interminable lucha. A continuación vamos a estudiar

cómo funciona el sistema que les llevó al primer puesto. Pero para ello estudiaremos primero las bases matemáticas necesarias para entender el criptosistema RSA. Éstas giran alrededor de la Teoría de Números, una rama de las matemáticas que se encarga del estudio de números enteros.

3.1 Los números enteros

Como la mayoría sabrán, los números enteros (**Z**) son aquellos englobados dentro de la parte de los números reales que no tienen decimales, sino que sólo se componen de unidades, decenas, centenas, etc. Pueden ser tanto pares como impares, son infinitos y engloba tanto números positivos como negativos. Nos vamos a centrar en un conjunto de los números enteros, los números naturales.

3.2 Los números naturales

Los números naturales (**N**) son todos aquellos números enteros mayores que 0, es decir, positivos. $N = \forall\, x \in Z{>}0$.

3.3 Los números coprimos

Los números coprimos son conjuntos de números enteros que no tienen divisores comunes, o lo que es igual, dos números son coprimos cuando su máximo común divisor es igual a uno. Para explicar esto cogeremos dos números, a=4 y b=6:
Mcd(4,6)=2 luego a y b no son coprimos entre si.

Pongamos otro caso en el que a=4 y b=9:
Mcd(4,9)=1 Lo que quiere decir que en este caso a y b serían una pareja de números coprimos.

Analizando los resultados podemos afirmar que los números coprimos nunca son divisibles el uno por el otro.

3.4 Los números primos

Los números primos, son unos números especiales que cumplen una serie de características, llamadas “criterios de primalidad”, las cuales son:
➤Sus únicos divisores son ellos mismos y uno (de ahí que todos ellos, salvo el dos, sean impares, ya que todos los pares son divisibles entre dos).
Llamaremos a nuestro número primo “p”:
Si p=5, y ponemos en fila los números menores o iguales que él (1,2,3,4,5) comprobamos que 5 no es divisible por ningún número que no sean él mismo o uno. Por tanto “p” es primo.
Luego podemos deducir que todos los números primos son a la vez coprimos entre sí, y no solo eso, sino que son coprimos de todos los números naturales.

➤Al realizar con ellos la Función (**φ**) de Euler, el resultado es inferior a ellos en una unidad. A continuación pasaremos a explicar qué es esta función.

3.5 Función (**φ**) de Euler

La función (***φ***) de Euler es una función (como su nombre indica) que nos permite saber la cantidad de coprimos inferiores a un número que éste tiene.
Esta función se simboliza como ***φ***(n). Vamos a explicarlo con un ejemplo:
Si n=12 cogemos todos los valores comprendidos entre 0 y n (que es 12), por lo que:
φ(n)➤1,2,3,4,5,6,7,8,9,10,11
De esa lista de números, los únicos que son coprimos con 12, según lo que hemos definido antes, son 1,5,7,9,11. Por tanto ***φ***(12)=5 ya que tiene cinco números coprimos menores que él.

Apliquemos este mismo procedimiento a un número primo p=13
φ(n)➤1,2,3,4,5,6,7,8,9,10,11,12 (todos son coprimos con p, porque este es primo) por tanto:
φ(p)=12
De esta forma podemos decir que $\varphi(p) = p-1$
De la misma forma podemos decir que $\varphi\,(p^n) = (p-1)\times p^{(n-1)}$ siempre que p sea primo. Por ejemplo, si $n = 25 = 5^2$:
φ(25)=φ(5^2)=(5-1)×($5^{(2-1)}$)=4×5^1=20
A partir de esta información, podemos crear una ecuación lógica para calcular ***φ*** de cualquier número. Para ello, descomponemos el número en factores y hacemos el producto de ***φ*** de cada factor. Cogeremos el ejemplo n=68:
68 se puede descomponer factorialmente como: $2^2\times 17$, por lo cual:
φ(68)=φ(2^2)×φ(17)=[(2-1)×(2^{2-1})]×[(17-1)×(17^{1-1})]=$1\times 2\times 16\times 1$=32.

3.6 Tipos de números primos

Desde que se comenzaron a buscar números primos hasta la actualidad se han encontrado una gran cantidad de estos y se han ido clasificando según sus propiedades. Entre los diversos tipos, destacan los siguientes:

-Mersenne: son los números primos formados por el polinomio 2^p-1, siendo “p” un número primo cualquiera.
-Perfectos: no se trata de números primos, de hecho todos son pares. Sin embargo, guardan relación con los primos de Mersenne. Los números perfectos se tratan de números cuyo valor es equivalente a la suma de sus propios divisores. Si (2^p-1) es un número primo de Mersenne, entonces (2^{p-1})×(2^p-1) es un número perfecto. Es por eso que conocemos tantos números perfectos como primos de Mersenne.

-Gemelos: los números primos gemelos son aquellos cuyos valores distan en dos unidades uno de otro (como serían el 5 y el 7, el 11 y el 13…) es decir, que cumplen la ecuación: p=q-2 siendo p y q números primos.
-Sophie Germain: se dice que un número es primo de Germain cuando el doble de él mismo +1 resulta también un número primo.
-Fermat: son los números primos que se pueden expresar como: $F_n = 2^{2^n}+1$ Siendo “n” un número entero positivo.
-Fuertes : los números primos fuertes son aquellos cuyo valor es superior a la media aritmética de sus primos predecesor y sucesor.

3.7 Obtención de números primos a lo largo de la historia

Para la criptografía, la obtención y el descubrimiento de nuevos números primos es uno de los pilares fundamentales. Por eso a lo largo de la historia se ha intentado encontrar una forma cada vez más eficiente y rápida de obtenerlos. La forma de generar números primos es mediante determinados polinomios. Los más conocidos son los siguientes:

-Polinomios de Euler:

$$x^2+x+41 \quad x\in[0,39] \qquad x^2-x+41 \quad x\in[0,40]$$

-Polinomios de Legendre:

$$2x^2+29 \qquad x\in[0,28] \qquad x^2+x+17 \qquad x\in[0,15]$$

Sin embargo, teniendo en cuenta la infinidad de números primos existentes supone cada vez un desafío mayor, hasta el punto de que se otorgan recompensas de considerable valor económico a personas capaces de batir récords en la búsqueda de números primos grandes. Para comparar números y saber si son primos se realizan tests de primalidad, que explicaremos más adelante.

3.8 Aritmética modular

La aritmética modular aparece por primera vez en los trabajos del griego Euclides, aunque la percepción moderna de esta rama la trae Carl Friedrich Gauss en 1801, en su trabajo “Disquisitiones Arithmeticae”.
El nombre suena bastante lejano, pero en realidad le damos uso todos los días, y es seguro que la aprendiste en una temprana edad. Esto de lo que hablo es de las horas.
La aritmética modular se conoce también como aritmética de reloj. En nuestro reloj habitual, cuando la unidad de las horas llega a 24, el sistema se reinicia y vuelve a marcar las 0 horas.

Desde siempre, cuando realizamos una división lo que intentamos es que el resto sea cero y lo único que nos interesa era el cociente. Ahora, con la aritmética modular, esto cambia y lo que nos interesa es el resto de la división.

El resto de una división en aritmética modular se expresa como sigue: $a\,(mod\,b) = c$ siendo “a” el dividendo, “b” el divisor y “c” el resto.
La aritmética modular tiene varias propiedades. La principal y básica es la congruencia: se dice que dos números son congruentes cuando, al dividirlos por uno mismo, el resto coincide. Matemáticamente diríamos que $a \equiv b\,(mod\,c)$. Es decir, la división de “a” por “c” y de “b” por “c” da como resultado el mismo resto. Existen muchos otros tipos de propiedades en la aritmética modular pero no nos son necesarias para este trabajo.

3.9 Test de primalidad

En conclusión, para este tipo de criptosistemas no solo es necesario crear números primos, si no también comprobar si un determinado número lo es. Estas son unas de las muchas formas que existen de saberlo:

-Método de Eratóstenes:
Su método se basaba simplemente en ir descartando. Se escribían en orden todos los números desde el uno hasta el que se establecía como límite y se iba comprobando número por número si era primo. Cada vez que se encontraba un número no primo se tachaba este y todos sus múltiplos. Aquellos que quedaban impunes formaban los primos encontrados en ese intervalo.

-Método de Fermat:
Este proceso sí usa propiedades matemáticas de la aritmética modular para averiguar si un número es primo. Un número es primo si:
$a^{\,p} \equiv a(mod\ p)$ siendo p=número primo y a=número cualquiera.
Por tanto se debe cumplir que:
$a^{\,p-1} \equiv 1(mod\ p)$
$\frac{a^{\,p}-a}{p} = Z$ siendo Z=número entero.

4 CÓDIGO RSA

4.1 Introducción

Entre los sistemas de cifrado podemos encontrar el código RSA, que es el más popularizado en la actualidad, siendo usado, por ejemplo, en el cifrado de comunicaciones vía *whatsapp.* Este sistema de cifrado se caracteriza por ser un criptosistema asimétrico, es decir, usa una clave para cifrar la información y otra diferente para descifrarla. Fue creada en 1977 por Ronald Rivest, Adi Shamir y Leonard Adelman. El nombre tiene su origen en la unión de las iniciales de los apellidos de los inventores. Pero este código realmente no se empezó a usar hasta que expiró la patente en el año 2000. La eficiencia de este sistema se basa

en la dificultad de encontrar la clave del descifrado, para lo que sería necesario factorizar números con una gran cantidad de cifras. Esto le llevaría a un ordenador demasiado tiempo. Sin embargo esto se podría ver afectado por la computación cuántica que podría hacer estos cálculos a una velocidad más rápida y por ello en menos tiempo. La longitud de las claves ronda los 1024 bits.

El sistema en general es sencillo; el receptor (a partir de ahora lo llamaremos Bea) genera tres claves y comparte dos de ellas, que pasarán a ser la clave pública. Estas claves son conocidas por todos y pueden utilizarlas todos aquellos que quieran enviarle un mensaje a Bea. Pongamos que un amigo de Bea (que a partir de ahora llamaremos Antonio) quiera enviarle un mensaje. Este solo tendrá que cifrarlo con las dos claves públicas y enviarlo.
Por otra parte, Bea también ha generado una clave que solo ella conoce, la clave privada. Gracias a esta puede descifrar cualquier mensaje recibido que haya sido cifrado con sus claves públicas. Sin embargo, nadie que desconozca la clave privada será capaz de descifrar estos mensajes. Antonio puede estar seguro de que su información está a salvo.
Pero, ¿qué pasa si Bea quiere contestar a Antonio? Para ello solo tendrá que utilizar la clave pública de Antonio, quien descifrará el mensaje con su propia clave privada.

4.2 Creación de claves

Visto cuál es el funcionamiento básico del sistema, vamos a explicar cómo se crean ambas claves:
Empezaremos por la creación de las claves públicas que conocerá todo el mundo y con las cuales Antonio codificará la información que quiera enviar. Para ello se siguen los siguientes pasos:

1. Se escogen aleatoriamente dos números primos de extensa longitud (mayores de 10^{100}) a los que llamaremos “p” y “q”.
2. Se hace el producto de esos dos números primos, al que llamaremos “n” es decir: (p·q) = n. Como “q” y “p” son primos, al multiplicarlos, serán los únicos divisores distintos de uno que tendrá el producto “n”.
3. Se calcula φ(n) y se le busca un coprimo al que llamaremos “e” (es decir: Mcd[e,φ(n)]=1) tal que: 1<e<φ(n).

Estos dos números, “n” y “e”, conformarán nuestra clave pública.

Ahora buscaremos la clave privada:
La clave privada estará conformada por dos números: “n” (que ya lo tenemos porque es común en las dos claves) y “d”. El número “d” cumple la siguiente propiedad: $e \times d \equiv 1 (mod \varphi(n))$ o lo que es igual: d=inv(e,$\varphi(n)$).
Una vez que tenemos las claves privada y pública creadas solo queda distribuir la clave pública para que cualquiera que quiera enviar un mensaje lo cifre con ella.

4.3 Ejemplo numérico

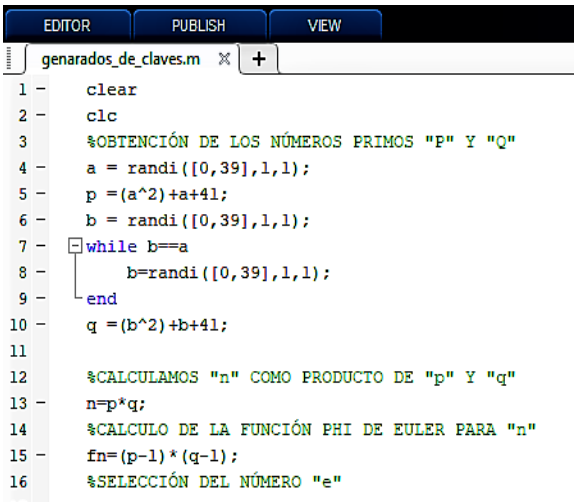
Ahora explicaremos un ejemplo con números sencillos para facilitar su comprensión:

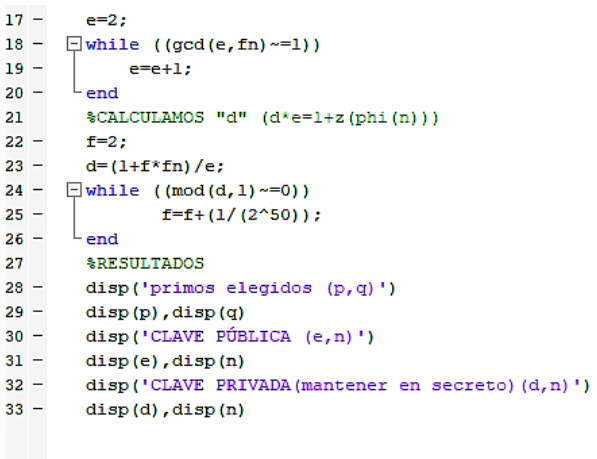
1. Para comenzar escogeremos dos números primos al azar, en nuestro caso serán 11 y 23. Los multiplicamos y obtenemos 253 que corresponde a “n”
2. Ahora calculamos $\varphi(253)=220$ y a continuación buscamos un coprimo del número obtenido (“e”), que en este caso será 3.
3. Con estos dos números (e,n)=(3,253) ya tenemos nuestra clave pública.
4. Buscamos “d” para que se dé que $d*3\equiv 1\,(mod\,220)$, que en este caso será 147. Así tendremos nuestra clave privada (d,n)=(147,253)

Supongamos, pues, que Antonio quiere enviarle a Bea un mensaje cifrado mediante nuestra clave pública (3,253). El mensaje que Antonio le quiere enviar lo llamaremos M y el mensaje cifrado será C.
El mensaje lo ciframos según la siguiente fórmula:
$C=M^{\,e}(mod\,n)$
Por lo que si Antonio, por ejemplo, quiere cifrar el mensaje “4” (M), la fórmula quedaría de la siguiente forma: C = $4^3(mod\,253)=64$. Así, Antonio ya tendría el mensaje cifrado y solo quedaría enviarlo a Bea para que lo descifre.
Cuando Antonio envía el mensaje cifrado (64) a Bea, ella lo descifra mediante esta fórmula: $M=C^{\,d}(mod\,n)$.
Recordemos que “C” es el mensaje cifrado y “M” el mensaje en claro. Al aplicar la fórmula nos quedaría: $M=64^{147}(mod\,253)=4$. Con lo que el mensaje habría sido enviado con éxito.

4.4 De la teoría a la práctica

Hemos programado en Matlab un algoritmo capaz de generar dos pares de





claves con los procedimientos del RSA, aquí el resultado:

Lo que hace este programa es utilizar los sistemas de búsqueda de primos que hemos mencionado antes para encontrar números primos aleatorios. Luego, realiza con ellos las operaciones explicadas anteriormente para obtener los dos pares de claves deseados. Este es el resultado mostrado en pantalla una vez iniciado el programa:

```
primos elegidos (p,q)
        1163

        1447

CLAVE PÚBLICA (e,n)
     5

     1682861

CLAVE PRIVADA(mantener en secreto)(d,n)
      672101

     1682861
```

Con esto ya tenemos todo lo que necesitamos para cifrar y descifrar mensajes.
Si quisiéramos cifrar el mensaje “DE CIFRAS A SECRETOS” habría que traducirlo a código ASCII, que es un código que transforma sets de 16 bits a números y letras ordinarios. Nos quedaría un mensaje claro con esta apariencia:

M= 68-69-67-73-70-82-65-83-65-83-69-67-82-69-84-79-83.

Realizamos la operación de cifrado ($C = M^{e} (mod\ n)$) con cada uno de esos números y obtendríamos el siguiente resultado:

C=1624525-653480-470585-1469702-1204722-55649-799396-1145903-
799396-1145903-653480-470585-55649-653480-209839-786491-1145903.

Al realizar la operación inversa volveríamos a obtener los valores iniciales del mensaje y solo habría que comparar cada letra con su valor en ASCII para poder leer el mensaje.

5 EL FUTURO YA ESTÁ AQUÍ: CRIPTOGRAFÍA CUÁNTICA

En la actualidad, la criptografía de RSA ha alcanzado un gran prestigio y aceptación debido a que resulta prácticamente imposible para un criptoanalista experimentado factorizar con éxito números tan grandes como los usados en este sistema.

Sin embargo, ¿qué sucedería si se inventase un ordenador capaz de llevar a cabo estos cálculos a una velocidad mucho mayor que el ordenador clásico más potente? Esto es lo que la computación cuántica amenaza con conseguir en los próximos años. Los ordenadores clásicos trabajan con el sistema binario, un “idioma” que entiende únicamente dos estados: el cero o el uno. Estos estados suponen la unidad mínima de información: el bit. Un cero, por ejemplo, significa apagado y un uno significa encendido. La combinación de ceros y unos forman la información que el ordenador es capaz de procesar, lo que permite a la computadora llevar a cabo una serie de cálculos bastante más complejos que los que una persona puede llegar a solucionar. No obstante, los cálculos necesarios para romper el criptosistema RSA le llevarían demasiado tiempo.

5.1 Computación cuántica

Aquí es donde entra en juego la computación cuántica: en rasgos generales, las computadoras cuánticas se diferencian de las clásicas en que en lugar de utilizar un bit de información que pueda ser un cero o un uno, utilizan un bit especial (conocido como qubit) que puede corresponderse con uno de estos estados o con algo intermedio. Puede incluso representar ambos al mismo tiempo. Este extraño fenómeno sucede gracias a un principio de la física cuántica, la superposición de estados.

Supongamos que tenemos una partícula que puede ser amarilla o azul y que tiene la misma posibilidad de ser de un color o del otro. En la física clásica, antes de saber el color que nos ha tocado, diríamos que hay un 50% de probabilidad de cada resultado y que al observar la partícula descubriríamos cuál de los dos era. En la física cuántica, sin embargo, las cosas no suceden así. Antes de conocer el tipo de partícula, esta sería de los dos colores al
mismo tiempo (al igual que sucede con el famoso gato de Schrödinger). Pero realmente curioso sucede a continuación: cuando observamos la partícula, esta se ve alterada por el hecho de estar siendo detectada, de tal forma que se decide por una de las dos alternativas y la observaremos de este color, ya sea amarilla o azul. Este fenómeno se conoce como superposición de estados, y podemos enunciarlo como que una partícula puede presentar al mismo tiempo todas las posibilidades para una característica siempre y cuando no intervenga un observador. En el mismo momento en que la propiedad de esta partícula es medida, esta propiedad queda determinada, desapareciendo las otras variables.

Análogamente, los qubits de la computación cuántica pueden estar al mismo tiempo en ambos estados uno y cero, representando simultáneamente todas las posibilidades. De esta forma, el ordenador es capaz de realizar paralelamente los cálculos con el qubit siendo un uno y con el qubit siendo un cero, lo que agiliza inimaginablemente los cálculos.

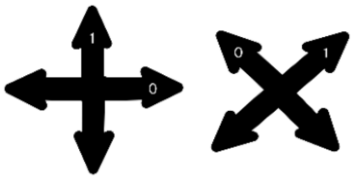
Ante tal amenaza, los criptógrafos han tratado de desarrollar un sistema que aproveche de la misma manera las leyes de la cuántica.

Este nuevo tipo de encriptado está basado en una de las propiedades principales de la física cuántica, el Principio de Schrödinger: “El mero hecho de observar un

sistema cuántico altera el propio sistema, imposibilitando así conocer su estado original.”
Veamos en qué consiste este nuevo tipo de codificación.

5.2 Encriptado de la clave

Pongamos un caso en el que Antonio quiere enviar un mensaje a Bea que no pueda ser decodificado por un ordenador cuántico. Para ello Antonio y Bea necesitan acordar una clave común mediante un sistema cuántico de encriptado. Para llevar a cabo esta comunicación necesitan tener en cuenta una información previa. Para enviar una clave se utilizan dos canales: un canal cuántico privado, normalmente de fibra óptica, y un canal convencional, que puede ser público ya que no importa si esa información es recibida por un tercero. A través del canal cuántico se envía una sucesión de fotones polarizados (“Polarización: dirección de oscilación de un campo eléctrico”). Dichos fotones pueden oscilar en cuatro direcciones: en vertical, en horizontal o en cualquiera de las dos diagonales. Antonio y Bea acuerdan asignar a cada una de estas posiciones un uno o un cero, siguiendo el siguiente esquema:



Al mismo tiempo, se utilizan dos tipos de filtros como los de la figura de la izquierda que recogen los datos de los fotones polarizados recibidos: uno recoge ambas diagonales y el otro la horizontal-vertical. El uso del filtro incorrecto alteraría al fotón, que reajustaría su polarización a la forma del filtro, de manera que lo atraviese pero cambiando su dirección de oscilación.
Para llevar a cabo el intercambio de la clave, Antonio le envía una serie de fotones (qubits) a Bea que previamente ha pasado por sus propios filtros, de manera que Antonio ha registrado las polarizaciones de los fotones enviados.
Por su parte, Bea debe escoger aleatoriamente qué filtro utilizar para cada qubit que recibe y anotar los resultados obtenidos. Algunos de estos resultados serán diferentes de los originales debido a que, al no conocer cuál de los dos filtros debía usar, habrá escogido el equivocado.
Completada esta fase, Bea, a través de la vía pública, le dice a Antonio los filtros que ha utilizado en cada caso. Este le responde informándola de cuáles han sido los filtros que ha escogido correctamente, consiguiendo así que ambos sepan cuales son los qubits que no han sido alterados a lo largo del proceso. Estos son los qubits que conformarán la clave.

De esta forma, Antonio ha enviado con éxito la clave a Bea sin que ningún intruso se entere… ¿o no? ¿Cómo pueden estar seguros de que su información está a salvo?

5.3 ¿Por qué es tan seguro este sistema?

A continuación, vamos a ver qué ocurriría si un espía intentase interceptar los fotones del canal privado pasando desapercibido.
La clave de esto la tiene un físico alemán del que hablamos anteriormente: Schrödinger. Como explicamos al comienzo, según el Principio de Schrödinger, un sistema cuántico no puede ser medido ni observado sin alterarse. Si esto es cierto, el espía lo tendría realmente complicado para obtener la información, pero ¿lo es?

Imaginemos que un amigo de Antonio y Bea, Enrique, tiene curiosidad por saber qué se traen en secreto ellos dos y decide intervenir en el intercambio de la clave sin que lo sepan.
Después de que Antonio envíe sus fotones, Enrique consigue que pasen por sus filtros, de manera que registra y anota la información obtenida. Después de su intervención, los fotones siguen su curso y Bea los registra con normalidad.

Esta información no le sería de mucha utilidad a Enrique si no interviniese también la información intercambiada por medio del canal público, ya que no sabría cuáles de los fotones han sido alterados al usar aleatoriamente sus filtros ni tampoco cuáles son los dígitos que Antonio y Bea van a desechar.
Supongamos, pues, que consigue también esta información. Bea y Antonio compartirían los filtros utilizados y concluirían cuáles son los fotones en los que Bea ha utilizado el filtro correcto, es decir, cuáles son los fotones válidos para la clave. Ninguno de ellos tendría por qué percatarse del engaño, ¿no?

Pues, no exactamente. Al obtener la clave, Antonio y Bea se ponen en contacto por medio del canal público de nuevo para comprobar si el mensaje ha sido enviado y recibido sin ser visto por ningún intruso. Para ello, los dos amigos sacrifican algunos de los bits de la clave compartiéndolos públicamente. Si todos estos dígitos coinciden entonces podrán estar seguros de la privacidad del sistema. Por el contrario, si un tercero hubiese intervenido, una parte de estos hubiesen sido modificados. Enrique habría sido pillado con las manos en la masa. De esta forma, al darse cuenta de la intrusión, la clave sería desechada antes siquiera de haber enviado ningún mensaje, asegurando así mantener la información alejada de miradas indiscretas.

6 CONCLUSIÓN

A modo de conclusión y para facilitar la comprensión vamos a hacer un breve repaso de lo estudiado a lo largo del proyecto. Hemos comenzado dando un paseo a través de la historia de lo criptografía, deteniéndonos en aquellos inventos más ingeniosos e interesantes del pasado.

A continuación nos hemos sumergido en el mundo de las matemáticas, explicando todas las bases necesarias para dar un salto temporal hasta los sistemas actuales de criptografía. Una vez preparados hemos explicado el funcionamiento del sistema RSA: cómo enviar y recibir mensajes de forma segura gracias a la ayuda que nos proporciona la aritmética modular, la teoría de números y un tipo particular de estos, los primos.
También en esta fase nos atrevimos a crear nuestro propio sistema RSA para codificar y descodificar un mensaje nosotros mismos.
Para terminar, dimos un salto al futuro explicando la computación y la criptografía cuánticas. Estos sistemas, que pueden sonar a la más profunda ciencia ficción, están en realidad siendo estudiados y desarrollados actualmente. Gracias a las leyes de la física, estos innovadores sistemas supondrán, antes de lo que muchos esperan, una auténtica revolución en el mundo de la tecnología y las comunicaciones.
Nuestro viaje juntos ha llegado a su fin y toca reflexionar: Todo esto…¿Para qué sirve? ¿De qué manera afecta la criptografía a nuestras vidas diarias?
Hoy en día, toda nuestra vida gira alrededor de la tecnología. Desde que despertamos por la mañana estamos continuamente compartiendo y produciendo información a través de internet: consultamos el pronóstico del tiempo, leemos y enviamos *whatsapps*, revisamos nuestras redes sociales e incluso hacemos transferencias de dinero.
¿Son seguras estas prácticas? ¿Estamos poniendo en juego nuestra privacidad? ¿Qué pasaría si toda esta información cayese en malas manos?
Aquí es donde nuestra superheroína, la criptografía, entra en acción. Gracias a los sistemas estudiados a lo largo del proyecto podemos estar seguros de que nuestra información está a salvo. Sin embargo, la tecnología es un arma de doble filo y al igual que permite mejorar los sistemas de encriptado, los espías y criptoanalistas también mejoraron sus métodos. Si los proyectos acerca de la computación cuántica se llevan a cabo con éxito, el sistemas RSA dejaría de ser seguro. Aquí reside la importancia de la continua investigación y desarrollo. No obstante, hay algo con lo que los criptoanalistas no cuentan y es que guardamos un As bajo la manga, un arma secreta que acabará con la histórica lucha entre criptógrafos y criptoanalistas: La criptografía cuántica.

7 AGRADECIMIENTOS

En nombre de todos los miembros de “Proyecto: END” queremos dar las gracias al profesor que nos animó a participar en este concurso y que nos ha acompañado a lo largo de todo el proyecto, Juan José Jiménez. Él ha sido una base en la que apoyarnos durante todo el proceso y se ha implicado tanto como nosotros para que todo saliese perfecto.
Por otra parte queremos agradecer a la empresa ec2ce por ofrecernos esta maravillosa oportunidad de aprender y de aplicar lo aprendido al mundo real, más allá del papel.

También nos gustaría dar las gracias a todas las personas que se interesan por el bien común de la divulgación científica, ya que ellas ayudan a gente llena de preguntas, (como nosotros) y nos hacen ver el mundo de manera diferente. Por dar algunos ejemplos; Crespo de QuantumFracture, Eduardo de derivando, Martí de CdeCiencia, Javier de Date un Vlog o Patricia de Antroporama.

8 BIBLIOGRAFÍA

General

➥https://www.uam.es/departamentos/ciencias/matematicas/premioUAM/premiados3/simulacion_criptografia.pdf

➥Matemáticos, espías y piratas informáticos (codificación y criptografía) [Joan Gómez]

Historia

➥https://www.genbetadev.com/seguridad-informatica/que-es-y-como-surge-la-criptografia-un-repaso-por-su-histori

➥https://joseluistabaracarbajo.gitbooks.io/criptografia-clasica/content/Cripto05.html

➥https://es.wikipedia.org/wiki/Enigma_(m%C3%A1quina)

RSA

➥https://hackingenvivo.blogspot.com.es/2017/11/cifrado-rsa.html

➥https://seguinfo.wordpress.com/2007/09/14/%C2%BFque-es-rsa/

➥http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/rsa2.html

Física cuántica

➥https://www.textoscientificos.com/criptografia/criptoquantica

➥http://www.eldiario.es/hojaderouter/seguridad/criptografia-cuantica-seguridad-ciberespionaje_0_315669050.html

➥http://www.criptored.upm.es/crypt4you/temas/cuantica/leccion2/leccion02.html

➥https://youtu.be/UXm9RhqQmZU

➥https://youtu.be/WqJ1NyEuwbg

➥https://es.gizmodo.com/como-funciona-la-computacion-cuantica-explicado-de-man-1796976460