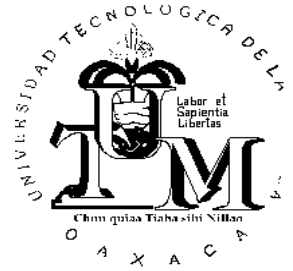

UNIVERSIDAD TECNOLÓGICA DE LA MIXTECA

Tesis:

"ESTUDIO Y ANÁLISIS COMPARATIVO DE MÉTODOS CRIPTOGRÁFICOS"

que para obtener el título de

LICENCIADO EN MATEMÁTICAS APLICADAS

presenta:

Paulo Sergio García Méndez

Director de tesis

M. en C. Adolfo Maceda Méndez

Huajuapan de León, Oaxaca.
Septiembre de 2003.

Contenido

Introducción

La criptografía estudia los métodos que permiten establecer comunicación entre dos entidades disfrazando la información para su intercambio en forma secreta. El que envía un mensaje usando un sistema criptográ…co lo hace sabiendo que el que recibirá el mensaje podrá remover el disfraz y recuperar el mensaje original; y que nadie más podrá hacerlo aunque haya interceptado el mensaje. Estas dos entidades comparten una clave privada que es la que les indica cómo disfrazar la información y a su vez cómo remover dicho disfraz.

Hasta antes de la segunda mitad de la década de los 70's, los usuarios de sistemas criptográ…cos tenían que con…ar ciegamente en que el acuerdo de la clave secreta se había dado de manera discreta, es decir, no había una tercera entidad que hubiese interceptado la forma de maquillar o desmaquillar la información. En 1976, Whit…eld Di¢e y Martin Hellman cambiarían la forma de entender la criptografía al proponer la creación de un nuevo esquema para el intercambio seguro de la clave secreta. En la misma dirección, en la primavera de 1977, Ron Rivest, Adi Shamir y Leonard Adleman, cientí…cos del MIT, inventaron el primer método criptográ…co que no requería de un intercambio previo de la clave secreta para poder establecer comunicación entre dos entidades. Lo único que se necesitaba era una especie de dirección que permanecía pública a todo el que quisiera comunicarse con alguna entidad en especí…co, esto se conocía como clave pública. RSA, como fue bautizado, se convirtió en el primer sistema criptográ…co de clave pública y hasta la fecha se mantiene como el más comunmente usado debido a que ha resultado muy seguro. Esta seguridad se fundamenta en la di…cultad computacional para factorizar un número entero "grande".

La criptografía de clave pública gana cada vez más adeptos dentro de la comunidad cientí…ca ya que ha probado ser fuente de aplicación continua de campos del conocimiento como matemáticas, computación y electrónica. También, el interés por parte de los sectores empresarial e industrial ha crecido enormemente debido a las aplicaciones que tiene en transacciones …nancieras, comercio electrónico y correo electrónico.

En este trabajo de tesis se realiza el estudio de un sistema criptográ…co sobre un campo cúbico (CCC) de tipo RSA.

Los objetivos del presente trabajo son:

1. Identi…car las semjanzas y diferencias teóricas que el CCC tiene con el sistema RSA.
2. Mostrar a la criptografía de clave pública como un área de aplicación de las matemáticas.

3. Finalmente, se investigará el funcionamiento práctico de los dos métodos al implementarlos y presentar una aplicación para el intercambio de mensajes cortos.

El presente trabajo está organizado de la siguiente manera:

Dentro del primer capítulo se encuentran algunos conceptos básicos de la criptografía. Éstos permitirán un mejor entendimiento de ella y de los objetivos que persigue. Además, el capítulo ofrece una clasi…cación de los métodos criptográ…cos.

En el capítulo II, se presenta el famoso sistema RSA. Básicamente, se dan a conocer las matemáticas que están detrás de este método y su esquema general de funcionamiento.

El tercer capítulo expone el CCC, clasi…cado como del tipo RSA. La discusión del método requiere conocimientos previos de álgebra moderna. El capítulo comienza estudiando algunos resultados de teoría algebraica de números. También, examina características de anillos que son importantes para la construcción del sistema. Para terminar, se describe el esquema general del CCC.

El capítulo IV está destinado a explicar las diferencias y semejanzas de tipo teórico que poseen los métodos, así como a mostrar de manera práctica el funcionamiento de los mismos. Además, se presenta una aplicación para el intercambio de mensajes cortos.

Finalmente, se señalan las conclusiones obtenidas a partir del trabajo realizado.

Los apéndices A y B, están destinados a una mejor comprensión del capítulo III. El apéndice A ofrece un recordatorio de de…niciones y resultados de álgebra moderna, así como una revisión de los elementos básicos de la teoría algebraica de números. El apéndice B provee algunas técnicas para realizar cálculos de caracteres cúbicos residuales y llevar a cabo aritmética en conjuntos especí…cos.

Capítulo I
Elementos de Criptografía

El objetivo de este capítulo es proporcionar algunos elementos que permitan adentrarse en el área de la criptografía. Nociones históricas, conceptos básicos y sus objetivos son revisados en las secciones 1, 2 y 3. Una de las de…niciones más importantes en la criptografía es la de criptosistema, ésta se ilustra mediante un ejemplo en la sección 4. Las secciones posteriores de este capítulo están destinadas a describir las dos grandes ramas en las que se divide la criptografía.

1 Algunos antecedentes históricos.

Con la invención de la escritura, se originó el deseo de transmitir la información de forma rápida y segura. Fue así como surgieron los primeros mecanismos para esconder o disfrazar la información. La palabra criptografía se deriva de las palabras griegas Kriptos que signi…ca esconder y Graphos que signi…ca escritura. Los datos más antiguos acerca de la criptografía que se tienen recopilados, pertenecen a la época de los egipcios. Hace casi 4000 años, los egipcios usaban algunas técnicas que utilizaban una substitución simbólica de jeroglí…cos. Grandes imperios y reinados han podido gestarse o destruirse dependiendo de la discreción que ofrecían los simpatizantes de estos emperadores o reyes. El miedo a que sus más valiosos secretos cayeran en manos enemigas y la amenaza de sus posibles consecuencias, motivó el desarrollo de códigos y la invención de métodos para hacer llegar el mensaje correcto a la persona indicada.

La criptografía también contempla el desciframiento de lenguajes desarrollados por antiguas civilizaciones. Gracias a estos desciframientos, hoy en día, se conoce mucho de los orígenes, desarrollo y evolución de civilizaciones como la egipcia. A …nales del siglo XVIII uno de los primeros hombres en interesarse por descifrar los jeroglí…cos egipcios, fue el notable inglés Thomas Young, quien a la edad de 14 años ya había estudiado griego, latín, francés, italiano, hebreo, siriaco, samaritano, árabe, persa, turco y etíope. Young sentó las bases del desciframiento de los jeroglí…cos egipcios al identi…car un buen número de estos, algunos tan importantes como el símbolo utilizado para denotar la terminación femenina, que se ponía después de los nombres de reinas y diosas.

Guerras han sido ganadas apoyándose en el desciframiento de los mensajes que algunos paises lograron sobre otros sistemas de cifrado pertenecientes a los paises enemigos de éstos.

Basta mencionar que una de las claves para que los aliados pudiesen ganar la Segunda Guerra Mundial, fue el conocimiento del funcionamiento de la famosa máquina Enigma, que los alemanes utilizaban para cifrar sus mensajes.

Con la invención de la máquina de escribir eléctrica, se establecieron los medios para introducir máquinas electromecánicas de cifrado. En 1915, Edward Hebern usó dos máquinas de escribir eléctricas conectadas aleatoriamente por 26 cables. Las conecciones dieron las ideas básicas para crear un rotor. En 1918, el alemán Arthur Scherbius obtuvo la patente para una máquina de cifrado con rotor a la que bautizó como Enigma. Los japoneses compraron la máquina Enigma para su propio uso en 1934 y desarrollaron su propio criptosistema, el cual era llamado Purple por los norteamericanos. Este sistema de cifrado fue criptoanalizado en 1940 por el Signal Intelligence Service de los Estados Unidos.

Por otro lado, los criptógrafos alemanes también tomaron la decisión de adoptar a Enigma como su máquina de cifrado. El criptosistema alemán fue criptoanalizado por los investigadores de la Code and Cipher School en Inglaterra. Uno de los más importantes investigadores presentes fue Allan Turing, quien diseñó una máquina para criptoanalizar a Enigma, llamada Bomba. Para 1940, estos investigadores descifraban mensajes hechos con la máquina Enigma de manera continua. Estos dos hechos fueron muy importantes para lograr la victoria de los aliados.

Una nueva época en la Criptografía vino con la invención de la Criptografía de clave pública en 1976. Desarrollada por Whit…eld Di¢e y Martin Hellman, la Criptografía de clave pública revolucionó la forma de encriptar y desencriptar mensajes ya que su principal ventaja reside en que no se necesita intercambiar la clave secreta, algo que no se había hecho antes.

2 La Criptografía y su objeto de estudio.

Cuando dos entidades desean establecer comunicación de tal manera que se pueda tener la certeza de que no habrá un tercero que llegue a entender lo que se está comunicando, no resulta fácil asegurar que exista algún medio que garantice esta discreción. Por esto, es necesario idear métodos para obtener la discreción requerida. La Criptografía se encarga de hacer esto posible, al representar la información de una manera en la que quien manda un mensaje y quien lo recibe son los únicos entes capaces de entender esta información que ha sido disfrazada.

La Criptografía se encarga de crear y mejorar los métodos que permiten el acceso y la transmisión de información de tal manera que puedan otorgar privacidad, autenticidad e integridad.

En un sentido inverso, el Criptoanálisis estudia los métodos que son útiles para restar la seguridad de las técnicas criptográ…cas. La Criptología, es la que se encarga del estudio de estos dos conceptos.

Los métodos criptográ…cos pretenden proporcionar las siguientes características en la transmisión de la información:

1. Privacidad. Se re…ere a que la información sólo puede ser accedida por personas autorizadas. Por ejemplo, en la comunicación por teléfono, alguien puede interceptar la comunicación y escuchar la conversación, esto indica que no existe privacidad. También, si alguien manda una carta y por alguna razón otra persona rompe el sobre para leer la carta, ha violado la privacidad.

2. Integridad. La información no se puede alterar durante su envío. Como ejemplo se puede mencionar lo que ocurre cuando se compra un boleto de avión y los datos del vuelo son cambiados, ya sea de manera intencional o accidental; esto puede afectar los planes del viajero. Una vez hecho un déposito en el banco, si la cantidad no fue capturada de manera correcta causaría problemas. La integridad es muy importante en las transmisiones militares ya que un cambio de información puede ocasionar serias di…cultades.

3. Autenticidad. La capacidad para con…rmar que el mensaje recibido haya sido enviado por quien dice haberlo mandado o que el mensaje recibido es el que se esperaba. Para ilustrar lo anterior, obsérvese que cuando se quiere cobrar un cheque a nombre de alguien, quien lo cobra debe de someterse a un proceso de veri…cación de identidad para comprobar que, en efecto, es la persona que dice ser. Esto, en general, se lleva a cabo con una credencial que anteriormente fue certi…cada y que acredita la identidad de la persona que la porta. La veri…cación se lleva a cabo comparando la persona con una foto o con la comparación de una …rma convencional.

4. No_rechazo. Se re…ere a que no es posible negar la autoría de un mensaje enviado.

Cuando se busca seguridad en la transmisión de información, se debe entender que se está hablando respecto a la búsqueda de estas cuatro características.

En los últimos años, con la tecnología que hoy se tiene al alcance, cabe mencionar la importancia que la criptografía tiene en una sociedad que vive dentro de una revolución informativa. En un mundo que se globaliza cada vez más, ya no es posible pensar en una sociedad sin acceso a la información. El auge en las telecomunicaciones ha hecho posible que diversas actividades comunes se puedan realizar con una simple llamada telefónica o con una computadora, por ejemplo, transacciones bancarias, correo y comercio electrónico.

La criptografía busca establecer nuevos y mejores mecanismos mediante los cuales sea posible el intercambio de información de una manera segura, es decir, que llegue a las personas autorizadas y sin que esta información pueda ser alterada durante su transmisión. Es así como el desarrollo de la tecnología está directamente relacionado con la criptografía.

3 De…niciones básicas.

En esta sección se revisarán algunas de las de…niciones de la criptografía con el objeto de ir formalizando las ideas anteriormente expuestas. Los siguientes son conceptos de la teoría de conjuntos, que serán de utilidad para las de…niciones propias de la criptografía.

De…nición 1.1. Un alfabeto es un conjunto no vacío y …nito de símbolos.

De…nición 1.2. Dado un alfabeto A, una cadena sobre A es una sucesión …nita de símbolos del alfabeto A:

De…nición 1.3. Un criptosistema es una quintupla $(P; C; K; E; D)$ que satisface:

1. P es un conjunto de cadenas de símbolos pertenecientes a algún alfabeto A que se utiliza para escribir un mensaje. Este conjunto se conoce como el texto común.
2. C es un conjunto de cadenas de símbolos, elementos de algún alfabeto B; que se usan para reemplazar los símbolos de un mensaje. A C se le llama el texto de cifrado.
3. K es un conjunto …nito de posibles claves, el cual puede ser un conjunto …nito de números o de n-adas que sirven para distinguir a cada elemento de los conjuntos E y D:
4. Para cada $k \in K$ existen elementos $e_k \in E$ y $d_k \in D$ tales que e_k es una biyección $e_k : P \to C$ llamada función de encripción, d_k es la función inversa de e_k; $d_k : C \to P$; conocida como función de desencripción, esto quiere decir que $d_k(e_k(x)) = x$ para cada $x \in P$:

Al proceso de aplicar la función e_k a los símbolos de algún mensaje $m \in P$ se le llama encripción y al proceso de aplicar la función d_k a los elementos de algún mensaje $c \in C$ se le llama desencripción.

4 Un sistema criptográ…co sencillo.

Supóngase que dos personas, Alicia y Roberto, se comunican frecuentemente a través de cartas y que una tercera persona, Oscar, siempre se entera de sus mensajes.

Ellos desean seguir comunicándose pero sin que Oscar sepa lo que se escriben. Alicia y Roberto podrían construir un pequeño sistema que les proporcione mayor discreción. Considérese la siguiente asignación entre el alfabeto español

$$fa; b; c; d; e; f; g; h; i; j; k; l; m; n; ñ; o; p; q; r; s; t; u; v; w; x; y; zg$$

y una colección de números, por decir,

$$A = f0; 1; 2; :::; 26g$$

que hace corresponder un número a cada letra como sigue:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

o	p	q	r	s	t	u	v	w	x	y	z
15	16	17	18	19	20	21	22	23	24	25	26

Esta será una convención para no hacer evidente el uso del alfabeto español. Alicia desea transmitir el siguiente mensaje:

reunamonosenoaxaca

Utilizando la correspondencia dada, Alicia obtiene la sucesión de números:

$$^1 = 18\ 4\ 21\ 13\ 0\ 12\ 15\ 13\ 15\ 19\ 4\ 13\ 15\ 0\ 24\ 0\ 2\ 0$$

Con el propósito de di…cultar la comprensión del mensaje para Oscar, Alicia tiene en mente utilizar una regla r que cambia el orden de los números, renombrando el último número como el primero, el penúltimo como el segundo, y así, sucesivamente. La regla r queda entonces:

0	1	2	3	4	5	6	7	8	9	10	11	12	13
26	25	24	23	22	21	20	19	18	17	16	15	14	13

14	15	16	17	18	19	20	21	22	23	24	25	26
12	11	10	9	8	7	6	5	4	3	2	1	0

Obsérvese que la regla r es una biyección. Veáse también que aplicándose la misma regla r dos veces es posible obtener el valor del elemento al que fue aplicado esta regla en primera instancia.

Es decir, si se toma 7 del primer renglón y se le aplica r, se obtiene 19. A este último número le corresponde el 7, bajo la misma regla r. De esta manera, aplicando la regla r a cada número de ¹, Alicia obtendrá :

$$\& = 8\ 22\ 5\ 13\ 26\ 14\ 11\ 13\ 11\ 7\ 22\ 13\ 11\ 26\ 2\ 26\ 24\ 26$$

Para que Roberto pueda recuperar el mensaje, es necesario que conozca la regla pensada por Alicia. Esto requiere de una comunicación previa entre ambos, a través de algún canal seguro, antes de comenzar a transmitirse mensajes. En la práctica, lo anterior puede resultar difícil de lograr. Por ejemplo, Roberto puede vivir en una ciudad distinta a la de donde Alicia reside. Si desean comunicarse vía telefónica o correo electrónico, no se puede tener la certeza de que estos medios serán canales seguros. Esta di…cultad es conocida como el problema de la distribución de la clave.

Ahora es posible identi…car a los elementos que componen al sistema construído en ese ejemplo.

Los conjuntos $P; C$ y K son $P = C = f0; 1; 2; :::; 26g$ y $K = frg$: Mientras que $E; D$ son $E = fe_r g; D = fd_r g$: Las funciones $e_r : P \to C$ y $d_r : C \to P$ vienen dadas por

$$e_r(x) = 26 \text{ ¡ } x \text{ con } x \in P \text{ y } d_r(y) = 26 \text{ ¡ } y \text{ con } y \in C:$$

Es posible observar que las correspondencias e_r y d_r son la misma, dicho de otra manera, es tan sencillo calcular & a partir de un mensaje ¹; como lo es calcular ¹ de &: Sería preferible construir una función con la que fuera sencillo calcular & a partir de ¹; pero que fuese muy difícil hallar ¹ a partir de &: A este tipo de función se le conoce como función de un sólo sentido.

5 Criptografía simétrica o de clave privada.

La criptografía simétrica se re…ere al conjunto de métodos que permiten tener comunicación segura entre dos partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente que se llamará clave simétrica. La simetría se re…ere a que ambas partes comparten la misma clave tanto para encriptar como para desencriptar. Este tipo de criptografía se conoce también como criptografía de clave privada.

La criptografía simétrica ha sido la más usada en toda la historia; ésta ha sido implementada en diferentes dispositivos: manuales, mecánicos, eléctricos. Los sistemas de cifrado de substitución son los más antiguos, éstos son los sistemas llamados de papel y lápiz.

Con la invención de la máquina de escribir tanto mecánica como eléctrica fue posible la automatización de la encripción; esto permitió que se desarrollaran sistemas de cifrado más rápidos y con menor tendencia a equivocarse. La era de la computación y la electrónica ha signi…cado una libertad sin precedente para los diseñadores de sistemas de cifrado. Incluso muchos de los algoritmos simétricos actuales son programables en cualquier computadora. La idea general es aplicar diferentes funciones al mensaje que se quiere cifrar de tal modo que sólo conociendo una clave pueda aplicarse de forma inversa para poder así descifrarlo y recuperar la información.

6 Criptografía asimétrica o de clave pública.

La criptografía asimétrica es por de…nición aquella que utiliza dos claves diferentes para cada usuario, una para encriptar que se le llama clave pública y otra para desencriptar que es la clave privada. El nacimiento de la criptografía asimétrica en el año de 1976 se dió al estar buscando un modo más práctico de intercambiar las claves simétricas. Whit…eld Di¢e y Martin Hellman propusieron una forma para hacer esto. Di¢e y Hellman estaban particularmente interesados en el problema de la distribución de las claves. Ellos transportaron el problema a un escenario físico donde nuevamente, Alicia y Roberto desean comunicarse secretamente. Whit…eld y Martin imaginaban una caja con dos candados distintos, donde Alicia tenía la llave que abría uno de las candados y la otra llave perteneciente al candado restante la poseía Roberto. De esta manera, si Alicia deseaba enviar un mensaje a Roberto, lo que tenía que hacer era escribir el mensaje y guardarlo dentro de la caja, cerrar la caja con su candado y enviarlo. Roberto, al recibir la caja, no podía usar su llave para abrir el candado de Alicia, en cambio, lo que tenía que hacer era utilizar su candado para cerrar por segunda ocasión la caja y enviarla de regreso a Alicia. Al recibir la caja, ella quitaría su candado y mandaría la caja de regreso a Roberto. Así que cuando éste recibía por segunda vez la caja, ésta ya solamente venía cerrada con un candado, su candado, y entonces podía abrir la caja y obtener el mensaje. De esta manera, se hacía posible la transmisión de información de una manera segura sin necesidad de un intercambio de las llaves. En términos de criptografía, abrir o cerrar el candado signi…ca encriptar o desencriptar el mensaje y las llaves que abren los candados son las claves de cada uno.

Sólo hacía falta entonces llevar la misma idea a un método práctico de resolver el problema de la distribución de claves. Comenzaron examinando varias funciones matemáticas. La mayoría de las funciones matemáticas son fáciles de calcular y fáciles de invertir, pero éstas no eran de interés para ellos. Mas bien, centraron su atención en las funciones de un sólo sentido. Una forma intuitiva de ilustrar una función de un sólo sentido es la acción de romper un huevo: es muy fácil romper un huevo, pero es imposible regresarlo a su condición original.

Di¢e y Hellman se concentraron en la Aritmética Modular, ya que ésta es rica en funciones de un sólo sentido.

Hellman se ocupó de las funciones de la forma $m^k \bmod n$ y construyó un esquema donde Alicia y Roberto se ponían de acuerdo en los valores m y n con la única restricción de que $m < n$: Estos valores son públicos y no importa que Oscar los conozca. Alicia y Roberto trabajan de la manera siguiente:

Supógase que Alicia y Roberto se han puesto de acuerdo en los valores $m = 7$ y $n = 11$: Ahora deben seguir los pasos siguientes:

	Alicia	Roberto
Paso 1	Alicia escóge un número secreto, por decir, $a = 3$.	Roberto escóge un número secreto, por decir, $b = 6$.
Paso 2	Alicia sustituye a en la función y calcula $® = m^a \bmod n$: $® = 7^3 \bmod 11 = 2$:	Roberto sustituye b en la función y calcula $¯ = m^b \bmod n$: $¯ = 7^6 \bmod 11 = 4$:
Paso 3	Alicia envía ® a Roberto.	Roberto envía ¯ a Alicia.
Paso 4	Alicia recibe ¯ y calcula $¯^a \bmod n$; es decir, $4^3 \bmod 11 = 9$:	Roberto recibe ® y calcula $®^b \bmod n$; es decir, $2^6 \bmod 11 = 9$:

Ambos coinciden y obtienen la misma clave 9. Desde el punto de vista de Oscar, aunque éste conociera ® y ¯; todavía tendría que intentar calcular a a partir de $® = 7^a \bmod 11$ o b a partir de $¯ = 7^b \bmod 11$; lo cual es bastante difícil de lograr. El esquema de Di¢e-Hellman-Merkle, como se le conoce, permite establecer comunicación secreta por una vía pública.

Mientras tanto, Di¢e había estado trabajando con un enfoque un tanto distinto. El concibió el concepto general de un sistema de cifrado asimétrico. Pensaba que en un sistema asimétrico la clave de encripción y la clave de desencripción no debían ser las mismas. Esto signi…caba que Alicia tendría un par de claves: Una para encriptar y otra para desencriptar. La clave de desencripción es su clave privada y la clave de encripción es su clave pública, y es esta última la que se pone abierta al público para que cualquiera tenga acceso a ella. Así, si Roberto deseaba enviar un mensaje a Alicia, únicamente tenía que buscar su clave pública en una especie de directorio telefónico y ponerse en contacto con ella. De esta manera, no sólo Roberto podría comunicarse con Alicia, también lo podrían hacer Carlos, Eduardo, Juan o cualquiera que deseara establecer comunicación con ella.

Al …nal de 1976, Di¢e y Hellman habían revolucionado el mundo de la criptografía. Con sus ideas habían persuadido al mundo de que había solución para el problema de la distribución de claves. Sin embargo, aún faltaba encontrar una función de un sólo sentido que fuera la apropiada para cumplir con los requerimientos de su esquema.

Fue entonces cuando Ronald Rivest, Adi Shamir y Leonard Adleman entraron a escena, al proponer en 1978 el sistema de cifrado de más in‡uencia en la criptografía moderna, el método RSA, cuyo funcionamiento está basado en la di…cultad computacional de factorizar números enteros grandes.

Desde entonces, varios métodos asimétricos fueron desarrollados basados en diferentes problemas computacionalmente difíciles. A continuación se presentan algunos de ellos según el problema en el que basan su seguridad.

Método de clave pública	Problema en el que basa su seguridad
RSA	Problema de factorización entera
Rabin	Raices cuadradas módulo n
ElGama1	Problema del logaritmo discreto
ElGamal generalizado	Problema del logaritmo discreto generalizado

Problema de factorización entera. Dados un entero positivo n el cual es producto de dos números primos distintos e impares p y q; un entero positivo e tal que $mcd(e;(p ¡ 1)(q ¡ 1)) = 1$ y un entero c; encontrar un entero m tal que $m^e \acute{} c \bmod n$:

Problema de raíces cuadradas. Dados un entero positivo n el cual es producto de dos números primos p; q; y un entero c; encontrar un entero x tal que $x^2 \acute{} c \bmod n$:

Problema del logaritmo discreto. Dados un número primo p; un generador ® de $Z_p^¤$ y un elemento $¯ 2 Z_p^¤$; encontrar el entero x con $0 · x · p ¡ 2$; tal que $®^x \acute{} ¯ \bmod p$:

Problema del logaritmo discreto generalizado. Dados un grupo cíclico …nito G de orden n; un generador ® de G y un elemento $¯ 2 G$; encontrar el entero x con $0 · x · n ¡ 1$; tal que $®^x = ¯$:

Actualmente la Criptografía asimétrica es muy usada; sus dos principales aplicaciones son el intercambio de claves privadas y la …rma digital. Esta última se utiliza para veri…car la autoría de un documento electrónico tal y como se hace con los documentos que llevan …rmas autógrafas.

Capítulo II
El criptosistema RSA

En el presente capítulo, se introducirá el famoso sistema RSA. Algunos aspectos sobre su origen y su desarrollo se proveen en la primera sección del capítulo. En la sección 2, se dará un breve recordatorio de algunos resultados básicos de la Teoría de grupos y la Teoría de números. Estos resultados serán fundamentales para determinar tanto el conjunto P de texto común y el conjunto C de texto de cifrado como las funciones de encripción y desencripción del criptosistema RSA. La tercera sección del capítulo describe la construcción de las funciones de encripción y desencripción del esquema RSA. Por último, la sección 4 presenta la de…nición del sistema RSA, el esquema general del mismo y un ejemplo.

1 Generalidades del sistema RSA.

El nacimiento de la criptografía de clave pública en 1976, trajo consigo que varios grupos de investigadores se interesaran por encontrar funciones de un sólo sentido que se ajustaran al esquema que Di¢e y Hellman habían propuesto. Tal fue el caso de un trío de investigadores del MIT, Ronald Rivest, Adi Shamir y Leonard Adleman, quienes pasaron alrededor de un año buscando funciones de un sólo sentido que fuesen ideales para el esquema de clave pública. En abril de 1977, Rivest, Shamir y Adleman encontraron dicha función al utilizar números primos para la construcción de las claves.

Como se mencionó anteriormente, el sistema RSA basa su seguridad en la di…cultad de factorizar el producto de dos números primos grandes. A pesar de los años de investigación en la búsqueda de técnicas para conocer los factores de un número, no se ha encontrado algún método sencillo para factorizar un número "grande". Existen varios algoritmos de factorización de números, los más rápidos sólo atacan características especí…cas del número, mientras que los más generales consumen mucho más tiempo que los anteriores. Aún con la combinación de todos estos métodos, RSA es capaz de proveer un alto grado de seguridad en sus diversos usos porque el tiempo que consumen estos algoritmos sigue siendo considerable cuando se trata de factorizar números grandes. En la práctica, se trabajan con claves de más de 200 dígitos de longitud, lo cual permite tener entre 10 y 20 años de seguridad antes de poder factorizar una clave. La medición de la seguridad de una clave utiliza como paramétro el poder de cómputo mundial. Este poder de cómputo se puede determinar para algún año en especí…co, calculando los millones de instrucciones por segundo (mips) de todas las computadoras disponibles en el mundo.

Luego, en base a la longitud del número que se desea factorizar, se calcula el poder de cómputo necesario para lograr tal factorización. Después, se ubica el año en el que se podría tener ese poder de cómputo; y el tiempo que resta para llegar a dicho año es el tiempo en que se garantiza la seguridad de la clave, suponiendo además, que no habrá cambios bruscos en la tecnología durante algunos años.

Otro punto importante para la seguridad de las claves es la generación de números primos, estos números se generan aleatoriamente con una cierta probabilidad de que el número generado no sea primo. Varias pruebas de primalidad son usadas en conjunto para asegurar con el mínimo margen de error que un número es primo.

Los usos más comunes de RSA son: El intercambio de claves secretas, el cifrado y descifrado de mensajes relativamente cortos y el empleo de la …rma digital.

2 Teoría de números y teoría de grupos.

Para el tratamiento de esta sección se supone el conocimiento de de…niciones y propiedades básicas de la Teoría de números y el Álgebra. Las pruebas de los resultados de esta sección pueden encontrarse en [1],[3] y [15].

Teorema 2.1. (Algoritmo de la división). Para cualquier entero a y cualquier entero $b \neq 0$, existen enteros únicos q y r tales que $0 \cdot r < |b|$ y $a = bq + r$.

Teorema 2.2. Si $a = bq + r$ para algunos enteros $a; b; q; r$; entonces $mcd(a; b) = mcd(b; r)$:

El siguiente algoritmo es conocido como el Algoritmo de Euclides. Se usa para el cálculo de máximos comunes divisores y en consecuencia, para resolver congruencias lineales. La utilidad que tiene en el criptosistema RSA es que permite encontrar el exponente de desencripción mediante la solución de una congruencia.

Algoritmo de Euclides.

Sea $a = bq_1 + r_1$ para algunos enteros $a; b; q_1; r_1$ donde $0 \cdot r_1 < |b|$ con $b \neq 0$:

Si $r_1 \neq 0$; sea r_2 tal que $b = r_1q_2 + r_2$ donde $0 \cdot r_2 < r_1$:

En general, sea r_{i+1} tal que $r_{i-1} = r_iq_{i+1} + r_{i+1}$ donde $0 \cdot r_{i+1} < r_i$:

Por el principio del buen orden, existe $t \in \mathbb{N}$ tal que la sucesión de residuos $r_1; r_2; :::$ debe terminar con algún $r_t = 0$: Si $r_1 = 0$; entonces $mcd(a; b) = b$: Si $r_1 \neq 0$ y r_s es el primer residuo igual a cero, entonces $mcd(a; b) = r_{s-1}$:

Esto es porque, según el teorema 2.2, $mcd(a;b) = mcd(b;r_1) = mcd(r_1;r_2) = ::: = mcd(r_{s-2};r_{s-1})$: Pero como $r_{s-2} = r_{s-1}q_s + r_s$ y $r_s = 0$; entonces $r_{s-2} = r_{s-1}q_s$ y se ve que $mcd(a;b)$ es el último residuo distinto de cero, esto es, $mcd(a;b) = mcd(r_{s-2};r_{s-1}) = r_{s-1}$:

Los teoremas y proposiciones que a continuación se exponen, permiten construir la función inversa de la función de encripción, es decir, la función de desencripción.

Teorema 2.3. (Teorema de Lagrange). Si $(G;¤)$ es un grupo …nito y $(S;¤)$ es un subgrupo de $(G;¤)$ entonces el orden de S es un divisor del orden de G:

Proposición 2.1. Si $(G;¤)$ es un grupo …nito con identidad e, entonces para cualquier $a \in G$ se cumple que $a^{|G|} = e$ donde $|G|$ denota el orden de G:

Proposición 2.2. La ecuación $ax \equiv b \bmod n$ tiene solución para x si y sólo si $mcd(a;n) \mid b$:

Proposición 2.3. Para cualquier $n > 1$; si $mcd(a;n) = 1$; entonces la ecuación $ax \equiv b \bmod n$ tiene una única solución módulo n:

Las congruencias de las proposiciones 2.2 y 2.3, se resuelven usando el algoritmo de Euclides.

Teorema 2.4. (Teorema de Euler). Para cualesquiera enteros $a;n$ con $n > 1$ y $mcd(a;n) = 1$:

$$a^{Á(n)} \equiv 1 \bmod n$$

donde $Á(n)$ es el número de enteros positivos primos relativos a n menores que n:

Teorema 2.5. (Teorema de Fermat). Si p es primo y $p \nmid a$, entonces

$$a^{p-1} \equiv 1 \bmod p:$$

3 Funciones de un sólo sentido en Z_n.

En el capítulo I, se mencionó que las funciones de la forma $f(x) = a^x \bmod n$ con $a;n$ enteros positivos, son funciones de un sólo sentido, esto es, calcular $f(x)$ a partir de x es fácil, mientras que obtener x partiendo de $f(x)$ no lo es.

El conjunto que actúa como dominio y contradominio de estas funciones es Z_n; el anillo de enteros módulo n: De aquí que los elementos de los conjuntos P; C sean enteros modulo n: RSA utiliza este tipo de funciones para encriptar y desencriptar.

Ahora, sea Z_n^* el conjunto formado por los elementos de Z_n que son primos relativos con n: Por de…nición, el orden de Z_n^* es Á(n): El conjunto Z_n^* se conoce como el grupo multiplicativo de Z_n: Si p es primo, $Z_p^* = p - 1$ pues todos los números enteros positivos menores que p son primos relativos a éste; de modo que Á(p) = p ¡ 1: En tanto que si n = pq con p; q primos, Á(n) = (p ¡ 1)(q ¡ 1) = Á(p)Á(q):

Bajo el supuesto de que n = pq con p; q primos, sean $m \in Z_n$ y $e \in Z_n^*$: Entonces, por la proposición 2.3 existe $d \in Z_n$ tal que $ed \equiv 1 \bmod Á(n)$; esto es, ed = 1 + kÁ(n) para algún $k \in Z$:

Analizando lo que sucede cuando se utiliza el valor e como exponente de encripción y d como el exponente de desencripción se obtiene lo siguiente:

Para el caso mcd(m; p) = 1; se tiene por el teorema 2.5 que $m^{p-1} \equiv 1 \bmod p$: Al elevar ambos lados de la congruencia a la potencia k(q ¡ 1); se obtiene $m^{k(p-1)(q-1)} \equiv 1 \bmod p$: Después, multiplicando la congruencia anterior por m; resulta $m^{1+k(p-1)(q-1)} \equiv m \bmod p$; esto es, $m^{ed} \equiv m \bmod p$:

Para el caso mcd(m; p) = p; se tiene m = kp para algún $k \in Z$: De aquí, $m \equiv 0 \bmod p$ y $m^{ed} \equiv 0 \bmod p$: Luego, $m^{ed} \equiv m \bmod p$:

Como los mismos argumentos son válidos para q; entonces $m^{ed} \equiv m \bmod q$: Finalmente, al ser p y q números primos distintos se tiene que mcd(p; q) = 1 y por lo tanto $m^{ed} \equiv m \bmod n$: Esto deja ver que es fácil calcular $m^e \bmod n$ a partir de m; pero para recuperar m partiendo de $m^e \bmod n$ se requiere del conocimiento de d: El conocimiento de d se di…culta cuando no se sabe Á(n); pues en este caso no se puede resolver $ed \equiv 1 \bmod Á(n)$: Ahora, Á(n) no se puede obtener si sólo se conoce el valor de n pues a partir de él no es posible saber quienes son p y q; lo cual es fundamental para calcular Á(n):

Las ideas del desarrollo anterior se encuentran en [13] y se pueden resumir en el siguiente teorema:

Teorema 2.6. Sea n = pq con p; q números primos. Considérese $e \in Z_n^*$ tal que mcd(e; Á(n)) = 1: Entonces exite $d \in Z_n$ tal que $m^{ed} \equiv m \bmod n$ para todo $m \in Z_n$:

4 Esquema general del sistema RSA.

Para Rivest, Shamir y Adleman uno de los puntos clave es la construcción del número n a partir de dos números primos.

En efecto, esta construcción es una función de un sólo sentido pues resulta muy complicado conocer algún factor de n; si no se conoce el otro factor. Al usar números con longitudes de más de 200 dígitos se requiere de un gran consumo de tiempo para calcular su factorización.

A continuación se de…ne de manera formal el criptosistema RSA.

Sea $n = pq$; donde p y q son números primos. Los conjuntos de texto común y de texto de cifrado $P; C$ son $P = C = Z_n$: El conjunto de claves viene dado por:

$$K = f(n; p; q; e; d) \; j \; n = pq \text{ y } ed \acute{} 1 \bmod Á(n)g:$$

Para $k \; 2 \; K$; las funciones de encripción y de desencripción e_k y d_k están de…nidas por:

$$e_k(x) = x^e \bmod n \text{ y } d_k(y) = y^d \bmod n$$

para $x; y \; 2 \; Z_n$: Los valores n y e son públicos, mientras que $p; q$ y d son secretos.

Obsérvese que el teorema 2.6, es el que permite recuperar el valor de $x \; 2 \; Z_n$ cuando se aplica la función d_k a un valor de $y \; 2 \; Z_n$:

Algoritmo RSA de clave pública

Generación de las claves pública y privada.
1. Generar dos números primos $p; q$:
2. Calcular $n = pq$ y $Á(n) = (p ¡ 1)(q ¡ 1)$:
3. Elegir un entero e tal que $1 < e < Á(n)$ y $mcd(e; Á(n)) = 1$:
4. Calcular d tal que $ed = 1 \bmod Á(n)$:
5. La clave pública es $(n; e)$ y la clave privada es (d):

Encripción. Representar el mensaje M como un elemento $m \; 2 \; Z_n$:
1. Calcular $c = m^e \bmod n$:
2. Enviar c.

Desencripción. Para recuperar el mensaje m a partir de c:
1. Calcular $m = c^d \bmod n$:

Para ilustrar el uso del algoritmo anterior, se desarrolló el siguiente ejemplo:

Ejemplo 2.1.

Generación de claves. Alicia crea su propia clave pública.

1. Alicia escóge $p = 17$ y $q = 11$:
2. Calcula $n = 187$ y $Á(n) = 160$:
3. Elige $e = 7$ ya que $mcd(7; 160) = 1$:
4. Resuelve $7d \acute{} 1 \mod 160$; obteniendo $d = 23$:
5. La clave pública de Alicia es $(187; 7)$ y su clave privada es (23):

Encripción. Roberto envía un mensaje a Alicia.

1. Representa su mensaje M como un entero m 2 $[0; 160]$; por decir, $m = 88$:
2. Calcula $c = 88^7 \mod 187 = 894432 \mod 187 = 11$:
3. Roberto envía $c = 11$:

Desencripción. Alicia recibe el mensaje c.

1. Calcula $m = 11^{23} \mod 187 = 88$; con lo que ha recuperado m:

Capítulo III

Un criptosistema de clave pública que utiliza campos cúbicos

En este capítulo se expone un criptosistema del tipo RSA el cual fundamenta su aritmética sobre el campo cúbico $Q(\pm)$ donde $\pm = \sqrt[3]{D}$ para algún $D \in Z$. Tanto la primera como la segunda sección del capítulo están destinadas a proporcionar las bases matemáticas del sistema. En la sección 1, se encuentran algunos elementos de la Teoría algebraica de números pues los conjuntos de texto común y de texto de cifrado para este sistema se de…nen como anillos cocientes. La sección 2 se dedica al estudio de algunas características de los elementos primos del anillo $Z[^3]$; donde $^3 = \frac{i\,1+\sqrt{i\,3}}{2}$; como el carácter cúbico residual y la ley de la reciprocidad cúbica. Los elementos primos de $Z[^3]$ son importantes para complementar la de…nición del dominio y el contradominio de las funciones de encripción y desencripción. Los resultados que aparecen en la sección 3 tienen como propósito exponer de manera especí…ca los conjuntos de texto común y de texto de cifrado y sustentar el teorema 3.4, el cual es el teorema principal del criptosistema pues provee tanto la forma de la función de encripción como la de la función de desencripción, así como la estructura que tienen los elementos con los que operan estas funciones. La cuarta sección comenta algunas consideraciones que facilitarán la representación, encripción y desencripción de un mensaje en la práctica. En la última sección del capítulo, se de…ne el sistema, se describe su esquema general y se ilustra mediante un ejemplo.

1 Teoría algebraica de números.

Durante esta sección, se supone el conocimiento de las de…niciones y propiedades básicas de la teoría de anillos y extensiones de campos (ver apéndice A). La demostración del teorema 3.1 puede consultarse en [7]. La prueba del teorema 3.2 está en [6]. También, L y E denotan extensiones …nitas sobre Q de grados r y s respectivamente; y L es una extensión de E de grado n:

De…nición 3.1. Sea B un anillo y A un subanillo de B. Un elemento $b \in B$ se llama integral sobre A si existen $a_i \in A$ tales que $f(b) = 0$ donde $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$: Obsérvese que si A y B son campos, entonces un elemento $b \in B$ es integral sobre A si y sólo si es algebraico sobre A:

De…nición 3.2. Sea A un anillo contenido en un campo L: Al conjunto B de elementos en L que son integrales sobre A; se le conoce como la cerradura integral de A en L:

El conjunto anterior es un anillo [6]. La cerradura integral de Z en L es conocida como el anillo de enteros de L; y se denota por O_L:

De…nición 3.3. Sea L una extensión de Galois de E y $¾_1; :::; ¾_n$ los distintos E-automor…smos de L: Sea b 2 L: El polinomio característico $g_b(x)$ de b con respecto a L=E es $\prod (x ¡ ¾_i(b))$ y la norma $N_{L=E}(b)$ de b respecto a L=E se de…ne como $\prod ¾_i(b)$:

La norma de b respecto a L=E es un elemento de E y el polinomio $g_b(x)$ pertenece a E[x] [6]. En lo que resta de la sección $N_{L=E}(b)$ se denotará sólo como N(b): En [4] se prueba que $N_{L=\mathbb{Q}}(a) 2 Z$.

Teorema 3.1. Todo ideal propio en el anillo O_L se puede representar de manera única como un producto de ideales maximales.

Teorema 3.2. Sea A el anillo de enteros de E y supóngase que el campo de cocientes de A es E. Sea B la cerradura integral de A en L: Además, supóngase que B = A[®] para algún ® 2 L: Sea f(x) 2 A[x] el polinomio mónico irreducible de ® sobre E: Sea ¼ un elemento primo de A y sean $f_i(x)$ 2 A[x] los polinomios mónicos tales que

$$f^1(x) = \prod_{i=1} f_i^1(x)^{e_i} \; 2 \; A_¼[x]$$

es la factorización de $f^1(x)$ en $A_¼ = A=¼A$ y $f_i^1(x)$ es un polinomio irreducible sobre $A_¼$: Entonces en B

$$¼B = \prod_{i=1} P_i^{e_i}$$

donde $P_i = (¼; f_i(®))$ es ideal maximal de B.

Obsérvese que si L=E es de Galois, aplicando el teorema A.12 se tiene que $¼B = \prod_{i=1}^{m} P_i^e$ donde efm = n:

De…nición 3.4. En las condiciones del teorema anterior se dice que ¼ se rami…ca en B si e > 1: Si e = f = 1; entonces se dice que ¼ se descompone totalmente y en este caso, $¼B = \prod_{i=1}^{m} P_i$: Finalmente, se dice que ¼ es inerte cuando m = 1 y f = [L : E]:

2 El anillo Z[³]:

Sea ³ una de las raices cúbicas complejas de 1, es decir, $³ = \frac{¡1 § \sqrt{¡3}}{2}$:

El conjunto $Z[\omega] = \{\alpha \mid \alpha = a + b\omega \text{ con } a, b \in Z\}$ es el anillo de enteros de $Q(\omega)$ [1]. Ahora, para $\alpha = a + b\omega$ con a, b en Q, la norma de α es $N_{Q(\omega)/Q}(\alpha) = (a + b\omega)(a - b - b\omega) = a^2 - ab + b^2$, ya que los Q-automor…smos de $Q(\omega)$ están de…nidos por $i(\omega) = \omega$ y $\sigma(\omega) = \omega^2 = -1 - \omega$. Por convención, en esta sección se entenderá $N(\alpha)$ como $N_{Q(\omega)/Q}(\alpha)$.

Las pruebas de las siguientes proposiciones pueden consultarse en [4].

Proposición 3.1. Supóngase que p es un número primo en Z tal que $p \equiv 1 \bmod 3$, entonces $p = \pi\bar{\pi}$, donde π es primo en $Z[\omega]$.

Proposición 3.2. Supóngase que π es un primo en $Z[\omega]$ tal que $N(\pi) \neq 3$ y que $\pi \nmid \alpha$. Entonces existe un único entero $m = 0, 1 \text{ o } 2$ tal que $\alpha^{\frac{N(\pi)-1}{3}} \equiv \omega^m \bmod \pi$.

De…nición 3.5. Si π y m son como en la proposición 3.2, el carácter cúbico residual de α módulo π está de…nido por $\left(\frac{\alpha}{\pi}\right) = \omega^m$. Cuando $N(\pi) \neq 3$ y $\pi \mid \alpha$, se de…ne $\left(\frac{\alpha}{\pi}\right) = 0$.

Proposición 3.3.

1. $\left(\frac{\alpha}{\pi}\right) = 1$ si y sólo si $x^3 \equiv \alpha \bmod \pi$ tiene solución. En este caso, se dice que α es un residuo cúbico módulo π.
2. $\alpha^{\frac{N(\pi)-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right) \bmod \pi$.
3. $\left(\frac{\alpha}{\pi}\right) = \left(\frac{\alpha}{\bar{\pi}}\right)^2$.
4. Si $\alpha \equiv \beta \bmod \pi$, entonces $\left(\frac{\alpha}{\pi}\right) = \left(\frac{\beta}{\pi}\right)$.

3 Funciones de un sólo sentido en $Z[\omega][\pm]_{\frac{1}{\pi}}$.

Al igual que el sistema RSA, el criptosistema de campos cúbicos que aquí se presenta utiliza funciones de un sólo sentido de la forma $f(x) = x^a \bmod n$ como sus funciones de encripción y desencripción. Es importante mencionar que las anteriores funciones de un sólo sentido tendrán un anillo cociente como su dominio y contradominio. A continuación, se estudiarán los conjuntos donde operarán dichas funciones y se hará énfasis en el uso de los resultados de las secciones 1 y 2, y del apéndice A para la demostración de los teoremas 3.3 y 3.4 que son fundamentales para entender el CCC.

Sean:
D un entero libre de potencias cúbicas,
$\pm$ la única raíz cúbica real de D; esto es, $\pm = \sqrt[3]{D}$;
$K = Q(\pm)$ el campo cúbico generado por $\pm$;
ω una raíz cúbica no trivial de la unidad, es decir, $\omega = \frac{-1+\sqrt{-3}}{2}$;
$k = Q(\omega)$ el campo generado por ω;
$L = K(\omega) = k(\pm) = Q(\omega, \pm)$.

Usando la de…nición A.20 y los teoremas A.5 y A.6 se obtiene que los grados de las extensiones $[K : Q]$; $[k : Q]$ y $[L : Q]$ son 3,2 y 6 respectivamente.

Para cada uno de los campos anteriores, considérese su anillo de enteros. Esto es, $O_k = Z[^3]$ es el anillo de enteros de k; $O_K \P Z[\pm]$ corresponde al anillo de enteros de K; mientras que $O_L \P Z[^3][\pm]$ es el anillo de enteros de L:

El conjunto de Q-automor…smos de L tiene dos generadores $¾; ¿$ de…nidos por

$$¿(\pm) = {}^3\pm; ¿(^3) = {}^3 \quad \text{y} \quad ¾(\pm) = \pm; ¾(^3) = {}^{3^2}:$$

Estos generadores satisfacen

$$¾^2 = ¿^3 = (¾¿)^2 = i;$$

donde i es el automor…smo identidad.

Para μ 2 L; se escribirá $¾(\mu) = \overset{1}{\mu}; ¿(\mu) = \mu^0; ¿^2(\mu) = \mu^{00}$: Entonces la norma de μ respecto a L=k es $N_{L=k}(\mu) = \mu\mu^0\mu^{00}$ 2 k: Si μ 2 K; $N_{L=k}(\mu) = N_{K=\mathbf{Q}}(\mu)$ 2 Q: En adelante $N_{L=k}(\mu)$ se denotará solamente como $N(\mu)$:

Como se ha mencionado anteriormente, los conjuntos P de texto común y C de texto de cifrado serán anillos cocientes. Por esto se considerará el anillo O_L y un ideal en él. A partir de un elemento primo ¼ 2 $Z[^3]$ se generan dos ideales; uno está en O_k y el otro en O_L: En seguida, se analizará lo que sucede al tomar en cuenta los ideales descritos previamente.

Sea p un número primo tal que p no divide a D y $p \acute{} 1 \mod 3$: Por la proposición 3.1, $p = ¼¼¼$ donde ¼ es un elemento primo en $Z[^3]$: Ahora, por la proposición 3.2, existe un único j 2 f0; 1; 2g tal que $\mu^{\frac{p\,j\,1}{3}} \acute{} {}^j \mod ¼$:

Considérense los anillos O_L y O_k: Aplicando el teorema 3.1 al ideal de O_L generado por ¼ se obtiene que

$$¼O_L = P_1^{e_1}P_2^{e_2}:::P_m^{e_m}$$

donde cada ideal primo P_i en O_L tiene grado de inercia f_i: Por el teorema A.11 se cumple que

$$e_1f_1 + e_2f_2 + ::: + e_mf_m = 3$$

ya que la extensión L=k es de grado 3.

Ahora, L=k es una extensión de Galois y por el teorema A.12, $e_i = e$ y $f_i = f$ para $i = 1;:::;m$; con $efm = 3$. Esto sólo deja tres posibilidades:

1. $e = 3$; $f = 1$; $m = 1$ con lo que $¼O_L = P^3$:
2. $e = 1$; $f = 3$; $m = 1$ de donde $¼O_L = P$ un ideal primo en O_L; es decir, ¼ es inerte.
3. $e = 1$; $f = 1$; $m = 3$ lo que implica $¼O_L = P_1P_2P_3$:

La extensión L=k es separable ya que es de Galois. También, el conjunto $f1;±;±^2g \; 2 \; L$ es linealmente independiente sobre k y el polinomio $x^3 ¡ D$ es minimal para ± sobre k: Por lo tanto, aplicando la proposición A.3 se tiene que el discriminante de la extensión L=k es $d_L = ¡27D^2$: Ahora, considérense todos los ideales de O_L que están sobre $¼O_k$: Los cocientes $O_L=P_i$ donde P_i es un ideal maximal que está sobre $¼O_k$ son campos …nitos [7], y por tanto, son perfectos [1]. Por lo tanto, se sigue de [2] que ¼ se rami…ca en O_L si y sólo si ¼ divide a d_L: Como ¼ divide a p; pero p no divide a D entonces ¼ no puede dividir a d_L y por lo anterior, la primera posibilidad queda descartada.

Por otra parte, se sabe por la proposición A.10 que $Z[³]=¼Z[³]$ es un campo …nito. Supóngase que D es un residuo cúbico módulo ¼; por decir, $D ´ u^3 \bmod ¼$ para alguna u en $Z[³]$. El polinomio $f(x) = x^3 ¡ D$ módulo ¼; puede factorizarse como

$$f(x) = (x ¡ u)(x ¡ ³u)(x ¡ ³^2u) \bmod ¼$$

donde cada polinomio lineal es irreducible modulo ¼ y con u; ³u; $³^2u$ en $Z[³]$: Entonces, aplicando el teorema 3.2, se tiene que $¼O_L$ se descompone en O_L en tres ideales primos distintos de O_L, esto es, $¼O_L = P_1P_2P_3$ donde $P_1 = (¼;± ¡ u)$; $P_2 = (¼;± ¡ ³u)$ y $P_3 = (¼;± ¡ ³^2u)$: Además, se puede ver que $¿(P_1) = P_3$ y $¿^2(P_1) = P_2$; aplicando el automor…smo ¿ a cada generador de P_1:

Por otro lado, si $¼O_L$ se descompone en tres ideales primos distintos en O_L; por el mismo teorema 3.2, $f(x) = x^3 ¡ D$ debe descomponerse en tres factores lineales diferentes módulo ¼; es decir,

$$f(x) = (x ¡ a)(x ¡ b)(x ¡ c) \bmod ¼:$$

Multiplicando y comparando los coe…cientes se obtienen las siguientes congruencias:

$$\begin{aligned} a + b + c &´ 0 \bmod ¼; \\ ab + ac + bc &´ 0 \bmod ¼; \\ abc &´ D \bmod ¼: \end{aligned}$$

Resolviendo el sistema, se deduce que $D \equiv abc \equiv a^3 \bmod \pi$; es decir, D es un residuo cúbico módulo π:

Todo lo anterior se puede resumir de la siguiente manera:

Teorema 3.3. El ideal πO_L se descompone en tres ideales primos distintos en O_L si y sólo si D es un residuo cúbico módulo π: Además, π es inerte en O_L si y sólo si D no es un residuo cúbico módulo π:

Con esta relación se ve que la conveniencia de considerar ideales generados por elementos primos en $Z[\zeta]$ radica en que al tomar un ideal πO_k es posible construir un ideal primo πO_L en O_L mediante la aplicación de la proposición A.6.

El siguiente desarrollo se deriva de la inercia de π y provee algunas propiedades para los elementos de $O_L/\pi O_L$. Suponiendo que π es inerte, πO_L es un ideal primo en O_L.

Por el teorema pequeño de Fermat, $D^p \equiv D \bmod p$ y entonces, también $D^p \equiv D \bmod \pi$; lo que implica $D^{p-1} \equiv 1 \bmod \pi$: Como D no es residuo cúbico módulo π entonces $\left(\frac{D}{\pi}\right)_3 = \zeta^j$ con $j \in \{1,2\}$ y por lo tanto, $\pm^{p-1} \equiv D^{\frac{p-1}{3}} \equiv \zeta^j \bmod \pi$; donde $\pm^p \equiv \zeta^j \pm \bmod \pi$: Esto signi…ca que $\pm^p \equiv \zeta \pm \bmod \pi$ o bien que $\pm^p \equiv \zeta^2 \pm \bmod \pi$: En ambos casos se tiene que

$$\begin{aligned} \pm^3 &\equiv D \bmod \pi; \\ (\pm^p)^3 &\equiv D \bmod \pi; \\ (\pm^{p^2})^3 &\equiv D \bmod \pi; \end{aligned}$$

y por tanto $\pm, \pm^p, \pm^{p^2}$ son las tres raices del polinomio $x^3 - D \bmod \pi$:

Por otro lado, las tres raices de $x^3 - D$ en L son $\pm, \sigma(\pm)$ y $\sigma^2(\pm)$: Así, los conjuntos $\{\pm, \sigma(\pm), \sigma^2(\pm)\}$ y $\{\pm, \pm^p, \pm^{p^2}\}$ deben ser los mismos en $O_L/\pi O_L$. Se tienen dos posibilidades, $\sigma(\pm) \equiv \pm^p \bmod \pi$ o $\sigma(\pm) \equiv \pm^{p^2} \bmod \pi$: Primero, se puede asumir que $\sigma(\pm) \equiv \pm^p \bmod \pi$:

Sea $\mu \in L$; esto es, $\mu = a + b\pm + c\pm^2$ con a, b, c en k: Por lo anterior, $\mu^0 = \sigma(\mu) \equiv \mu^p \bmod \pi$; es decir, σ resulta ser el automor…smo de Frobenius en $O_L/\pi O_L$. Por tanto, $N(\mu) \equiv \mu^{p^2+p+1} \bmod \pi$ en O_L: En el caso donde $N(\mu) \equiv 1 \bmod \pi$; se sigue que

$$\mu^{\frac{p^2+p+1}{3}} \equiv \zeta^i \bmod \pi$$

para algún $i \in \{0,1,2\}$:

Sea $\alpha \in \mathcal{O}_L$ con $\pi \mid \alpha$; $N = N(\alpha) \in \mathbb{Z}[\zeta]$ y sea $\beta = \frac{\alpha}{\alpha^0} = \frac{\alpha^2 \alpha''}{N}$: Entonces $N(\beta) = 1$ y por tanto $\beta^{\frac{p^2+p+1}{3}} \equiv \zeta^i \bmod \pi$ para algún $i \in \{0,1,2\}$: Como $\alpha^p \equiv \alpha^0 \bmod \pi$; entonces $\beta \equiv \alpha^{1-p} \bmod \pi$ y $\beta^{-\frac{p^2+p+1}{3}} \equiv (\alpha^{p^2+p+1})^{\frac{1-p}{3}} \equiv N^{\frac{1-p}{3}} \equiv \left(\frac{N}{\pi}\right)^{-1} \bmod \pi$:

De manera análoga, si se supone que $\varphi(\pi) \equiv \pi^{p^2} \bmod \pi$; entonces $\alpha^p \equiv \alpha'' \bmod \pi$; lo que implica que $\beta \equiv \alpha^{1-p^2} \bmod \pi$ y $\beta^{-\frac{p^2+p+1}{3}} \equiv (N^{p+1})^{\frac{1-p}{3}} \equiv N^{2\frac{1-p}{3}} \equiv \left[\frac{N}{\pi}\right] \bmod \pi$:

Por construcción, $\beta \in \mathcal{O}_L$; pero las operaciones se realizarán con su clase de equivalencia módulo π: El conjunto donde operarán las funciones de encripción y desencripción será al subanillo de $\mathcal{O}_L/\rho\mathcal{O}_L$ para algún ρ de…nido por:

$$\mathbb{Z}[\zeta][\pi]_\rho = \{\mu + \rho\mathcal{O}_L \mid \mu \in \mathbb{Z}[\zeta][\pi]\}.$$

Supóngase ahora que se tienen dos números primos p, q tales que $p, q \equiv 1 \bmod 3$. Por la proposición 3.1 existen $\pi, \Delta \in \mathbb{Z}[\zeta]$ tales que $p = \pi\pi''$ y $q = \Delta\Delta''$: Nuevamente, sin pérdida de generalidad se puede suponer que $\left(\frac{D}{\pi}\right) = \zeta$ y que $\left(\frac{D}{\Delta}\right) = \zeta^2$; ya que en caso de que $\left(\frac{D}{\pi}\right) = \left(\frac{D}{\Delta}\right)$ se puede sustituir Δ por $\bar{\Delta}$. Para los elementos α y β de…nidos anteriormente, se tiene que $\alpha^p \equiv \alpha^0 \bmod \pi$ y $\alpha^q \equiv \alpha'' \bmod \Delta$: Además, $\beta \equiv \alpha^{1-p} \bmod \pi$ y $\beta \equiv \alpha^{1-q^2} \bmod \Delta$: Por lo tanto,

$$\beta^{-\frac{p^2+p+1}{3}} \equiv \left(\frac{N}{\pi}\right)^{-1} \equiv \left(\frac{N}{\bar{\pi}}\right) \bmod \pi \text{ y}$$
$$\beta^{-\frac{q^2+q+1}{3}} \equiv \left(\frac{N}{\bar{\Delta}}\right) \bmod \Delta.$$

Como $p, q \equiv 1 \bmod 3$; entonces $\frac{p^2+p+1}{3} \equiv \frac{q^2+q+1}{3} \equiv 1 \bmod 3$: Así,

$$\beta^{-f} \equiv \left(\frac{N}{\bar{\Delta}}\right)^{\frac{q^2+q+1}{3}} \equiv \left(\frac{N}{\bar{\Delta}}\right) \bmod \pi \text{ y}$$
$$\beta^{-f} \equiv \left(\frac{N}{\bar{\Delta}}\right)^{\frac{p^2+p+1}{3}} \equiv \left(\frac{N}{\bar{\Delta}}\right) \bmod \Delta$$

donde $f = \frac{p^2+p+1}{3} \cdot \frac{q^2+q+1}{3}$: Por lo tanto, de lo anterior se concluye que $\beta^{-f} \equiv \left[\frac{N}{\Delta}\right] \equiv \zeta^k \bmod \rho$ donde $\rho = \pi\Delta$ y $0 \leq k \leq 2$:

El desarrollo anterior se resume en el siguiente teorema:

Teorema 3.4. Supóngase que $p; q$ son dos primos distintos tales que $p; q \equiv 1 \bmod 3$ y que $\wp; \tilde{A}$ en $Z[^3]$ son divisores primos de p y q; respectivamente. Sean $½ = \wp\tilde{A}$; $R = pq = ½½$ y $f = \frac{(p^2+p+1)(q^2+q+1)}{9}$: Además, considérese $D \in Z$ tal que $\left(\frac{D}{\wp}\right)_3 = \left(\frac{D}{\tilde{A}}\right)_3 \neq 1$: Sea $® \in Z[\pm]$ tal que $\frac{N(®)}{½} = 1$ y $¯ = \frac{®}{®'}$: Entonces $¯^f \equiv {}^3\kappa \bmod ½$ para algún $i \in \{0; 1; 2\}$:

Corolario 3.1. Sean $e; d \in Z$ tales que $3ed \equiv 1 \bmod f$: Entonces $¯^{3ed} \equiv {}^3\iota¯ \bmod ½$ para algún $\iota \in \{0; 1; 2\}$:

En efecto, $¯^{3ed} \equiv ¯^{1+xf} \equiv (¯^f)^x¯ \equiv {}^{3ix}¯ \equiv {}^3\iota¯ \bmod ½$ donde $\iota \equiv ix \bmod 3$ con $i \in \{0; 1; 2\}$: Esto muestra dos funciones de un sólo sentido, la primera es $e(x) = x^{3e} \bmod ½$; mientras que la segunda es $d(y) = y^d \bmod ½$ para $x; y \in Z[^3][\pm]$:

El corolario 3.1 indica que si $¯$ representa un mensaje que se encripta como $m = ¯^{3e} \bmod ½$; entonces para recuperarlo basta aplicar el exponente d a m: De esta manera, se rescata ${}^3\iota¯$ y con información adicional sobre ι; …nalmente se obtiene $¯$.

El desconocimiento del exponente d di…culta la recuperación de $¯$: Este desconocimiento se da cuando no se tiene f: Este valor es difícil de obtener si no se conoce alguno de los factores de R; es decir, o p o q: Así, la seguridad de este criptosistema radica también en el problema de la factorización.

4 Encripción y desencripción en $Z[^3][\pm]_½$:

No existe una descripción sencilla de los elementos de O_L; por esto sólo se usará el conjunto $Z[^3][\pm] \mu O_L$ para la encripción de mensajes: En la práctica esto puede simpli…carse aún más. En seguida se exponen algunas consideraciones para llevar a cabo esta tarea. Las técnicas que se utilizan para hacer los cálculos de esta sección se pueden encontrar en el apéndice B.

Sean $m_0; m_1$ dos números enteros tales que $\mathrm{mcd}(m_0 m_1; R) = 1$ con R como en el teorema 3.4 y $0 < m_0; m_1 < R$. A partir de estos dos números se construye el entero algebraico $¹ = m_0 + m_1\pm + \pm^2 \in Z[\pm]$: Nótese que tener $\mathrm{mcd}(m_0; R) \neq 1$ o $\mathrm{mcd}(m_1; R) \neq 1$ da a conocer la factorización de R; por lo que se supone $\mathrm{mcd}(m_0; R) = 1$ y $\mathrm{mcd}(m_1; R) = 1$: Esto equivale a $\mathrm{mcd}(m_0 m_1; R) = 1$.

El número $¹ = m_0 + m_1\pm + \pm^2$ escrito de esta forma garantiza que al tomar $\frac{1}{¹⁰}$ como en el teorema 3.4, determine de manera única los coe…cientes $m_0; m_1$:

Además, se debe asegurar que $\mathrm{mcd}(N(¹); R) = 1$: Para esto basta que $\mathrm{mcd}(m_0; R) = 1$; pues si $\wp \mid N(¹)$; entonces $\wp \mid ¹¹⁰¹⁰⁰$ en O_L y de aquí, $\wp$ divide a alguno de los tres factores.

Supóngase que ¼ j ¹; esto es, ¹ = k¼ para algún k 2 O_L; luego, $¹^0 = k^0¼^0 = k^0¼$; por lo que ¼ j $¹^0$: De la misma manera, ¼ j $¹^{00}$ y por lo tanto, ¼ divide a cada uno de los tres factores. De lo anterior se tiene que ¼ j ¹ + $¹^0$ + $¹^{00}$ = $3m_0$ en O_L: Así, p = ¼¼ divide a $9m_0^2$ en O_L y por tanto en Z; lo que contradice que mcd(m_0; R) = 1:

En general, se tiene $\left\langle \frac{N(¹)}{½} \right\rangle = ³^m$ con m 2 f0; 1; 2g y no necesariamente $\left\langle \frac{N(¹)}{½} \right\rangle = 1$ como lo requiere el teorema 3.4. Sea Á = s + ± donde 0 < s < R; mcd(s; R) = 1 y $\left\langle \frac{N(Á)}{½} \right\rangle = ³^²$ con ² = 1 ó 2: Entonces

$$\left\langle \frac{N(¹Á^{2²m})}{½} \right\rangle = \left\langle \frac{N(¹)}{½} \right\rangle \left\langle \frac{N(Á)}{½} \right\rangle^{2²m} = ³^{m+2²²m} = 1:$$

Establecer ® = $¹Á^{2²m}$ permite satisfacer las hipótesis del teorema 3.4 y tener ¯ = $\frac{®}{®^0}$ ´ $b_0 + b_1± + b_2±^2$ mod ½ donde 0 · $b_0; b_1; b_2$ < R. El número Á puede ser público ya que su única utilidad es la de complementar las hipótesis del teorema 3.4.

Como se mencionó anteriormente, el mensaje cifrado también es un elemento de Z[³][±]½, es por eso que a continuación se describirán algunas reglas que simpli…can el trabajo de enviar y recibir un mensaje C:

A partir de lo anterior se puede calcular $¯^e$ ´ $b_0^{(e)} + b_1^{(e)}± + b_2^{(e)}±^2$ mod ½; este número es el mensaje cifrado. Para la transmisión de un mensaje cifrado se usará la siguiente convención. Se empezará ubicando el primer coe…ciente b_i^e no cero del número $¯^e$ mod ½ y se encontrará su inverso multiplicativo b¤: Al multiplicar b¤ por $¯^e$ mod ½ se obtiene un número » que tiene la forma

- » ´ $1 + E_1± + E_2±^2$ mod ½ si $b_0^{(e)}$ fue el primer coe…ciente no cero,
- » ´ $E_2 + ± + E_1±^2$ mod ½ si $b_1^{(e)}$ fue el primer coe…ciente no cero o
- » ´ $E_1 + E_2± + ±^2$ mod ½ si $b_2^{(e)}$ fue el primer coe…ciente no cero.

Esta operación permite tener nuevamente dos enteros ($E_1; E_2$) en el mensaje cifrado, tal y como se tienen en el mensaje original. Sin embargo, al enviar el par ($E_1; E_2$) también hace falta dar información de cómo deben ir colocados estos coe…cientes para reconstruir el número ». Esto se resuelve añadiendo al mensaje cifrado un valor l donde 0 · l · 2 que dé la ubicación del primer coe…ciente b_l^e no cero, es decir, b_l^e: Entonces el mensaje cifrado es una tripleta de la forma ($E_1; E_2$; l):

El siguiente proceso ilustra cómo se recupera el número ¯ a partir de ($E_1; E_2$; l) y la reconstrucción de »: De lo anterior se sabe que » ´ $b^{¤¯^e}$ mod ½: De aquí, $N_» = N(») ´ N(b^{¤¯^e}) ´ N(b^¤)N(¯)^e ´ (b^¤)^3$ mod ½:

Por otro lado, $»^3 \acute{} (b^{¤})^{3-3e} \bmod ½$ y entonces $(N_»^{¤}»^3)^d \acute{} (N_»^{¤}(b^{¤})^{3-3e})^d \acute{} (N_»^{¤}N_»^{-3e})^d \acute{} {}^{-3ed} \acute{} {}^{3k-} \bmod ½$ para algún $k \ 2 \ f0;1;2g$ y donde $N_»^{¤} \acute{} N_»^{i\ 1} \bmod R$:

Después de haber recuperado ${}^{3k-} \bmod ½$; queda por remover el factor ^{3k}: Esto se logra multiplicando ${}^{3k-} \bmod ½$ por ${}^{3\,3\,i\,k}$: La siguiente convención explica más detalladamente cómo recuperar $^{-}$ sin conocer directamente el valor de k: Basándose en el hecho de que ${}^{3} \acute{} r \bmod ½$ (ver apéndice B); el que envía un mensaje puede calcular los valores de ${}^{3k-} \bmod ½$ para cada uno de los valores posibles de k de la manera siguiente:

Para k = 0; 1; 2 calcúlese ${}^{3k-} \acute{} r^{k-} \bmod ½$; esto es, $(r^k b_0; r^k b_1; r^k b_2) \bmod R$: Después, ordénense las tripletas lexicogra…camente para obtener un orden correspondiente de los valores r^{k-}; por decir, $^{-}{}_0 < {}^{-}{}_1 < {}^{-}{}_2$: Identifíquese el valor n tal que $^{-} = {}^{-}{}_n$:

Por otro lado, el que recibe un mensaje lleva a cabo lo siguiente:

Sea $\mu \acute{} {}^{3k-} \acute{} t_0 + t_1 ± + t_2 ±^2 \bmod ½$; calcúlese para $i = 0; 1; 2$; $r^i \mu \bmod ½$, es decir, $(r^i t_0; r^i t_1; r^i t_2) \bmod R$ y ordénense lexicogra…camente para tener $\mu_0 < \mu_1 < \mu_2$: Con esto se cubren todas las posibilidades para el valor de k: Esto signi…ca que $r^i \mu \acute{} {}^{-} \bmod ½$ para algún i; mientras que los otros dos restantes valores de i son congruentes con ${}^{3-} \bmod ½$ y ${}^{3^2-} \bmod ½$; por lo que el trío $(^{-}{}_0; {}^{-}{}_1; {}^{-}{}_2)$ es el mismo que $(\mu_0; \mu_1; \mu_2)$: Por lo tanto, $\mu_n = {}^{-}{}_n = {}^{-}$:

Recuérdese que lo que se desea recuperar es $(m_0; m_1)$; es decir, ^{1}: Hasta este momento sólo se ha obtenido $^{-}$; pero como $^{-} = \frac{®}{®_0} = \frac{1}{1_0} \left(\frac{Á}{Á^0}\right)^{2^2 m}$ entonces $\acute{} = \mu_n \left(\frac{Á^0}{Á}\right)^{3\,2^2 m} = \frac{1}{1_0} \acute{} e_0 + e_1 ± + e_2 ±^2 \bmod ½$:

En resumen, si el que envía un mensaje añade el valor de n a $(E_1; E_2; l)$; el que recibe el mensaje puede fácilmente recuperar $^{-}$ sin conocer el valor de k directamente, y obtener $\frac{1}{1_0}$ si se adiciona también el valor de m; pues como Á es público, entonces el valor de ² es fácil de calcular. Esto hace ver que un mensaje cifrado C es $C = (E_1; E_2; l; m; n)$:

Sea ${}^{1} \acute{} x + y ± + z ±^2 \bmod ½$; entonces ${}^{1_0} \acute{} x + y^3 ± + z^{3^2} ±^2 \acute{} x + yr ± + zr^2 ±^2 \bmod ½$: De aquí,

$$ {}^{1} \acute{} x + y ± + z ±^2 \acute{} (e_0 + e_1 ± + e_2 ±^2)(x + yr ± + zr^2 ±^2) \bmod ½: $$

Esto es equivalente al sistema de congruencias dado por:

$$ \begin{matrix} 2 \\ 4 \end{matrix} \begin{matrix} e_0 ¡ 1 & e_2 Dr & e_1 Dr^2 \\ e_1 & e_0 r ¡ 1 & e_2 Dr^2 \\ e_2 & e_1 r & e_0 r^2 ¡ 1 \end{matrix} \begin{matrix} 3\,2 \\ 5\,4 \end{matrix} \begin{matrix} x \\ y \\ z \end{matrix} \begin{matrix} 3 \\ 5 \end{matrix} \acute{} 0 \bmod R: $$

Nótese que $\det(M) \cdot N(\cdot) \equiv 1 \cdot 0 \bmod R$ donde M representa la matriz cuadrada de arriba. La solución $x + y\pm + z\pm^2 \cdot F^1 \cdot Fm_0 + Fm_1\pm + F\pm^2 \bmod ½$ para algún $F \in Z$: Por lo tanto, $F \cdot z \bmod R$ y $m_0 \cdot xz^{i1} \cdot \hat{m}_0 \bmod R$; $m_1 \cdot yz^{i1} \cdot \hat{m}_1 \bmod R$: Como $0 < m_0; m_1; \hat{m}_0; \hat{m}_1 < R$; entonces $m_0 = \hat{m}_0$ y $m_1 = \hat{m}_1$:

5 Esquema general del criptosistema de campos cúbicos.

Actualmente existen varios sistemas del tipo RSA. Michael Rabin fue uno de los primeros en crear un esquema similar a RSA utilizando como exponente de encripción 2e en lugar de e: Este método utiliza una aritmética en un campo numérico cuadrático. Siguiendo con la idea de utilizar campos ciclotómicos de grado mayor, los matemáticos Renate Scheidler y Hugh Williams desarrollaron un criptosistema que basa su aritmética sobre el campo cúbico $Q(\pm)$ donde $\pm = \sqrt[3]{D}$ para algún $D \in Z$: Los mensajes se codi…can como unidades de este campo cúbico. El exponente de encripción es de la forma 3e; por lo que al utilizar la clave secreta d para desencriptar, lo que se obtiene es la tercera potencia del mensaje. El conjunto de números primos que se pueden utilizar para este método son los de la forma $p; q \cdot 1 \bmod 3$:

La idea básica de este sistema es codi…car un mensaje como una unidad $¯ = \frac{®}{®'} \in Z[³][\pm]_½$ y encriptarla como $¯^{3e} \bmod ½$: Para desencriptar, se calcula $(¯^{3e})^{d} \cdot ³^{l}¯ \bmod ½$ como en el corolario 3.1. Si el que desencripta conoce l; entonces puede obtener $¯$ y recuperar el mensaje.

En seguida, se de…ne el criptosistema:

Sean $½ = ¼Ã$; $R = pq = ½'½$ y $f = \frac{(p^2+p+1)(q^2+q+1)}{9}$; donde $p; q$ son dos números primos tales que $p; q \cdot 1 \bmod 3$ y $¼; Ã$ en $Z[³]$ son divisores primos de p y q; respectivamente. Considérese $\pm = \sqrt[3]{D}$ para algún $D \in Z$: Los conjuntos $P; C$ son $P = C = \{a + b\pm + \pm^2 \in Z[\pm] \mid a; b \in Z_R\}$; mientras el conjunto K se describe de la manera siguiente:

$$K = \{(R; p; q; ½; D; e; d) \mid R = pq; 3ed \cdot 1 \bmod f\}:$$

Para $k \in K$; las funciones e_k y d_k vienen dadas por:

$$e_k(x) = x^{3e} \bmod ½ \text{ y } d_k(y) = y^{d} \bmod ½$$

para $x; y \in \{a + b\pm + \pm^2 \in Z[\pm] \mid a; b \in Z_R\}$: Los valores $R; D; ½; e$ son públicos y los elementos $p; q; d$ permanecen secretos.

A continuación se presenta el algoritmo general del CCC, mismo que se encuentra en [11].

Algoritmo general

Generación de las claves pública y privada.

1. Generar dos números primos grandes $p; q$ tales que $p \equiv 1 \bmod 3$ y $q \equiv 1 \bmod 3$. Calcular $R = pq$ y $f = \frac{(p^2+p+1)(q^2+q+1)}{9}$:
2. Encontrar dos divisores primos $\pi; \tilde{A}$ en $Z[^3]$ de p y q; respectivamente. Calcular $½ = \pi\tilde{A} = r_0 + r_1{}^3$ con $r_0; r_1 \in Z$:
3. Encontrar $D \in Z$ tal que $0 < D < R$; $\mathrm{mcd}(D; R) = 1$ y $\left(\frac{D}{\pi}\right)^{¤} = \left(\frac{D}{\tilde{A}}\right)^{i\,1} \neq 1$:
4. Generar $e \in Z$ tal que $0 < e < R$ y resolver $3ed \equiv 1 \bmod f$ para d con $0 < d < f$:
5. Encontrar $Á = s + \pm \in Z[\pm]$ tal que $0 < s < R$; $\mathrm{mcd}(s; R) = 1$ y $\left(\frac{N(Á)}{½}\right) \neq 1$:
6. La clave pública es $K_p = (D; s; r_0; r_1; e)$ y la clave secreta es $K_s = \{d\}$:

Precálculo. Sólo se necesita hacer una vez por generación de claves.

1. Calcular $r \equiv ¡ r_0 r_1{}^{i\,1} \bmod R$ con $0 < r_i < R$:
2. Calcular $N_Á = N(Á) = s^3 + D$ y $\frac{N_Á}{½} = {}^{3^2}$ con $² = 1$ o 2:
3. Calcular $N_Á^{¤} \equiv N_Á^{j\,1} \bmod R$ con $0 < N_Á^{¤} < R$:

Encripción. Encriptar un mensaje $(m_0; m_1)$ con $0 < m_0 < R$; $0 < m_1 < R$ y $\mathrm{mcd}(m_0 m_1; R) = 1$:

1. Definir $¹ = m_0 + m_1\pm + \pm^2$ y calcular $N_¹ = N(¹) = m_0 + m_1^3 D + D^2 ¡ 3m_0 m_1 D$:
2. Calcular $\frac{N_¹}{½} = {}^{3^m}$; $m \in \{0; 1; 2\}$ y $N_1^{¤} \equiv N_¹{}^{i\,1} \bmod R$ con $0 < N_1^{¤} < R$:
3. Calcular $® \equiv {}^1Á^{2^{2m}} \bmod ½$ y $¯ = \frac{®}{®^0} \equiv (N_Á^{¤})^{2^{2m}} N_1^{¤} ®^2 ®^{00} \equiv b_0 + b_1\pm + b_2\pm^2 \bmod ½$ con $0 \cdot b_0; b_1; b_2 < R$:
4. Para $i = 0; 1; 2$; calcular $r^i ¯ \bmod ½$: Ordenar las tripletas $(r^i b_0; r^i b_1; r^i b_2) \bmod R$ en orden lexicográfico obteniendo un ordenamiento correspondiente de los valores $r^i ¯$; $i = 0; 1; 2$; por decir, $¯_0 < ¯_1 < ¯_2$: Identificar $n \in \{0; 1; 2\}$ tal que $¯ = ¯_n$:
5. Calcular $¯^{e} \equiv b_0^{(e)} + b_1^{(e)}\pm + b_2^{(e)}\pm^2 \bmod ½$; $0 \cdot b_i^{(e)} < R$ para $i = 0; 1; 2$:
6. Encontrar $l = \min\{i \mid j \text{ no se cumpla que } b_i^{(e)} \equiv 0 \bmod R\} \in \{0; 1; 2\}$: Calcular $b^{¤} \equiv (b_l^{(e)})^{i\,1} \bmod R$ con $0 < b^{¤} < R$ y $E_1 \equiv b^{¤} b_{(l+1) \bmod 3}^{(e)} \bmod R$, $E_2 \equiv b^{¤} b_{(l+2) \bmod 3}^{(e)} \bmod R$, $0 \cdot E_1 < R$; $0 \cdot E_2 < R$; donde los subíndices se toman entre 0 y 2.
7. Transmitir $C = (E_1; E_2; l; m; n)$:

Desencripción. Habiendo recibido $C = (E_1; E_2; l; m; n)$:

1. Si $l = 0$; entonces $» = 1 + E_1\pm + E_2\pm^2$:
   Si $l = 1$; entonces $» = E_2 + \pm + E_1\pm^2$:
   Si $l = 2$; entonces $» = E_1 + E_2\pm + \pm$:

Calcular $N(\text{»})$:

2. Calcular $N_{\text{»}}^{\text{¤}} \acute{} N(\text{»})^{i\,1} \bmod R; 0 < N_{\text{»}}^{\text{¤}} < R$:
   Después calcular $\mu \acute{} (N_{\text{»}}^{\text{¤}}\text{»}^3)^d \acute{} t_0 + t_1\pm + t_2\pm^2 \bmod \text{½}$
   con $0 \cdot t_0 < R; 0 \cdot t_1 < R$ y $0 \cdot t_2 < R$:
3. Para $i = 0; 1; 2$; calcular $r^i\mu \bmod \text{½}$: Ordenar las tripletas
   $(r^i t_0; r^i t_1; r^i t_2) \bmod R$ en orden lexicográ…co, obteniendo un ordenamiento correspondiente de los valores $r^i\mu (i = 0; 1; 2)$; por decir,
   $\mu_0 < \mu_1 < \mu_2$: Identi…car μ_n:
4. Calcular $\acute{} = \mu_n(\frac{\acute{A}^0}{\tilde{A}})^{2^2 m} \acute{} \mu_n((\acute{A}^0)^2\acute{A}^{00}N_{\tilde{A}}^{\text{¤}})^{2^2 m} \acute{}$
   $e_0 + e_1\pm + e_2\pm^2 \bmod R$ con $0 \cdot e_0 < R; 0 \cdot e_1 < R$ y $0 \cdot e_2 < R$:
5. De…nir

$$M = \begin{matrix} \mathbf{2} \\ \mathbf{4} \\ \end{matrix} \begin{matrix} e_0 \text{¡} 1 & e_2 \text{D} r & e_1 \text{D} r^2 \\ e_1 & e_0 r \text{¡} 1 & e_2 \text{D} r^2 \\ e_2 & e_1 r & e_0 r^2 \text{¡} 1 \end{matrix} \begin{matrix} \mathbf{3} \\ \mathbf{5} \\ \end{matrix}$$

y resolver el sistema de congruencias lineales dado por

$$M \begin{matrix} \mathbf{2} \\ \mathbf{4} \\ \end{matrix} \begin{matrix} x \\ y \\ z \end{matrix} \begin{matrix} \mathbf{3} \\ \mathbf{5} \\ \end{matrix} \acute{} 0 \bmod R:$$

Luego, $\hat{m}_0 \acute{} xz^{i\,1} \bmod R; \hat{m}_1 \acute{} yz^{i\,1} \bmod R$;
$0 < \hat{m}_0 < R$ y $0 < \hat{m}_1 < R$:

Para ilustrar el uso del algoritmo anterior, se desarrolló el siguiente ejemplo:

Ejemplo 3.1.

Generación de claves. Alicia crea sus claves.

1. Alicia escoge $p = 7; q = 13$:
2. Calcula $R = 91; f = 1159; ¼ = 3 + 2^3; \tilde{A} = 4 + 3^3$ y $\text{½} = 6 + 11^3$:
3. Elige $D = 2$ ya que 2 no es residuo cúbico módulo 7, ni residuo cúbico módulo 13.
4. Selecciona $e = 53$ como exponente de encripción y resuelve
   $159d \acute{} 1 \bmod 1159$ para $0 < d < 1159$; $d = 277$:
5. Opta por $s = 1$ ya que $\text{mcd}(1; 91) = 1$ y con $\acute{A} = 1 + \pm$ se tiene que
   $[\frac{N(\acute{A})}{\text{½}}]\Theta 1$:
6. Su clave pública es $k_p = fR; D; s; r_0; r_1; eg = f91; 2; 1; 6; 11; 53g$ y su clave privada es $k_s = fdg = f277g$:

Precálculo. Roberto hace estos cálculos antes de enviar un mensaje

1. Calcula $11r \acute{} 6 \bmod 91$ para $0 < r < 91$; $r = 16$:
2. Calcula $N_{\acute{A}} = 3$ y $[\frac{N_{\acute{A}}}{\text{½}}] = {}^3; {}^2 = 2$:
3. Calcula $3N_{\acute{A}}^{\text{¤}} \acute{} 1 \bmod 91$ para $0 < N_{\acute{A}}^{\text{¤}} < 91$; $N_{\acute{A}}^{\text{¤}} = 61$:

Encripción. Roberto envía un mensaje a Alicia.

1. Representa su mensaje como $(m_0; m_1) = (1; 1)$:
2. Establece $^{1} = 1 + \pm + \pm^2$; $N_{\imath} = 1$:
3. Calcula $[\frac{N_{\imath}}{\frac{1}{2}}] = 1$; $m = 0$ y $N_1^{\square} \acute{} 1 \bmod 91$ para $0 < N_1^{\square} < 91$; $N_1^{\square} = 1$:
4. Escribe $® = {}^{1} \acute{} 1 + \pm + \pm^2 \bmod ½$ y $^{-} \acute{} ®^2®^{00} \bmod ½ \acute{}$ $31 + 15\pm + 15\pm^2 \bmod ½$:
5. Para $i = 0; 1; 2$; calcula $r^{i-} \bmod ½$ y obtiene $f(19; 18; 18); (31; 15; 15);$ $(41; 58; 58)g$; identi…cando $n = 1$:
6. Calcula $^{-53} \acute{} 40 + 46\pm + 87\pm^2 \bmod ½$:
7. Encuentra $l = 0$ y calcula $40b^{\square} \acute{} 1 \bmod 91$ para $0 < b^{\square} < 91$; $b^{\square} = 66$: Después, obtiene $E_1 \acute{} 33 \bmod 91$ y $E_2 \acute{} 9 \bmod 91$:
8. Roberto envía $C = (33; 9; 0; 0; 1)$:

Desencripción. Alicia recibe el mensaje C:

1. Como $l = 0$; $» = 1 + 33\pm + 9\pm^2$ y calcula $N(») = N_{»} = 27$:
2. Calcula $27N_{»}^{\square} \acute{} 1 \bmod 91$ para $0 < N_{»}^{\square} < 91$; $N_{»}^{\square} = 27$. También, escribe $\mu \acute{} (27»^3)^{277} \acute{} 31 + 15\pm + 15\pm^2 \bmod ½$:
3. Para $i = 0; 1; 2$; calcula $r^{i}\mu \bmod ½$ y obtiene $f(19; 18; 18); (31; 15; 15);$ $(41; 58; 58)g$; identi…cando μ_1:
4. Calcula $\acute{} \acute{} \mu_1 \acute{} 31 + 15\pm + 15\pm^2 \bmod ½$:
5. De…ne la matriz

$$M = \begin{matrix} \mathbf{2} \\ \mathbf{4} \\ \\ \end{matrix} \begin{matrix} 30 & 25 & 36 \\ 15 & 40 & 36 \\ 15 & 58 & 18 \end{matrix} \begin{matrix} \\ \\ \mathbf{5} \end{matrix} \begin{matrix} \mathbf{3} \\ \\ \\ \end{matrix}:$$

Resuelve

$$M \begin{matrix} \mathbf{2} \\ \mathbf{4} \\ \\ \end{matrix} \begin{matrix} x \\ y \\ z \end{matrix} \begin{matrix} \mathbf{3} \\ \mathbf{5} \\ \\ \end{matrix} \acute{} 0 \bmod 91$$

para $x; y; z$; obteniendo $x = 1$; $y = 1$ y $z = 1$: Con lo que recupera el mensaje $m̂_0 = 1$ y $m̂_1 = 1$:

Capítulo IV

Análisis comparativo de los criptosistemas RSA y CCC

En el capítulo actual se presenta un análisis de las diferencias y semejanzas de los dos sistemas criptográficos expuestos anteriormente. En la sección 1, esto se hace desde el punto de vista teórico, mientras que en la segunda sección, se contrastan las implementaciones de ambos métodos utilizando la plataforma de Mathematica y se efectúan algunas pruebas comparativas.

1 Diferencias y semejanzas teóricas entre el criptosistema RSA y el CCC.

El sistema RSA y el sistema de Campos Cúbicos basan su seguridad en el Problema de la Factorización. Los métodos de este tipo se definen en anillos y utilizan funciones de un sólo sentido de la forma $f(x) = x^a \bmod b$. Las diferencias entre estos sistemas radican en los conjuntos donde se definen y los dominios y contradominios donde operan sus funciones de encripción y desencripción.

RSA utiliza Z que es el anillo de enteros de Q. En éste se considera el producto $n = pq$ de dos números primos y se construye el anillo cociente Z/nZ que servirá como dominio y contradominio de las funciones de encripción y desencripción. Los mensajes dentro de este sistema son elementos de Z/nZ; es decir, son enteros $m \bmod n$.

La proposición 2.3 asegura que si $mcd(e; \acute{A}(n)) = 1$; entonces $ed \acute{} 1 \bmod \acute{A}(n)$ tiene solución única para d módulo n. Esto junto con el teorema 2.6 permiten definir la función de encripción $e : Z/nZ \to Z/nZ$ y la función de desencripción $d : Z/nZ \to Z/nZ$ de la siguiente manera:

$$\begin{aligned} e(x) &= x^e \bmod n \\ d(y) &= y^d \bmod n \end{aligned}$$

para $x; y \in Z/nZ$. Si para un par $p; q$ de números primos se pueden obtener los valores $n; e; d$; entonces las funciones de encripción y desencripción se pueden expresar en función de cada $k = (n; p; q; e; d)$.

Por otro lado, CCC considera O_L el anillo de enteros de $Q(\sqrt[3]{}; \pm)$ donde $\pm = \sqrt[3]{D}$ para algún $D \in Z$ y $\sqrt[3]{} = \frac{-1+\sqrt{-3}}{2}$:

A partir de esto, basta tomar el producto ½ = ¼Ã de dos elementos primos inertes en $Z[^3]$ para construir el cociente $O_L=½O_L$: Este anillo es el dominio y contradominio de las funciones de encripción y desencripción del sistema. Cada mensaje de este sistema es un elemento de $O_L=½O_L$; esto es, un entero algebraico $^1 \bmod ½$: Sin embargo, llevar esto a la práctica no es sencillo, es más conveniente tomar $^1 \ 2 \ Z[±] \ ½ \ Z[^3][±] \ µ \ O_L$ y mediante las técnicas del apédice B calcular $^1 \bmod ½$:

La proposición 3.1 simpli…ca la tarea de encontrar elementos primos en $Z[^3]$; pues asegura que para un número primo p tal que $p \acute{} 1 \bmod 3$ existe ¼ divisor primo en $Z[^3]$ que cumple $p = ¼¼$: En CCC; el corolario 3.1 asegura que si $3ed \acute{} 1 \bmod f$; entonces para un elemento $¯ \ 2 \ O_L=½O_L$ como en el teorema 3.3 se satisface $¯^{3ed \acute{} 3^{l}} ¯ \bmod ½$: Esto permite de…nir las funciones de encripción $e : O_L=½O_L \ ! \ O_L=½O_L$ y de desencripción $d : O_L=½O_L \ ! \ O_L=½O_L$ como sigue:

$$\begin{aligned} e(x) &= x^{3e} \bmod ½ \\ d(y) &= y^{d} \bmod ½ \end{aligned}$$

para $x;y \ 2 \ O_L=½O_L$: De la misma manera que en RSA, las funciones de encripción y de desencripción dependen de un conjunto de valores $k = (R;½;p;q;D;e;d)$:

El siguiente cuadro comparativo resume las diferencias de los sistemas criptográ…cos expuestos:

Criptosistema	RSA	CCC
Texto común y de cifrado	$Z=nZ$	$O_L=½O_L$
Elementos primos	$p;q \ 2 \ Z$	$¼;Ã \ 2 \ Z[^3]$
Funciones de encripción y funciones de desencripción	$e(x) = x^e \bmod n$ $d(y) = y^d \bmod n$	$e(x) = x^{3e} \bmod ½$ $d(y) = y^d \bmod ½$

2 Implementación de los sistemas criptográ…cos RSA y CCC.

Mathematica V4.0 es una herramienta computacional versátil que permite trabajar con los estilos de programación procedimental, funcional y lógico. Además, cuenta con funciones integradas que simpli…can la tarea de programación. Ambos criptosistemas han sido implementados sobre la plataforma Mathematica V4.0.

Para la generación de números primos se utilizaron dos funciones de Mathematica V4.0: Prime[i], la cual origina el i-ésimo número primo, y Random[x; fx; 1; 100g] que de manera seudoaleatoria produce un número en un rango de 1 a 100 usando una función de densidad uniforme. Esta disposición permite tener de manera casi aleatoria, los 100 primeros números primos para la creación de las claves públicas. Con esto, RSA tiene 100 £ 99 = 9900 claves públicas posibles, mientras que CCC sólo puede tener 47 £ 46 = 2162; esto debido a que CCC únicamente opera con números primos p ´ 1 mod 3:

La función generaclavesrsa se encarga de crear las claves pública y privada para el sistema RSA. Esta función genera dos números primos seudoaleatoriamente y siguiendo los pasos para la generación de claves del algoritmo RSA de clave pública del capítulo II produce una clave pública fe; ng y una clave privada d:

```
In[2]:= generaclavesrsa[]

        La clave pública es {25639, 28841}

        La clave privada es 259
```

Para CCC la función generaclavesccc produce una clave pública fR; D; s; r_0; r_1; eg y una clave privada d a partir de dos números primos p; q ´ 1 mod 3 generados seudoaleatoriamente. Esta función se apoya en algunas funciones auxiliares que se ocupan de algunas tareas especí…cas dentro de la generación de las claves pública y privada. Por ejemplo:

Función	Entradas	Salidas	Descripción
primocong	Ninguna	Un entero p	Genera un número primo p ´ 1 mod 3
divprimo	Un entero p ´ 1 mod 3	Un vector entero fa; bg	Encuentra ¼ 2 Z[³] tal que p = ¼¼̄
caracres	Dos vectores enteros fa; bg; fc; dg	Un entero j 2 f0; 1; 2g	Encuentra el carácter cúbico residual de ·; ! 2 Z[³]

En la función divprimo el vector entero fa; bg representa a ¼ = a + b³; mientras que las entradas fa; bg; fc; dg en caracres representan los números · = a + b³ y ! = c + d³; y la salida j es el exponente de ³ tal que $\left(\frac{\cdot}{!}\right)_3 = ³^j$:

```
In[8]:= primocong[]

Out[8]= 421

In[9]:= divprimo[421]

Out[9]= {21, 20}

In[10]:= caracres[{21, 20}, {-10, -1}]

Out[10]= 0
```

Una función indispensable para la generación de la clave pública es encuentraD, dicha función halla el valor de D adecuado para los números ¼ y Ã; es decir, obtiene el mínimo residuo no cúbico D tal que $\left[\frac{D}{¼}\right] = \left[\frac{D}{Ã}\right]^{-1} \neq 1$ y $mcd(R; D) = 1$: Las entradas para encuentraD son los dos números primos $p; q$ generados con primocong; los divisores primos ¼ y Ã; de p y q repectivamente, encontrados por divprimo; y el valor $R = pq$: La ejecución de encuentraD se observa de la siguiente manera:

```
In[11]:= encuentraD[91, 7, 13, {2, 3}, {4, 3}]

Out[11]= 2
```

Las funciones descritas anteriormente están contenidas dentro de generaclavesccc. La ejecución de esta función se ve a continuación:

```
In[15]:= generaclavesccc[]

         La clave pública es {50161, 2, 1, {-235, -24}, 43406}

         La clave privada es 168757465
```

Una vez generadas las claves pública y privada para los dos sistemas, puede comenzar el proceso de encripción de mensajes. Para encriptar mensajes en el sistema RSA, se usa la función de encripción encriptarsa que tiene como entradas una clave pública fe; ng y un mensaje representado como un número entero m donde $0 < m < n$: La salida es un mensaje cifrado $c = m^e \bmod n$: En seguida se muestra la ejecución de la función anterior para encriptar el mensaje $m = 10093$ utilizando la clave pública f25639; 28841g; generada previamente.

```
In[4]:= encriptarsa[]

Out[4]= 16993
```

El número c = 16993 es el que se envía como mensaje cifrado. Por otro lado, la función desencriptarsa sirve para recuperar el mensaje original. Esta función tiene como entradas la clave pública fe; ng; el mensaje cifrado c y la clave privada d: La salida es el mensaje original m: En el caso ilustrativo, la clave privada es d = 259:

```
In[6]:= desencriptarsa[]

Out[6]= 10093
```

En lo que respecta al CCC, las funciones de encripción y de desencripción son mas elaboradas que las de RSA. Estas funciones requieren de funciones auxiliares que realizan tareas o pasos especí…cos tanto del algoritmo de encripción como del algoritmo de desencripción del CCC. Algunas de ellas son:

Función	Entradas	Salidas	Descripción
multiplica	Dos vectores enteros $fx_0; x_1; x_2g$ $fy_0; y_1; y_2g$	Un vector entero $fz_0; z_1; z_2g$	Calcula el producto de Â; Á 2 Z[±] módulo ½
potencia	Un vector entero $fb_0; b_1; b_2g$ y un valor entero e	Un vector entero $fb_0^{(e)}; b_1^{(e)}; b_2^{(e)}g$	Calcula $^{-e}$ mod ½ con $^{-}$ 2 Z[±] mod ½
precalculo	Los valores de la clave pública $fR; D; s; r_0; r_1g$	Los valores enteros $fr; N_{Á}^{¤}; ²g$	Lleva a cabo el proceso del precalculo

Los vectores $fx_0; x_1; x_2g$ y $fy_0; y_1; y_2g$ que son las entradas de la función multiplica representan a los números Â ´ $x_0 + x_1± + x_2±^2$ mod ½ y Á ´ $y_0 + y_1± + y_2±^2$ mod ½ en Z[±] módulo ½: De la misma manera la salida $fz_0; z_1; z_2g$ representa a ÂÁ ´ $z_0 + z_1± + z_2±^2$ mod ½: En la función potencia, la entrada $fb_0; b_1; b_2g$ signi…ca $^{-}$ ´ $b_0 + b_1± + b_2±^2$ mod ½ y e es precisamente el exponente de encripción, esto es, el último valor de la clave pública. Por último, tanto las entradas como las salidas en la función precalculo son los mismos valores que como en el precálculo. En seguida se muestra el despliegue de la última función con los primeros cinco valores de la clave pública f50161; 2; 1; ¡ 235; ¡ 24; 43406g como entradas.

```
In[23]:= precalculo[50161, 2, 1, -235, -24]

Out[23]= {39701, 2, 33441}
```

Otra función importante para la encripción en CCC es creabeta. Esta función calcula el número ¯ mod½ a partir de los valores ¹; Á; N¤1; N¤Á; ²; m; R; D; r como entradas, pues primero calcula ® ´ ¹Á$^{2^2 m}$ mod½ para después obtener ¯ = $\frac{®}{®^0}$ ´ $(N^{¤}_{Á})^{2^2 m} N^{¤}_{1} ®^{2} ®^{00}$ mod½: El número ¹ = $m_0 + m_1 ± + ±^2$ es el que trae el mensaje fm_0; m_1g; este número se representa como un vector entero fm_0; m_1; 1g; así mismo Á = s + ± se representa como el vector fs; 1; 0g: Finalmente, el número ¯ mod½ se presenta en forma de un vector entero fb_0; b_1; b_2g: Aplicando la misma clave pública f50161; 2; 1; ¡235; ¡24; 43406g y los valores f39701; 2; 33441g obtenidos en el precalculo, la ejecución de la función creabeta muestra lo siguiente:

```
In[15]:= creabeta[{2445, 8574, 1}, {1, 1, 0}, 27448, 33441, 2,
           0, 2, 50161, 39701]

Out[15]= {26062, 41817, 8978}
```

La función de encripción en CCC encriptaccc requiere como entradas la clave pública fR; D; s; r_0; r_1; eg y un mensaje M = fm_0; m_1g donde 0 < m_0; m_1 < R; teniendo como salida un vector C = fE_1; E_2; l; m; ng: Usando la clave pública f50161; 2; 1; ¡235; ¡24; 43406g; la encripción del mensaje M = f2445; 8574g queda de la siguiente manera:

```
In[10]:= encriptaccc[]

Out[10]= {1906, 39456, 0, 0, 2}
```

La función desencriptaccc permite recuperar el mensaje original teniendo como entradas la clave pública fR; D; s; r_0; r_1; eg; el mensaje cifrado C = fE_1; E_2; l; m; ng y la clave privada d: En el ejemplo la clave privada es d = 168757465:

```
In[12]:= desencriptaccc[]

Out[12]= {2445, 8574}
```

3 Una aplicación para el intercambio de mensajes cortos.

Los sistemas criptográ…cos estudiados en este trabajo pueden utilizarse para intercambiar mensajes cortos, una de las aplicaciones comunes de los criptosistemas de clave pública. Para llevar a cabo esto, se hacen las siguientes convenciones:

1. Se ha elegido el conjunto de letras minúsculas siguiente:
A ={a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z}.

2. La regla de equivalencia entre cada símbolo del conjunto A y un número entero viene dada por:

a	b	c	d	e	f	g	h	i	j	k	l	m
11	12	13	14	15	16	17	18	19	20	21	22	23
n	o	p	q	r	s	t	u	v	w	x	y	z
24	25	26	27	28	29	30	31	32	33	34	35	36

Esta regla permite que cada símbolo se represente como un número entero de dos dígitos.

3. Un mensaje se escribirá en forma de cadena sin dejar espacios. Por ejemplo, un posible mensaje sería "nosvemosalauna".

4. La representación numérica de un mensaje se hace aplicando la regla anterior y concatenando cada número para formar uno único. Así, se obtiene un único número entero m de 2k-dígitos de longitud donde k es el número de letras usadas en un determinado mensaje. En el mensaje "nosvemosalauna", el número construído es 2425293215232529112211312411:

5. Particionar m en bloques de longitud menor o igual a 4-dígitos ya que si m_i representa el i-ésimo bloque, entonces se debe cumplir que $m_i < R$ o n; según el criptosistema que se esté usando. En el ejemplo, tomando en cuenta las claves generadas anteriormente, n = 28841 para RSA y R = 50161 para CCC, el número 2425293215232529112211312411 queda dividido en 7 bloques 4-dígitos de longitud, M = f2425; 2932; 1523; 2529; 1122; 1131; 2411g

Para llevar a cabo los tres últimos puntos se implementó la función mensajentero que convierte texto en bloques de números enteros. Esta función se apoya en la función ToCharacterCode de Mathematica V4.0 para encontrar la representación entera de cualquier caracter usando el código estándar americano para el intercambio de información (ASCII). Ahora, la representación entera ASCII de los símbolos del conjunto A toman un rango de 97 a 122, es por eso que se determinó sustraer la cantidad de 86 a cada número representativo para obtener el rango deseado de 11 a 36. Cabe señalar que la letra "ñ" no entra en esta consideración debido a que su representación en código ASCII es el número 241. Si se desea incluir el símbolo "ñ" es necesario ampliar la representación de cada símbolo a tres dígitos; y con respecto a los sistemas RSA y CCC que se manejan en este trabajo, aumentar el rango de números primos a utilizar pues las claves públicas alcanzan una longitud de 4 o 5 dígitos en promedio.

Usando mensajentero el mensaje “nosvemosalauna” queda representado como sigue:

```
In[19]:= mensajentero["nosvemosalauna"]

Out[19]= {2425, 2932, 1523, 2529, 1122, 1131, 2411}
```

Por otro lado, la contraparte está dada por enteromensaje. Esta función se ocupa de representar un conjunto de números enteros como una cadena de caracteres de A. El conjunto de números M se ve representado de la siguiente forma:

```
In[20]:= enteromensaje[{2425, 2932, 1523, 2529, 1122, 1131, 2411}]

Out[20]= nosvemosalauna
```

Ahora, sólo resta adaptar estas funciones a cada sistema criptográ…co. Para el sistema RSA, usando las claves generadas anteriormente la función que encripta mensajes cortos se llama encriptatextorsa. La encripción del mensaje “nosvemosalauna” usando la clave pública f25639; 28841g tiene la siguiente salida:

```
In[19]:= encriptatextorsa[]

Out[19]= {6919, 10018, 3599, 10895, 18042, 15216, 28252}
```

Para recuperar el mensaje original se ejecuta la función desencriptatextorsa. La desencripción del mensaje cifrado anteriormente aplicando la clave privada d = 259 se ve:

```
In[20]:= desencriptatextorsa[]

Out[20]= nosvemosalauna
```

Por otra parte, la función encriptatextoccc es la función que encripta texto para el sistema CCC. La encripción del mensaje “nosvemosalauna” utilizando la clave pública f50161; 2; 1; ¡ 235; ¡ 24; 43406g se ve como sigue:

```
In[21]:= encriptatextoccc[]

Out[21]= {{5777, 39604, 0, 1, 0},
          {43343, 43793, 0, 1, 1}, {27068, 18834, 0, 0, 2},
          {40281, 48905, 0, 1, 0}, {11743, 13147, 0, 2, 0},
          {28735, 12315, 0, 1, 2}, {9575, 26915, 0, 2, 2}}
```

En contraparte, la función llamada desencriptatextoccc, servirá para desencriptar texto mediante el mismo método. A continuación, se despliega la salida del mensaje recuperado con el mensaje cifrado anterior y la clave privada d = 168757465 como entradas:

```
In[22]:= desencriptatextoccc[]

Out[22]= nosvemosalauna
```

Conclusiones

Los objetivos planteados en el presente trabajo fueron alcanzados satisfactoriamente. Se logró identi…car las semejanzas en ambos métodos al examinar la construcción tanto de RSA como de CCC. En cuanto a éste último sistema, también se completaron algunos desarrollos como los de los teoremas 3.3 y 3.4. Las diferencias existentes entre los dos criptosistemas se pudieron distinguir cuando para entender el funcionamiento de CCC se requirió profundizar en la teoría algebraica de números, así como revisar nuevamente resultados de teoría de números, álgebra y extensiones de campos. Esto en consecuencia mostró a la disciplina de las matemáticas como campo de aplicación en la criptografía de clave pública.

Por otro lado, el funcionamiento de ambos criptosistemas pudo ser apreciado desde el punto de vista práctico pues estos métodos fueron implementados y adaptados para presentar una aplicación concreta y real como el intercambio de mensajes cortos.

Es importante mencionar que el campo de investigación en el área de la criptografía de clave pública es muy amplio y fértil. Actualmente, existe una tendencia muy clara por usar cada vez más matemáticas en el desarrollo de nuevos métodos criptográ…cos y métodos criptoanalíticos por lo que esto representa una buena opción para el desarrollo profesional de aquellos que deseen aplicar sus conocimientos de matemáticas en el área.

Finalmente, esta obra deja abiertas posibilidades para trabajos futuros relacionados con ésta:

Desarrollo de un criptosistema de…niendo su aritmética en un campo de grado mayor a tres.

Comparación de las complejidades algorítmicas de cada criptosistema y optimización de los mismos algoritmos.

Criptoanálisis de los métodos criptográ…cos estudiados.

Apéndice A

Definición A.1. Un anillo conmutativo unitario es un conjunto R junto con dos operaciones binarias $(+, \cdot)$ definidas en él, llamadas suma y multiplicación, respectivamente, que satisfacen los siguientes axiomas:

1. $(R; +)$ es un grupo abeliano.
2. La multiplicación es asociativa.
3. La multiplicación es conmutativa.
4. Para cualesquiera $a; b; c \in R$ se cumple que $a(b + c) = ab + ac$:
5. Existe un elemento $1 \in R$; conocido como elemento unitario, tal que $1 \cdot x = x$ para toda $x \in R$:

Definición A.2. Un dominio entero D es un anillo conmutativo con elemento unitario tal que si a y b son dos elementos de D con $ab = 0$; entonces $a = 0$ ó $b = 0$:

Definición A.3. Un campo es un anillo conmutativo con elemento unitario donde para cada $x \in R - \{0\}$ existe $x^{-1} \in R$, el inverso multiplicativo de x; tal que $x \cdot x^{-1} = 1$:

Definición A.4. Un subconjunto no vacío U de un anillo conmutativo unitario R es un ideal de R si:

1. U es un subgrupo de R bajo la suma.
2. Para cada $u \in U$ y $r \in R$; $ur \in U$:

Definición A.5. Si U y V son ideales de un anillo conmutativo unitario R:

1. La suma $U + V$ de U y V se define por $U + V = \{u + v \mid u \in U \text{ y } v \in V\}$:
2. El conjunto $UV = \{u_1v_1 + u_2v_2 + \cdots + u_nv_n \mid u_i \in U \text{ y } v_i \in V\}$ donde n es finito, se conoce como el producto de U y V:

Tanto la suma $U + V$ como el producto UV son anillos.

Definición A.6. Si U es un ideal de R, entonces el anillo de las clases laterales $r + U$ bajo las operaciones dadas por: $(r + U) + (s + U) = (r + s) + U$ y $(r + U)(s + U) = rs + U$ para cualesquiera $r; s \in R$ se conoce como el anillo cociente o el anillo de las clases laterales módulo U; y se denota por R/U:

Definición A.7. Un ideal maximal de un anillo conmutativo unitario R es un ideal $M \neq R$ tal que si N es un ideal propio de R que contiene a M, entonces $M = N$.

De…nición A.8. Un ideal $U \subsetneq R$ en un anillo conmutativo unitario R es un ideal primo si $ab \in U$ implica que $a \in U$ o $b \in U$ para todas las $a; b \in R$:

Teorema A.1. Sea R un anillo conmutativo unitario y M un ideal de R. Entonces M es un ideal maximal de R si y sólo si $R=M$ es un campo.

Teorema A.2. Sea $U \subsetneq R$ un ideal en R: Entonces $R=U$ es un dominio entero si y sólo si U es un ideal primo en R:

De…nición A.9. Un elemento u de un dominio entero D es una unidad de D; si u tiene inverso multiplicativo en D: Dos elementos $a; b \in D$ son asociados en D si $a = bu$, donde u es una unidad de D:

De…nición A.10. Un elemento p distinto de cero que no sea unidad de un dominio entero D es un irreducible de D; si en cualquier factorización $p = ab$ en D; a o b es una unidad.

De…nición A.11. Un elemento p de un dominio entero D; distinto de cero, no unidad, con la propiedad de que $p \mid ab$ implica que $p \mid a$ o $p \mid b$; es un primo.

De…nición A.12. Una evaluación euclidiana en un dominio entero D es una función $º$ que transforma a los elementos distintos de cero de D; en los enteros no negativos tal que se satisfacen las condiciones siguientes:

1. Para todos los $a; b$ en D con $b \neq 0$ existen q y r en D tales que $a = bq + r$ donde $r = 0$ o $º(r) < º(b)$:
2. Para cualesquiera $a; b \in D$; donde ni a ni b son cero, $º(a) \cdot º(ab)$:

De…nición A.13. Un campo E es un campo de extensión de un campo F; denotado por $E=F$; si F es un subconjunto de E tal que F es un campo bajo las operaciones inducidas de todo el campo E. También se dice que F es un subcampo de E y se escribe $F \cdot E$:

De…nición A.14. Una función $Á$ de un campo F en sí mismo es un automor…smo de F si:

1. $Á$ es biyectiva.
2. $Á(a + b) = Á(a) + Á(b)$ para cada $a; b \in F$:
3. $Á(ab) = Á(a)Á(b)$ para cualesquiera $a; b \in F$:

Si $E \cdot F$; se dice que E está …jo bajo $Á$ si $Á(x) = x$ para cada $x \in E$:

De…nición A.15. Un elemento $®$ de un campo de extensión E de un campo F es algebraico sobre F si $f(®) = 0$ para algún $f(x) \in F[x]$ distinto de cero.

Definición A.16. Un campo extensión E de F se dice algebraico si todo elemento de E es algebraico sobre F.

Definición A.17. Un campo F está algebraicamente cerrado si todo polinomio no cero en $F[x]$ tiene algún cero en F.

Definición A.18. La cerradura algebraica de un campo F es una extensión algebraica $\bar{F}$ que está algebraicamente cerrada.

Teorema A.3. Todo campo F tiene una cerradura algebraica.

Teorema A.4. Sea E un campo de extensión de F y sea $\alpha \in E$ donde α es algebraico sobre F. Entonces, existe algún polinomio irreducible $p(x) \in F[x]$ tal que $p(\alpha) = 0$. Este polinomio irreducible $p(x)$ está determinado de manera única salvo un factor constante en F y es un polinomio de grado mínimal ≥ 1 en $F[x]$ que tiene a α como un cero. Es decir, si $f(\alpha) = 0$ para $f(x) \in F[x]$ con $f(x) \neq 0$, entonces $p(x)$ divide a $f(x)$.

Definición A.19. Sea E un campo de extensión del campo F y sea $\alpha \in E$ algebraico sobre F. El único polinomio mónico $p(x)$ del teorema A.4, es el polinomio irreducible para α sobre F y se denotará por $irr(\alpha, F)$. El grado de $irr(\alpha, F)$ es el grado de α sobre F y se denota por $grad(\alpha, F)$.

Definición A.20. Si un campo de extensión E de un campo F es de dimensión finita n como espacio vectorial sobre F; entonces se dice que E es una extensión finita de grado n sobre F. Se denota por $[E : F]$ al grado n de E sobre F.

Definición A.21. Sea E un campo de extensión de un campo F y $\alpha \in E$. Se denota por $F(\alpha)$ al menor subcampo de E que contiene a F y a α. En general, si se tiene un conjunto finito de elementos de E; por decir, $\alpha_1, \alpha_2, \ldots, \alpha_n$; el menor subcampo de E que contiene a F y a $\alpha_1, \alpha_2, \ldots, \alpha_n$ se escribe como $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Teorema A.5. Sea E un campo de extensión de un campo F y $\alpha \in E$ algebraico sobre F. Si $grad(\alpha, F) = n$; entonces $F(\alpha)$ es una extensión de grado n sobre F con base $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Mas aún, todo elemento β de $F(\alpha)$ es algebraico sobre F y $grad(\beta, F) \cdot grad(\alpha, F)$.

Teorema A.6. Si E es un campo de extensión finita de un campo F y K es un campo de extensión finita de E; entonces K es una extensión finita de F y $[K : F] = [K : E][E : F]$.

Definición A.22. Sea E una extensión de F. Un polinomio $f(x) \in F[x]$ es separable si todas sus raices en la cerradura algebraica de F son distintas.

Un elemento $a \in E$ es separable sobre F si $irr(a; F)$ es separable. La extensión E/F se dice separable si cada elemento de E es separable sobre F.

Definición A.23. Si para un anillo conmutativo unitario R existe algún entero positivo n tal que $n \cdot a = 0$ para toda $a \in R$; entonces el menor de dichos enteros positivos se le denomina la característica del anillo R. Si no existen dichos enteros, entonces se dice que R es de característica cero.

Teorema A.7. Sea F un campo finito de característica p. La transformación $\varphi_p : F \to F$ dada por $\varphi_p(a) = a^p$ para $a \in F$ es un automorfismo llamado el automorfismo de Frobenius de F.

Definición A.24. Un campo es perfecto si toda extensión finita es separable.

Teorema A.8. Todo campo de característica cero o finito es perfecto.

Definición A.25. Sea F un campo con cerradura algebraica $\bar{F}$. Sea $\{f_i(x) \mid i \in I\}$ una colección de polinomios en $F[x]$. Un campo $E \subseteq \bar{F}$ es el campo de descomposición de $\{f_i(x) \mid i \in I\}$ sobre F si E es el menor subcampo de $\bar{F}$ que contiene a F y a todos los ceros en $\bar{F}$ de cada uno de los $f_i(x)$ para $i \in I$. Un campo $K \subseteq \bar{F}$ es un campo de descomposición sobre F si es el campo de descomposición de algún conjunto de polinomios en $F[x]$.

Definición A.26. Una extensión algebraica E de F es una extensión de Galois si E es el campo de descomposición de algunos polinomios separables f_i de F.

Definición A.27. Sea R un anillo. Un R-módulo consta de un grupo abeliano M junto con una operación de multiplicación externa de cada elemento de M por cada elemento de R; tal que para cualesquiera $\alpha, \beta \in M$ y $r, s \in R$ se cumplen las siguientes condiciones:

1. $r\alpha \in M$.
2. $r(\alpha + \beta) = r\alpha + r\beta$.
3. $r(s\alpha) = (rs)\alpha$.
4. $(r + s)\alpha = r\alpha + s\alpha$.

Definición A.28. Un subgrupo aditivo A de un R-módulo M se llama submódulo de M si para $r \in R$ y $a \in A$; $ra \in A$.

Definición A.29. Un módulo M sobre un anillo R se llama módulo noetheriano si satisface una de las siguientes condiciones equivalentes:

1. Cada submódulo de M es finitamente generado.

2. Cada sucesión ascendente de submódulos de M; $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$; tal que $M_i \neq M_{i+1}$ es finito.
3. Cada familia no vacía de submódulos de M contiene un elemento maximal.

Definición A.30. Un anillo R es noetheriano si es un R-módulo noetheriano.

Teorema A.9. Cualquier dominio entero D puede incrustarse en un campo F; tal que todo elemento de F puede expresarse como cociente de dos elementos de D: Dicho campo F se le llama el campo de cocientes de D:

Definición A.31. Un dominio entero D es un anillo de Dedekind si:

1. D es un anillo noetheriano.
2. D coincide con su cerradura integral dentro de su campo de cocientes.
3. Cada ideal primo no cero de D es maximal.

Proposición A.1. El anillo de enteros O_E de una extensión finita E de Q es un anillo de Dedekind.

Teorema A.10. Sea D un anillo de Dedekind. Cada ideal propio de D se puede representar únicamente como un producto de ideales maximales.

Proposición A.2. Sean α y $\beta \in L$ y $a \in E$: La norma tiene las siguientes propiedades:
1. $N(\alpha\beta) = N(\alpha)N(\beta)$:
2. $N(a\beta) = a^n N(\beta)$:

Definición A.32. Sea L una extensión de Galois de E de grado n, sean $\sigma_1, \ldots, \sigma_n$ los distintos E-automorfismos de L: Sea $b_1, \ldots, b_n$ una base de L sobre E: El discriminante $D(b_1, \ldots, b_n)$ se define como $\det(\sigma_i(b_j))^2$:

El discriminante de una base de O_L se le llama el discriminante de L; denotándose d_L [5].

Proposición A.3. Supóngase que $1, \beta, \ldots, \beta^{n-1}$ están en L y son linealmente independientes sobre E: Sea $f(x) \in E[x]$ el polinomio minimal de β sobre E: Si L=E es separable entonces

$$D(1, \beta, \ldots, \beta^{n-1}) = (-1)^{(n(n-1))/2} N(f'(\beta))$$

donde $f'(x)$ es la derivada de $f(x)$:

Proposición A.4. Sea O_L el anillo de enteros de L. Para cualquier elemento no cero a 2 O_L

$$|O_L/aO_L| = |N_{L/\mathbb{Q}}(a)|$$

donde $|O_L/aO_L|$ denota el número de elementos del anillo cociente O_L/aO_L:

Proposición A.5. $|O_L/aO_L| = |a|^r$ para cualquier elemento no cero a 2 Z:

De…nición A.33. La norma N(I) de un ideal no cero I de O_L se de…ne como $|O_L/I|$:

De…nición A.34. Sean O_E y O_L los anillos de enteros de E y L; respectivamente. Sea P un ideal maximal de O_E y Q un ideal maximal de O_L: Se dice que Q está sobre P y que P está bajo Q si una de las siguientes condiciones equivalentes se satisface:

1. $PO_L \subseteq Q$:
2. $P \subseteq Q$:
3. $Q \cap O_E = P$:

En los anillos O_L y O_E, todo ideal primo es maximal [7].

Proposición A.6. Todo ideal maximal de O_L está sobre un ideal maximal único P de O_E: Para un ideal maximal P de O_E el ideal PO_L es un ideal propio no cero de O_L: Sea $PO_L = \prod_{Q} Q_i$ la factorización en un producto de ideales maximales de O_L: Entonces todos los Q_i son exactamente aquellos ideales maximales de O_L que están sobre P:

Proposición A.7. Sea P un ideal maximal de O_E: Entonces $P \cap Z = pZ$ para un número primo p y N(P) es una potencia positiva de p:

De…nición A.35. Sea P un ideal maximal de O_E que está bajo un ideal maximal Q de O_L: Al grado de O_L/Q sobre O_E/P se le llama grado de inercia $f(Q \mid P)$ de Q sobre P: Si $PO_L = \prod_{Q} Q_i^{e_i}$ es la factorización de PO_L con distintos ideales maximales Q_i de O_L; entonces e_i es conocido como el índice de rami…cación $e(Q_i \mid P)$ de Q_i sobre P:

Lema A.1. Sea M una extensión …nita de L y sean $P \subseteq Q \subseteq R$ ideales maximales de O_E; O_L y O_M; respectivamente. Entonces

$$f(R \mid P) = f(R \mid Q)f(Q \mid P) \text{ y } e(R \mid P) = e(R \mid Q)e(Q \mid P) \text{ [7]:}$$

Teorema A.11. Sean $Q_1; :::; Q_m$ los ideales maximales distintos de O_L que están sobre un ideal maximal P de O_E: Entonces

$$\sum_{i=1}^{X} e(Q_i \mid P) f(Q_i \mid P) = n:$$

Teorema A.12. Junto con las hipótesis del teorema 3.2, supóngase que L es una extensión de Galois sobre E: Entonces

$$e(Q_1 \mid P) = e(Q_2 \mid P) = ::: = e(Q_m \mid P) = e \quad y$$

$$f(Q_1 \mid P) = f(Q_2 \mid P) = ::: = f(Q_m \mid P) = f:$$

Además, $efm = n$.

Proposición A.8. Un elemento $® 2 Z[³]$ es una unidad si y sólo si $N(®) = 1$: Las unidades en $Z[³]$ son $1; ¡1, ³; ¡³; ³^2; ¡³^2$:

Proposición A.9. Si $¼ 2 Z[³]$ es tal que $N(¼) = p$; con p un número primo, entonces $¼$ es un primo en $Z[³]$:

Proposición A.10. Sea $¼ 2 Z[³]$ un elemento primo, entonces $Z[³]=¼Z[³]$ es un campo …nito con $N(¼)$ elementos.

Obsérvese que el grupo multiplicativo de $Z[³]=¼Z[³]$ tiene orden $N(¼) ¡ 1$: Usando el teorema de Lagrange para grupos se obtiene el siguiente resultado análogo al teorema pequeño de Fermat.

Proposición A.11. Si $¼ - ®$; entonces

$$®^{N(¼)¡1} ´ 1 \mod ¼:$$

De…nición A.36. Si $¼ = a + b³$ es un primo en $Z[³]$; se dice que $¼$ es primario si $a ´ 2 \mod 3$ y $b ´ 0 \mod 3$:

Teorema A.13 (Ley de la reciprocidad cúbica). Sean $¼_1$ y $¼_2$ primarios con $N(¼_1) 6= 3$ y $N(¼_2) 6= 3$: Entonces

$$\left(\frac{¼_1}{¼_2}\right)^* = \left(\frac{¼_2}{¼_1}\right)^*:$$

Apéndice B

División euclidiana en $\mathbb{Z}[\omega]$. Para $\alpha, \beta \in \mathbb{Z}[\omega]$, los enteros algebraicos $\lambda, \rho \in \mathbb{Z}[\omega]$ tales que $\alpha = \lambda\beta + \rho$ y $N(\rho) < N(\beta)$ pueden encontrarse de la siguiente manera:

Sean $x_0, x_1 \in \mathbb{Q}$ tales que $\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{N(\beta)} = x_0 + x_1\omega$; defínanse $y_0 = Ne(x_0)$ y $y_1 = Ne(x_1)$ donde $Ne(z)$ denota el entero más cercano a z; es decir, $|z - Ne(z)| \leq \frac{1}{2}$ para cualquier $z \in \mathbb{Q}$. El número λ viene dado por $\lambda = y_0 + y_1\omega$; mientras que $\rho = \alpha - \lambda\beta$. Además,

$$\frac{N(\rho)}{N(\beta)} = (x_0 - y_0)^2 - (x_0 - y_0)(x_1 - y_1) + (x_1 - y_1)^2 \leq \frac{3}{4}.$$

Así, $N(\rho) \leq \frac{3}{4}N(\beta) < N(\beta)$.

Cálculo de carácteres cúbicos residuales. El carácter cúbico residual $\left[\frac{\alpha}{\beta}\right]$ está definido para ciertos valores específicos de α; estos son $\left[\frac{\pm 1}{\beta}\right] = 1$; $\left[\frac{\omega}{\beta}\right] = \omega^{\frac{1}{3}(N(\beta)-1)}$; $\left[\frac{1-\omega}{\beta}\right] = \omega^{\frac{2}{3}(w_0+1)}$ donde $\beta = w_0 + w_1\omega$ es un elemento primario. Estos valores se conocen como valores complementarios.

Dados $\alpha, \beta \in \mathbb{Z}[\omega]$ primos relativos, para calcular $\left[\frac{\alpha}{\beta}\right]$; primero encuéntrese el único primario δ de β; es decir, $\delta = \pm\omega^i\beta$ para algún $i \in \{0,1,2\}$. Luego, mediante la división euclidiana calcúlese $\lambda, \rho \in \mathbb{Z}[\omega]$ tales que $\alpha = \lambda\beta + \rho$ y $N(\rho) < N(\beta)$. En seguida, extraíganse las potencias de $1 - \omega$ del número ρ para obtener γ tal que $\rho = \gamma(1-\omega)^j$ para algún $j \geq 0$ y $1 - \omega \nmid \gamma$, o equivalentemente $3 \nmid \rho\bar{\rho}$. Determínese el único primario $\tilde{\gamma} = \pm\omega^k\gamma$ para algún $k \in \{0,1,2\}$. Aplíquese la ley de la reciprocidad cúbica a $\left[\frac{\tilde{\gamma}}{\delta}\right]$. Luego, de todo lo anterior se tiene que

$$\left[\frac{\alpha}{\beta}\right] = \left[\frac{\rho}{\beta}\right] = \left[\frac{\gamma}{\delta}\right] = \left[\frac{\gamma}{\delta}\right]\left[\frac{1-\omega}{\delta}\right]^j$$

$$= \left[\frac{\tilde{\gamma}}{\delta}\right]\left[\frac{\omega}{\delta}\right]^{-k}\left[\frac{1-\omega}{\delta}\right]^j = \left[\frac{\delta}{\tilde{\gamma}}\right]\omega^{\frac{1}{3}(1-N(\beta))k + \frac{2}{3}(w_0+1)j}$$

donde $\delta = w_0 + w_1\omega$. Este proceso se repite con $\left[\frac{\delta}{\tilde{\gamma}}\right]$ en lugar de $\left[\frac{\alpha}{\beta}\right]$ y como γ^{-1} es un entero positivo que decrece estrictamente en cada iteración, el algoritmo terminará con un valor primario de γ tal que $\gamma^{-1} = 1$, es decir, $\gamma = \pm 1$; punto en el cual $\left[\frac{\alpha}{\beta}\right]$ puede ser evaluada directamente con el valor complementario correspondiente.

Aritmética módulo ½ en $Z[^3]$: Sea $½ = r_0 + r_1{}^3;\ r_0; r_1 \ 2\ Z$ entonces $R = ½½ = r_0^2 ¡ r_0 r_1 + r_1^2$: Luego, $mcd(r_0; R) = mcd(r_1; R) = 1$: Sea $r ´ ¡ r_0 r_1^{i\,1} \bmod R$ donde $0 < r < R$: Se tiene que $r ´ {}^3 \bmod ½$ y cualquier entero algebraico $x_0 + x_1{}^3 \ 2\ Z[^3]$ satisface que $x_0 + x_1{}^3 ´ x \bmod ½$ donde $x \ 2\ Z$ y $x ´ x_0 + x_1 r \bmod R$, $0 · x < R$: Por lo tanto, aritmética módulo ½ en $Z[^3]$ se puede reducir a aritmética entera módulo R:

Aritmética módulo ½ en $Z[^3][±]$: Por lo anterior, cualquier entero algebraico en $Z[^3][±]$ es congruente módulo ½ a un entero en $Z[±]$: Sea $° \ 2\ Z[±]$; el criptosistema de campos cúbicos requiere calcular cocientes de la forma $\frac{°}{°0} \bmod ½$: En la práctica esto se hará de la siguiente manera:

$$\frac{°}{°0} = \frac{°\circ\circ 00}{°0\circ\circ 00} = \frac{°2\circ 00}{N_\circ} ´ N_\circ^{¤}{}^{\circ 2\circ 00} \bmod ½$$

donde $N_\circ = N(°) \bmod R$ y $N_\circ^{¤} ´ N_\circ{}^{i\,1} \bmod R$: El producto $°{}^{2\circ 00} \bmod ½$ es sencillo obtener utilizando la aritmética módulo ½ en $Z[^3]$ para encontrar un entero algebraico congruente con $°^{00}$ módulo ½ en $Z[±]$; y después hacer uso de la multiplicación en $Z[±]$ módulo ½ que a continuación se describe:

Multiplicación en $Z[±]$ módulo ½: Sean $Â ´ x_0 + x_1 ± + x_2 ±^2 \bmod ½$ y $Ã ´ y_0 + y_1 ± + y_2 ±^2 \bmod ½$: El producto de la forma $ÂÃ ´ z_0 + z_1 ± + z_2 ±^2 \bmod ½$ se puede calcular utilizando:

$$\begin{aligned} z_0 &´ x_0 y_0 + x_1 y_2 D + x_2 y_1 D \bmod R \\ z_1 &´ x_0 y_1 + x_1 y_0 + x_2 y_2 D \bmod R \\ z_2 &´ x_0 y_2 + x_1 y_1 + x_2 y_0 \bmod R: \end{aligned}$$

Exponenciación en $Z[±]$ módulo ½: Sea $¯ ´ b_0 + b_1 ± + b_2 ±^2 \bmod ½$ donde $0 · b_0; b_1; b_2 < R$ y $n \ 2\ N$: Se puede calcular $¯^n \bmod ½$ siguiendo los siguientes pasos:

Sean $µ = 1$ y $´ = ¯$; defínanse $b = n \bmod 2$ y $n = ¥\frac{n}{2}¦$ donde $¥\frac{n}{2}¦$ denota el cociente de la división $\frac{n}{2}$: Si $b = 1$; entonces calcúlese $µ´ \bmod ½$, reemplácese $µ$ por $µ´ \bmod ½$ y si además, $n = 0$; entonces el valor de $¯^n \bmod ½$ es $µ$ y el proceso se detiene. En caso contrario, cámbiese $´$ por $´^2 = ´´ \bmod ½$ y nuevamente, defínase b y n: Esta operación es …nita pues el valor de n decrece y termina cuando $n = 0$:

Bibliografía

Matemáticas

[1] Fraleigh, John B., Álgebra abstracta, Addison Wesley Publishing Company, 1987.

[2] Frölich, A. and Taylor, M. J., Algebraic number theory, Cambridge University Press, 1993.

[3] Herstein, I. N., Topics in algebra, John Wiley & Sons Inc., 1976.

[4] Ireland, K. and Rosen, M., A classical introduction to modern number theory, Second edition, Springer-Verlag, 1994.

[5] Lang, Serge, Algebra, Addison Wesley Publishing Company, 1971.

[6] Lang, Serge, Algebraic number theory, Second edition, Springer-Verlag, 1994.

[7] Lecture notes on algebraic number theory
http://www.math.nott.ac.uk/personal/ibf/aln/aln.pdf

Criptografía

[8] Buchmann, Johannes A., Introduction to cryptography, Springer-Verlag, 2001.

[9] Koblitz, Neal, A course in number theory and cryptography, Springer-Verlag, 1998.

[10] Menezes, Alfred J., Handbook of applied cryptography, CRC Press, 1997.

[11] Scheidler, Renate, A public key cryptosystem using purely cubic …elds, Journal of Cryptology, Vol. 11, Number 2, Pages 109-124, 1998.

[12] Singh, Simon, The code book, First edition, Anchor books, 2000.

[13] Stinson, Douglas R., Cryptography: Theory and practice, CRC Press, 1995.

Computación

[14] Blachman, Nancy and Williams, Colin P., Mathematica: A practical approach, Second edition, Prentice Hall Inc., 1999.

[15] Cormen, Thomas H., Introduction to algorithms, MIT Press/McGraw Hill, 1996.