

UNIVERSIDAD ABIERTA INTERAMERICANA

Facultad de Tecnología Informática



Carrera: Licenciatura en Matemática

CRIPTOGRAFÍA

Modelo compacto del algoritmo Diffie-Hellman utilizando cuaterniones

Autora: Cecilia Andrea Prieto

Directora: Dra. Samira Abdel Masih

***TESIS PRESENTADA PARA OPTAR AL TÍTULO DE
LICENCIADA EN MATEMÁTICA***

- Diciembre 2019-

Resumen

Cuando se realizan transacciones en las cuales se envía información que no debe ser leída por personas no autorizadas, se ponen en funcionamiento ciertos protocolos de seguridad. Es así como aparecen los criptosistemas, es decir, un conjunto de procedimientos que utiliza técnicas criptográficas para garantizar la seguridad de la información transmitida por un determinado canal. Con el avance de la tecnología y de la informática, la seguridad de los criptosistemas se torna cada vez más vulnerable. Por este motivo las investigaciones realizadas en este campo son permanentes, ya que se precisa encontrar métodos criptográficos más eficaces que sean infalibles frente a eventuales ataques que intenten romperlos.

El presente trabajo tiene como objetivo el estudio del primer algoritmo criptográfico de intercambio de claves por canales públicos, conocido como *Protocolo de Intercambio de Claves de Diffie-Hellman* [1]. El mismo fue presentado en 1976 y sentó las bases para el surgimiento de lo que se conoce como Criptografía de Clave Pública o Asimétrica. En particular, se analizará la publicación presentada por Kamlofsky, J. & Hecht, P. [2], que es una modificación del Protocolo de Diffie-Hellman en la que utiliza el anillo no conmutativo de los cuaterniones. Esta tesis consta de cuatro capítulos:

El primer capítulo servirá como introducción a la Criptografía en general y se mencionarán los antecedentes históricos más relevantes de la misma.

En el segundo capítulo se estudiarán los conceptos matemáticos preliminares necesarios para entender el protocolo criptográfico que desarrollará el trabajo.

En el tercer capítulo se mencionarán algunos de los criptosistemas simétricos más importantes.

El cuarto capítulo trabajará en profundidad el algoritmo criptográfico Diffie-Hellman y su modificación aplicando el anillo no conmutativo de los cuaterniones.

Finalmente, se realizará una comparación del protocolo utilizando cuaterniones con el algoritmo Diffie-Hellman clásico. Dicha comparación servirá para extraer las conclusiones necesarias que enfatizarán los beneficios que posee el primero sobre el segundo.

Palabras claves:

Criptografía, Diffie-Hellman, criptografía asimétrica, aritmética modular, logaritmos discretos, anillos no conmutativos, cuaterniones.

Índice

Introducción	6
<i>Relevancia del tema</i>	7
Capítulo 1: Introducción a la Criptografía	8
<i>Clasificación de la Criptografía</i>	9
<i>Antecedentes históricos de la Criptografía</i>	9
Capítulo 2: Conceptos matemáticos previos	15
<i>Aritmética Modular</i>	15
<i>Divisibilidad de números enteros y congruencia</i>	16
<i>Conjunto $\mathbb{Z}_n$</i>	18
<i>Operaciones en $\mathbb{Z}_n$</i>	19
<i>Cálculo de potencias modulares</i>	25
<i>Grupos, anillos y cuerpos finitos</i>	30
<i>Grupos</i>	30
<i>Anillos</i>	43
<i>Cuerpos finitos</i>	44
<i>Logaritmos discretos</i>	47
<i>El problema de los logaritmos discretos</i>	50
<i>Criptosistemas basados en logaritmos discretos</i>	51
<i>Cuaterniones</i>	51
<i>Conjunto H</i>	52
<i>Operaciones entre cuaterniones</i>	54

<i>Diferentes representaciones de un cuaternión</i>	55
<i>Cálculo de potencias de exponente natural de un cuaternión</i>	58
<i>Estructura algebraica de cuaterniones</i>	59
Capítulo 3: Algoritmos criptográficos simétricos	60
<i>Codificación del alfabeto</i>	60
<i>El método de Julio César</i>	60
<i>Cómo descriptar el mensaje con el Método de Julio César</i>	61
<i>Método lineal o de Julio César mejorado</i>	63
<i>Cómo descriptar un mensaje con el método de Julio César Mejorado</i>	65
Capítulo 4: Algoritmo de Diffie-Hellman	68
<i>Criptografía asimétrica</i>	68
<i>Algoritmo de Diffie-Hellman</i>	70
<i>Aplicaciones del algoritmo Diffie-Hellman</i>	73
<i>Los ordenadores cuánticos y su amenaza a la criptografía clásica</i>	75
<i>Algoritmo de Diffie-Hellman aplicado a cuaterniones</i>	77
<i>Análisis del tiempo requerido para la ejecución del Algoritmo de Diffie-Hellman aplicando cuaterniones</i>	89
<i>Análisis del espacio de memoria requerido para la ejecución del Algoritmo de Diffie-Hellman aplicando cuaterniones</i>	94
<i>Análisis de la seguridad criptográfica del Algoritmo aplicando cuaterniones</i>	98

Introducción

Criptografía es una palabra que proviene del griego “kryptos” que significa oculto y “graphia”, que significa escritura.

Por lo que se entiende como Criptografía a la ciencia que se ocupa de alterar, mediante algoritmos matemáticos, las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

Según Xifré Solana, Patricia [3]: *“El objetivo de la criptografía es permitir la transmisión de información secreta por un canal público. El problema de la comunicación segura fue de gran interés en la antigüedad y sigue considerándose vital en la actualidad, debido a los millones de ordenadores intercambiando constantemente información por Internet, una red pública al alcance de cualquiera y desde cualquier lugar del mundo.”*

Por lo tanto, la finalidad de la criptografía es

- Garantizar el secreto del mensaje en la comunicación entre dos entidades, sean éstas personas u organizaciones.
- Asegurar que la información que se envía en dichos mensajes sea auténtica, es decir, que el remitente sea efectivamente quien dice ser y que el contenido del mensaje no haya sido modificado en el tránsito.

A lo largo de la historia, se han utilizado diferentes métodos criptográficos entre los cuales se encuentran los protocolos criptográficos asimétricos, que se sustentan en problemas matemáticos complejos como el problema de factorizar números enteros grandes o el de resolver ecuaciones con logaritmos discretos. Pero una de sus desventajas es que se conocen ataques de complejidad subexponencial [4] para muchos de ellos y potenciales ataques eficaces a través de algoritmos cuánticos [5], por lo que existen motivos para desconfiar de su seguridad.

Además, estos protocolos requieren el uso de bibliotecas de precisión extendida y demandan mayor tiempo de procesamiento para la obtención de claves. Debido a estas limitaciones, en los últimos años ha surgido el interés por la *criptografía no conmutativa*, es decir, aquélla que se basa en estructuras algebraicas no conmutativas. En particular, se desarrollaron sistemas de criptografía asimétrica utilizando anillos no conmutativos, entre los cuales se destaca el anillo no conmutativo de los cuaterniones. Una de las ventajas que poseen estos esquemas es que no requieren el uso de bibliotecas

de precisión extendida, lo que permite su aplicación en entornos de bajo poder computacional y memoria RAM reducida.

Relevancia del tema

Todas las industrias disponen de sistemas de control y redes de mando diseñados para supervisar y ejecutar sus procesos. Estos sistemas están presentes no sólo en fábricas que producen bienes transables, sino también en plantas de potabilización de agua, de producción y distribución de energía, gas, petróleo y telecomunicaciones. Es decir, se hallan en infraestructuras asociadas a una nación.

Entre los más difundidos se encuentra el sistema SCADA (**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition), que produce softwares para controlar y supervisar procesos industriales a distancia (por ejemplo, apertura/cierre de una bomba o entrada/salida de un dato). También es muy utilizado el sistema PLC (**C**ontrol **L**ógico **P**rogramable) en la automatización industrial, para automatizar procesos electromecánicos, tales como el control de las maquinarias en líneas de montaje.

Este tipo de sistemas utiliza dispositivos de capacidad limitada, a fin de reducir las tareas de mantenimiento y maximizar los costos de operación.

Hasta hace pocos años, era imposible pensar que un sistema industrial pudiera ser infectado por un virus informático, hasta que en 2010 las plantas de desarrollo nuclear de Irán fueron atacadas por un virus informático llamado Stuxnet. El ataque de Stuxnet desconcertó a los analistas estratégicos de todo el mundo. Dicho virus fue diseñado específicamente para propagarse en los sistemas de software industrial. En particular, ataca los SCADA marca Siemens (entorno Windows), difundidos por todo el mundo. Este hecho produjo que la comunidad internacional mostrara preocupación por su seguridad informática [6]. Los mecanismos de criptografía asimétrica basan su seguridad en la elevada complejidad computacional requerida para el cálculo de logaritmos discretos y la factorización de números enteros. Así, algoritmos criptográficos como RSA con claves de 2048 bits de tamaño se consideran seguros, pero resulta imposible aplicarlos en dispositivos con bajo poder de cómputo como son los PLC o autómatas industriales. De este modo, estos dispositivos quedan vulnerables y en desventaja tecnológica frente a los computadores ordinarios actuales. El uso de algoritmos criptográficos asimétricos basados en cuaterniones, que se desarrollará en este trabajo, permitirá que procesadores pequeños puedan implementar algoritmos criptográficos seguros y así evitar ataques informáticos indeseables.

Capítulo 1

Introducción a la Criptografía

¿Qué es la Criptografía?

La Criptografía es la ciencia de escribir mensajes en forma cifrada o codificada utilizando algoritmos, con el fin de ocultar su significado y hacerlos ininteligibles a personas no autorizadas.

La criptografía se compone de dos pasos: *Encriptado* y *Desencriptado*.

- *Encriptado*: consiste en convertir un mensaje (texto llano) a un texto cifrado.
- *Desencriptado*: consiste en recuperar el mensaje original a partir del texto cifrado.

El encriptado lo realiza el emisor del mensaje, mientras que el desencriptado lo lleva a cabo el receptor del mensaje.

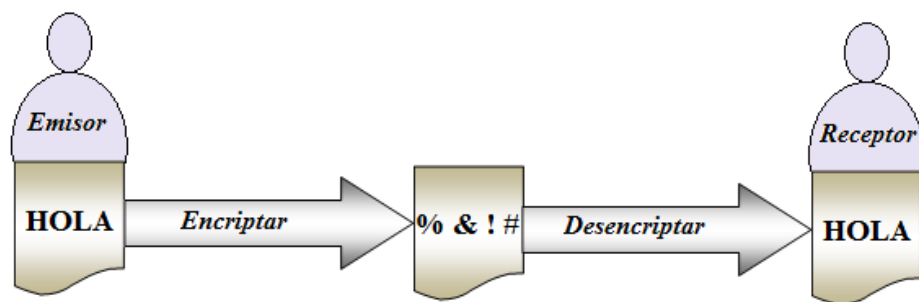


Figura 1.1: Pasos que componen la Criptografía.

Mediante el ocultamiento de la información, la criptografía proporciona:

- *Confidencialidad*: Garantiza que sólo las personas autorizadas puedan acceder a la información.
- *Autenticación*: Asegura que la información provenga del lugar indicado y que no haya sufrido modificaciones.
- *Integridad*: Detecta que la información no haya sido modificada por personas no autorizadas.
- *Control de acceso*: Restringe el acceso a la información.
- *No repudio*: Garantiza la autoría del mensaje enviado.

Clasificación de la Criptografía

La criptografía se clasifica en dos grandes ramas: *Simétrica* y *Asimétrica o de Clave Pública*.

■ *Criptografía Simétrica*

Cuando se utiliza la misma clave para encriptar y desencriptar. El principal problema de la Criptografía Simétrica es que para desencriptar es necesario conocer la clave con la que se ha encriptado y por lo tanto, hay que enviar la clave junto con el mensaje, pudiendo ser interceptado y desencriptado fácilmente.

El *Método de Julio César* y el *Método Lineal o de Julio César Mejorado*, que se expondrán en el Capítulo 3, son ejemplos de Criptografía Simétrica.

■ *Criptografía Asimétrica o de Clave Pública*

Cuando se utilizan distintas claves para encriptar y desencriptar. En este caso, la clave que se utiliza para encriptar puede ser pública (conocida por todos) y la clave para desencriptar debe ser privada, es decir, conocida sólo por el destinatario (ni siquiera es conocida por el remitente).

La Criptografía Asimétrica utiliza como base de su seguridad problemas matemáticos difíciles de resolver, como por ejemplo la factorización de números enteros o el cálculo de logaritmos discretos.

El *Algoritmo RSA* y el *Algoritmo de Diffie-Hellman*, que se analizarán en el Capítulo 4, son ejemplos de Criptografía Asimétrica.

Antecedentes históricos de la Criptografía

El origen de la criptografía se remonta a los orígenes del hombre, desde que aprendió a comunicarse. A partir de ese momento, tuvo que encontrar medios para asegurar la confidencialidad de las comunicaciones.

El primer sistema criptográfico de la historia fue la ESCÍTALA. Fue utilizado por los espartanos en el año 400 a.C. para el envío de mensajes secretos. La escítala está compuesta por dos varas de similar grosor y una tira de cuero o papiro sobre la cual se escribía el mensaje. Cada una de las varas era entregada a los participantes de la comunicación. Para enviar el mensaje se enrollaba la tira de cuero o papiro en forma de espiral a uno de los bastones y se escribía el mensaje longitudinalmente, de forma tal que en cada vuelta de cinta apareciese cada vez una letra. Una vez escrito el mensaje, se

desenrollaba la tira y se la enviaba al receptor, que sólo tenía que enrollar a la vara gemela para leer el mensaje original.

Este método se puede considerar el primer sistema de criptografía por **trasposición**, que se caracteriza por ocultar el significado real de un texto alterando el orden de los signos que lo conforman.



Figura 1.2: La Escítala. Fuente: <http://ojoscuriosos.com/la-escitala/>.

En la antigua Roma, Julio César (100 a.C.- 44 a.C.) enviaba mensajes encriptados a sus generales en el frente. El Método de Julio César fue el primer método algorítmico de cifrado y fue llamado así por su creador. El mismo consiste en sustituir cada letra del mensaje por la letra ubicada tres posiciones más adelante en el alfabeto, haciendo una correspondencia cíclica para las últimas letras. Por ejemplo, a la letra A le corresponde la letra D, mientras que a la letra Z le corresponde la letra C. La siguiente figura muestra un ejemplo del método de cifrado de Julio César.

C	R	I	P	T	O	G	R	A	F	I	A
f	v	m	s	y	r	k	v	d	i	m	d

Figura 1.3: Cifrado de la palabra Criptografía mediante el Método de Julio César.

Las civilizaciones mencionadas anteriormente emplearon métodos de cifrados por **sustitución** y por **trasposición**. Son dos procedimientos de cifrado básicos que se han ido repitiendo en épocas posteriores hasta llegar a la actualidad. El significado de estos métodos se formaliza de la siguiente manera:

■ **Cifrado por sustitución:** consiste en establecer una correspondencia biunívoca entre las letras del alfabeto en el que está escrito el mensaje original y los elementos de otro conjunto. Así, cada letra del texto llano se sustituye por su símbolo asociado de dicho conjunto. El receptor de la comunicación, que conoce la correspondencia establecida, sustituye cada símbolo por el correspondiente del alfabeto, recuperando de este modo el mensaje original.

■ **Cifrado por trasposición:** consiste en colocar los símbolos del mensaje original en un orden distinto, de manera que el mensaje contenga los mismos elementos del texto llano pero éstos colocados de tal forma que resulten incomprensibles. El receptor de la comunicación, conociendo la trasposición, coloca los símbolos desordenados en su posición original.

En la época del Renacimiento (1300 – 1600 d.C.), los Estados Pontificios se caracterizaban por el uso intensivo de la criptografía. Leon Battista Alberti (1404-1472) se destacó en esa época porque inventó para el Vaticano un disco de cifrado, llamado “El disco de Alberti”. El modo de emplearlo figura en su tratado “De Cifris”, en 1466. Constituye un cifrado por sustitución, mediante el cual era posible transformar textos sin que existiera una correspondencia única entre el alfabeto original del mensaje y el alfabeto usado para el cifrado.

El disco está compuesto por dos anillos concéntricos. El anillo externo es fijo, y contiene 24 casillas abarcando los 20 caracteres en latín (sin incluir la H J K Ñ U W Y) y los números 1, 2, 3, y 4 para el texto a cifrar. Dichos números indican un giro. Por el contrario, el anillo interno es móvil, disponiendo de los 24 caracteres en latín, además del signo & que son utilizados para cifrar el texto. Las 20 letras del anillo externo están en orden alfabético mientras que las 24 minúsculas del anillo interno no.



Figura 1.4: El disco de Alberti.

Fuente: <https://www.xlsemanal.com/conocer/tecnologia/20180614/historia-de-la-criptografia.html>.

El siguiente Ejemplo ayudará a comprender su funcionamiento:

Ejemplo 1.1

Se desea cifrar el texto MA3L. En este caso, el número 3 sólo indicará un giro del anillo interior, por lo que el texto a cifrar es en realidad la palabra MAL. Observando la Figura 1.4, se puede comprobar que el orden de los caracteres del disco móvil es

g k l n p r t u z x y s o m q i h f d b a c e

Primer Paso:

Se elige una letra del anillo fijo como clave, conocida únicamente por el emisor y el receptor. Se supondrá que la letra clave elegida es la **A**.

Se hace coincidir la letra **A** con una letra del anillo móvil, por ejemplo la **m**. En este caso los anillos quedarán dispuestos de la siguiente manera:

A	B	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	2	3	4
m	q	i	h	f	d	b	a	c	e	g	k	l	n	p	r	t	u	z	&	x	y	s	o

Figura 1.5: Forma en que quedan ordenados los símbolos del disco de Alberti. La primera fila de la tabla contiene los símbolos del anillo fijo, mientras que la segunda fila contiene los símbolos del anillo móvil.

Segundo Paso:

El mensaje cifrado comenzará con la letra **m**, la cual indicará al receptor cómo están dispuestos los anillos. De este modo, el receptor sabrá que debe alinear la **A** del anillo fijo con la **m** del anillo móvil. Se continúa sustituyendo cada letra del texto a cifrar hasta encontrar el número **3**, que indicará que hay que mover el anillo interior. Hasta el momento, el texto cifrado es el siguiente:

Texto a cifrar: **M A 3 L**

Texto cifrado: **m e m s**

Tercer Paso:

El cifrado del número **3**, que en este caso es **s**, indicará que hay que girar el anillo móvil, de modo tal de alinear la letra **s** con la clave **A**. De este modo los anillos quedarán ordenados del siguiente modo:

A	B	C	D	E	F	G	I	L	M	N	O	P	Q	R	S	T	V	X	Z	1	2	3	4
s	o	m	q	i	h	f	d	b	a	c	e	g	k	l	n	p	r	t	u	z	&	x	y

Figura 1.6: Forma en que quedan ordenados los símbolos del disco de Alberti luego de girar el disco móvil.

Sólo resta cifrar la letra **L**, que le corresponderá la letra **b** del anillo móvil. Por lo tanto, se tiene finalmente:

Texto a cifrar: **M A 3 L**

Texto cifrado: **m e m s b**

El disco de Alberti fue considerado, durante mucho tiempo, uno de los algoritmos criptográficos más seguros. Sin embargo, con el advenimiento de las computadoras, el proceso de descifrado de los mensajes encriptados mediante esta técnica se tornó relativamente sencillo.

La criptografía clásica abarca desde los tiempos inmemorables hasta la mitad del siglo XX y en ella las técnicas utilizadas son básicamente operaciones de sustitución y trasposición de caracteres, con o sin clave secreta.

En la Primera Guerra Mundial (1914-1918) los cifrados todavía eran hechos por trasposición y los mensajes eran llevados por el hombre, utilizando medios de transporte muy lentos. Incluso había lugares en los cuales era imposible llevar mensajes como barcos, aviones o submarinos. Por este motivo se empezaron a utilizar teléfonos, radios y telégrafos, cambiando radicalmente las comunicaciones.

Hasta 1918 los cifrados se hacían manualmente, lo que causaba muchos errores en el proceso de cifrar y descifrar. En dicho año los científicos alemanes Arthur Scherbius y Richard Ritter investigaron cómo sustituir los inadecuados sistemas de criptografía utilizados en la Primera Guerra Mundial, que utilizaban lápiz y papel, recurriendo a la tecnología. Así fue que en 1920 desarrollaron la máquina Enigma.

Dicha máquina era un dispositivo electromecánico. Estaba compuesto por un teclado similar al de las máquinas de escribir, cuyas letras eran interruptores eléctricos, un engranaje mecánico y un tablero en el que se mostraba el mensaje codificado. Cada letra del texto a cifrar se pulsaba en el teclado y la unidad modificadora lo transformaba en otra diferente antes de mostrarla en el tablero.

También disponía de un reflector mediante el cual los receptores del mensaje podían descifrarlo.



Figura 1.7: La máquina Enigma. Fuente: http://www.belt.es/expertos/HOME2_experto.asp?id=2030

Cuando éste llegaba al destino, los receptores estaban preparados con otra máquina Enigma, con los rotores colocados en la misma posición que la máquina que enviaba el mensaje cifrado.

El ejército alemán aseguraba que Enigma proporcionaba el sistema de cifrado más seguro del mundo y por esta razón, durante la Segunda Guerra Mundial, adquirieron una gran cantidad de estas máquinas. En ese entonces el gobierno inglés contrató a Alan Turing (1912-1954), un destacado matemático, informático y criptógrafo inglés, con el fin de descifrar los códigos de las máquinas Enigma. Gracias a su investigación, Turing creó la máquina BOMBE, mediante la cual pudieron descubrirse los códigos nazis. Enigma fue finalmente descifrada...

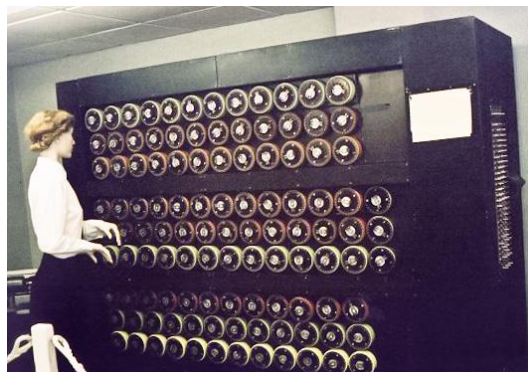


Figura 1.8: La máquina Bombe.

Fuente: <https://es.wikipedia.org/wiki/Bombe#/media/File:TuringBombeBletchleyPark.jpg>

Después de la Segunda Guerra Mundial se inició el desarrollo de las computadoras. Con ello también avanzaron los criptosistemas, con algoritmos más sofisticados para la transmisión de información.

Un año importante para la criptografía fue 1976, cuando W. Diffie (1944-) y M. Hellman (1945-) crearon el concepto de criptografía asimétrica o de clave pública.

En la década de los ochenta se comenzó a desarrollar la computación cuántica gracias a los aportes de D. Deutsch (1982-) y R. Feynman (1918-1988), quienes sugirieron que los sistemas cuánticos se podrían utilizar como herramienta de cálculo. En particular, la criptografía cuántica es una de las aplicaciones más importantes de la computación cuántica.

A pesar de que la criptografía tradicional permite mantener una comunicación segura entre dos partes, las propuestas algorítmicas que usan las propiedades de un hipotético ordenador cuántico pondrían en peligro los sistemas criptográficos más utilizados.

Se cree que en un futuro no muy lejano, la criptografía cuántica será un sólido candidato para relevar las técnicas criptográficas que hoy se utilizan.

Capítulo 2

Conceptos matemáticos previos

En este capítulo se describirán las nociones matemáticas que serán aplicadas en el desarrollo de este trabajo.

2.1 Aritmética Modular

Definición 2.1.1: Aritmética Modular

La aritmética modular es la parte de la Aritmética que opera con números enteros, considerando el resto de la división de dichos números enteros por un número natural “n” fijo, llamado “el módulo n”.

La aritmética modular fue creada por Gauss (1777-1855) y estudiada sistemáticamente hacia fines del siglo XVIII. Gauss elaboró este tipo de aritmética para resolver, de una manera más sencilla, las Ecuaciones Diofánticas. Estas ecuaciones fueron planteadas por Diofanto de Alejandría (200-284), y son de la forma:

$$a x + b y = c$$

Donde $a, b, c \in \mathbb{Z}$ y las incógnitas son $x, y \in \mathbb{Z}$.

El siguiente ejemplo ilustra este tipo de ecuaciones.

Ejemplo 2.1.2

Un hombre va a una tienda de ropa y compra 12 trajes, unos negros y otros grises, por \$1200. Los trajes negros valen \$30 más que los grises y ha comprado el mínimo posible de estos últimos. Suponiendo que los precios de cada traje son números enteros, ¿cuántos trajes ha comprado de cada color?

Solución

Se definen las siguientes incógnitas:

x : Cantidad de trajes negros.

y : Precio de un traje gris.

En consecuencia,

$12 - x$: Cantidad de trajes grises.

$y + 30$: Precio de un traje negro.

Luego, queda planteada la siguiente ecuación:

$$x (y + 30) + (12 - x) y = 1200$$

Al aplicar la propiedad distributiva, se obtiene la siguiente ecuación diofántica:

$$30x + 12y = 1200$$

Despejando la incógnita y se tiene:

$$y = 100 - \frac{5}{2}x$$

Como $y \in \mathbb{Z}$ entonces x debe ser par. Por otro lado, como el hombre compró la mínima cantidad de trajes grises, entonces adquirió la máxima cantidad de trajes negros. De este modo, x debe ser el mayor número par que verifique:

$$1 \leq x < 12$$

En consecuencia, $x = 10$. Por lo tanto, $y = 100 - \frac{5}{2}x = 100 - \frac{5}{2}(10) = 75$.

Respuesta:

Trajes negros: 10

Trajes grises: 2

Precio de un traje gris: \$75

Precio de un traje negro: \$105

Este ejemplo será resuelto de una manera más sencilla luego de presentar la teoría de la Aritmética Modular.

Divisibilidad de números enteros y congruencia

Teorema 2.1.3: Algoritmo de la División Entera

Sean $a, b \in \mathbb{Z}$ con $b \neq 0$ Entonces existen dos números enteros q y r , llamados cociente y resto, que verifican:

$$1) a = bq + r$$

$$2) 0 \leq r < |b|$$

Demostración

Está detallada en [7]. ■

Definición 2.1.4: Divisibilidad

Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Se dice que “ b divide a a ” y se escribe $b \mid a$ si $a = k \cdot b$ para algún $k \in \mathbb{Z}$ o equivalentemente, si al dividir a por b , el resto da 0.

Definición 2.1.5: Máximo Común Divisor y Mínimo Común Múltiplo

Sean $a, b \in \mathbb{Z}$ tales que no son simultáneamente nulos. Se dice que d es el máximo común divisor entre a y b si verifica:

- 1) $d > 0$
- 2) $d \mid a \wedge d \mid b$
- 3) Si existe $c \in \mathbb{Z}$ tal que $c \mid a \wedge c \mid b \Rightarrow c \mid d$

Por otro lado, se dice que m es mínimo común múltiplo entre a y b si verifica:

- 1) $m > 0$
- 2) $a \mid m \wedge b \mid m$
- 3) Si existe $c \in \mathbb{Z}$ tal que $a \mid c \wedge b \mid c \Rightarrow m \mid c$

Notación: Al máximo común divisor entre a y b se lo simbolizará por $\text{mcd}(a, b)$, mientras que al mínimo común múltiplo se lo representará por $\text{mcm}(a, b)$.

El siguiente Teorema es utilizado con frecuencia cuando se trabaja con un máximo común divisor:

Teorema 2.1.6

Sean $a, b \in \mathbb{Z}$ tales que no son simultáneamente nulos.

- 1) Si $d = \text{mcd}(a, b) \Rightarrow \exists p, q \in \mathbb{Z}$ tales que $d = p \cdot a + q \cdot b$
- 2) Si $d > 0 \wedge \exists p, q \in \mathbb{Z}$ tales que $d = p \cdot a + q \cdot b \wedge d \mid a \wedge d \mid b \Rightarrow d = \text{mcd}(a, b)$

Demostración

Véase [8]. ■

Definición 2.1.7: Congruencia

Sea n un número natural mayor que 1. Dados dos números enteros $a, b \in \mathbb{Z}$, se dice que a es congruente con b “módulo n ” y se lo representa:

$$a \equiv b \pmod{n}$$

Si y sólo si $n \mid (b - a)$ ó $n \mid (a - b)$.

Ejemplo 2.1.8

1) $36 \equiv 12 \pmod{6}$ pues $6 \mid (36 - 12)$. Es decir, $6 \mid 24$.

2) $43 \not\equiv 5 \pmod{3}$ pues $3 \nmid (43 - 5)$. Es decir, $3 \nmid 38$.

La siguiente proposición enumera ciertas propiedades de la congruencia que se aplicarán en esta tesis:

Proposición 2.1.9

Sean $a, b, c \in \mathbb{Z}$ entonces:

- 1) *Propiedad Reflexiva:* $a \equiv a \pmod{n}$.
- 2) *Propiedad Simétrica:* Si $a \equiv b \pmod{n}$ entonces $b \equiv a \pmod{n}$.
- 3) *Propiedad Transitiva:* Si $a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.
- 4) $a \equiv 0 \pmod{n} \Leftrightarrow n \mid a$
- 5) Si $a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \Rightarrow a.c \equiv b.d \pmod{n}$.
- 6) Si $a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \Rightarrow a + c \equiv b + d \pmod{n}$.
- 7) Si $a \equiv b \pmod{n} \wedge c \neq 0 \Rightarrow a.c \equiv b.c \pmod{n}$.
- 8) Si $a \equiv b \pmod{n} \wedge k \in \mathbb{N} \Rightarrow a^k \equiv b^k \pmod{n}$.
- 9) $a \equiv b \pmod{n} \Leftrightarrow a \wedge b$ tienen el mismo resto en la división entera por n .
- 10) $a \equiv r_a \pmod{n}$ donde r_a es el resto de la división entera de a por n .
- 11) $a \equiv n + a \pmod{n}$

Demostración

Está detallada en [7]. ■

El conjunto $\mathbb{Z}_n$

De la Proposición 2.1.9 inciso 10), se sabe que si $a \in \mathbb{Z}$ y n es un natural mayor que 1, entonces $a \equiv r_a \pmod{n}$, donde r_a es el resto de la división entera de a por n . Esto permite clasificar a los números enteros según el resto de su división entera por n . Como los posibles restos son $0, 1, \dots, n-1$, surge la siguiente:

Definición 2.1.10: El conjunto $\mathbb{Z}_n$

Si n es un número natural mayor que 1, el conjunto $\mathbb{Z}_n$ es

$$\mathbb{Z}_n = \{ 0, 1, 2, \dots, n-1 \}.$$

A dicho conjunto se le definirán ciertas operaciones, a fin de dotarlo de una estructura algebraica conveniente.

Operaciones en $\mathbb{Z}_n$

En $\mathbb{Z}_n$ se definen las operaciones de *suma* y *multiplicación* del siguiente modo:

Definición 2.1.11: Suma y producto en $\mathbb{Z}_n$

Sean $a, b, c \in \mathbb{Z}_n$ Entonces

- 1) $a + b = c$ en $\mathbb{Z}_n \Leftrightarrow c$ es el resto de la división entera de $(a+b)$ por n .
- 2) $a \cdot b = c$ en $\mathbb{Z}_n \Leftrightarrow c$ es el resto de la división entera de $(a \cdot b)$ por n .

De la definición anterior se deduce la siguiente

Proposición 2.1.12

Sean $a, b, c \in \mathbb{Z}_n$ Entonces

- 1) $a + b = c$ en $\mathbb{Z}_n \Leftrightarrow a + b \equiv c \pmod{n}$
- 2) $a \cdot b = c$ en $\mathbb{Z}_n \Leftrightarrow a \cdot b \equiv c \pmod{n}$

Demostración

1) De las Definiciones 2.1.4 y 2.1.11 resulta

$$\begin{aligned} a + b = c \text{ en } \mathbb{Z}_n &\Leftrightarrow c \text{ es el resto de la división entera de } (a+b) \text{ por } n \\ &\Leftrightarrow a + b = k n + c \text{ para algún } k \text{ entero (Por el Algoritmo de la División Entera)} \\ &\Leftrightarrow (a + b) - c = k n \text{ para algún } k \text{ entero} \Leftrightarrow n \mid (a+b) - c \Leftrightarrow a + b \equiv c \pmod{n}. \end{aligned}$$

2) Se demuestra de manera similar al inciso anterior. ■

Definición 2.1.13: Elementos neutros para la suma y la multiplicación en $\mathbb{Z}_n$

- 1) El neutro para la suma es 0 pues $a + 0 \equiv a \pmod{n} \quad \forall a \in \mathbb{Z}_n$.
- 2) El neutro para el producto es 1 pues $a \cdot 1 \equiv a \pmod{n} \quad \forall a \in \mathbb{Z}_n$.

Definición 2.1.14: El opuesto en $\mathbb{Z}_n$

Dado $a \in \mathbb{Z}_n$, el opuesto de a es un número $b \in \mathbb{Z}_n$ tal que $a + b = 0$ en $\mathbb{Z}_n$.

La siguiente proposición muestra cómo calcular el opuesto de un elemento en $\mathbb{Z}_n$:

Proposición 2.1.15

Si $a \in \mathbb{Z}_n$ entonces su opuesto es $(n - a)$.

Demostración

Por el inciso 4) de la Proposición 2.1.9 resulta:

$$a + (n - a) = n \equiv 0 \pmod{n}.$$

Al aplicar la Propiedad Transitiva (Proposición 2.1.9, inciso 3)) se obtiene:

$$a + (n - a) \equiv 0 \pmod{n}$$

Por lo tanto, por definición de la operación suma en $\mathbb{Z}_n$, se tiene

$$a + (n - a) = 0 \text{ en } \mathbb{Z}_n. \quad \blacksquare$$

Definición 2.1.16: Inverso en $\mathbb{Z}_n$

Dado $a \in \mathbb{Z}_n$, el inverso de a es un número $b \in \mathbb{Z}_n$ tal que $a \cdot b = 1$ en $\mathbb{Z}_n$.

Notación: al inverso de $a \in \mathbb{Z}_n$ se simbolizará por a^{-1} , mientras que al opuesto de a se lo representará por $-a$.

No todo elemento de $\mathbb{Z}_n$ tiene inverso, como se verá en el siguiente ejemplo:

Ejemplo 2.1.17

Dado $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

- Hallar el opuesto de 3.
- Indicar los elementos de $\mathbb{Z}_8$ que tienen inverso.

Solución

- Sea $3 \in \mathbb{Z}_8$. Entonces, por la Proposición 2.1.12 su opuesto es $(8 - 3) = 5$.
- Se elaborará la siguiente tabla, que contendrá los productos entre dos elementos no nulos de $\mathbb{Z}_8$:

•	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	4	4
7	7	6	5	4	3	2	1

Para explicar cómo se completó la tabla, se desarrollará la tercera fila de la misma:

$$2.(1) = 2 \neq 1.$$

$$2.(2) = 4 \neq 1.$$

$$2.(3) = 6 \neq 1.$$

$$2.(4) = 8 \equiv 0 \neq 1.$$

$$2.(5) = 10 \equiv 2 \neq 1.$$

$$2.(6) = 12 \equiv 4 \neq 1.$$

$$2.(7) = 14 \equiv 6 \neq 1.$$

Por lo tanto, 2 no tiene inverso. Observando los datos de la tabla, se puede determinar qué elementos tienen inverso: Si una fila de la tabla contiene el 1, entonces el elemento que encabeza dicha fila tiene inverso. Además, su inverso es el elemento que encabeza la columna que contiene al 1. De este modo,

<i>Elemento de $\mathbb{Z}_8$</i>	<i>Inverso en $\mathbb{Z}_8$</i>
1	1
2	No tiene
3	3
4	No tiene
5	5
6	No tiene
7	7

El siguiente teorema indica en qué casos un elemento de $\mathbb{Z}_n$ es invertible:

Teorema 2.1.18: Teorema de Invertibilidad en $\mathbb{Z}_n$

Un elemento $a \in \mathbb{Z}_n$ es invertible $\Leftrightarrow \text{mcd}(a, n) = 1$

Demostración

$\Rightarrow$) Como a es invertible en $\mathbb{Z}_n$, $\exists x \in \mathbb{Z}_n$ tal que $ax = 1$ en $\mathbb{Z}_n$. Por lo tanto,

$$ax \equiv 1 \pmod{n} \Rightarrow n \mid (ax - 1) \Rightarrow \exists k \in \mathbb{Z} / ax - 1 = nk. \text{ Luego,}$$

$$ax = 1 + nk \tag{1}$$

Por otro lado, sea $d = \text{mcd}(a, n)$. Entonces $d \mid a \wedge d \mid n \Rightarrow \exists k_1, k_2 \in \mathbb{Z}$ tales que

$$\begin{cases} a = k_1 d \\ n = k_2 d \end{cases} \tag{2}$$

Reemplazando [2] en [1] se obtiene $k_1 dx = 1 + k_2 kd \Rightarrow (k_1 x - k_2 k) d = 1$.

De esta última ecuación se concluye que

$$((k_1 x - k_2 k) = 1 \wedge d = 1) \vee ((k_1 x - k_2 k) = -1 \wedge d = -1)$$

Como $d > 0$, resulta que $d = 1$. Luego, $\text{mcd}(a, n) = 1$.

$\Leftarrow$) Como $\text{mcd}(a, n) = 1$, $\exists p, q \in \mathbb{Z}$ tales que

$$1 = pa + qn$$

Entonces $1 - pa = qn$, es decir, $n \mid (1 - pa)$. En consecuencia,

$$pa \equiv 1 \pmod{n} \tag{3}$$

Por otro lado, sea r_p el resto de la división entera de p por n . Entonces, por la Proposición 2.1.9 inciso 10) resulta

$$p \equiv r_p \pmod{n} \tag{4}$$

De [3], [4] y aplicando Proposición 2.1.9 inciso 5) se tiene:

$$r_p a \equiv pa \equiv 1 \pmod{n} \Rightarrow r_p a \equiv 1 \pmod{n}$$

En consecuencia,

$$r_p a = 1 \text{ en } \mathbb{Z}_n$$

Luego, a es invertible en $\mathbb{Z}_n$ y su inverso es r_p . ■

Corolario del Teorema de Invertibilidad en $\mathbb{Z}_n$

Si n es primo entonces todo elemento no nulo de $\mathbb{Z}_n$ es invertible.

Demostración

Sea $a \in \mathbb{Z}_n$ con $a \neq 0$. Como n es primo, $\text{mcd}(a, n) = 1$.

Por lo tanto, por el Teorema de Invertibilidad, resulta que a es invertible. ■

La siguiente proposición determinará cómo calcular el inverso de un elemento en $\mathbb{Z}_n$:

Proposición 2.1.19

Sea $a \in \mathbb{Z}_n$ con $a \neq 0$ y tal que a es invertible en $\mathbb{Z}_n$. Entonces su inverso es

$$a^{-1} = \frac{1 + n k}{a}$$

Para algún $k \in \mathbb{Z}$ con $0 \leq k \leq a$ y tal que $\frac{1 + n k}{a} \in \mathbb{Z}_n$.

Demostración

Como a es invertible, $\exists a^{-1} \in \mathbb{Z}_n$ tal que $a a^{-1} = 1$ en $\mathbb{Z}_n$. Por lo tanto

$$a a^{-1} \equiv 1 \pmod{n} \Rightarrow n \mid (a a^{-1} - 1) \Rightarrow \exists k \in \mathbb{Z} \text{ tal que } a a^{-1} - 1 = n k.$$

En consecuencia,

$$a^{-1} = \frac{1 + n k}{a}.$$

De aquí resulta que, como $a^{-1} \in \mathbb{Z}_n$, entonces $\frac{1 + n k}{a} \in \mathbb{Z}_n$.

Además, como $a, a^{-1} \in \mathbb{Z}_n \wedge a, a^{-1} \neq 0 \Rightarrow a \cdot a^{-1} \geq 1 \Rightarrow a \cdot a^{-1} - 1 \geq 0 \Rightarrow n k \geq 0$.

Luego,

$$k \geq 0 \quad [1]$$

Por otro lado, como

$$a^{-1} \in \mathbb{Z}_n \Rightarrow \frac{1 + n k}{a} \in \mathbb{Z}_n \Rightarrow \frac{1 + n k}{a} \leq n - 1 \Rightarrow k \leq \frac{a(n-1)-1}{n} \Rightarrow k \leq a - \underbrace{\frac{(a+1)}{n}}_{\geq 0}.$$

Por lo tanto

$$k \leq a \quad [2]$$

De [1] y [2] resulta $0 \leq k \leq a$. ■

Ejemplo 2.1.20

Calcular los siguientes inversos, en caso que existan, en el conjunto que se indica:

1) 9^{-1} en $\mathbf{Z}_{27}$

2) 8^{-1} en $\mathbb{Z}_{11}$

Solución:

1) Como $\text{mcd}(9, 27) = 9 \neq 1$, por el Teorema 2.1.18 (Teorema de Invertibilidad) resulta que 9 no tiene inverso.

2) Como $\text{mcd}(8, 11) = 1$, entonces 8 tiene inverso en $\mathbb{Z}_{11}$. Por la Proposición 2.1.19,

$$8^{-1} = \frac{1 + 11k}{8}$$

Para algún $k \in \mathbb{Z}$ con $0 \leq k \leq 8$ y tal que $\frac{1 + 11k}{8} \in \mathbb{Z}_{11}$.

A fin de determinar cuál es el valor de k , se diseña la siguiente tabla:

k	$\frac{1 + 11k}{8}$
0	$\frac{1}{8} \notin \mathbb{Z}_{11}$
1	$\frac{12}{8} = \frac{3}{2} \notin \mathbb{Z}_{11}$
2	$\frac{23}{8} \notin \mathbb{Z}_{11}$
3	$\frac{34}{8} = \frac{17}{4} \notin \mathbb{Z}_{11}$
4	$\frac{45}{8} \notin \mathbb{Z}_{11}$
5	$\frac{56}{8} = 7 \in \mathbb{Z}_{11}$

Luego, $8^{-1} = 7$ en $\mathbb{Z}_{11}$.

Potencias modulares

Las potencias modulares se encuentran presentes en la mayoría de los algoritmos criptográficos. Su definición se basa en el producto modular y se expone a continuación:

Definición 2.1.21: Potencia modular

Sean $a \in \mathbb{Z}$ con $a \geq 0$ y $k \in \mathbb{Z}$. Entonces

$a^k = c \pmod{n} \Leftrightarrow c$ es el resto de la división entera de a^k por n .

Observación 2.1.22

Si “ a ” fuera un número entero muy grande y se intentara hallar $a^k \pmod{n}$ calculando primeramente a^k y luego efectuando su división entera por n para hallar el resto, resultaría bastante tedioso e ineficiente. Inclusive, si se hiciera este cálculo en un computador, se correría el riesgo de producirse *overflow* o *desbordamiento*. Este hecho ocurre cuando un cálculo de enteros produce un resultado mayor a lo que puede almacenar el registro de un ordenador.

Por esta razón se presentará el siguiente algoritmo que permitirá calcular $a^k \pmod{n}$ de un modo más sencillo y eficiente.

Algoritmo para calcular potencias modulares

El algoritmo para calcular $a^k \pmod{n}$ se basa en el siguiente hecho:

Si se efectúa la división entera de k por 2, se obtiene:

$$k = 2 \left\lfloor \frac{k}{2} \right\rfloor + r$$

Donde

$$\left\lfloor \frac{k}{2} \right\rfloor : \text{Parte entera de } \frac{k}{2}.$$

r : Resto de la división ($0 \leq r \leq 1$).

En consecuencia,

$$a^k = a^{2 \left\lfloor \frac{k}{2} \right\rfloor + r} = \left(a^2\right)^{\left\lfloor \frac{k}{2} \right\rfloor} \cdot a^r$$

Esta expresión permite generar las siguientes sucesiones:

$$\{a_0, a_1, a_2, \dots\}, \{k_0, k_1, k_2, \dots\}, \{c_0, c_1, c_2, \dots\}, \{r_0, r_1, r_2, \dots\}$$

Donde

$$\begin{cases} a_0 = a \\ k_0 = k \\ c_0 = 1 \\ r_0 = r \end{cases}$$

Los demás términos de las sucesiones se definen del siguiente modo, aplicando las propiedades de congruencia enunciadas en los incisos 5), 8) y 9) de la Proposición 2.1.9:

$$a^k = a^{2 \left\lfloor \frac{k}{2} \right\rfloor + r_0} = \left(a^2\right)^{\left\lfloor \frac{k}{2} \right\rfloor} \cdot a^{r_0} \equiv a_1^{k_1} \cdot c_1 = \left(a_1^2\right)^{\left\lfloor \frac{k_1}{2} \right\rfloor} \cdot a_1^{r_1} \cdot c_1 \equiv a_2^{k_2} \cdot c_2 = \dots$$

$$\begin{array}{ccc} \uparrow & & \uparrow \\ \begin{cases} a_1 \equiv a^2 \pmod{n} \\ k_1 = \left\lfloor \frac{k}{2} \right\rfloor \\ c_1 \equiv a^{r_0} = a^{r_0} \cdot c_0 \pmod{n} \end{cases} & & \begin{cases} a_2 \equiv a_1^2 \pmod{n} \\ k_2 = \left\lfloor \frac{k_1}{2} \right\rfloor \\ c_2 \equiv a_1^{r_1} \cdot c_1 \pmod{n} \end{cases} \end{array}$$

El proceso sigue hasta que $k_i \leq 1$ para algún i . El pseudocódigo del algoritmo se muestra a continuación:

Algoritmo para calcular $a^k \pmod{n}$

$$a_0 = a, k_0 = k, c_0 = 1, i = 1$$

Mientras $k_{i-1} > 1$ hacer:

$$a_i \equiv a_{i-1}^2 \pmod{n}$$

Si k_{i-1} es par entonces

$$c_i = c_{i-1}$$

$$\text{Sino } c_i = a_{i-1} \cdot c_{i-1}$$

Fin si

$$k_i = \left\lfloor \frac{k_{i-1}}{2} \right\rfloor$$

$$i = i + 1$$

Fin mientras

$$a^k \equiv a_{i-1} \cdot c_{i-1} \pmod{n}$$

Programa hecho con Wolfram Mathematica 9.0 para calcular potencias modulares

```

Interpretation [
{n = 0, a = 0, k = 0},
Panel [ Grid[{"Ingrese el valor de n", InputField[ Dynamic[n] ] },
{"Ingrese el valor de a: ", InputField[ Dynamic[ a ] ] },
{"Ingrese el valor de k:", InputField[ Dynamic[ k ] ] }]]
],
j = 1;
c = 1;
While [ k > 1,
If [ EvenQ[ k ], c = c , c = a*c ];
a = Mod[ a^2, n ];
k = IntegerPart[ k/2 ];
j = j++;
]
Mod[ a*c, n ];
Panel[ Grid [{"La potencia modular es:", Mod[ a*c, n ] }]] ] ]

```

El siguiente Ejemplo ilustrará cómo calcular una potencia modular.

Ejemplo 2.1.23

Calcular $72^{21} \pmod{141}$

Solución

En este caso, $a_0 = 72$, $c_0 = 1$ y $k_0 = 21$. A fin de ordenar los cálculos, se diseña la siguiente tabla:

i	a_i	c_i	k_i
0	72	1	21
1	108	72	10
2	102	72	5
3	111	12	2
4	54	12	1

Los detalles de los datos que figuran en la tabla se explican a continuación:

Para $i = 1$

$$a_1 = a_0^2 = (72)^2 = 5184 \equiv 108 \pmod{141}$$

$$c_1 = a_0 \cdot c_0 = (72) \cdot 1 = 72 \pmod{141}$$

$$k_1 = \left\lfloor \frac{k_0}{2} \right\rfloor = \left\lfloor \frac{21}{2} \right\rfloor = 10$$

Para $i = 2$

$$a_2 = a_1^2 = (108)^2 = 11664 \equiv 102 \pmod{141}$$

$$c_2 = c_1$$

$$k_2 = \left\lfloor \frac{k_1}{2} \right\rfloor = \left\lfloor \frac{10}{2} \right\rfloor = 5$$

Para $i = 3$

$$a_3 = a_2^2 = (102)^2 = 10404 \equiv 111 \pmod{141}$$

$$c_3 = a_2 \cdot c_2 = (102) \cdot (72) = 7344 \equiv 12 \pmod{141}$$

$$k_3 = \left\lfloor \frac{k_2}{2} \right\rfloor = 2$$

Para $i = 4$

$$a_4 = a_3^2 = (111)^2 = 12321 \equiv 54 \pmod{141}$$

$$c_4 = c_3$$

$$k_4 = \left\lfloor \frac{k_3}{2} \right\rfloor = \left\lfloor \frac{2}{2} \right\rfloor = 1$$

Como $k_4 \leq 1$ el proceso se detiene y por lo tanto:

$$(72)^{21} \equiv a_4 \cdot c_4 = (54) \cdot (21) = 648 \equiv 84 \pmod{141}$$

Del inciso 9) de la Proposición 2.1.9 resulta que 84 es el resto de la división entera de 72^{21} por 141. Luego, $72^{21} \equiv 84 \pmod{141}$.

Se finalizará esta sección mostrando cómo resolver una ecuación diofántica utilizando Aritmética Modular. Previamente se demostrará la siguiente:

Proposición 2.1.24

Sea d un número entero no nulo. Si $d \mid a \wedge d \mid b \wedge d \mid n$ entonces

$$a \equiv b \pmod{n} \Leftrightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$$

Demostración

Como $d \mid a \wedge d \mid b \wedge d \mid n$ entonces $\frac{a}{d}$, $\frac{b}{d}$ y $\frac{n}{d}$ son números enteros. Por lo tanto

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a-b) \Leftrightarrow \exists k \in \mathbb{Z} : a-b = k.n \Leftrightarrow \exists k \in \mathbb{Z} : \frac{a-b}{d} = \frac{k.n}{d} \Leftrightarrow$$

$$\exists k \in \mathbb{Z} : \frac{a}{d} - \frac{b}{d} = k \frac{n}{d} \Leftrightarrow \frac{n}{d} \mid \left(\frac{a}{d} - \frac{b}{d} \right) \Leftrightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}. \quad \blacksquare$$

Ejemplo 2.1.25

Resolver la ecuación diofántica del Ejemplo 2.1.2 aplicando Aritmética Modular.

Solución

La ecuación diofántica a resolver es

$$30x + 12y = 1200 \quad [1]$$

Donde, además, x es el mayor número entero que verifica:

$$1 \leq x < 12$$

De la ecuación [1] resulta

$$30x - 1200 = -12y$$

Es decir,

$$30x - 1200 \equiv 0 \pmod{12}$$

O equivalentemente

$$30x \equiv 1200 \pmod{12} \quad [2]$$

Como $30 \equiv 6 \pmod{12}$ y $1200 \equiv 0 \pmod{12}$ entonces la ecuación [2] es equivalente a

$$6x \equiv 0 \pmod{12} \quad [3]$$

Por el Teorema 2.1.18, 6 no tiene inverso en $\mathbb{Z}_{12}$. Luego, no es posible multiplicar miembro a miembro la ecuación [3] por 6^{-1} a fin de despejar x .

Sin embargo, si se aplica la Proposición 2.1.24 con $d = 6$ resulta:

$$\frac{6}{6}x \equiv \frac{0}{6} \pmod{\frac{12}{6}}$$

Por lo tanto

$$x \equiv 0 \pmod{2}$$

De aquí resulta que $x = 2k$ con $k \in \mathbb{Z}$. Teniendo en cuenta que x es el mayor número entero que verifica:

$$1 \leq x < 12$$

Entonces $x = 10$. Reemplazando este valor de x en la ecuación [1] se obtiene finalmente que $y = 75$. En consecuencia, la solución es $x = 10$ e $y = 75$.

2.2 Grupos, Anillos y Cuerpos Finitos

En esta sección se introducirán los conceptos de Grupos, Anillos y Cuerpos finitos. Además se demostrarán sus propiedades básicas, las cuales serán fundamentales para probar que $(\mathbb{Z}_p - \{0\}, \bullet)$ es un grupo cíclico. Este resultado será de suma importancia a la hora de definir los logaritmos discretos.

Grupos

Definición 2.2.1: Grupo

Sea G un conjunto no vacío y $*$ una operación binaria definida sobre los elementos de G . El par $(G, *)$ es un grupo si y sólo si verifica las siguientes propiedades:

- 1) $*$ es Ley de Composición Interna: Si $a, b \in G \Rightarrow a * b \in G$.
- 2) Propiedad asociativa: Si $a, b, c \in G \Rightarrow (a * b) * c = a * (b * c)$.
- 3) Existencia de elemento neutro o Identidad: $\exists e \in G / a * e = e * a \quad \forall a \in G$.
- 3) Existencia de inversos: $\forall a \in G \exists a^{-1} \in G / a * a^{-1} = a^{-1} * a = e$.

Definición 2.2.2: Grupo abeliano o conmutativo

Un grupo $(G, *)$ es abeliano si verifica la Propiedad conmutativa:

Si $a, b \in G \Rightarrow a * b = b * a$.

Definición 2.2.3: Subgrupo

Sea $(G, *)$ un grupo y $\emptyset \neq H \subset G$. Se dice que $(H, *)$ es un subgrupo de $(G, *)$ sii $(H, *)$ es grupo.

El siguiente Teorema resulta sumamente útil para probar que un determinado subconjunto de un grupo es subgrupo.

Teorema 2.2.4

Sea $(G, *)$ un grupo y $H \subset G$. Si se verifica que:

- 1) $H \neq \emptyset$
- 2) Si $x, y \in H \Rightarrow x * y^{-1} \in H$

Entonces $(H, *)$ es un subgrupo de $(G, *)$

Demostración

Véase [7]. ■

Definición 2.2.5: Potencia de un elemento de un grupo

Sea $(G, *)$ un grupo y “ e ” su elemento neutro. Si $x \in G$ y $n \in \mathbb{Z}$ entonces:

$$1) x^n = \underbrace{x * x * \dots * x}_{n \text{ veces}}$$

$$2) x^{-n} = \underbrace{x^{-1} * x^{-1} * \dots * x^{-1}}_{n \text{ veces}}$$

$$3) x^0 = e$$

La siguiente Proposición prueba algunas propiedades elementales de la potencia de un elemento de un Grupo que serán utilizadas con frecuencia.

Proposición 2.2.6

Sea $(G, *)$ un grupo. Si $a, b \in G$ y $m, n \in \mathbb{Z}$ entonces:

$$1) a^m * a^n = a^{m+n}$$

$$2) (a^m)^n = a^{m \cdot n}$$

$$3) (a^{-m})^n = a^{-m \cdot n}$$

$$4) a^{-n} = (a^n)^{-1}$$

$$5) a^m * a^{-n} = a^{m-n}$$

$$6) \text{ Si } (G, *) \text{ es abeliano entonces } (a * b)^n = a^n * b^n$$

Demostración

$$1) a^m * a^n = \underbrace{a * a * \dots * a}_{m \text{ veces}} * \underbrace{a * a * \dots * a}_{n \text{ veces}} = a^{m+n}$$

2) Se probará este resultado aplicando el Principio de Inducción sobre n :

Para $n = 1$ se verifica, pues $(a^m)^1 = a^m = a^{m \cdot 1}$.

A continuación se supondrá que este resultado es válido para n , es decir,

$$(a^m)^n = a^{m \cdot n} \quad (\text{Hipótesis Inductiva})$$

Se probará entonces que esta igualdad sigue siendo válida para $(n+1)$:

$$\begin{array}{ccccccc} (a^m)^{n+1} & = & (a^m)^n & * & a^1 & = & a^{m \cdot n} * a^n = a^{m \cdot n + n} = a^{n(m+1)}. \\ & \uparrow & & \uparrow & & \uparrow & \\ & \text{inciso 1)} & & H. \text{ Inductiva} & & \text{inciso 1)} & \end{array}$$

3)

$$\begin{aligned} (a^{-m})^n &= \underbrace{a^{-m} * \dots * a^{-m}}_{n \text{ veces}} = \underbrace{a^{-1} * \dots * a^{-1}}_{m \text{ veces}} * \dots * \underbrace{a^{-1} * \dots * a^{-1}}_{m \text{ veces}} = \underbrace{a^{-1} * \dots * a^{-1}}_{m \cdot n \text{ veces}} = \\ &= a^{-m \cdot n} \end{aligned}$$

4) Se aplicará nuevamente el Principio de Inducción sobre n :

Para $n = 1$ se verifica, pues $a^{-1} = (a^1)^{-1}$.

Se supone ahora que este resultado es válido para n , es decir,

$$a^{-n} = (a^n)^{-1} \quad (\text{Hipótesis Inductiva})$$

Se probará entonces que esta igualdad es válida para $(n+1)$. Para ello se demostrará que $a^{-(n+1)}$ es el inverso de $a^{(n+1)}$. Haciendo uso de la Propiedad Asociativa, del inciso 1) y de la Hipótesis Inductiva resulta:

$$\begin{aligned} a^{n+1} * a^{-(n+1)} &= (a * a^n) * \underbrace{(a^{-1} * a^{-1} * \dots * a^{-1} * a^{-1})}_{n+1 \text{ veces}} = (a * a^n) * \left(\underbrace{(a^{-1} * a^{-1} * \dots * a^{-1})}_{n \text{ veces}} * a^{-1} \right) = \\ &= (a * a^n) * (a^{-n} * a^{-1}) = \left(a * (a^n * a^{-n}) \right) * a^{-1} = \left(a * \left(a^n * (a^n)^{-1} \right) \right) * a^{-1} = (a * e) * a^{-1} = \\ &\quad \uparrow \\ &\quad \text{Hipótesis Inductiva} \\ &= a * a^{-1} = e \end{aligned}$$

Por lo tanto, por la unicidad del elemento inverso, se obtiene $a^{-(n+1)} = (a^{n+1})^{-1}$.

5) Se consideran los siguientes casos:

Si $m = n$

Por el inciso 3) se tiene

$$a^m * a^{-n} = a^m * a^{-m} = a^m * (a^m)^{-1} = e$$

Por otro lado,

$$a^{m-n} = a^{m-m} = a^0 = e$$

Si $m > n$

En este caso, aplicando sucesivas veces la Propiedad Asociativa y la del elemento neutro, resulta

$$\begin{aligned} a^m * a^{-n} &= \underbrace{a * a * \dots * a}_{m \text{ veces}} * \underbrace{a^{-1} * a^{-1} * \dots * a^{-1}}_{n \text{ veces}} = \underbrace{a * \dots * a}_{m-1 \text{ veces}} * (a * a^{-1}) * \underbrace{a^{-1} * \dots * a^{-1}}_{n-1 \text{ veces}} = \\ &= \underbrace{a * \dots * a}_{m-1 \text{ veces}} * e * \underbrace{a^{-1} * \dots * a^{-1}}_{n-1 \text{ veces}} = \underbrace{a * \dots * a}_{m-1 \text{ veces}} * \underbrace{a^{-1} * \dots * a^{-1}}_{n-1 \text{ veces}} = \dots = \underbrace{a * a * \dots * a}_{m-n \text{ veces}} = a^{m-n} \end{aligned}$$

Si $m < n$

Aplicando nuevamente la Propiedad Asociativa y la del elemento neutro, se obtiene

$$\begin{aligned} a^m * a^{-n} &= \underbrace{a * a * \dots * a}_{m \text{ veces}} * \underbrace{a^{-1} * a^{-1} * \dots * a^{-1}}_{n \text{ veces}} = \underbrace{a * \dots * a}_{m-1 \text{ veces}} * (a * a^{-1}) * \underbrace{a^{-1} * \dots * a^{-1}}_{n-1 \text{ veces}} = \\ &= \underbrace{a * \dots * a}_{m-1 \text{ veces}} * e * \underbrace{a^{-1} * \dots * a^{-1}}_{n-1 \text{ veces}} = \underbrace{a * \dots * a}_{m-1 \text{ veces}} * \underbrace{a^{-1} * \dots * a^{-1}}_{n-1 \text{ veces}} = \dots = \underbrace{a^{-1} * a^{-1} * \dots * a^{-1}}_{n-m \text{ veces}} = \\ &= a^{-(n-m)} = a^{-n+m} = a^{m-n} \end{aligned}$$

6) Se aplicará el Principio de Inducción sobre n :

Para $n = 1$ se verifica, pues $(a * b)^1 = a * b = a^1 * b^1$.

Se supone ahora que este resultado es válido para n , es decir,

$$(a * b)^n = a^n * b^n \quad (\text{Hipótesis Inductiva})$$

Se probará que esta igualdad es válida para $(n+1)$:

$$\begin{aligned} (a * b)^{n+1} &= (a * b)^n * (a * b) = \left(a^n * b^n \right) * (a * b) = \left(a^n * (b^n * a) \right) * b = \left(a^n * (a * b^n) \right) * b = \\ &\quad \begin{array}{ccccccc} \uparrow & & \uparrow & & \uparrow & & \uparrow \\ \text{inciso 1)} & & H. Inductiva & & Prop. Asociativa & & Prop. Conmutativa \end{array} \\ &= \left(a^n * a \right) * \left(b^n * b \right) = a^{n+1} * b^{n+1}. \quad \blacksquare \\ &\quad \quad \quad \uparrow \\ &\quad \quad \quad \text{inciso 1)} \end{aligned}$$

Definición 2.2.7: Subgrupo generado por un elemento del grupo

Sea $(G, *)$ un grupo y $x \in G$. El "subgrupo generado por x ", simbolizado por $\langle x \rangle$, es

$$\langle x \rangle = \{ x^k \mid k \in \mathbb{Z} \}$$

La siguiente Proposición es útil para caracterizar al subgrupo generado por un elemento de un grupo:

Proposición 2.2.7

Sea $(G, *)$ un grupo finito y $x \in G$. Entonces

- 1) $\exists n_0 \in \mathbb{N}$ tal que $n_0 = \min \{n \in \mathbb{N} / x^n = e\}$
- 2) $\langle x \rangle = \{x^1, x^2, \dots, x^{n_0} = e\}$

Demostración

Véase [7]. ■

Definición 2.2.8: Grupo cíclico

Sea $(G, *)$ un grupo. Se dice que es un grupo cíclico si existe $x \in G$ tal que $G = \langle x \rangle$.

En este caso, se dice que x es un generador de G .

Definición 2.2.9: Orden de un grupo y de un elemento de un grupo

Sea $(G, *)$ un grupo finito. Entonces:

- 1) El orden de G , simbolizado por $\text{ord}(G)$, es la cantidad de elementos que tiene G .
- 2) Si $x \in G$ el orden de x , simbolizado por $\text{ord}(x)$, es la cantidad de elementos que tiene $\langle x \rangle$. Es decir, $\text{ord}(x) = \text{ord}(\langle x \rangle)$ Por lo tanto, $\text{ord}(x) = \min \{n \in \mathbb{N} / x^n = e\}$.

La siguiente Proposición prueba que el conjunto generado por un elemento de un grupo es efectivamente un subgrupo cíclico.

Proposición 2.2.10

Sea $(G, *)$ un grupo finito y $x \in G$. Entonces

- 1) x tiene orden finito.
- 2) Si $x \in G$ y $\text{ord}(x) = n_0$ entonces $\langle x \rangle = \{x^1, x^2, \dots, x^{n_0} = e\}$ es un subgrupo cíclico de G .

Demostración

- 1) Como $\langle x \rangle \subseteq G$ y G es finito, entonces $\text{ord}(\langle x \rangle) \leq \text{ord}(G) < \infty$.
- 2) Por la Proposición 2.2.7 se tiene que

$$\langle x \rangle = \{x^1, x^2, \dots, x^{n_0} = e\}$$

Donde $n_0 = \min \{n \in \mathbb{N} / x^n = e\}$

Para probar que $(\langle x \rangle, *)$ es subgrupo, se aplicará el Teorema 2.2.4:

a) $\langle x \rangle \neq \emptyset$ pues $e \in \langle x \rangle$.

b) Sean $a, b \in \langle x \rangle$. Entonces $a = x^m$, $b = x^n$ para algún m, n con $1 \leq m, n \leq n_0$.

Aplicando la Proposición 2.2.6 se tiene:

$$a * b^{-1} = x^m * (x^n)^{-1} = x^m * x^{-n} = x^{m-n}$$

Por otro lado, por el Algoritmo de la División Entera, $\exists q, r \in \mathbb{N}$ tales que $m - n = q \cdot n_0 + r$ con $0 \leq r < n_0$. Aplicando nuevamente la Proposición 2.2.6 resulta:

$$x^{m-n} = x^{q \cdot n_0 + r} = x^{q \cdot n_0} * x^r = (x^{n_0})^q * x^r = (e)^q * x^r = e * x^r = x^r$$

En consecuencia, $a * b^{-1} = x^r$ con $0 \leq r < n_0$. Luego, $a * b^{-1} \in \langle x \rangle$.

Por lo tanto, por el Teorema 2.2.4, queda probado que $(\langle x \rangle, *)$ es un subgrupo. ■

Las siguientes proposiciones, referentes a números enteros, serán utilizadas para demostrar las propiedades de los elementos de un grupo finito.

Proposición 2.2.11

Sean $a, b \in \mathbb{Z}$ Entonces:

$$1) \text{ Si } d = \text{mcd}(a, b) \Rightarrow \text{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

$$2) \text{ Si } a \mid b \cdot c \wedge \text{mcd}(a, b) = 1 \Rightarrow a \mid c$$

Demostración

$$1) \text{ Obviamente, } 1 \mid \frac{a}{d} \wedge 1 \mid \frac{b}{d}.$$

Por otro lado, sea c tal que $c \mid \frac{a}{d} \wedge c \mid \frac{b}{d}$. Se probará que $c \mid 1$.

Por el Teorema 2.16 inciso 1), $\exists p, q \in \mathbb{Z}$ tales que $d = p \cdot a + q \cdot b$. Por lo tanto,

$$1 = p \cdot \frac{a}{d} + q \cdot \frac{b}{d} \quad [1]$$

Como $c \mid \frac{a}{d} \wedge c \mid \frac{b}{d}$, $\exists k_1, k_2 \in \mathbb{Z}$ tales que $\frac{a}{d} = k_1 \cdot c \wedge \frac{b}{d} = k_2 \cdot c$.

Reemplazando estas expresiones en [1] resulta:

$$1 = p \cdot k_1 \cdot c + q \cdot k_2 \cdot c = (p \cdot k_1 + q \cdot k_2) \cdot c.$$

Luego, $c \mid 1$ y por lo tanto queda probado que $\text{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

2) Como $a \mid b \cdot c$ entonces $\exists k \in \mathbb{Z}$ tal que

$$b \cdot c = k \cdot a \quad [2]$$

Por otro lado, como $\text{mcd}(a, b) = 1$, por el Teorema 2.1.6 inciso 1) $\exists p, q \in \mathbb{Z}$ tales que

$$1 = p \cdot a + q \cdot b \quad [3]$$

Aplicando las expresiones [2] y [3] se obtiene

$$c = c \cdot 1 = c \cdot (p \cdot a + q \cdot b) = c \cdot p \cdot a + c \cdot q \cdot b = c \cdot p \cdot a + q \cdot k \cdot a = (c \cdot p + q \cdot k) \cdot a.$$

Por lo tanto $a \mid c$ ■

Proposición 2.2.12

Sean $a, b \in \mathbb{Z}$ Entonces:

1) Si p es un número primo positivo y $p \mid a \cdot b \Rightarrow p \mid a \vee p \mid b$.

2) Si p es primo positivo y $p \mid a_1 \cdot a_2 \cdot \dots \cdot a_n \Rightarrow p \mid a_i$ para algún $i \in \{1, 2, \dots, n\}$.

3) Sean $m, n \in \mathbb{Z}$ tales que $m \mid n \wedge n = \prod_{i=1}^k p_i^{r_i}$ su descomposición como producto de factores primos positivos $p_1, p_2, \dots, p_k$, con $r_i \in \mathbb{Z}$, $\forall i=1, 2, \dots, k$ entonces

$$m = \prod_{i=1}^k p_i^{m_i} \text{ con } m_i \geq 0 \quad \forall i = 1, 2, \dots, k.$$

Demostración

1) Si $p \mid a$ no hay nada que probar. Si p no divide a a entonces $\text{mcd}(a, p) = 1$ pues:

Si se supone que $\text{mcd}(a, p) = d \neq 1$ entonces, como $d|p$, $d \neq 1$ y p es un número primo positivo resulta que $d = p$. Luego, como $d|a$, se tiene que $p|a$, lo cual es un absurdo.

Por lo tanto, Por el Teorema 2.1.6 inciso 1) $\exists s, t \in \mathbb{Z}$ tales que

$$1 = s \cdot a + t \cdot p \quad [1]$$

Como $p|a \cdot b$ entonces $\exists k \in \mathbb{Z}$ tal que

$$a \cdot b = k \cdot p \quad [2]$$

Aplicando [1] y [2] resulta

$$b = b \cdot 1 = b \cdot (s \cdot a + t \cdot p) = b \cdot s \cdot a + b \cdot t \cdot p = s \cdot k \cdot p + b \cdot t \cdot p = (s \cdot k + b \cdot t) \cdot p$$

Por lo tanto, $p|b$.

2) Se aplicará el principio de Inducción sobre n :

Para $n=1$ se verifica obviamente. Se supondrá que vale para n , es decir,

Si p es primo y $p|a_1 \cdot a_2 \cdot \dots \cdot a_n \Rightarrow p|a_i$ para algún $i \in \{1, 2, \dots, n\}$ (Hipótesis Inductiva)

Se probará que esta afirmación es válida para $i = (n+1)$:

Sea p un número primo positivo tal que $p|a_1 \cdot a_2 \cdot \dots \cdot a_n \cdot a_{n+1}$. Por el inciso 1), se tiene que

$$p|a_1 \cdot a_2 \cdot \dots \cdot a_n \vee p|a_{n+1}$$

Si $p|a_{n+1}$, queda probada la afirmación. Si $p|a_1 \cdot a_2 \cdot \dots \cdot a_n$ entonces, por Hipótesis Inductiva, $p|a_i$ para algún $i \in \{1, 2, \dots, n\}$.

En consecuencia, $p|a_i$ para algún $i \in \{1, 2, \dots, n+1\}$.

3) Como $m|n$, $\exists k_1 \in \mathbb{Z}$ tal que $n = k_1 \cdot m$. Por lo tanto,

$$\prod_{i=1}^k p_i^{r_i} = k_1 \cdot m$$

Por el Teorema Fundamental de la Aritmética, $\exists q_1, q_2, \dots, q_s$ números primos positivos distintos y $\exists \bar{r}_1, \bar{r}_2, \dots, \bar{r}_s$ enteros positivos tales que

$$m = \prod_{i=1}^s q_i^{\bar{r}_i}$$

En consecuencia,

$$\prod_{i=1}^k p_i^{r_i} = k_1 \cdot \prod_{i=1}^s q_i^{\bar{r}_i}$$

Sea $q_i \in \{q_1, q_2, \dots, q_s\}$. Como q_i es primo y $q_i \mid \prod_{i=1}^k p_i^{r_i}$, por el inciso 2) resulta que $q_i \mid p_j$ para algún j . Como q_i y p_j son primos positivos entonces $q_i = p_j$. Luego, si se define para $i = 1, 2, \dots, k$:

$$m_i = \begin{cases} r_i & \text{si } q_i = p_j \text{ para algún } j \in \{1, 2, \dots, k\} \\ 0 & \text{si } q_i \neq p_j \quad \forall j \in \{1, 2, \dots, k\} \end{cases}$$

Resulta finalmente que $m = \prod_{i=1}^k p_i^{m_i}$ ■

Las siguientes Proposiciones prueban algunas propiedades importantes de los elementos de un grupo.

Proposición 2.2.13

Sea $(G, *)$ un grupo finito y e su elemento neutro. Si $x, y \in G$ y $k \in \mathbb{N}$ entonces

1) $x^k = e \Leftrightarrow \text{ord}(x) \mid k$

2) $\text{ord}(x^{-1}) = \text{ord}(x)$

3) Si $\text{ord}(x) = n \Rightarrow \text{ord}(x^k) = \frac{n}{\text{mcd}(n, k)}$

4) Si $\text{ord}(x) = n, \text{ord}(y) = m$ y $\text{mcd}(n, m) = 1 \Rightarrow \langle x \rangle \cap \langle y \rangle = \{e\}$

5) Si $(G, *)$ es un grupo abeliano y $\text{mcd}(\text{ord}(x), \text{ord}(y)) = 1$ entonces $\text{ord}(x * y) = \text{ord}(x) \cdot \text{ord}(y)$.

Demostración

1) Se probará la doble implicación:

$\Rightarrow$) Por el Algoritmo de la División Entera, $\exists q, r \in \mathbb{N}$ tales que

$$k = q \cdot \text{ord}(x) + r \text{ con } 0 \leq r < \text{ord}(x)$$

Se probará que $r = 0$, suponiendo por el absurdo que $r \neq 0$. Entonces, aplicando la Proposición 2.2.6 se tiene:

$$e = x^k = x^{q \cdot \text{ord}(x) + r} = \left(x^{\text{ord}(x)}\right)^q \cdot x^r = e^q \cdot x^r = x^r$$

De aquí resulta que, como $\text{ord}(x) = \min \{n \in \mathbb{N} / x^n = e\}$ entonces $r \geq \text{ord}(x)$. De este modo se llega a un absurdo pues $r < \text{ord}(x)$. Por lo tanto $k = q \cdot \text{ord}(x)$ y, en consecuencia, $\text{ord}(x) \mid k$.

$\Leftarrow$) Es obvia, aplicando nuevamente la Proposición 2.2.6.

2) De la Proposición 2.2.6 inciso 4) resulta:

$$\left(x^{-1}\right)^{\text{ord}(x)} = \left(x^{\text{ord}(x)}\right)^{-1} = e^{-1} = e$$

Por lo tanto,

$$\text{ord}(x) \geq \text{ord}\left(x^{-1}\right)$$

Por otro lado, sea $n_0 = \text{ord}\left(x^{-1}\right)$. Teniendo en cuenta nuevamente la Proposición 2.2.6

inciso 4) y que $\left(a^{-1}\right)^{-1} = a \quad \forall a \in G$, se tiene:

$$x^{n_0} = \left(\left(x^{n_0}\right)^{-1}\right)^{-1} = \left(x^{-n_0}\right)^{-1} = \left(\left(x^{-1}\right)^{n_0}\right)^{-1} = e^{-1} = e$$

Por lo tanto, $n_0 \geq \text{ord}(x)$. Es decir,

$$\text{ord}\left(x^{-1}\right) \geq \text{ord}(x)$$

En consecuencia, $\text{ord}\left(x^{-1}\right) = \text{ord}(x)$.

3) Como $n \mid \text{mcm}(k, n)$ entonces $\text{mcm}(k, n) = q \cdot n$ para algún $q \in \mathbb{N}$. Por otro lado,

teniendo en cuenta que $\text{mcm}(k, n) = \frac{k \cdot n}{\text{mcd}(k, n)}$, resulta:

$$\left(x^k\right)^{\frac{n}{\text{mcd}(k, n)}} = x^{\frac{k \cdot n}{\text{mcd}(k, n)}} = x^{\text{mcm}(k, n)} = x^{q \cdot n} = \left(x^n\right)^q = e^q = e$$

Por lo tanto, por el inciso 1) se tiene que

$$\text{ord}\left(x^k\right) \mid \frac{n}{\text{mcd}(k, n)} \quad [1]$$

Si se define $m = \text{ord}\left(x^k\right)$ entonces

$$x^{m \cdot k} = \left(x^k\right)^m = e$$

Por lo tanto, $n \mid m \cdot k$ y en consecuencia,

$$\frac{n}{\text{mcd}(k, n)} \Big| m \cdot \frac{k}{\text{mcd}(k, n)}$$

Por otro lado, de la Proposición 2.2.11 inciso 1) resulta

$$\text{mcd}\left(\frac{n}{\text{mcd}(k, n)}, \frac{k}{\text{mcd}(k, n)}\right) = 1$$

Luego, por la Proposición 2.2.11 inciso 2) se concluye que $\frac{n}{\text{mcd}(k, n)} \Big| m$. Es decir,

$$\frac{n}{\text{mcd}(k, n)} \Big| \text{ord}(x^k) \quad [2]$$

De [1] y [2] resulta finalmente que $\text{ord}(x^k) = \frac{n}{\text{mcd}(n, k)}$.

4) Sea $z \in \langle x \rangle \cap \langle y \rangle$. Entonces $\exists k, k_1 \in \mathbb{N}$ tales que $z = x^k \wedge z = y^{k_1}$. Por el inciso 3) se tiene:

$$\text{ord}(z) = \frac{\text{ord}(x)}{\text{mcd}(\text{ord}(x), k)} \wedge \text{ord}(z) = \frac{\text{ord}(y)}{\text{mcd}(\text{ord}(y), k_1)}$$

Por lo tanto,

$$\text{ord}(z) \cdot \text{mcd}(\text{ord}(x), k) = \text{ord}(x) \wedge \text{ord}(z) \cdot \text{mcd}(\text{ord}(y), k_1) = \text{ord}(y)$$

Luego, por definición de máximo común divisor, se obtiene:

$$\text{ord}(z) \Big| \text{mcd}(\text{ord}(x), \text{ord}(y))$$

Es decir, $\text{ord}(z) \Big| 1$. De aquí resulta que $\text{ord}(z) = 1$. Así, $z^1 = e$, es decir, $z = e$.

5) Como $(G, *)$ es abeliano, de la Proposición 2.2.6 incisos 2) y 6) resulta:

$$(x * y)^{\text{ord}(x) \cdot \text{ord}(y)} = x^{\text{ord}(x) \cdot \text{ord}(y)} * y^{\text{ord}(x) \cdot \text{ord}(y)} = \left(x^{\text{ord}(x)}\right)^{\text{ord}(y)} * \left(y^{\text{ord}(y)}\right)^{\text{ord}(x)} = e$$

Por lo tanto, por la Proposición 2.2.13 inciso 1) se tiene:

$$\text{ord}(x * y) \Big| \text{ord}(x) \cdot \text{ord}(y) \quad [3]$$

Por otro lado, sea $m = \text{ord}(x * y)$. Entonces, nuevamente de la Proposición 2.2.6 inciso 4) resulta:

$$(x * y)^m = e \Rightarrow x^m * y^m = e \Rightarrow x^m = (y^m)^{-1} \Rightarrow x^m = y^{-m}$$

De esta última igualdad y del inciso 4) se deduce que:

$$x^m \in \langle x \rangle \cap \langle y \rangle = \{e\} \wedge y^{-m} \in \langle x \rangle \cap \langle y \rangle = \{e\}.$$

En consecuencia,

$$x^m = e \wedge y^{-m} = e$$

Es decir,

$$x^m = e \wedge (y^{-1})^m = e$$

De los incisos 1) y 2) se obtiene:

$$\text{ord}(x) \mid m \wedge \text{ord}(y^{-1}) \mid m \Rightarrow \text{ord}(x) \mid m \wedge \text{ord}(y) \mid m$$

Por lo tanto,

$$\text{mcm}(\text{ord}(x), \text{ord}(y)) \mid m \Rightarrow \frac{\text{ord}(x) \cdot \text{ord}(y)}{\text{mcd}(\text{ord}(x), \text{ord}(y))} \mid m \Rightarrow \text{ord}(x) \cdot \text{ord}(y) \mid m$$

Pues $\text{mcd}(\text{ord}(x), \text{ord}(y)) = 1$. En consecuencia,

$$\text{ord}(x) \cdot \text{ord}(y) \mid \text{ord}(x * y) \quad [4]$$

De [3] y [4] se obtiene que $\text{ord}(x * y) = \text{ord}(x) \cdot \text{ord}(y)$. ■

Proposición 2.2.14

Sea $(G, *)$ un grupo finito y e su elemento neutro. Entonces Si $\exists y \in G$ tal que

$$x^{\text{ord}(y)} = e \quad \forall x \in G.$$

Demostración

Como G es finito, $\exists y \in G$ de orden máximo. Es decir,

$$\text{ord}(y) = \max \{ \text{ord}(x) / x \in G \}.$$

Se supondrá por el absurdo que $\exists x \in G / x^{\text{ord}(y)} \neq e$. Sea $n = \text{ord}(G)$. Por el Teorema Fundamental de la Aritmética, existen $p_1, p_2, \dots, p_k \wedge r_1, r_2, \dots, r_k$ enteros positivos tales que:

$$n = \prod_{i=1}^k p_i^{r_i}.$$

Como $\text{ord}(x) \mid m \wedge \text{ord}(y) \mid m$, de la Proposición 2.2.12 inciso 3) resulta:

$$\text{ord}(x) = \prod_{i=1}^k p_i^{m_i} \wedge \text{ord}(y) = \prod_{i=1}^k p_i^{n_i}$$

Luego,

$$\exists j \in \{1, 2, \dots, k\} \text{ tal que } p_j^{n_j} < p_j^{m_j}$$

Pues, si se supone que $p_i^{n_i} \geq p_i^{m_i} \quad \forall i=1, 2, \dots, k$, entonces $p_i^{n_i} = q_i \cdot p_i^{m_i}$, donde

$$q_i = p_i^{n_i - m_i}.$$

Por lo tanto,

$$\text{ord}(y) = \prod_{i=1}^k (p_i^{m_i} \cdot q_i) = \prod_{i=1}^k p_i^{m_i} \cdot \prod_{i=1}^k q_i = \text{ord}(x) \cdot q$$

Con $q = \prod_{i=1}^k q_i$. En consecuencia,

$$x^{\text{ord}(y)} = x^{\text{ord}(x) \cdot q} = (x^{\text{ord}(x)})^q = e,$$

Lo cual es una contradicción. Sin pérdida de generalidad, se supondrá que $j=1$, es decir,

$$p_1^{n_1} < p_1^{m_1}. \text{ Sean } z = y^{p_1^{n_1}} \wedge w = x^{p_2^{m_2} \dots p_k^{m_k}}. \text{ De la Proposición 2.2.13 inciso 3)}$$

se obtiene:

$$\text{ord}(z) = p_2^{n_2} \dots p_k^{n_k} \wedge \text{ord}(w) = p_1^{m_1}$$

Del inciso 5) de la Proposición anteriormente mencionada se tiene:

$$\text{ord}(w \cdot z) = \text{ord}(w) \cdot \text{ord}(z) = p_1^{m_1} \cdot p_2^{n_2} \dots p_k^{n_k} > p_1^{n_1} \cdot p_2^{n_2} \dots p_k^{n_k} = \text{ord}(y).$$

De este modo se llega a un absurdo, ya que y tiene orden máximo. En consecuencia,

$$x^{\text{ord}(y)} = e \quad \forall x \in G. \blacksquare$$

El siguiente teorema relaciona el orden de un grupo con el orden de un subgrupo:

Teorema 2.2.15: Teorema de Lagrange

Si $(G, *)$ un grupo finito y $(H, *)$ es un subgrupo de $(G, *)$ entonces

$$\text{ord}(H) \mid \text{ord}(G)$$

Demostración

Véase [9]. ■

Corolario del Teorema de Lagrange

Si $(G, *)$ es un grupo finito y $x \in G$, entonces $\text{ord}(x) \mid \text{ord}(G)$.

Demostración

Es inmediata, considerando $H = \langle x \rangle$. ■

Anillos

Definición 2.2.16: Anillo

Un anillo es una terna $(A, \oplus, \otimes)$ formada por un conjunto no vacío A y dos operaciones $\oplus$ y $\otimes$ definidas en A , llamadas suma y producto respectivamente, que verifican:

1) $(A, \oplus)$ es un grupo abeliano. El elemento neutro de A se simbolizará con 0 .

2) El producto es asociativo.

3) El producto es doblemente distributivo con respecto a la suma:

$$\begin{cases} a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c \\ (b \oplus c) \otimes a = b \otimes a \oplus c \otimes a \end{cases} \quad \forall a, b, c \in A$$

Definición 2.2.17: Anillo unitario

Si un anillo $(A, \oplus, \otimes)$ tiene elemento neutro para la operación producto, que se denotará con 1 , se dice que es un anillo unitario.

Definición 2.2.18: Anillo conmutativo

Sea $(A, \oplus, \otimes)$ un anillo. Se dice que es un anillo conmutativo cuando la operación producto es conmutativa.

Definición 2.2.19: Elemento invertible de un anillo

Un elemento a en un anillo $(A, \oplus, \otimes)$ es invertible si existe un elemento $b \in A$ tal que $a \otimes b = b \otimes a = 1$. En este caso al elemento b , que es único, se lo denotará con a^{-1} .

Definición 2.2.20: Anillo de división

Sea $(A, \oplus, \otimes)$ un anillo unitario. Se dice que es un anillo de división si todos los elementos no nulos de A son invertibles.

Definición 2.2.21: Anillos con divisores de cero

Un anillo $(A, \oplus, \otimes)$ tiene divisores de cero si y sólo si existen elementos no nulos que dan producto nulo.

Cuando un anillo no tiene divisores de cero se dice que es un dominio de integridad o un dominio.

Cuerpos Finitos

Definición 2.2.22: Cuerpo

La terna $(K, \oplus, \otimes)$ es un cuerpo si y sólo si es un anillo conmutativo con unidad, cuyos elementos no nulos admiten inverso multiplicativo.

Los axiomas que caracterizan la estructura de cuerpo son:

- 1) $(K, \oplus)$ es grupo abeliano.
- 2) $(K - \{0\}, \otimes)$ es grupo abeliano.
- 3) El producto es distributivo con respecto a la suma.

Definición 2.2.23: Cuerpo finito

Un cuerpo $(K, \oplus, \otimes)$ es un cuerpo finito si K tiene un número finito de elementos.

Una consecuencia inmediata de la definición de cuerpo es que no admiten divisores de cero, como lo demuestra la siguiente Proposición.

Proposición 2.2.24

Un cuerpo $(K, \oplus, \otimes)$ no admite divisores de cero.

Demostración

Sean $x, y \in K$ tales que

$$x \otimes y = 0 \tag{1}$$

Se trata de probar que $x = 0 \vee y = 0$.

Si $x = 0$ no hay nada que demostrar porque la proposición $x = 0 \vee y = 0$ es verdadera.

Si $x \neq 0$ entonces, por definición de cuerpo, existe x^{-1} . Multiplicando [1] por x^{-1} y aplicando la propiedad asociativa, se tiene

$$x^{-1} \otimes (x \otimes y) = x^{-1} \otimes 0 \Rightarrow (x^{-1} \otimes x) \otimes y = 0 \Rightarrow 1 \otimes y = 0$$

Es decir, $y = 0$. ■

La siguiente Proposición indica en qué casos la terna $(\mathbb{Z}_p, +, \cdot)$ es un cuerpo.

Proposición 2.2.25

$(\mathbb{Z}_p, +, \cdot)$ es un cuerpo si y sólo si p es un número primo.

Demostración

$\Rightarrow$) Se demostrará esta implicación aplicando el contra recíproco. Si se supone que p no es un número primo, entonces existen $a, b \in \mathbb{Z}$ con $1 < a, b < p$ tales que $p = a \cdot b$. De la Definición 2.1.11 de producto en $\mathbb{Z}_p$ resulta

$$a \cdot b = 0 \text{ en } \mathbb{Z}_p$$

Ya que el resto de la división de $a \cdot b$ por p es cero. De este modo, $(\mathbb{Z}_p, +, \cdot)$ admite divisores de cero, lo cual es una contradicción pues es cuerpo.

$\Leftarrow$) Se deberá probar que todo elemento no nulo de $\mathbb{Z}_p$ es invertible. Sea $0 \neq a \in \mathbb{Z}_p$. Entonces $0 < a < p$. Por otro lado, como p es primo se cumple que $\text{mcd}(a, p) = 1$. Por lo tanto, por el Teorema 2.1.18 (Teorema de Invertibilidad en $\mathbb{Z}_p$), a es un elemento invertible en $\mathbb{Z}_p$. ■

Teorema 2.2.26

Sea $(K, \oplus, \cdot)$ un cuerpo finito y $(G, \cdot)$ un subgrupo de $(K - \{0\}, \cdot)$. Entonces $(G, \cdot)$ es cíclico.

Demostración

Por la Proposición 2.2.14, $\exists y \in G$ tal que $x^{\text{ord}(y)} = 1 \forall x \in G$. Por el Corolario del Teorema de Lagrange, resulta que $\text{ord}(y) \mid \text{ord}(G)$. Por lo tanto

$$\text{ord}(y) \leq \text{ord}(G) \tag{1}$$

Por otro lado, se sabe que todo polinomio de grado n en $K[X]$, el anillo de polinomios a coeficientes en el cuerpo K , tiene a lo sumo n raíces distintas. En particular, la ecuación

$$x^{\text{ord}(y)} = 1$$

Es satisfecha para todos los elementos de G . Es decir, todos los elementos de G son raíces de dicha ecuación. En consecuencia,

$$\text{ord}(G) \leq \text{ord}(y) \quad [2]$$

De [1] y [2] se obtiene

$$\text{ord}(y) = \text{ord}(G)$$

Es decir,

$$\text{ord}(\langle y \rangle) = \text{ord}(G)$$

En consecuencia,

$$\langle y \rangle = G$$

Y por lo tanto $(G, \cdot)$ es cíclico. ■

El siguiente Teorema prueba finalmente que la dupla $(\mathbb{Z}_p - \{0\}, \cdot)$ es un grupo cíclico si p es primo. Este resultado es sumamente importante para definir logaritmos discretos.

Teorema 2.2.27

$(\mathbb{Z}_p - \{0\}, \cdot)$ es un grupo cíclico $\Leftrightarrow p$ es primo.

Demostración

$\Rightarrow$) Se supondrá por el absurdo que p no es primo. Entonces, $\exists a \in \mathbb{Z}$ con $1 < a < p$ y tal que $a|p$. Como además $a|a$ entonces

$$a|mcd(a, p) \quad [1]$$

Por otro lado, como $(\mathbb{Z}_p - \{0\}, \cdot)$ es grupo, todo elemento de $\mathbb{Z}_p - \{0\}$ tiene inverso. En particular, a tiene inverso. Por lo tanto, por el Teorema 2.1.18, se tiene

$$mcd(a, p) = 1 \quad [2]$$

De [1] y [2] resulta que $a|1$. En consecuencia, $a=1$, lo cual es una contradicción.

$\Leftarrow$) De la Proposición 2.2.25, resulta que $(\mathbb{Z}_p, +, \cdot)$ es un cuerpo finito pues p primo.

Si se considera $G = \mathbb{Z}_p - \{0\}$ entonces por el Teorema 2.2.26 resulta que $(\mathbb{Z}_p - \{0\}, \cdot)$ es cíclico. ■

Notación 2.2.28:

El conjunto $\mathbb{Z}_p - \{0\}$ será simbolizado por $\mathbb{Z}_p^*$. Es decir,

$$\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$$

2.3 Logaritmos Discretos

Los logaritmos discretos se definen para grupos cíclicos finitos y, en particular, para $(\mathbb{Z}_p^*, \cdot)$, donde p es un número primo. Su importancia radica en la seguridad del algoritmo Diffie-Hellman, el cual se basa en la dificultad para resolver logaritmos discretos. Revisten el nombre de discretos en contraposición con los logaritmos continuos que se conoce habitualmente; y tiene que ver con la finitud del conjunto donde se define.

Definición 2.3.1: Logaritmo discreto

Sea $(G, *)$ un grupo cíclico finito de orden n , y " a " un elemento generador de G . Es decir,

$$G = \langle a \rangle = \{a^0, a^1, \dots, a^{n-1}\}$$

El logaritmo discreto en base " a " de un elemento $x \in G$ es un número entero $y \in \{0, 1, \dots, n-1\}$ que verifica

$$\log_a(x) = y \Leftrightarrow a^y = x$$

Observación 2.3.2

En la definición de logaritmo discreto, se pide que la base " a " sea un elemento generador del grupo para que $\log_a(x)$ quede definido $\forall x \in G$. Por otro lado, en virtud del Teorema 2.2.27, $(\mathbb{Z}_p^*, \cdot)$ es un grupo cíclico finito de orden p si p es primo. Por lo tanto, si p es primo, el logaritmo discreto quedará definido en $(\mathbb{Z}_p^*, \cdot)$ del siguiente modo:

Definición 2.3.3: Logaritmo discreto en $\mathbb{Z}_p^*$

Sea $(\mathbb{Z}_p^*, \cdot)$ con p un número primo y " a " un elemento generador de $\mathbb{Z}_p^*$. El logaritmo discreto en base " a " de un número $x \in \mathbb{Z}_p^*$ es un número $y \in \{0, 1, \dots, p-1\}$ que verifica:

$$\log_a(x) = y \Leftrightarrow a^y = x \text{ en } \mathbb{Z}_p$$

O equivalentemente,

$$\log_a(x) = y \Leftrightarrow a^y \equiv x \pmod{p}$$

Los siguientes ejemplos ilustrarán cómo calcular logaritmos discretos.

Ejemplo 2.3.4

Sea $(\mathbb{Z}_7^*, \cdot)$ donde $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

- 1) Indicar si $\log_3(x)$ queda definido en $\forall x \in \mathbb{Z}_7^*$.
- 2) Determinar si $\log_2(x)$ queda definido en $\forall x \in \mathbb{Z}_7^*$.

Solución

Primeramente, obsérvese que $(\mathbb{Z}_7 - \{0\}, \cdot)$ es un grupo cíclico pues 7 es un número primo. Por otro lado, para que $\log_3(x)$ quede definido, 3 debe ser un generador de $\mathbb{Z}_7^*$.

Se verificará entonces si $\langle 3 \rangle = \mathbb{Z}_7^*$, calculando las potencias de 3 en $\mathbb{Z}_7^*$:

i	0	1	2	3	4	5	6
3^i	1	3	2	6	4	5	1

Por lo tanto, como las potencias de 3 generan todos los elementos de $\mathbb{Z}_7^*$, $\log_3(x)$ queda definido $\forall x \in \mathbb{Z}_7^*$ del siguiente modo:

$$\log_3(1) = 0 \text{ pues } 3^0 = 1 \text{ en } \mathbb{Z}_7^*$$

$$\log_3(2) = 2 \text{ pues } 3^2 = 9 = 2 \text{ en } \mathbb{Z}_7^*$$

$$\log_3(3) = 1 \text{ pues } 3^1 = 3 \text{ en } \mathbb{Z}_7^*$$

$$\log_3(4) = 4 \text{ pues } 3^4 = 81 = 4 \text{ en } \mathbb{Z}_7^*$$

$$\log_3(5) = 5 \text{ pues } 3^5 = 243 = 5 \text{ en } \mathbb{Z}_7^*$$

$$\log_3(6) = 3 \text{ pues } 3^3 = 27 = 6 \text{ en } \mathbb{Z}_7^*$$

- 2) Se verificará primeramente si 2 es generador de $\mathbb{Z}_7^*$:

i	0	1	2	3
2^i	1	2	4	1

Como $\langle 2 \rangle = \{1, 2, 4\} \neq \mathbb{Z}_7^*$, se concluye que 2 no es generador de $\mathbb{Z}_7^*$ y, en consecuencia, $\log_2(x)$ no queda definido $\forall x \in \mathbb{Z}_7^*$.

Ejemplo 2.3.5

Identificar los generadores de $\mathbb{Z}_{11}^*$.

Solución

Los posibles generadores de $\mathbb{Z}_{11}^*$ pueden ser 2, 3, 4, ..., 10. Para hallarlos, se diseña la siguiente tabla que contiene las potencias de estos números:

Valor de x x^i	2	3	4	5	6	7	8	9	10
x^0	1	1	1	1	1	1	1	1	1
x^1	2	3	4	5	6	7	8	9	10
x^2	4	9	5	3	3	5	9	4	1
x^3	8	5	9	4	7	2	6	3	10
x^4	5	4	3	9	9	3	4	5	1
x^5	10	1	1	1	10	10	10	1	10
x^6	9	3	4	5	5	4	3	9	1
x^7	7	9	5	3	8	6	2	4	10
x^8	3	5	9	4	4	9	5	3	1
x^9	6	4	3	9	2	8	7	5	10

Los generadores serán los elementos de la tabla que encabezan las columnas que contienen a todos los elementos de $\mathbb{Z}_{11}^*$. De este modo, los generadores de $\mathbb{Z}_{11}^*$ son 2, 6, 7 y 8. En consecuencia, estos números sirven de base para el logaritmo discreto en $\mathbb{Z}_{11}^*$.

Ejemplo 2.3.6

Calcular, si existen, los siguientes logaritmos discretos:

1) $\log_3(5)$ en $\mathbb{Z}_{11}^*$

2) $\log_5(2)$ en $\mathbb{Z}_{11}^*$

Solución

1) Se calcularán las distintas potencias de 3 y se comprobará si alguna de ellas da por resultado 5 en $\mathbb{Z}_{11}^*$:

$$3^0 = 1 \text{ en } \mathbb{Z}_{11}^*$$

$$3^1 = 3 \text{ en } \mathbb{Z}_{11}^*$$

$$3^2 = 9 \text{ en } \mathbb{Z}_{11}^*$$

$$3^3 = 27 = 5 \text{ en } \mathbb{Z}_{11}^* \Rightarrow \log_3(5) = 3$$

Este inciso también podría haberse resuelto observando la tabla del ejemplo anterior: Ubicándose en la columna cuyo encabezado es 3, se busca en dicha columna al número 5. El encabezado de la fila que contiene a 5 indicará el valor del logaritmo.

2) Nuevamente, se calculan las distintas potencias de 5 y se verifica si alguna de ellas da por resultado 2 en $\mathbb{Z}_{11}^*$:

$$5^0 = 1 \text{ en } \mathbb{Z}_{11}^*$$

$$5^1 = 5 \text{ en } \mathbb{Z}_{11}^*$$

$$5^2 = 25 = 3 \text{ en } \mathbb{Z}_{11}^*$$

$$5^3 = 125 = 4 \text{ en } \mathbb{Z}_{11}^*$$

$$5^4 = 625 = 9 \text{ en } \mathbb{Z}_{11}^*$$

$$5^5 = 3125 = 1 \text{ en } \mathbb{Z}_{11}^*$$

Se comprueba que a partir del exponente 5, las potencias de 5 se repiten sin lograr obtener el número 2. En consecuencia, $\log_5(2)$ no existe.

Otra forma de demostrar que este logaritmo no existe es observando nuevamente la tabla del ejemplo anterior: al ubicarse en la columna cuyo encabezado es 5, se comprueba que el número 2 no figura en dicha columna. Luego, $\log_5(2)$ no está definido.

El problema de los logaritmos discretos (PLD)

Cabe preguntarse si existe algún algoritmo que permita calcular logaritmos discretos de una manera más sencilla, sin hacerlos “a fuerza bruta”. La respuesta es NO. Se tiene que hacer por exhaustión, y mientras más grande sea el módulo p , mayor será el tiempo que

tome hallar el logaritmo. La dificultad del cálculo de los logaritmos discretos es lo que da seguridad al algoritmo de Diffie-Hellman.

Criptosistemas basados en logaritmos discretos

La mayoría de los algoritmos asimétricos que se usan en la actualidad para proporcionar seguridad en la información se apoyan en el llamado Problema de los Logaritmos Discretos (PLD). Se cree que el Problema de los Logaritmos Discretos es, computacionalmente, tan complejo como el problema de la factorización de números primos grandes.

Criptosistemas como El Gamal, Diffie-Hellman, Ciss-Cheik h-Sow, Blum-Micali, El Algoritmo de Firma Digital (DSA), de Massey-Omura e incluso la moderna Criptografía de Curva Elíptica depositan su seguridad en el problema del logaritmo discreto. Todos ellos descansan en la imposibilidad de resolverlos de forma algorítmicamente eficiente.

2.4 Cuaterniones

En esta sección se estudiará la estructura algebraica de los cuaterniones, partiendo de su definición y explicando algunas de sus propiedades y operaciones.

Mientras que los números complejos son una extensión de los números reales por la adición de la unidad imaginaria i tal que $i^2 = -1$, los cuaterniones constituyen una generalización de los números complejos, al agregar las unidades imaginarias j, k de modo tal que $j^2 = k^2 = i \cdot j \cdot k = -1$. Estos números forman un sistema llamado “*El Sistema de números Hipercomplejos*”, al igual que los cocuaterniones, bicuaterniones, octoniones, tessarines y sedeniones. Todos ellos tienen estructura n -dimensional sobre los números reales. Los cuaterniones fueron inventados por Hamilton en 1843 para poder demostrar la Conjetura de Euler, que afirmaba que todo número natural n puede expresarse como suma de cuatro cuadrados perfectos, es decir,

$$n = a^2 + b^2 + c^2 + d^2 \quad \text{con } a, b, c, d \in \mathbb{Z}$$

Además, fue el primer ejemplo de estructura de anillo de división no conmutativo.

Sus aplicaciones son muy variadas, y van desde la Geometría, ya que son utilizados para rotar figuras en el espacio de una manera más sencilla [11], hasta aplicaciones físicas dentro del Electromagnetismo y Mecánica Cuántica, entre otras.

Definición 2.4.1: Cuaternión

Un cuaternión es un número q de la forma:

$$q = a + b i + c j + d k$$

Donde $a, b, c, d \in \mathbb{R}$ e i, j, k son unidades imaginarias que verifican las siguientes igualdades:

$$i^2 = j^2 = k^2 = i \cdot j \cdot k = -1$$

Dichas unidades imaginarias tienen la Propiedad Asociativa y además conmutan con cualquier constante real.

El conjunto H

El conjunto que engloba a todos los cuaterniones se denomina **H**, simbolizado así en honor al matemático irlandés William R. Hamilton (1805-1865), y se lo define como:

$$H = \{ q = a + b i + c j + d k : a, b, c, d \in \mathbb{R} \}$$

Obsérvese que $\mathbb{R} \subset H$ considerando $c = d = 0$.

La siguiente Proposición muestra los resultados que se obtienen al multiplicar unidades imaginarias:

Proposición 2.4.2

Sean i, j, k las unidades imaginarias que verifican $i^2 = j^2 = k^2 = i \cdot j \cdot k = -1$.

Entonces

$\mathbb{I}$	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

Demostración

1) $i \cdot j = k$ pues

Como $i \cdot j \cdot k = -1$, multiplicando miembro a miembro por k y teniendo en cuenta la Propiedad Asociativa resulta

$$i \cdot j \cdot k = -1 \Rightarrow i \cdot j \cdot k \cdot k = -k \Rightarrow i \cdot j \cdot k^2 = -k \Rightarrow -i \cdot j = -k \Rightarrow i \cdot j = k$$

2) $j \cdot k = i$ pues

$$i \cdot j \cdot k = -1 \Rightarrow i \cdot i \cdot j \cdot k = -i \Rightarrow i^2 \cdot j \cdot k = -i \Rightarrow -j \cdot k = -i \Rightarrow j \cdot k = i$$

3) $i \cdot k = -j$ pues

Nuevamente, como $i \cdot j \cdot k = -1$ y asociando convenientemente se tiene

$$\begin{aligned} i \cdot j \cdot k = -1 &\Rightarrow -i \cdot j \cdot i^2 \cdot k = -1 \Rightarrow -(i \cdot j) \cdot i \cdot (i \cdot k) = -1 \Rightarrow -k \cdot i \cdot (i \cdot k) = -1 \Rightarrow \\ &\Rightarrow -j \cdot k \cdot i \cdot (i \cdot k) = -j \Rightarrow -(i \cdot j \cdot k) \cdot i \cdot (i \cdot k) = -i \cdot j \Rightarrow i \cdot (i \cdot k) = -i \cdot j \Rightarrow \\ (i \cdot i) \cdot (i \cdot k) &= -i^2 \cdot j \Rightarrow (i \cdot i) \cdot (i \cdot k) = -i^2 \cdot j \Rightarrow -(i \cdot k) = j \Rightarrow i \cdot k = -j \end{aligned}$$

4) $j \cdot i = -k$ pues

$$\begin{aligned} i \cdot j \cdot k = -1 &\Rightarrow -i \cdot j \cdot i^2 \cdot k = -1 \Rightarrow -i \cdot (j \cdot i) \cdot i \cdot k = -1 \Rightarrow -i \cdot (j \cdot i) \cdot (-j) = -1 \Rightarrow \\ &\Rightarrow -i^2 \cdot (j \cdot i) \cdot (-j) = -i \Rightarrow (j \cdot i) \cdot (-j) = -i \Rightarrow (j \cdot i) \cdot (-j \cdot j) = -i \cdot j \Rightarrow j \cdot i = -k \end{aligned}$$

5) $k \cdot i = j$ pues

$$\begin{aligned} i \cdot j \cdot k = -1 &\Rightarrow i \cdot j \cdot k \cdot i = -i \Rightarrow i \cdot i \cdot j \cdot (k \cdot i) = -i^2 \Rightarrow -j \cdot (k \cdot i) = 1 \Rightarrow \\ &\Rightarrow -j \cdot j \cdot (k \cdot i) = j \Rightarrow k \cdot i = j \end{aligned}$$

6) $k \cdot j = -i$ pues

$$\begin{aligned} i \cdot j \cdot k = -1 &\Rightarrow i \cdot j \cdot (k \cdot j) = -j \Rightarrow i^2 \cdot j \cdot (k \cdot j) = -i \cdot j \Rightarrow -j \cdot (k \cdot j) = -i \cdot j \Rightarrow \\ &\Rightarrow -j \cdot (k \cdot j) = -k \Rightarrow -j \cdot j \cdot (k \cdot j) = -j \cdot k \Rightarrow -j^2 \cdot (k \cdot j) = -j \cdot k \Rightarrow k \cdot j = -i \quad \blacksquare \end{aligned}$$

Observación 2.4.3: La tabla que figura en la Proposición anterior es conocida como la Tabla de Cayley y permitirá definir el producto de cuaterniones. Previamente se introducirá la siguiente definición.

Definición 2.4.4: El conjugado y el módulo de un cuaternión

Sea $q = a + b i + c j + d k$ un cuaternión. Entonces

1) El conjugado de q es

$$\bar{q} = a - b i - c j - d k$$

2) El módulo de q es

$$|q| = \sqrt{a^2 + b^2 + c^2 + d^2}$$

Si un cuaternión tiene módulo 1 se dice que es un cuaternión unitario.

Operaciones entre cuaterniones

Si $q_1 = a_1 + b_1 i + c_1 j + d_1 k$ y $q_2 = a_2 + b_2 i + c_2 j + d_2 k$ son dos cuaterniones entonces:

Suma de cuaterniones

$$q_1 + q_2 = (a_1 + a_2) + (b_1 + b_2) i + (c_1 + c_2) j + (d_1 + d_2) k$$

Producto de cuaterniones

El producto se lo define teniendo en cuenta la Tabla de Cayley y aplicando la propiedad distributiva del producto con respecto a la suma:

$$\begin{aligned} q_1 \cdot q_2 &= (a_1 + b_1 i + c_1 j + d_1 k) \cdot (a_2 + b_2 i + c_2 j + d_2 k) = \\ &= a_1 a_2 + a_1 b_2 i + a_1 c_2 j + a_1 d_2 k + b_1 a_2 i + b_1 b_2 i^2 + b_1 c_2 i j + \\ &+ b_1 d_2 i k + c_1 a_2 j + c_1 b_2 j i + c_1 c_2 j j + c_1 d_2 j k + d_1 a_2 k + d_1 b_2 k i + \\ &+ d_1 c_2 k j + d_1 d_2 k k = \\ &= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2) i + \\ &+ (a_1 c_2 + a_2 c_1 + d_1 b_2 - b_1 d_2) j + (a_1 d_2 + b_1 c_2 + d_1 a_2 - c_1 b_2) k \end{aligned}$$

El módulo de un cuaternión expresado en términos de su conjugado

De acuerdo a la definición de producto de cuaterniones, se puede comprobar que

$$|q| = \sqrt{q \cdot \bar{q}} = \sqrt{a^2 + b^2 + c^2 + d^2}$$

Cociente de cuaterniones

Si $q_2 \neq 0$ entonces:

$$\frac{q_1}{q_2} = \frac{q_1 \cdot \bar{q_2}}{q_2 \cdot \bar{q_2}} = \frac{q_1 \cdot \bar{q_2}}{|q_2|^2}$$

Inverso de un cuaternión

Dado un cuaternión $q \neq 0$, su inverso es $q^{-1} = \frac{1}{q} = \frac{\bar{q}}{q \cdot \bar{q}} = \frac{\bar{q}}{|q|^2}$

Normalización de un cuaternión

Dado un cuaternión $q \neq 0$ cuyo módulo no sea igual a uno, se lo puede normalizar definiendo un nuevo cuaternión unitario, asociado al primero, mediante la operación:

$$q_1 = \frac{q}{|q|}$$

Diferentes representaciones de un cuaternión

Existen diversas maneras de expresar un cuaternión. Según cómo se quiera operar con él, es conveniente expresarlo de una determinada forma. Dado un cuaternión q , sus distintas representaciones son:

Forma vectorial:

Es la forma en la que fue definida el cuaternión. Es decir,

$$q = a + b i + c j + d k$$

Forma cartesiana:

Consiste en representar al cuaternión como un vector en $\mathbb{R}^4$, es decir,

$$q = (a, b, c, d)$$

Forma trigonométrica:

Es muy utilizada para calcular las potencias de un cuaternión. El siguiente teorema justifica esta representación.

Teorema 2.4.5: Forma trigonométrica de un cuaternión

Sea $q = a + b i + c j + d k$ con $q \neq 0$. Entonces

$$q = |q| (\cos(\theta) + \sin(\theta) \cdot v')$$

Donde

$$\theta = \arccos\left(\frac{a}{|q|}\right), 0 \leq \theta \leq \pi$$

$$v' = \begin{cases} 0 & \text{si } b = c = d = 0 \\ \frac{b i + c j + d k}{|b i + c j + d k|} & \text{en otro caso} \end{cases}$$

O expresado en forma cartesiana,

$$v' = \begin{cases} 0 & \text{si } b = c = d = 0 \\ \frac{(b, c, d)}{|(b, c, d)|} & \text{en otro caso} \end{cases}$$

Demostración

1) Si $b \neq 0 \vee c \neq 0 \vee d \neq 0$ entonces

$$q = |q| \left(\frac{a}{|q|} + \frac{(b i + c j + d k)}{|q|} \cdot \frac{|b i + c j + d k|}{|b i + c j + d k|} \right) \quad [1]$$

Si se define

$$v = b i + c j + d k$$

$$v' = \frac{b i + c j + d k}{|b i + c j + d k|}$$

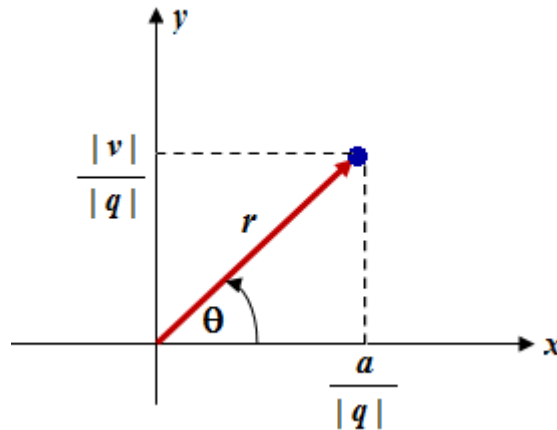
Y se reemplaza estas expresiones en [1] resulta:

$$q = |q| \left(\frac{a}{|q|} + \frac{|v|}{|q|} \cdot v' \right) \quad [2]$$

Si se considera el siguiente punto del plano:

$$\left(\frac{a}{|q|}, \frac{|v|}{|q|} \right)$$

Entonces dicho punto se encuentra en el primer o segundo cuadrante, según sea $a \geq 0$ o bien $a \leq 0$. Si se lo expresa en coordenadas polares, se tiene:



$$\begin{cases} \cos(\theta) = \frac{\frac{a}{|q|}}{r} \\ \text{sen}(\theta) = \frac{\frac{|v|}{|q|}}{r} \end{cases} \Rightarrow \begin{cases} \frac{a}{|q|} = r \cos(\theta) \\ \frac{|v|}{|q|} = r \text{sen}(\theta) \end{cases}$$

Como $\frac{|v|}{|q|} \geq 0$, se obtiene que $0 \leq \theta \leq \pi$.

Por otro lado, como

$$\frac{a^2}{|q|^2} + \frac{|v|^2}{|q|^2} = r^2 \cos^2(\theta) + r^2 \text{sen}^2(\theta) = r^2$$

Y además

$$\frac{a^2}{|q|^2} + \frac{|v|^2}{|q|^2} = \frac{a^2 + |v|^2}{|q|^2} = \frac{a^2 + b^2 + c^2 + d^2}{|q|^2} = \frac{|q|^2}{|q|^2} = 1$$

Entonces $r^2 = 1$ y por lo tanto $r = 1$. Así,

$$\begin{cases} \frac{a}{|q|} = \cos(\theta) \\ \frac{|v|}{|q|} = \sin(\theta) \end{cases} \quad [3]$$

Reemplazando [3] en [2] se tiene:

$$q = |q| (\cos(\theta) + \sin(\theta) \cdot v')$$

Donde

$$\theta = \arccos\left(\frac{a}{|q|}\right), 0 \leq \theta \leq \pi$$

2) Si $b = c = d = 0$ entonces $q = a$. Por otro lado,

$$\cos(\theta) = \frac{a}{|q|} = \frac{a}{|a|}$$

Luego, teniendo en cuenta que $v' = 0$ se obtiene

$$q = a = |a| \frac{a}{|a|} = |a| \cos(\theta) = |q| \cos(\theta) = |q| (\cos(\theta) + \sin(\theta) \cdot v') \quad \blacksquare$$

El siguiente ejemplo ilustra cómo expresar en forma trigonométrica un cuaternión escrito en forma vectorial.

Ejemplo 2.4.6

Expresar en forma trigonométrica el cuaternión $q = 1 + 2i + 3j + \sqrt{2}k$.

Solución

En este caso: $a = 1$, $b = 2$, $c = 3$, $d = \sqrt{2}$. Entonces

$$|q| = \sqrt{a^2 + b^2 + c^2 + d^2} = \sqrt{1^2 + 2^2 + 3^2 + (\sqrt{2})^2} = \sqrt{16} = 4$$

Trabajando con dos decimales se obtiene

$$\theta = \arccos\left(\frac{a}{|q|}\right) = \arccos\left(\frac{1}{4}\right) = 1.32$$

$$v' = \frac{b i + c j + d k}{|b i + c j + d k|} = \frac{2 i + 3 j + \sqrt{2} k}{|2 i + 3 j + \sqrt{2} k|} = \frac{2 i + 3 j + \sqrt{2} k}{\sqrt{2^2 + 3^2 + (\sqrt{2})^2}} = \frac{2 i + 3 j + \sqrt{2} k}{\sqrt{15}}$$

O expresado en forma cartesiana:

$$v' = \frac{(2, 3, \sqrt{2})}{\sqrt{15}}$$

Por lo tanto,

$$q = |q| (\cos(\theta) + \sin(\theta) \cdot v') = 4 \left(\cos(1.32) + \sin(1.32) \cdot \frac{(2, 3, \sqrt{2})}{\sqrt{15}} \right)$$

Cálculo de potencias de exponente natural de un cuaternión

La forma trigonométrica de un cuaternión permitirá calcular, de una manera más sencilla, la potencia de exponente natural de un cuaternión.

Teorema 2.4.7: Fórmula de De Moivre para cuaterniones

Sea $q = a + b i + c j + d k$ un cuaternión no nulo cuya forma trigonométrica es

$$q = |q| (\cos(\theta) + \sin(\theta) \cdot v')$$

Si $n \in \mathbb{Z}$ entonces

$$q^n = |q|^n (\cos(n\theta) + \sin(n\theta) \cdot v')$$

Demostración

Se aplicará el Principio de Inducción sobre n .

Para $n = 1$ se verifica claramente pues

$$q^1 = q = |q| (\cos(\theta) + \sin(\theta) \cdot v') = |q|^1 (\cos(1\theta) + \sin(1\theta) \cdot v')$$

Se supone a continuación que la igualdad es válida para n (Hipótesis Inductiva). Es decir,

$$q^n = |q|^n (\cos(n\theta) + \sin(n\theta) \cdot v')$$

Con

$$v' = \begin{cases} 0 & \text{si } b = c = d = 0 \\ \frac{b i + c j + d k}{|b i + c j + d k|} & \text{en otro caso} \end{cases}$$

Se demostrará que la igualdad es válida para $(n+1)$:

1) Si $b \neq 0 \vee c \neq 0 \vee d \neq 0$, obsérvese que $(v')^2 = -1$ pues

$$\begin{aligned} (v')^2 &= \frac{(b i + c j + d k) (b i + c j + d k)}{|b i + c j + d k| \cdot |b i + c j + d k|} = \frac{-b^2 + bc k - bd j - bc k - c^2 + cd i - db j - dc i - d^2}{b^2 + c^2 + d^2} = \\ &= \frac{-b^2 - c^2 - d^2}{b^2 + c^2 + d^2} = -1 \end{aligned}$$

Por lo tanto, haciendo uso de la Hipótesis Inductiva se tiene

$$\begin{aligned} q^{n+1} &= q^n \cdot q = \underbrace{|q|^n (\cos(n\theta) + \operatorname{sen}(n\theta) \cdot v')}_{\text{Hipótesis Inductiva}} \cdot |q| (\cos(\theta) + \operatorname{sen}(\theta) \cdot v') = \\ &= |q|^{n+1} (\cos(n\theta)\cos(\theta) + \cos(n\theta)\operatorname{sen}(\theta)v' + \operatorname{sen}(n\theta)\cos(\theta) \cdot v' + \operatorname{sen}(n\theta)\operatorname{sen}(\theta) \cdot (v')^2) = \\ &= |q|^{n+1} (\cos(n\theta)\cos(\theta) + \cos(n\theta)\operatorname{sen}(\theta)v' + \operatorname{sen}(n\theta)\cos(\theta) \cdot v' - \operatorname{sen}(n\theta)\operatorname{sen}(\theta)) = \\ &= |q|^{n+1} (\cos((n+1)\theta) + \operatorname{sen}((n+1)\theta) \cdot v') \end{aligned}$$

2) Si $b = c = d = 0$, la demostración es trivial. ■

Estructura algebraica de los cuaterniones

Los cuaterniones son un ejemplo de anillo de división no conmutativo. Tienen una estructura algebraica similar a la de un cuerpo, es decir, satisfacen todas las propiedades de un cuerpo con la excepción de que el producto no es conmutativo (por ejemplo, $i \cdot j \neq j \cdot i$).

Forman un álgebra asociativa 4-dimensional sobre los reales y los complejos constituyen un subconjunto de ella.

Capítulo 3

Algoritmos criptográficos simétricos

Mucho antes de la computación electrónica moderna, se hacía criptografía con métodos que resultan primitivos en la actualidad. Los mensajes se codificaban muy sencillamente y eran fácilmente decodificables. En un mundo de poca comunicación, no parecía haber necesidad de métodos demasiado sofisticados. Los primeros algoritmos criptográficos utilizaban criptografía simétrica. En este capítulo se verá uno de los primeros y que tienen todavía alguna relevancia en la criptografía moderna: el Método de Julio César y el Método Lineal o de Julio César Mejorado. Ellos se basan en la codificación numérica del alfabeto, tema que se expondrá a continuación.

Codificación del alfabeto

En criptografía, cada letra del alfabeto se puede codificar con dos dígitos según la siguiente tabla, llamada tabla de equivalencia numérica (TEN).

A	B	C	D	E	F	G	H	I	J	K	L	M	N
01	02	03	04	05	06	07	08	09	10	11	12	13	14

Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
15	16	17	18	19	20	21	22	23	24	25	26	00	

Figura 3.1: Tabla de Equivalencia Numérica (TEN)

El Método de Julio César

Este algoritmo criptográfico, con clave $k \in \mathbb{Z}$, utiliza la siguiente función para encriptar un mensaje:

$$f(x) = x + k \pmod{27}$$

Donde

x : Es el número que le corresponde, en la tabla TEN, a una letra del mensaje.

El nombre de este método es en honor al político y militar romano Julio César (100- 44 a.C.). Se dice que en la antigua Roma, Julio César enviaba mensajes encriptados a sus generales en el frente, utilizando la clave $k = 3$.

De este modo, cada letra del mensaje era reemplazada por la letra ubicada tres letras más adelante en el alfabeto. El siguiente ejemplo ilustra el procedimiento de encriptado al aplicar este método.

Ejemplo 3.1

Encriptar el mensaje ATAQUEN mediante el método de Julio César con clave $k = 3$.

Solución

Para encriptar el mensaje, se identifica cada letra con su número correspondiente “ x ” en la Tabla TEN, que luego se transforma en $x+3 \pmod{27}$. Finalmente, a ese número se le asocia la letra que le corresponde en la Tabla TEN.

El siguiente diagrama muestra cómo se obtiene el mensaje encriptado:

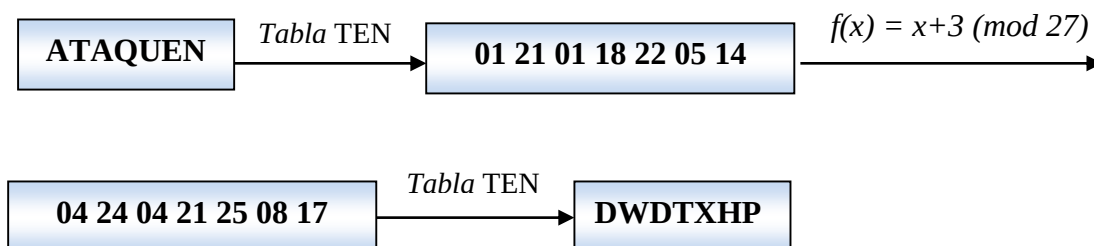


Figura 3.2: Diagrama que muestra cómo encriptar el mensaje ATAQUEN con el Método de Julio César, con clave $k=3$.

Por lo tanto, el mensaje encriptado es DWDTXHP.

Cómo desencriptar el mensaje con el Método de Julio César

Para desencriptar el mensaje, se calcula la función inversa de $f(x)$, que será simbolizada por $g(x)$. Para ello se despeja “ x ” de la ecuación $y = f(x)$. Es decir,

$$y = f(x) \Rightarrow y = x + k \Rightarrow x = y - k.$$

Intercambiando “ x ” e “ y ” en esta última ecuación resulta $y = x - k$. Por lo tanto, la función inversa es $g(x) = x - k \pmod{27}$.

Observación 3.2

Para descryptar, el receptor debe conocer la clave, que es la función inversa $g(x)$. La posibilidad de comunicación criptográfica depende entonces de que emisor y receptor estén de acuerdo en la clave a ser usada. Este detalle obliga a que antes de aplicar este sistema criptográfico, emisor y receptor deben haberse comunicado no criptográficamente. Pudiera ser una entrevista, como posiblemente tuvo que hacer el César con sus generales y éstos debieron recordar la clave y no revelarla.

Este sistema en que emisor y receptor se entrevistan y se comunican la clave se llama de *clave privada*, y es *simétrico*, pues los roles de emisor y receptor pueden intercambiarse.

Ejemplo 3.3

En el ejemplo anterior, descryptar el mensaje DWDTXHP.

Solución:

En este caso, la clave para descryptar es la función $g(x) = x - 3 \pmod{27}$. El siguiente diagrama muestra el proceso de descryptado:

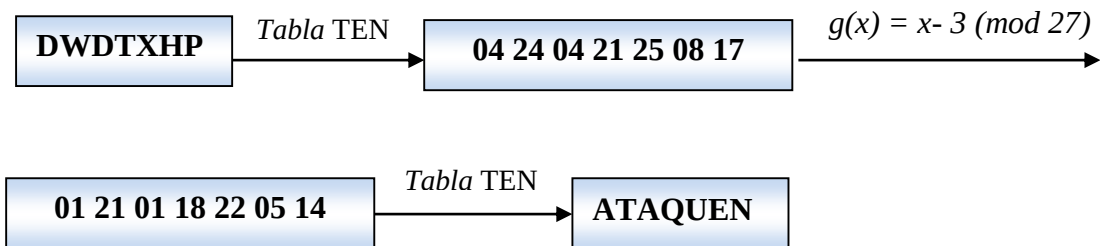


Figura 3.3: Diagrama que muestra cómo descryptar el mensaje DWDTXHP con el Método de Julio César, con clave $k = 3$.

Observación 3.4

Hay tantas claves en el método de Julio César como posibles valores no nulos de $k \in \mathbb{Z}_{27}$, es decir, 26. Por lo tanto son códigos fáciles de romper, ya que habría que hacer un máximo de 26 pruebas hasta obtener un mensaje comprensible. La siguiente proposición corrobora esta afirmación:

Proposición 3.5

Sea $k \in \mathbb{Z}$ entonces

$$f(x) = x + k \pmod{27} \Leftrightarrow f(x) = x + r \pmod{27}$$

Donde r es el resto de la división entera de k por 27.

Demostración

De la Proposición 2.1.9 inciso 10) se tiene que $k \equiv r \pmod{27}$ donde r es el resto de la división entera de k por 27. Por lo tanto, $x + k \equiv x + r \pmod{27}$. ■

Método Lineal o de Julio César Mejorado

Un simple desplazamiento de letras es un sistema cuya clave es muy fácil de detectar. El Método César puede ser ligeramente mejorado con la introducción de un nuevo parámetro en la función a encriptar y convertirla en una función afín.

Más precisamente, el Método de Julio César Mejorado consiste en aplicar la siguiente función para encriptar un mensaje:

$$f(x) = ax + b \pmod{27}$$

Donde $a, b \in \mathbb{Z}_{27}$. Además, “ a ” debe ser invertible en $\mathbb{Z}_{27}$ a fin de que $f(x)$ tenga inversa y de este modo poder desencriptar.

Por lo tanto, por el Teorema 2.2.18, los posibles valores de “ a ” son aquellos que son coprimos con el número 27. Es decir,

$$a \in \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}$$

Este nuevo sistema no es demasiado superior al del César, pero aumenta notablemente el número de funciones a encriptar, como se prueba en la siguiente Proposición.

Proposición 3.6

Sea la función afín

$$f(x) = ax + b \pmod{27}$$

Donde $a, b \in \mathbb{Z}_{27}$ y “ a ” invertible en $\mathbb{Z}_{27}$. Entonces existen 485 funciones afines distintas aplicables al Método de Julio César Mejorado.

Demostración

Posibles valores de “ a ”: 18.

Posibles valores de “ b ”: 27.

Luego, por el Principio de la Multiplicación, existen $(18) \cdot (27) = 486$ funciones afines distintas. Descartando la función $f(x) = x$ (que corresponde al caso $a = 1$ y $b = 0$) pues no produce un texto encriptado, resulta que existen 485 funciones afines distintas aplicables al Método de Julio César Mejorado. ■

Ejemplo 3.7

Aplicar el Método de Julio César Mejorado para encriptar la palabra LINEAL mediante la función afín $f(x) = 4x + 3 \pmod{27}$

Solución

El siguiente diagrama muestra cómo se obtiene el mensaje encriptado:

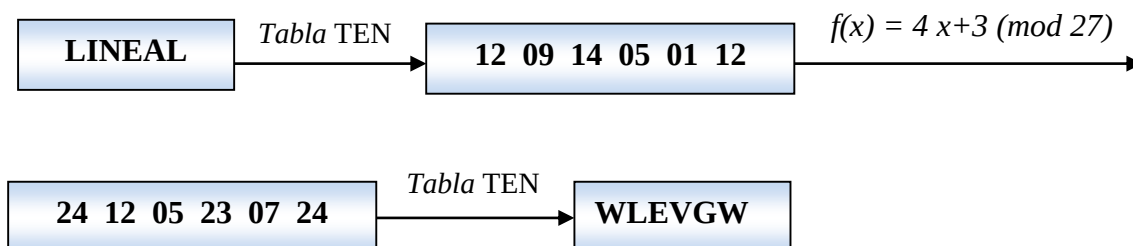


Figura 3.4: Diagrama que muestra cómo encriptar el mensaje LINEAL con el Método de Julio César Mejorado, con función afín $f(x) = 4x + 3$.

Por lo tanto, el mensaje encriptado es WLEVGW.

Cómo desencriptar un mensaje con el método de Julio César Mejorado

Para desencriptar el mensaje, se calcula la función inversa de $f(x)$, que será simbolizada por $g(x)$. Para ello se despeja “x” de la ecuación $y = f(x)$. Es decir,

$$y = f(x) \Rightarrow y = ax + b \Rightarrow x = a^{-1}(y - b).$$

Nótese que, para despejar x, se ha utilizado la hipótesis de la invertibilidad de “a” en $\mathbb{Z}_{27}$.

Intercambiando “x” e “y” en esta última ecuación resulta $y = a^{-1}(x - b)$. Por lo tanto, la función inversa es $g(x) = a^{-1}(x - b) \pmod{27}$.

Ejemplo 3.8

Por medios “impropios” se ha interceptado el siguiente mensaje:

RQ KEKBADQ FK RQ WQJKWQJZAQ KE EÑ RZVKZJQF AQB JLZ

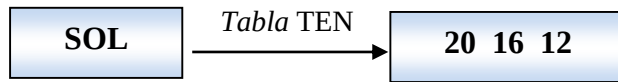
Se sabe que fue encriptado con el método de Julio César Mejorado y se sospecha que al texto llano “SOL” le corresponde el texto encriptado “ELR”. Descifrar el mensaje.

Solución

Para descryptar el mensaje, se debe hallar la función inversa de

$$f(x) = a x + b \pmod{27}$$

En consecuencia, se tratará de determinar primeramente los valores de “a” y “b”. Se sabe que al texto llano “SOL” le corresponde el texto encriptado “ELR”. Entonces



De donde se deduce que:

$$\begin{cases} f(20) = 05 \pmod{27} \\ f(16) = 12 \pmod{27} \\ f(12) = 19 \pmod{27} \end{cases} \Rightarrow \begin{cases} a \cdot 20 + b = 05 \pmod{27} & [I] \\ a \cdot 16 + b = 12 \pmod{27} & [II] \\ a \cdot 12 + b = 19 \pmod{27} & [III] \end{cases}$$

De la ecuación [II] se despeja b:

$$16 \cdot a + b = 12 \pmod{27} \Rightarrow b = 12 - 16 \cdot a \pmod{27}$$

Reemplazando esta última ecuación en [I] resulta

$$\begin{aligned} 20 \cdot a + 12 - 16 \cdot a &= 5 \pmod{27} \\ 4 \cdot a &= -7 \pmod{27} \\ 4 \cdot a &= 20 \pmod{27} \\ a &= 20 \cdot 4^{-1} \pmod{27} \\ a &= 20 \cdot (7) \pmod{27} \\ a &= 140 \pmod{27} \\ a &= 5 \pmod{27} \end{aligned}$$

Por lo tanto

$$b = 12 - 16 \cdot a = 12 - 16 \cdot (5) = -68 = 13 \pmod{27}$$

Se puede verificar que estos valores de “a” y “b” satisfacen la ecuación [III]. En consecuencia

$$f(x) = 5 x + 13 \pmod{27}$$

De aquí se obtiene la función inversa $g(x) = a^{-1}(x - b) = 5^{-1}(x - 13) \pmod{27}$.

Teniendo en cuenta que $5^{-1} = 11 \pmod{27}$, se tiene

$$g(x) = 11(x - 13) \pmod{27}.$$

De este modo, para descryptar el mensaje se aplica la función $g(x)$ y se obtiene el siguiente texto:

LA ESENCIA DE LA MATEMATICA ES SU LIBERTAD CANTOR

El Método de Julio César Mejorado diseñado con Wolfram Mathematica 9.0

El siguiente programa, hecho con el software Wolfram Mathematica 9.0, permite ingresar un texto encriptado y descifrarlo probando con las 485 funciones afines de la forma $f(x) = ax + b \pmod{27}$.

```
Interpretation[{Mensajec="RQKEKBADQFKRQWQJKWQJDAQKEE_JRDVKZJQ
FAQBJLZ"},Panel[Grid[{{Style["Ingrese el mensaje a decodificar (entre comillas
y con mayúsculas):",Bold],SpanFromLeft},{",",InputField[Dynamic[Mensajec]]}]
}
]
],

Lista={"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"};
Inversibles={1,2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26};
n=Length[Characters[Mensajec]];
Print["El texto descryptado puede ser:"];

For[j=1,j<=Length[Inversibles],j++,
a=Part[Inversibles,j];
Print["a= ",a];
For[b=1,b<=27,b++,
Mensaje="";
For[i=1,i<=n,i++,
Buscoletra=Part[Characters[Mensajec],i];
PosLetra=Part[Part[Position[List,Buscoletra],1],1];
If[Mod[a*PosLetra+b,27]==0,Lugarc=27,Lugarc=Mod[a*PosLetra+b,27]];
Letra=Part[List,Lugarc];
Mensaje=StringInsert[Mensaje,Letra,Length[Characters[Mensaje]]+1]
];
Print["b: ",b," Mensaje: ",Mensaje]
]
]
]
```

Para ejecutar el programa, se ingresa el texto encriptado en el siguiente cuadro de diálogo:

Ingrese el mensaje a decodificar (entre comillas y con mayúsculas):

"RQKEKBADQFKRQWQJKWQJDAQKE`.
EÑRDVKZJQFAQBJLZ"

Tras ejecutar 485 pruebas, el mensaje decodificado será aquél cuyo texto sea coherente y entendible. En este caso, se obtiene:

LA ESENCIA DE LA MATEMATICA ES SU LIBERTAD CANTOR

Si bien el Método de Julio César Mejorado fue en su momento un algoritmo criptográfico seguro, con el uso de los ordenadores es muy fácil de romper.

Capítulo 4:

Algoritmo de Diffie-Hellman aplicando cuaterniones

En este capítulo se analizará detalladamente el algoritmo de Diffie-Hellman aplicado a cuaterniones. Previamente se recordará el concepto de Criptografía Asimétrica para luego describir el algoritmo original de Deffie-Hellman, tal como lo idearon sus autores. Posteriormente se mencionarán algunas de sus aplicaciones para finalmente presentar un estudio exhaustivo del algoritmo de Deffie-Hellman aplicado a cuaterniones, sobre el cual se basa este trabajo de tesis.

4.1 Criptografía Asimétrica

La criptografía asimétrica (o criptografía de llave pública) fue propuesta en 1976 por Whit Diffie y Martin Hellman. Es una criptografía que se basa en emplear dos claves: una clave pública, conocida por todo el mundo y una clave privada, conocida por una única persona. La clave pública se utiliza para cifrar el mensaje, mientras que la privada se emplea para descifrarlo. La clave pública del receptor es conocida por cualquier entidad emisora que quiera enviar un mensaje cifrado, en cambio la clave privada es conocida y protegida únicamente por el receptor. Este tipo de criptografía proporciona confidencialidad, autenticación e integridad. El siguiente esquema ilustra el procedimiento general para este tipo de cifrado.

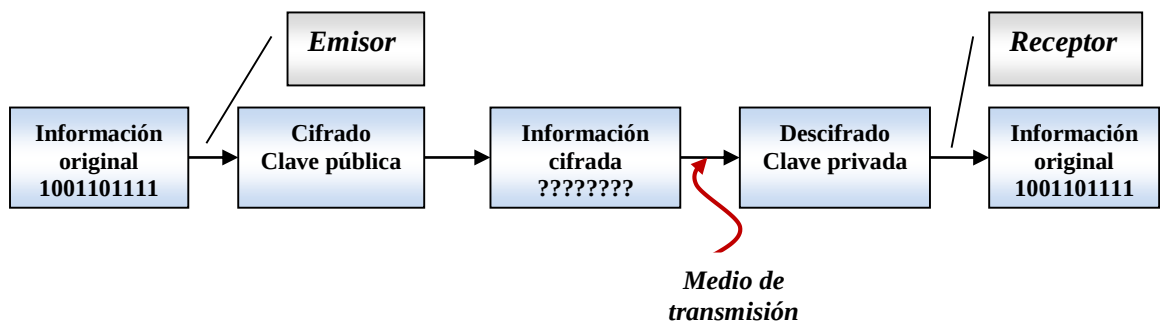


Figura 4.1: Esquema de operación del cifrado en criptografía de llave pública.

La primera publicación que incluyó este concepto criptográfico fue un artículo escrito en 1976 por Whitfield Diffie y Martin Hellman, titulado “New Directions in Cryptography”.

La idea fundamental de Diffie y Hellman para la definición de criptosistema con clave pública se basa en la existencia de funciones unidireccionales. Una función $f(x)$ sobre un dominio U se llama unidireccional si $\forall x \in U$, $f(x)$ es fácilmente calculable, mientras que para casi todo $y \in f(U)$, no es computacionalmente factible encontrar $x \in U$, tal que $f(x) = y$. Una de las candidatas a función unidireccional fue la del logaritmo discreto, propuesta por los mismos Diffie y Hellman.

Más precisamente, dados un número primo grande p y a un elemento del cuerpo F_p , la función exponencial $f(x) = a^x \pmod{p}$ es computacionalmente eficiente calcularla. En cambio, la inversa de la exponencial, el logaritmo discreto $x = \log_a(f(x))$, no es computacionalmente eficiente calcularlo si p es un número primo muy grande.

La criptografía asimétrica ofrece mayores niveles de seguridad en comparación con la criptografía simétrica. La seguridad de una criptografía de dos claves depende de cuestiones matemáticas de una manera que no ocurre en una criptografía simétrica. Los algoritmos asimétricos se diseñan en torno a la dificultad de resolver problemas matemáticos. Si se encuentra un algoritmo mejorado que puede resolver el problema, el criptosistema se ve debilitado. Por ejemplo, la computación cuántica podría resolver los problemas de la criptografía asimétrica en tiempos razonables.

Algunos ejemplos de algoritmos de clave asimétrica son: Diffie-Hellman, RSA, DSA, ElGamal.

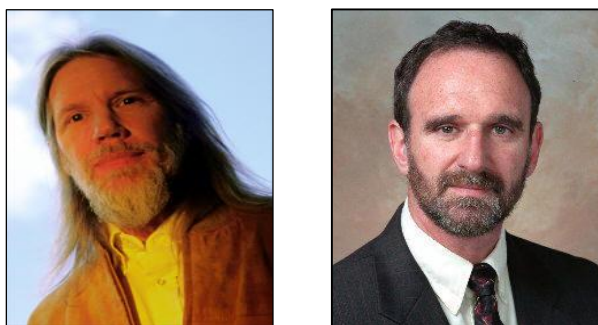


Figura 4.2: Izquierda: Whitfield Diffie. Derecha: Martin Hellman

4.2 El Algoritmo de Diffie-Hellman

Este algoritmo es un criptosistema perteneciente a la rama de la criptografía asimétrica y su seguridad se basa en la dificultad para calcular logaritmos discretos.

Permite generar una clave secreta para ser compartida por dos personas, a las que se llamarán **Alicia** y **Bernardo**. Consta de los siguientes pasos, diagramados en la siguiente figura:

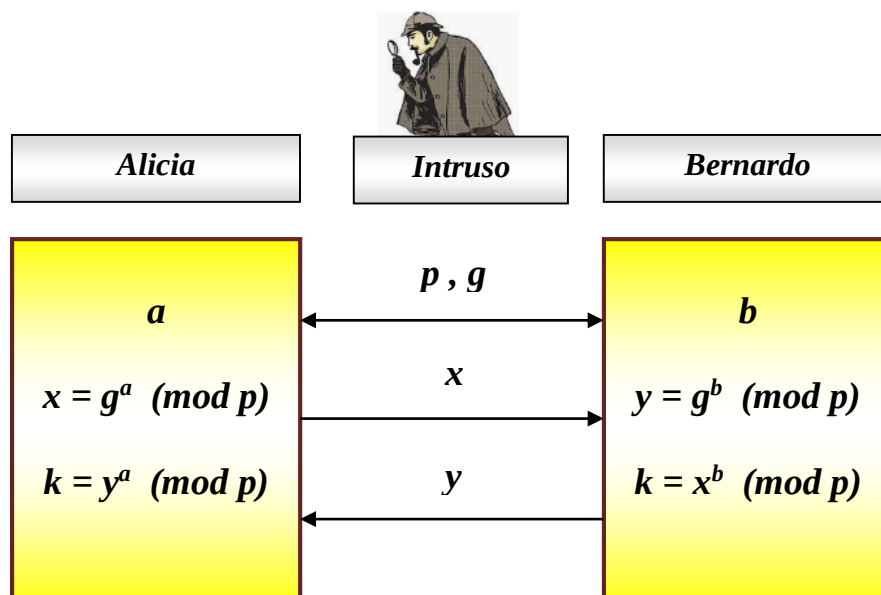


Figura 4.3: Diagrama que ilustra los pasos del Algoritmo de Deffie-Hellman.

Fuente imagen gif: <https://www.gettyimages.es/ilustraciones/sherlock-holmes>

Primer Paso

A través de un medio público (Internet por ejemplo) Alicia y Bernardo se ponen de acuerdo en usar un número primo p muy grande y un número g menor que p . El “intruso” puede detectar ambos números.

Segundo Paso

Alicia escoge un número natural “ a ” menor que p que usará como exponente y lo mantiene en secreto. Bernardo hace lo propio, escoge un número natural “ b ” menor que p que usará como exponente y lo mantiene en secreto.

Tercer Paso

Con su exponente secreto Alicia calcula $x = g^a \pmod{p}$ y envía el valor “ x ” a Bernardo. De este modo, Bernardo conoce “ x ” pero no conoce “ a ”. Bernardo por su

parte calcula $y = g^b \pmod{p}$ y envía el valor “y” a Alicia. De este modo, el intruso puede ver los resultados “x” e “y” pero no ve “a” ni “b”.

Cuarto Paso

Alicia recibe “y” y con su exponente secreto calcula $k = y^a \pmod{p}$.

Bernardo hace lo propio: recibe “x” y con su exponente secreto calcula $k = x^b \pmod{p}$. De este modo, Alicia y Bernardo comparten en forma secreta la misma clave **k**.

Justificación de porqué Alicia y Bernardo obtienen la misma clave “k”.

Como

$$y^a = (g^b)^a = g^{b \cdot a} \pmod{p}$$

Y por otro lado

$$x^b = (g^a)^b = g^{a \cdot b} = g^{b \cdot a} \pmod{p}$$

Resulta entonces que $y^a = x^b = k \pmod{p}$.

El intruso ataca para descubrir la clave

El intruso conoce **p**, **g**, **x**, **y**. No conoce **a** ni **b**. Conociendo “a” podría descubrir la clave **k** ya que $y^a = k \pmod{p}$.

Como $g^a = x \pmod{p}$ entonces $a = \log_g(x) \pmod{11}$. De este modo, para hallar “a”, el intruso debería calcular un logaritmo discreto. Para ello podría recurrir a la computadora y calcular las sucesivas potencias de $g : g^1, g^2, g^3, g^4, \dots$ hasta que le dé **x**. El teorema de Euler asegura que dicho exponente es menor que $p-1$. Pero si el primo **p** tiene más de 200 dígitos, el proceso puede tomar años.

Por esta razón, si el número primo **p** es suficientemente grande, el Algoritmo de Diffie-Hellman es muy seguro debido a que es prácticamente imposible descifrar su clave en un tiempo prudencial.

El siguiente Ejemplo muestra cómo implementar este algoritmo.

Ejemplo 4.2.1

Alicia y Bernardo acuerdan usar el primo $p = 2003$ y $g = 106$. Alicia escoge su exponente $a = 381$, no se lo revela a nadie y calcula $g^a = (106)^{381} = 1717 \pmod{2003}$ y envía “1717” a Bernardo. Por otro lado, Bernardo escoge su exponente $b = 751$, no se lo revela a nadie y calcula $g^b = (106)^{751} = 158 \pmod{2003}$ y envía “158” a Alicia. Alicia, en secreto, hace el cálculo $(158)^{381} = 1193 \pmod{2003}$. Bernardo, en secreto, hace el cálculo $(1717)^{751} = 1193 \pmod{2003}$. De este modo, $k = 1193$ es la clave que comparten. El intruso conoce $p = 2003$, $g = 106$, $x = 1717$, $y = 158$. Su problema es hallar $a = \log_g(x) \pmod{p}$ ó $b = \log_g(y) \pmod{p}$. Con un número p de 4 cifras, el algoritmo que calcula las potencias modulares expuesto en el Capítulo 2 puede dar la respuesta. Pero si p tuviera 200 cifras o más, el cálculo de cualquiera de los dos logaritmos sería muy costoso en términos de tiempo.

El siguiente Ejemplo muestra cómo el “intruso” podría llegar a descubrir la clave secreta.

Ejemplo 4.2.2

Eres un intruso, navegas por los portales de Alicia y Bernardo y en ambos hallas $p = 43$ y $g = 18$. Luego, ves el misterioso número 11 en la página de Bernardo y el misterioso número 15 en la de Alicia. ¿Podrías determinar el número secreto que Alicia y Bernardo comparten?

Solución

Se sabe que $p = 43$ y $g = 18$. También que $x = 11$ e $y = 15$.

Entonces, se procede a calcular a y b :

$$a = \log_g(x) \pmod{p} \Rightarrow a = \log_{18}(11) \pmod{43}$$

Por lo tanto, mediante el algoritmo del Capítulo 2, se calcularán las potencias modulares

$18^i \pmod{43}$ hasta encontrar un " i " que verifique que $18^i = 11 \pmod{43}$. La siguiente tabla muestra los resultados correspondientes:

i	0	1	2	3	4	5	6	7	8	9	10	11
$18^i \pmod{43}$	1	18	23	27	13	19	41	7	40	32	17	5

i	12	13	14	15	16	17	18	19	20	21	22	23
$18^i \pmod{43}$	4	29	6	22	9	33	35	28	31	42	25	20

i	24	25	26	27	28	29	30
$18^i \pmod{43}$	16	30	24	2	36	3	11

Por lo tanto, $a = \log_{18}(11) \pmod{43} = 30$.

Por otro lado,

$$b = \log_g(y) \pmod{p} \Rightarrow b = \log_{18}(15) \pmod{43}$$

Con el mismo procedimiento, se llega a que $b = \log_{18}(15) \pmod{43} = 40$.

Finalmente, se calcula la clave k que Alicia y Bernardo comparten:

$$k = (15)^{30} = 16 \pmod{43}$$

$$k = (11)^{40} = 16 \pmod{43}$$

Por lo tanto, el número secreto que Alicia y Bernardo comparten es $k = 16$.

4.3 Aplicaciones del Algoritmo Diffie-Hellman

Protocolo SSH

SSH o Secure Shell es un protocolo de administración remota que permite a los usuarios controlar y modificar sus servidores remotos a través de Internet. Utiliza técnicas criptográficas para garantizar que todas las comunicaciones hacia y desde el servidor remoto sean seguras.

La ventaja significativa ofrecida por SSH es la utilización del cifrado para asegurar la transferencia segura entre el host y el cliente. Host se refiere al servidor remoto al que está intentando acceder y el cliente es el equipo que está utilizando para acceder al host. Hay tres tecnologías de cifrado diferentes que utiliza SSH: Encriptación Simétrica, Encriptación Asimétrica y Hashing.

La forma en que funciona SSH es mediante un modelo de cliente-servidor para permitir la autenticación de dos sistemas remotos y el cifrado de los datos que pasa entre ellos. Opera en el puerto TCP 22.

El conjunto de protocolos TCP (Transmission Control Protocol) es uno de los más utilizados en servicios de red. Es el encargado de establecer “conexiones” a fin de crear un flujo de datos. El número 22 hace referencia al puerto de conexión.

Hay dos etapas para establecer una conexión: en la primera ambos sistemas deben acordar estándares de encriptación para proteger futuras comunicaciones y en la segunda el usuario debe autenticarse.

Cuando un cliente intenta conectarse al servidor a través de TCP, el servidor presenta los protocolos de cifrado y las versiones que soporta. Si el cliente tiene uno parecido similar de protocolo y versión, se alcanza un acuerdo y se inicia la conexión con el protocolo aceptado. El servidor también utiliza una clave pública asimétrica que el cliente puede utilizar para verificar la autenticidad del host.

Una vez que esto se establece, las dos partes utilizan el algoritmo de intercambio de claves Diffie-Hellman para crear una clave simétrica. Este algoritmo permite que el cliente y el servidor lleguen a una clave de cifrado compartida que se utilizará para cifrar toda la sesión de comunicación.

El algoritmo trabaja de la siguiente manera:

- Cliente y servidor coinciden en un número primo muy grande. Este número primo se conoce como valor de la semilla.
- Las dos partes acuerdan un mecanismo de cifrado común para generar otro conjunto de valores manipulando los valores de semilla.
- Ambas partes generan en forma independiente otro número primo. Esto se utiliza como una clave privada para la interacción.
- Esta clave privada, con el número compartido y el algoritmo de cifrado se utiliza para calcular la clave pública que se distribuye a la otra computadora.
- Las partes utilizan su clave privada personal, la clave pública compartida de la otra máquina y el número primo original para crear una clave compartida final.
- Con esta clave compartida, pueden encriptar simétricamente toda la sesión SSH.

Finalmente, cuando se establece la sesión cifrada segura simétricamente, el usuario debe ser autenticado.

Protocolo TLS

El protocolo TLS (Transport Layer Security) es una evolución del protocolo SSL (Secure Sockets Layer). Es un protocolo mediante el cual se establece una conexión segura por medio de un canal cifrado entre el cliente y servidor. De esta forma, el intercambio de información se realiza en un entorno seguro y libre de ataques.

El protocolo TLS se basa en tres fases básicas:

1. **Negociación:** Los dos extremos de la comunicación (cliente y servidor) negocian qué algoritmos criptográficos utilizarán para autenticarse y cifrar la información. Existen diferentes opciones:

- Para criptografía de clave pública: RSA, Diffie-Hellman, DSA.
- Para cifrado simétrico: RC2, RC4, IDEA, DES, Triple DES o AES.
- Con funciones Hash: MD5 o de la familia SHA.

2. **Autenticación y claves:** Los extremos de la comunicación se autentican mediante certificados digitales y según la negociación, intercambian las claves para el cifrado.

3. **Transmisión segura:** Los extremos de la comunicación pueden iniciar el tráfico de información cifrada y auténtica.

Los objetivos del protocolo son los siguientes: seguridad criptográfica, interoperabilidad, extensibilidad y eficiencia.

4.4 Los ordenadores cuánticos y su amenaza a la criptografía clásica

Los ordenadores cuánticos se basan en ciertas propiedades de las partículas subatómicas para almacenar información y se sirve, por ejemplo, de dos estados diferentes de un electrón o de dos polarizaciones distintas de un fotón. Su unidad básica de información es el bit cuántico o qubit. Un bit cuántico (o qubit) es el equivalente al bit tradicional, pero se diferencia de éste en que puede valer 0, 1 o ambos valores al mismo tiempo. Es decir que, si se dispone de varios qubits, se podría codificar simultáneamente una cantidad impresionante de información.

Para los investigadores en Criptografía Cuántica, si los ordenadores cuánticos de altas prestaciones llegaran a construirse algún día, la criptografía convencional resultaría totalmente insegura. Los ordenadores cuánticos, junto con nuevos algoritmos de cálculo que exploten sus posibilidades, reducirían drásticamente las tareas de criptoanálisis.

Los criptosistemas de clave pública, basados en la dificultad de factorizar números enteros grandes o en hallar un logaritmo discreto, pueden ser rotos con los actuales ordenadores convencionales, pero en un período de tiempo exponencialmente creciente con respecto a la cantidad de dígitos del número. Sin embargo, en un ordenador cuántico, este tipo de problemas se podría resolver en un período de tiempo cuadráticamente creciente en relación a la cantidad de dígitos del número.



Figura 4.3: Ordenador cuántico

4.5 El Algoritmo de Diffie-Hellman aplicado a cuaterniones

En esta sección se presenta una variación del algoritmo Diffie-Hellman aplicando cuaterniones. Como se verá más adelante, esto permitirá mejorar el tiempo requerido para generar claves, manteniendo al mismo tiempo su seguridad.

Procedimiento

Alicia y Bernardo generarán una clave de seguridad para ser compartida. Los pasos a seguir se diagraman en el siguiente gráfico:

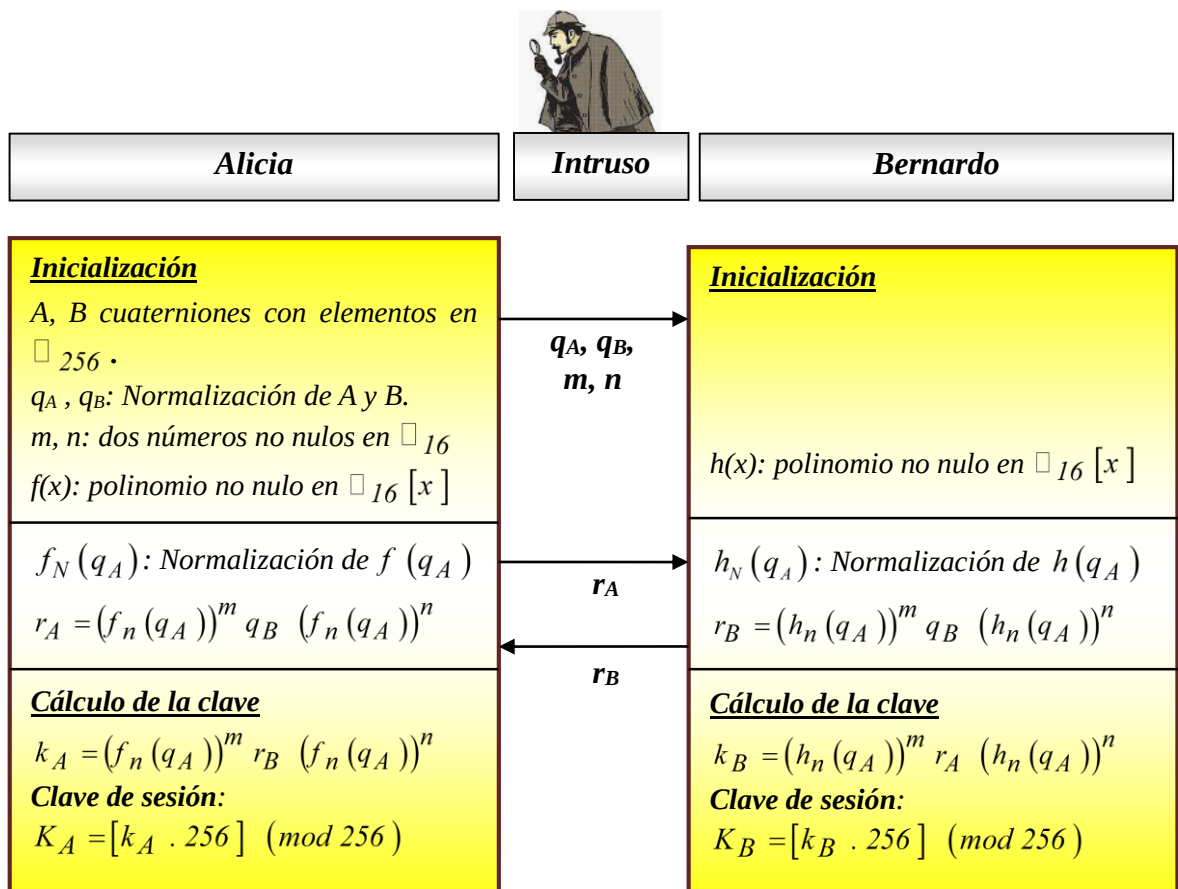


Figura 4.4: Diagrama que ilustra los pasos del Algoritmo de Deffie-Hellman aplicando cuaterniones.

Primer Paso

Alicia elige dos cuaterniones A y B no nulos, a coeficientes en $\mathbb{F}_{256}$. Además, elige dos elementos no nulos m y n pertenecientes a $\mathbb{F}_{16}$.

Segundo Paso

Alicia calcula la normalización de A y B, es decir, $q_A = \frac{A}{|A|}$ y $q_B = \frac{B}{|B|}$.

Tercer Paso

Alicia elige como clave privada un polinomio $f(x)$ con coeficientes y exponentes en $\mathbb{Z}_{16}$ y tal que $f(q_A) \neq 0$.

Cuarto Paso

Alicia envía a Bernardo q_A , q_B , m y n por un canal inseguro.

Quinto Paso

Bernardo elige como clave privada un polinomio $h(x)$ con coeficientes y exponentes en $\mathbb{Z}_{16}$ y tal que $h(q_A) \neq 0$.

Sexto Paso

Alicia calcula

$$f_N(q_A) = \frac{f(q_A)}{|f(q_A)|}$$

$$r_A = (f_N(q_A))^m \cdot q_B \cdot (f_N(q_A))^n$$

Y envía a Bernardo el valor de r_A por un canal inseguro.

Séptimo Paso

Bernardo calcula

$$h_N(q_A) = \frac{h(q_A)}{|h(q_A)|}$$

$$r_B = (h_N(q_A))^m \cdot q_B \cdot (h_N(q_A))^n$$

Y envía a Alicia el valor de r_B por un canal inseguro.

Cálculo de claves**Octavo Paso**

Alicia calcula su clave

$$k_A = (f_N(q_A))^m \cdot r_B \cdot (f_N(q_A))^n.$$

Por otro lado, Bernardo calcula su clave

$$k_B = (h_N(q_A))^m \cdot r_A \cdot (h_N(q_A))^n.$$

Se puede verificar, como se demostrará en la Proposición 4.5.7, que

$$k_A = k_B.$$

Noveno Paso

A fin de que las componentes de k_A y k_B , que son cuaterniones, sean elementos de $\mathbb{H}_{256}$, se consideran como claves a

$$K_A = [k_A \cdot 256] \pmod{256}$$

$$K_B = [k_B \cdot 256] \pmod{256}$$

Donde $[k_A \cdot 256]$ y $[k_B \cdot 256]$ son los números que se obtienen de truncar, respectivamente, la parte decimal de $k_A \cdot 256$ y de $k_B \cdot 256$. Mientras que K_A y K_B son los restos de la división entera de $[k_A \cdot 256]$ y $[k_B \cdot 256]$ por 256. ■

Observación

Las normalizaciones realizadas permiten que el cálculo de las potencias de cuaterniones se limiten a multiplicaciones del argumento de *senos* y *cosenos* por el valor del exponente, logrando de este modo operaciones más sencillas, manteniendo además la esencia del cuaternión original.

A continuación se demostrarán las siguientes Proposiciones que serán utilizadas para probar que $k_A = k_B$.

Proposición 4.5.1

Si q es un cuaternión y $a, b \in \mathbb{H}$ entonces

- 1) $a \cdot b \cdot q = b \cdot a \cdot q$
- 2) $a \cdot q = q \cdot a$

Demostración

- 1) Es inmediata, ya que $a \cdot b = b \cdot a$, $\forall a, b \in \mathbb{H}$.
- 2) Surge de la definición de producto de dos cuaterniones, y de la conmutatividad del producto de números reales. ■

Proposición 4.5.2

Si $q \in \mathbb{H}$ y $m, n \in \mathbb{Z}$ entonces: $q^m \cdot q^n = q^{m+n}$.

Demostración

Se considera la representación trigonométrica de q . Es decir, si $q = a + b.i + c.j + d.k$ entonces:

$$q = |q| \cdot (\cos(\theta) + \text{sen}(\theta) \cdot v')$$

Donde:

$$|q| = \sqrt{a^2 + b^2 + c^2 + d^2}$$

$$\theta = \arccos\left(\frac{a}{|q|}\right), \quad 0 \leq \theta \leq \pi$$

$$v' = \frac{b.i + c.j + d.k}{|b.i + c.j + d.k|}$$

Entonces, por el Teorema 2. 4.7 se tiene:

$$q^m = |q|^m \cdot (\cos(m.\theta) + \operatorname{sen}(m.\theta).v')$$

$$q^n = |q|^n \cdot (\cos(n.\theta) + \operatorname{sen}(n.\theta).v')$$

Por lo tanto, teniendo en cuenta la Proposición 4.5.1 y que $(v')^2 = -1$ resulta:

$$\begin{aligned} q^m \cdot q^n &= |q|^m \cdot (\cos(m.\theta) + \operatorname{sen}(m.\theta).v') \cdot |q|^n \cdot (\cos(n.\theta) + \operatorname{sen}(n.\theta).v') = \\ &= |q|^m \cdot |q|^n \cdot (\cos(m.\theta) + \operatorname{sen}(m.\theta).v') \cdot (\cos(n.\theta) + \operatorname{sen}(n.\theta).v') = \\ &= |q|^{m+n} \cdot (\cos(m.\theta).\cos(n.\theta) + \cos(m.\theta).\operatorname{sen}(n.\theta).v' + \operatorname{sen}(m.\theta).v'.\cos(n.\theta) + \\ &\quad + \operatorname{sen}(m.\theta).v'.\operatorname{sen}(n.\theta).v') = |q|^{m+n} \cdot (\cos(m.\theta).\cos(n.\theta) + \cos(m.\theta).\operatorname{sen}(n.\theta).v' + \\ &\quad + \operatorname{sen}(m.\theta).\cos(n.\theta).v' + \operatorname{sen}(m.\theta).\operatorname{sen}(n.\theta).v'.v') = \\ &= |q|^{m+n} \cdot (\cos(m.\theta).\cos(n.\theta) + \operatorname{sen}(m.\theta + n.\theta).v' + \operatorname{sen}(m.\theta).\operatorname{sen}(n.\theta).v'.v') = \\ &= |q|^{m+n} \cdot (\cos(m.\theta).\cos(n.\theta) + \operatorname{sen}((m+n).\theta).v' - \operatorname{sen}(m.\theta).\operatorname{sen}(n.\theta)) = \\ &= |q|^{m+n} \cdot (\cos(m.\theta + n.\theta) + \operatorname{sen}((m+n).\theta).v') = \\ &= |q|^{m+n} \cdot (\cos((m+n).\theta) + \operatorname{sen}((m+n).\theta).v') = q^{m+n}. \quad \blacksquare \end{aligned}$$

Proposición 4.5.3

Sean $q_i, w_j \in H \quad \forall i, j=1, \dots, n$ entonces $\left(\sum_{i=0}^n q_i\right) \cdot \left(\sum_{j=0}^n w_j\right) = \sum_{i=0}^n \sum_{j=0}^n q_i \cdot w_j$.

Demostración

Se aplicará el Principio de Inducción sobre n , entonces:

Para $n=1$ se verifica pues:

$$\left(\sum_{i=0}^1 q_i\right) \cdot \left(\sum_{j=0}^1 w_j\right) = (q_0 + q_1) \cdot (w_0 + w_1) = q_0 \cdot w_0 + q_0 \cdot w_1 + q_1 \cdot w_0 + q_1 \cdot w_1 \quad [1]$$

Por otro lado,

$$\sum_{i=0}^1 \sum_{j=0}^1 q_i \cdot w_j = \sum_{i=0}^1 (q_i \cdot w_0 + q_i \cdot w_1) = q_0 \cdot w_0 + q_0 \cdot w_1 + q_1 \cdot w_0 + q_1 \cdot w_1 \quad [2]$$

De [1] y [2] se verifica que $\left(\sum_{i=0}^1 q_i \right) \cdot \left(\sum_{j=0}^1 w_j \right) = \sum_{i=0}^1 \sum_{j=0}^1 q_i \cdot w_j$.

Ahora, se supone que vale para n , es decir, se cumple que

$$\left(\sum_{i=0}^n q_i \right) \cdot \left(\sum_{j=0}^n w_j \right) = \sum_{i=0}^n \sum_{j=0}^n q_i \cdot w_j \quad (\text{Hipótesis Inductiva})$$

A continuación se verificará que la igualdad es válida para $(n+1)$:

$$\begin{aligned} \sum_{i=0}^{n+1} \sum_{j=0}^{n+1} q_i \cdot w_j &= \sum_{i=0}^{n+1} \left(\sum_{j=0}^n q_i \cdot w_j + q_i \cdot w_{n+1} \right) = \\ &= \sum_{i=0}^{n+1} \sum_{j=0}^n q_i \cdot w_j + \sum_{i=0}^{n+1} q_i \cdot w_{n+1} = \sum_{i=0}^n \sum_{j=0}^n q_i \cdot w_j + \sum_{j=0}^n q_{n+1} \cdot w_j + \sum_{i=0}^{n+1} q_i \cdot w_{n+1} \end{aligned} \quad [3]$$

Por otro lado

$$\begin{aligned} \left(\sum_{i=0}^{n+1} q_i \right) \cdot \left(\sum_{j=0}^{n+1} w_j \right) &= \left(\sum_{i=0}^n q_i + q_{n+1} \right) \cdot \left(\sum_{j=0}^n w_j + w_{n+1} \right) = \\ &= \sum_{i=0}^n q_i \cdot \sum_{j=0}^n w_j + \sum_{i=0}^n q_i \cdot w_{n+1} + q_{n+1} \cdot \sum_{j=0}^n w_j + q_{n+1} \cdot w_{n+1} = \\ &= \sum_{i=0}^n \sum_{j=0}^n q_i \cdot w_j + \sum_{i=0}^n q_i \cdot w_{n+1} + \sum_{j=0}^n q_{n+1} \cdot w_j + q_{n+1} \cdot w_{n+1} = \\ &\downarrow \\ &= \sum_{i=0}^n \sum_{j=0}^n q_i \cdot w_j + \sum_{i=0}^{n+1} q_i \cdot w_{n+1} + \sum_{j=0}^n q_{n+1} \cdot w_j \end{aligned} \quad [4]$$

Hip. Inductiva

$$\text{De [3] y [4] resulta } \left(\sum_{i=0}^{n+1} q_i \right) \cdot \left(\sum_{j=0}^{n+1} w_j \right) = \sum_{i=0}^{n+1} \sum_{j=0}^{n+1} q_i \cdot w_j \quad \blacksquare$$

Proposición 4.5.4

Si $f(x) = \sum_{i=0}^n a_i \cdot x^i$ con $a_i \in \square \quad \forall i=0, \dots, n$; $h(x) = \sum_{j=0}^n b_j \cdot x^j$ con $b_j \in \square \quad \forall j=0, \dots, n$ y

sea $q \in H$. Entonces $f(q) \cdot h(q) = h(q) \cdot f(q)$.

Demostración

$$\begin{aligned}
 f(q) \cdot h(q) &= \left(\sum_{i=0}^n a_i \cdot q^i \right) \cdot \left(\sum_{j=0}^n b_j \cdot q^j \right) = \sum_{i=0}^n \sum_{j=0}^n a_i \cdot q^i \cdot b_j \cdot q^j = \sum_{i=0}^n \sum_{j=0}^n a_i \cdot b_j \cdot q^i \cdot q^j = \\
 &= \sum_{i=0}^n \sum_{j=0}^n b_j \cdot a_i \cdot q^{i+j} = \sum_{i=0}^n \sum_{j=0}^n b_j \cdot a_i \cdot q^{j+i} = \sum_{i=0}^n \sum_{j=0}^n b_j \cdot a_i \cdot q^j \cdot q^i \stackrel{\downarrow}{=} \sum_{j=0}^n \sum_{i=0}^n b_j \cdot a_i \cdot q^j \cdot q^i
 \end{aligned} \quad [1]$$

Conmutatividad de la suma en H.

Por otro lado,

$$h(q) \cdot f(q) = \left(\sum_{j=0}^n b_j \cdot q^j \right) \cdot \left(\sum_{i=0}^n a_i \cdot q^i \right) = \sum_{j=0}^n \sum_{i=0}^n b_j \cdot q^j \cdot a_i \cdot q^i = \sum_{j=0}^n \sum_{i=0}^n b_j \cdot a_i \cdot q^j \cdot q^i \quad [2]$$

De [1] y [2] resulta que $f(q) \cdot h(q) = h(q) \cdot f(q)$. ■

Proposición 4.5.5

Sean $q, w \in H$ tales que $q \cdot w = w \cdot q$ y $n \in \mathbb{N}$. Entonces:

- 1) $q^n \cdot w = w \cdot q^n$
- 2) $w^n \cdot q = q \cdot w^n$
- 3) $(q \cdot w)^n = q^n \cdot w^n$

Demostración

1) Se probará este resultando aplicando el Principio de Inducción sobre n . Entonces:

Para $n = 1$ obviamente se verifica pues

$$q^1 \cdot w = q \cdot w = w \cdot q = w \cdot q^1$$

Se supone ahora que la igualdad es válida para n , es decir,

$$q^n \cdot w = w \cdot q^n \quad (\text{Hipótesis Inductiva})$$

Se probará que la igualdad es válida para $(n+1)$:

$$\begin{aligned}
 q^{n+1} \cdot w &\stackrel{\downarrow}{=} q^n \cdot q^1 \cdot w \stackrel{\downarrow}{=} q^n \cdot w \cdot q^1 \stackrel{\downarrow}{=} w \cdot q^n \cdot q^1 = w \cdot q^{n+1} \\
 &\quad \text{Por Prop. 4.5.2} \quad \text{Por hipótesis.} \quad \text{H. Inductiva}
 \end{aligned}$$

2) y 3) Se demuestran de manera similar, aplicando el Principio de Inducción sobre n . ■

Proposición 4.5.6

Sean $f(x), h(x)$ dos polinomios de grado menor o igual que n y a coeficientes reales.

Sean $m \in \mathbb{N}$ y $q \in H$. Entonces: $[f(q)]^m \cdot [h(q)]^m = [h(q)]^m \cdot [f(q)]^m$.

Demostración

Por la Proposición 4.5.5 inciso 3) se tiene que: $[f(q)]^m \cdot [h(q)]^m = [f(q) \cdot h(q)]^m$.

Por otro lado, de la Proposición 4.5.4 resulta $f(q) \cdot h(q) = h(q) \cdot f(q)$.

Entonces

$$[f(q)]^m \cdot [h(q)]^m = [f(q) \cdot h(q)]^m = [h(q) \cdot f(q)]^m.$$

Finalmente, aplicando nuevamente la proposición 4.5.5 inciso 3), se obtiene:

$$[f(q)]^m \cdot [h(q)]^m = [f(q) \cdot h(q)]^m = [h(q) \cdot f(q)]^m = [h(q)]^m \cdot [f(q)]^m. \blacksquare$$

En base a estas proposiciones, se demostrará a continuación que las claves de Alicia y de Bernardo son las mismas.

Proposición 4.5.7

Sean

$$k_A = [f_N(q_A)]^m \cdot r_B \cdot [f_N(q_A)]^n$$

$$k_B = [h_N(q_A)]^m \cdot r_A \cdot [h_N(q_A)]^n$$

Donde

$$r_B = [h_N(q_A)]^m \cdot q_B \cdot [h_N(q_A)]^n$$

$$r_A = [f_N(q_A)]^m \cdot q_B \cdot [f_N(q_A)]^n$$

Entonces $k_A = k_B$

Demostración

De la Proposición 4.5.6 resulta

$$k_A = [f_N(q_A)]^m \cdot r_B \cdot [f_N(q_A)]^n = [f_N(q_A)]^m \cdot [h_N(q_A)]^m \cdot q_B \cdot [h_N(q_A)]^n \cdot [f_N(q_A)]^n$$

Por otro lado,

$$k_B = [h_N(q_A)]^m \cdot r_A \cdot [h_N(q_A)]^n = [h_N(q_A)]^m \cdot [f_N(q_A)]^m \cdot q_B \cdot [f_N(q_A)]^n \cdot [h_N(q_A)]^n = \\ = [f_N(q_A)]^m \cdot [h_N(q_A)]^m \cdot q_B \cdot [h_N(q_A)]^n \cdot [f_N(q_A)]^n = k_A$$

En consecuencia, $k_A = k_B$ ■

El siguiente Ejemplo numérico mostrará en detalle cómo generar una clave en el Algoritmo de Diffie-Hellman aplicando cuaterniones.

Ejemplo 4.5.8

Primer Paso

Alicia elige dos cuaterniones A y B no nulos, a coeficientes en $\mathbb{Z}_{256}$.

$$A = (2, 2, 2, 2)$$

$$B = (3, 0, 4, 0)$$

Además, elige dos elementos no nulos m y n pertenecientes a $\mathbb{Z}_{16}$.

$$m = 3$$

$$n = 2$$

Segundo Paso

Alicia calcula la normalización de A y B , es decir, $q_A = \frac{A}{|A|}$ y $q_B = \frac{B}{|B|}$.

$$q_A = \frac{A}{|A|} = \frac{(2, 2, 2, 2)}{\sqrt{2^2 + 2^2 + 2^2 + 2^2}} = \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)$$

$$q_B = \frac{B}{|B|} = \frac{(3, 0, 4, 0)}{\sqrt{3^2 + 0^2 + 4^2 + 0^2}} = \left(\frac{3}{5}, 0, \frac{4}{5}, 0\right)$$

Tercer Paso

Alicia elige como clave privada un polinomio $f(x)$ con coeficientes y exponentes en

$\mathbb{Z}_{16}$ y tal que $f(q_A) \neq 0$:

$$f(x) = 2x^5 + 3x^4$$

Cuarto Paso

Alicia envía a Bernardo q_A , q_B , m y n por un canal inseguro.

Quinto Paso

Bernardo elige como clave privada un polinomio $h(x)$ con coeficientes y exponentes en

$\mathbb{Z}_{16}$ y tal que $h(q_A) \neq 0$:

$$h(x) = 3x^6 + 4x^8$$

Sexto Paso

Alicia calcula

$$f_N(q_A) = \frac{f(q_A)}{|f(q_A)|}$$

$$r_A = [f_N(q_A)]^m \quad q_B \quad [f_N(q_A)]^n$$

Y envía a Bernardo el valor de r_A por un canal inseguro. Para ello se expresa primeramente q_A en la forma trigonométrica:

$$q_A = |q_A| \cdot (\cos(\theta) + \operatorname{sen}(\theta) \cdot v')$$

$$|q_A| = 1,$$

$$\theta = \arccos\left(\frac{a}{|q_A|}\right) = \arccos\left(\frac{\frac{1}{2}}{1}\right) = \arccos\left(\frac{1}{2}\right) = \frac{\pi}{3},$$

$$\begin{aligned} v' &= \frac{(b, c, d)}{|(b, c, d)|} = \frac{\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)}{\left|\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)\right|} = \frac{\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)}{\sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2}} = \frac{\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)}{\sqrt{\frac{1}{4} + \frac{1}{4} + \frac{1}{4}}} = \\ &= \frac{\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)}{\sqrt{\frac{3}{4}}} = \left(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right) \end{aligned}$$

Por lo tanto:

$$q_A = \cos\left(\frac{\pi}{3}\right) + \operatorname{sen}\left(\frac{\pi}{3}\right) \cdot v'.$$

Entonces, aplicando la fórmula de De Moivre, resulta:

$$\begin{aligned} f(q_A) &= 2q_A^5 + 3q_A^4 = 2 \cdot \left[\cos\left(\frac{5\pi}{3}\right) + \operatorname{sen}\left(\frac{5\pi}{3}\right) \cdot v' \right] + 3 \cdot \left[\cos\left(\frac{4\pi}{3}\right) + \operatorname{sen}\left(\frac{4\pi}{3}\right) \cdot v' \right] = \\ &= 2 \cdot \left[\frac{1}{2} - \frac{\sqrt{3}}{2} \cdot \left(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right) \right] + 3 \cdot \left[-\frac{1}{2} - \frac{\sqrt{3}}{2} \cdot \left(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right) \right] = \\ &= 2 \cdot \left[\frac{1}{2} + \left(-\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}\right) \right] + 3 \cdot \left[-\frac{1}{2} + \left(-\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}\right) \right] = \\ &= 1 + (-1, -1, -1) - \frac{3}{2} + \left(-\frac{3}{2}, -\frac{3}{2}, -\frac{3}{2}\right) = 1 - i - j - k - \frac{3}{2} - \frac{3}{2}i - \frac{3}{2}j - \frac{3}{2}k = \\ &= -\frac{1}{2} - \frac{5}{2}i - \frac{5}{2}j - \frac{5}{2}k \end{aligned}$$

Luego

$$f(q_A) = -\frac{1}{2}i - \frac{5}{2}j - \frac{5}{2}k.$$

Y también se tiene que:

$$\begin{aligned} f_N(q_A) &= \frac{f(q_A)}{|f(q_A)|} = \frac{\left(-\frac{1}{2}, -\frac{5}{2}, -\frac{5}{2}, -\frac{5}{2}\right)}{\left|\left(-\frac{1}{2}, -\frac{5}{2}, -\frac{5}{2}, -\frac{5}{2}\right)\right|} = \frac{\left(-\frac{1}{2}, -\frac{5}{2}, -\frac{5}{2}, -\frac{5}{2}\right)}{\sqrt{\left(-\frac{1}{2}\right)^2 + \left(-\frac{5}{2}\right)^2 + \left(-\frac{5}{2}\right)^2 + \left(-\frac{5}{2}\right)^2}} = \\ &= \frac{\left(-\frac{1}{2}, -\frac{5}{2}, -\frac{5}{2}, -\frac{5}{2}\right)}{\sqrt{\frac{1}{4} + 3 \cdot \frac{25}{4}}} = \frac{\left(-\frac{1}{2}, -\frac{5}{2}, -\frac{5}{2}, -\frac{5}{2}\right)}{\sqrt{19}} = \left(-\frac{1}{2\sqrt{19}}, -\frac{5}{2\sqrt{19}}, -\frac{5}{2\sqrt{19}}, -\frac{5}{2\sqrt{19}}\right) \end{aligned}$$

A continuación se expresa $f_N(q_A)$ en forma trigonométrica:

$$f_N(q_A) = |f_N(q_A)| \cdot (\cos(\theta) + \text{sen}(\theta) \cdot v')$$

Entonces

$$|f_N(q_A)| = 1$$

Para calcular θ y v' se consideran dos decimales:

$$\theta = \arccos\left(\frac{a}{|f_N(q_A)|}\right) = \arccos\left(-\frac{1}{2\sqrt{19}}\right) = 1,69,$$

$$\begin{aligned} v' &= \frac{(b, c, d)}{|(b, c, d)|} = \frac{\left(-\frac{5}{2\sqrt{19}}, -\frac{5}{2\sqrt{19}}, -\frac{5}{2\sqrt{19}}\right)}{\left|\left(-\frac{5}{2\sqrt{19}}, -\frac{5}{2\sqrt{19}}, -\frac{5}{2\sqrt{19}}\right)\right|} = \\ &= \frac{\left(-\frac{5}{2\sqrt{19}}, -\frac{5}{2\sqrt{19}}, -\frac{5}{2\sqrt{19}}\right)}{\sqrt{\left(-\frac{5}{2\sqrt{19}}\right)^2 + \left(-\frac{5}{2\sqrt{19}}\right)^2 + \left(-\frac{5}{2\sqrt{19}}\right)^2}} = \\ &= \frac{\left(-\frac{5}{2\sqrt{19}}, -\frac{5}{2\sqrt{19}}, -\frac{5}{2\sqrt{19}}\right)}{\sqrt{3 \cdot \frac{25}{76}}} = \frac{\left(-\frac{5}{2\sqrt{19}}, -\frac{5}{2\sqrt{19}}, -\frac{5}{2\sqrt{19}}\right)}{\sqrt{\frac{75}{76}}} = \\ &= \left(-\frac{5}{\sqrt{75}}, -\frac{5}{\sqrt{75}}, -\frac{5}{\sqrt{75}}\right) \end{aligned}$$

Por lo tanto:

$$f_N(q_A) = \cos(1,69) + \text{sen}(1,69) \cdot v'$$

Finalmente se calcula r_A :

$$\begin{aligned} r_A &= [f_N(q_A)]^m \cdot q_B \cdot [f_N(q_A)]^n = \\ &= [\cos(3.(1,69)) + \operatorname{sen}(3.(1,69)) \cdot v'] \cdot \left(\frac{3}{5}, 0, \frac{4}{5}, 0\right) \cdot [\cos(2.(1,69)) + \operatorname{sen}(2.(1,69)) \cdot v'] = \\ &= (0,06145, 0,05370, -0,4969, -0,8640) \end{aligned}$$

Es decir,

$$r_A = (0,06145, 0,05370, -0,4969, -0,8640)$$

Séptimo Paso

Bernardo calcula

$$h_N(q_A) = \frac{h(q_A)}{|h(q_A)|}$$

$$r_B = [h_N(q_A)]^m \cdot q_B \cdot [h_N(q_A)]^n$$

Y envía a Alicia el valor de r_B por un canal inseguro.

Entonces

$$\begin{aligned} h(q_A) &= 3.q_A^6 + 4.q_A^8 = 3. [\cos(2\pi) + \operatorname{sen}(2\pi) \cdot v'] + 4. \left[\cos\left(\frac{8\pi}{3}\right) + \operatorname{sen}\left(\frac{8\pi}{3}\right) \cdot v' \right] = \\ &= 3.[1 - 0] + 4. \left[-\frac{1}{2} + \frac{\sqrt{3}}{2} \cdot \left(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}} \right) \right] = 3 + 4. \left[-\frac{1}{2} + \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2} \right) \right] = \\ &= 3 - 2 + (2, 2, 2) = 3 - 2 + 2i + 2j + 2k = 1 + 2i + 2j + 2k \end{aligned}$$

Luego

$$\begin{aligned} h_N(q_A) &= \frac{h(q_A)}{|h(q_A)|} = \frac{(1, 2, 2, 2)}{|(1, 2, 2, 2)|} = \frac{(1, 2, 2, 2)}{\sqrt{1^2 + 2^2 + 2^2 + 2^2}} = \\ &= \frac{(1, 2, 2, 2)}{\sqrt{13}} = \left(\frac{1}{\sqrt{13}}, \frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}} \right) \end{aligned}$$

A continuación se expresa $h_N(q_A)$ en forma trigonométrica:

$$h_N(q_A) = |h_N(q_A)| \cdot (\cos(\theta) + \operatorname{sen}(\theta) \cdot v') .$$

Entonces

$$|h_N(q_A)| = 1 .$$

Se calcula θ y v' considerando dos decimales

$$\theta = \arccos \left(\frac{a}{|h_N(q_A)|} \right) = \arccos \left(\frac{1}{\sqrt{13}} \right) = 1,29 ,$$

$$\begin{aligned}
v' &= \frac{(b,c,d)}{|(b,c,d)|} = \frac{\left(\frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}\right)}{\left|\left(\frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}\right)\right|} = \frac{\left(\frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}\right)}{\sqrt{\left(\frac{2}{\sqrt{13}}\right)^2 + \left(\frac{2}{\sqrt{13}}\right)^2 + \left(\frac{2}{\sqrt{13}}\right)^2}} = \\
&= \frac{\left(\frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}\right)}{\sqrt{3 \cdot \frac{4}{13}}} = \frac{\left(\frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}, \frac{2}{\sqrt{13}}\right)}{\sqrt{\frac{12}{13}}} = \left(\frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right)
\end{aligned}$$

Por lo tanto:

$$h_N(q_A) = \cos(1,29) + \operatorname{sen}(1,29) \cdot v'$$

Finalmente se calcula r_B :

$$\begin{aligned}
r_B &= [h_N(q_A)]^m \cdot q_B \cdot [h_N(q_A)]^n = \\
&= [\cos(3.(1,29)) + \operatorname{sen}(3.(1,29)) \cdot v'] \cdot \left(\frac{3}{5}, 0, \frac{4}{5}, 0\right) \cdot [\cos(2.(1,29)) + \operatorname{sen}(2.(1,29)) \cdot v'] = \\
&= (0,5156, -0,1976, 0,4680, 0,6899)
\end{aligned}$$

Es decir,

$$r_B = (0,5156, -0,1976, 0,4680, 0,6899)$$

Cálculo de claves

Octavo Paso

Alicia calcula su clave k_A

$$k_A = [f_N(q_A)]^m \cdot r_B \cdot [f_N(q_A)]^n$$

Es decir,

$$\begin{aligned}
k_A &= [f_N(q_A)]^m \cdot r_B \cdot [f_N(q_A)]^n = \\
&= [\cos(3.(1,69)) + \operatorname{sen}(3.(1,69)) \cdot v'] \cdot r_B \cdot [\cos(2.(1,69)) + \operatorname{sen}(2.(1,69)) \cdot v'] = \\
&= (0,185, -0,492, 0,068, -0,848)
\end{aligned}$$

Por lo tanto

$$k_A = (0,185, -0,492, 0,068, -0,848)$$

Por otro lado, Bernardo calcula su clave

$$k_B = [h_N(q_A)]^m \cdot r_A \cdot [h_N(q_A)]^n$$

Entonces

$$\begin{aligned}
k_B &= [h_N(q_A)]^m \cdot r_A \cdot [h_N(q_A)]^n = \\
&= [\cos(3 \cdot (1,29)) + \operatorname{sen}(3 \cdot (1,29)) \cdot v'] \cdot r_A \cdot [\cos(2 \cdot (1,29)) + \operatorname{sen}(2 \cdot (1,29)) \cdot v'] = \\
&= (0,185, -0,492, 0,068, -0,848)
\end{aligned}$$

En consecuencia

$$k_B = (0,185, -0,492, 0,068, -0,848)$$

Noveno Paso

A fin de que las componentes de k_A y k_B tenga sus elementos en $\square_{256}$, se consideran como claves a

$$K_A = [k_A \cdot 256] \pmod{256}$$

$$K_B = [k_B \cdot 256] \pmod{256}$$

Es decir

$$\begin{aligned}
K_A = K_B &= [(0,185, -0,492, 0,068, -0,848) \cdot 256] = \\
&= [(47,36, -125,952, 17,408, -217,088)] = \\
&= (47, -125, 17, -217) \equiv (47, 130, 17, 39) \pmod{256}
\end{aligned}$$

De este modo,

$$K_A = K_B \equiv (47, 130, 17, 39) \pmod{256} \quad \blacksquare$$

Análisis del tiempo requerido para la ejecución del Algoritmo de Diffie-Hellman aplicando cuaterniones

Cuando se analiza el tiempo de ejecución de un determinado algoritmo, se cuentan solamente la cantidad de multiplicaciones y divisiones, ya que el tiempo que tarda el ordenador en efectuar una multiplicación o división es predominantemente mayor al tiempo requerido para efectuar una suma o resta.

Por esta razón sólo se contarán las multiplicaciones y divisiones que lleva a cabo el algoritmo.

Primeramente se supondrá que, para calcular una raíz cuadrada, el ordenador aplica el Método de Newton Raphson, el cual se detalla brevemente a continuación:

Si $a > 0$, para calcular $\sqrt{a}$ se plantea la ecuación

$$\sqrt{a} = x \Leftrightarrow a = x^2 \Leftrightarrow x^2 - a = 0$$

Luego, tomando $f(x) = x^2 - a$ y un valor inicial x_0 , el Método de Newton Raphson queda planteado del siguiente modo:

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} \quad n = 0, 1, 2, \dots$$

En este caso,

$$x_{n+1} = \frac{x_n^2 + a}{2x_n} \quad n = 0, 1, 2, \dots$$

Se supondrá que basta efectuar 3 iteraciones para obtener la precisión deseada. Como una iteración realiza 3 operaciones de multiplicación y división, entonces serán necesarias 9 operaciones para calcular una raíz cuadrada. Ésta aparecerá cuando se deba hallar el módulo de un cuaternión, que demandará entonces un total de $9 + 4 = 13$ multiplicaciones y divisiones.

Por otro lado, para calcular un *seno*, un *coseno* o un *arco-coseno*, se considera el desarrollo de Taylor asociado a estas funciones. Es decir,

$$\text{sen}(x) = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}$$

$$\cos(x) = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!}$$

$$\arccos(x) = \frac{\pi}{2} - \sum_{n=0}^{\infty} \frac{(2n)!}{4^n \cdot (n!)^2 \cdot (2n+1)} x^{2n+1} = \frac{\pi}{2} - \sum_{n=0}^{\infty} \frac{(2n)(2n-1)\dots(2n-(n-1))}{4^n \cdot (n!) \cdot (2n+1)} x^{2n+1}$$

Si se toman los 6 primeros términos de la serie para el cálculo aproximado de estas funciones entonces:

Para el seno: Cada término contiene $2n + 2n + 1 = 4n + 1$ multiplicaciones y divisiones. Luego, el total de multiplicaciones y divisiones es

$$\sum_{n=1}^5 (4n+1) = 4 \sum_{n=1}^5 n + \sum_{n=1}^5 1 = 4 \cdot \frac{5 \cdot (5+1)}{2} + 5 = 65$$

Así, son necesarias 65 multiplicaciones y divisiones para valorar el seno de un ángulo.

Para el coseno: Cada término contiene $2n - 1 + 2n - 1 + 1 = 4n - 1$ multiplicaciones y divisiones. Luego, el total de multiplicaciones y divisiones es

$$\sum_{n=1}^5 (4n-1) = 4 \sum_{n=1}^5 n - \sum_{n=1}^5 1 = 4 \cdot \frac{5 \cdot (5+1)}{2} - 5 = 55$$

Por lo tanto, son necesarias 55 multiplicaciones y divisiones para valorar el coseno de un ángulo.

Para el arco-coseno: Cada término contiene $2n - 1 + 2n + n - 1 + n - 1 + 7 = 6n + 4$ multiplicaciones y divisiones. Luego, el total de multiplicaciones y divisiones es

$$\sum_{n=1}^5 (6n+4) = 6 \sum_{n=1}^5 n + \sum_{n=1}^5 4 = 6 \cdot \frac{5 \cdot (5+1)}{2} + 20 = 110$$

Por lo tanto, son necesarias 110 multiplicaciones y divisiones para valuar el arco-coseno de un ángulo. Estas funciones trigonométricas aparecerán cuando se deba expresar un cuaternión en forma trigonométrica a fin de calcular sus potencias de una manera más sencilla.

El siguiente cuadro muestra, en cada paso, la cantidad de operaciones que lleva a cabo el algoritmo.

Paso	Operación a realizar	Cantidad de multiplicaciones y divisiones
1	Alicia elige dos cuaterniones A y B no nulos, y dos elementos no nulos m y n .	
2	Alicia calcula $q_A = \frac{A}{ A } \text{ y } q_B = \frac{B}{ B }.$	Para q_A : $13 + 4 = 17$ Para q_B : $13 + 4 = 17$ Total: $17+17 = 34$
3	Alicia selecciona un polinomio $f(x) = \sum_{i=0}^{15} a_i \cdot x^i \text{ con } a_i \in \mathbb{F}_{16}$	
4	Alicia envía q_A , q_B , m y n .	
5	Bernardo selecciona un polinomio $h(x) = \sum_{i=0}^{15} b_i \cdot x^i \text{ con } b_i \in \mathbb{F}_{16}$	
6	Alicia calcula $f_N(q_A) = \frac{f(q_A)}{ f(q_A) }$ $r_A = [f_N(q_A)]^m \cdot q_B \cdot [f_N(q_A)]^n$	Para q_A^i en forma trigonométrica: $1 + 55 + 65 + 110 + 3 + 9 + 3 + 3 = 249$ Para $f_N(q_A)$ $15(140) + 4 + 13 = 2117$ Para $[f_N(q_A)]^m$: 139 Para $[f_N(q_A)]^n$: 139 Para r_A : $16 + 16 = 32$ Total: $2117 + 249 + 139 + 139 + 32 = 2676$.
7	Bernardo calcula $h_N(q_A) = \frac{h(q_A)}{ h(q_A) }$ $r_B = [h_N(q_A)]^m \cdot q_B \cdot [h_N(q_A)]^n$	Es similar al paso anterior. Por lo tanto, Total: $2117 + 249 + 139 + 139 + 32 = 2676$

Paso	Operación a realizar	Cantidad de multiplicaciones y divisiones
8	<i>Alicia calcula su clave</i> $k_A = [f_N(q_A)]^m \cdot r_B \cdot [f_N(q_A)]^n.$ <i>Bernardo calcula su clave</i> $k_B = [h_N(q_A)]^m \cdot r_A \cdot [h_N(q_A)]^n.$	Total: 16 + 16 = 32 Total: 16 + 16 = 32
9	<i>Alicia calcula</i> $K_A = [k_A \cdot 256] \pmod{256}$ <i>Bernardo calcula</i> $K_B = [k_B \cdot 256] \pmod{256}$	Total: 4 Total: 4 (Los restos de la división entera de $[k_A \cdot 256]$ y $[k_B \cdot 256]$ por 256 no se consideran, pues se programan mediante sucesivas restas)

Luego,

Total de operaciones efectuadas en la computadora de Alicia:

$$34 + 2676 + 32 + 4 = 2746.$$

Total de operaciones efectuadas en la computadora de Bernardo:

$$2676 + 32 + 4 = 2712.$$

Comparación con el Algoritmo de Diffie-Hellman clásico.

En la página 25 de este trabajo, se expuso el pseudocódigo del algoritmo que calcula potencias modulares. El mismo se muestra nuevamente, a fin de contar la cantidad de multiplicaciones y divisiones requeridas. En este caso, los restos de las divisiones enteras por “n” tampoco se consideran, pues se programan mediante sucesivas restas.

Algoritmo para calcular $a^k \pmod n$

$$a_0 = a, k_0 = k, c_0 = 1, i = 1$$

Mientras $k_{i-1} > 1$ hacer:

- $a_i \equiv a_{i-1}^2 \pmod n$ 1 multiplicación.
- Si k_{i-1} es par entonces
 - $c_i = c_{i-1}$
 - Sino $c_i \equiv a_{i-1} \cdot c_{i-1} \pmod n$ 1 multiplicación.
- Fin si
- $k_i = \left\lfloor \frac{k_{i-1}}{2} \right\rfloor$ 1 división
- $i = i + 1$

Fin mientras

$$a^k \equiv a_{i-1} \cdot c_{i-1} \pmod n$$
 1 multiplicación.

El ciclo “Mientras $k_{i-1} > 1$ ” significa que las instrucciones que figuran dentro de dicho ciclo deberán ejecutarse $(L_k - 1)$ veces, donde L_k es la cantidad de dígitos binarios que tiene el exponente k . Por lo tanto, para calcular $a^k \pmod n$ se necesitan $3(L_k - 1) + 1 = 3L_k - 2$ operaciones.

Como Alicia calculará $g^a \pmod p$ e $y^a \pmod p$, mientras que Bernardo deberá computar $g^b \pmod p$ y $x^b \pmod p$, entonces

Total de operaciones efectuadas en la computadora de Alicia:

$$2(3L_a - 2) = 6L_a - 4$$

Total de operaciones efectuadas en la computadora de Bernardo:

$$2(3L_b - 2) = 6L_b - 4$$

Teniendo en cuenta que, por una cuestión de seguridad del algoritmo, tanto “ a ” como “ b ” son números naturales muy grandes y por lo tanto, tienen numerosos dígitos binarios, el Algoritmo de Diffie-Hellman empleando cuaterniones efectúa un número de operaciones considerablemente menor que el Diffie-Hellman clásico.

Análisis del espacio de memoria requerido para la ejecución del Algoritmo de Diffie-Hellman aplicando cuaterniones

Para este análisis se tendrá en cuenta que un número en $\mathbb{Z}_{256}$ tiene a lo sumo 8 dígitos binarios y por lo tanto, ocupa 8 bits. Luego, un cuaternión a coeficientes en $\mathbb{Z}_{256}$ ocupará 32 bits. Del mismo modo, si un número pertenece a $\mathbb{Z}_{16}$ entonces tiene a lo sumo 4 dígitos binarios y en consecuencia ocupa 4 bits. Por otro lado, al efectuar las operaciones aritméticas entre cuaterniones, es suficiente hacerlas en formato de simple precisión, que es un formato de número que ocupa 32 bits.

En base a estas observaciones, los siguientes cuadros muestran la cantidad de memoria que requiere el algoritmo.

Para la computadora de Alicia

<i>Elemento</i>	<i>Cantidad de bits requeridos</i>
Cuaterniones A y B	$32 \text{ bits} + 32 \text{ bits} = 64 \text{ bits}$
Números m y n	$8 \text{ bits} + 8 \text{ bits} = 16 \text{ bits.}$
q_A	$4 (32) \text{ bits} = 128 \text{ bits}$
q_B	$4 (32) \text{ bits} = 128 \text{ bits}$
$f(x)$	$16 (4) \text{ bits} = 64 \text{ bits}$
$f_N(q_A)$	$4 (32) \text{ bits} = 128 \text{ bits}$
r_A	$4 (32) \text{ bits} = 128 \text{ bits}$
k_A	$4 (32) \text{ bits} = 128 \text{ bits}$
K_A	$4 (32) \text{ bits} = 128 \text{ bits}$

Además, se utilizan los siguientes espacios auxiliares de memoria, utilizados para el cómputo de los elementos de la tabla anterior:

<i>Espacio para el cómputo de:</i>	<i>Cantidad de bits requeridos</i>
<i>Módulo de un cuaternión</i>	<i>32 bits</i>
θ	<i>32 bits.</i>
v'	<i>3 (32) bits = 96 bits</i>
$\cos(n \theta)$, con $n \in \mathbb{Z}$	<i>32 bits.</i>
$\sin(n \theta)$, con $n \in \mathbb{Z}$	<i>32 bits</i>

Por lo tanto,

Total de espacio de memoria requerido en la computadora de Alicia:

1136 bits = 142 bytes.

Para la computadora de Bernardo

<i>Elemento</i>	<i>Cantidad de bits requeridos</i>
Números m y n	<i>8 bits + 8 bits = 16 bits.</i>
q_A	<i>4 (32) bits = 128 bits</i>
q_B	<i>4 (32) bits = 128 bits</i>
$h(x)$	<i>16 (4) bits = 64 bits</i>
$h_N(q_A)$	<i>4 (32) bits = 128 bits</i>
r_B	<i>4 (32) bits = 128 bits</i>
k_B	<i>4 (32) bits = 128 bits</i>
K_B	<i>4 (32) bits = 128 bits</i>

Al igual que para el caso de Alicia, también se consideran los siguientes espacios auxiliares de memoria:

<i>Espacio para el cómputo de:</i>	<i>Cantidad de bits requeridos</i>
<i>Módulo de un cuaternión</i>	32 bits
θ	32 bits.
v'	3 (32) bits = 96 bits
$\cos(n \theta)$, con $n \in \mathbb{Z}$	32 bits.
$\sin(n \theta)$, con $n \in \mathbb{Z}$	32 bits

En consecuencia,

Total de espacio de memoria requerido en la computadora de Bernardo:

1072 bits = 134 bytes.

Comparación con el Algoritmo de Diffie-Hellman clásico.

Si L_n es la cantidad de dígitos binarios que tiene el número natural n , para el cálculo de $a^k \pmod{n}$, se supondrá que los números a y k ocupan también L_n dígitos binarios (pues a y k son números menores que p).

De este modo, la cantidad de espacio de memoria ocupado por cada variable que interviene en el algoritmo de la potencia modular se muestra en el siguiente cuadro:

<i>Espacio de memoria para:</i>	<i>Cantidad de bits requeridos</i>
n	L_n bits
a_i	$2 L_n$ bits. (pues $a_i \equiv a_{i-1}^2 \pmod{n}$)
c_i	$2 L_n$ bits. (pues $c_i = a_{i-1} \cdot c_{i-1} \pmod{n}$)
k_i	L_n bits.

Luego, para calcular $a^k \pmod{n}$ se necesitan $6 L_n$ bits de memoria.

Como Alicia calculará $g^a \pmod{p}$ e $y^a \pmod{p}$, mientras que Bernardo deberá computar $g^b \pmod{p}$ y $x^b \pmod{p}$, entonces

Total de espacio de memoria en la computadora de Alicia: $2(6L_p) \text{ bits} = 12 L_p \text{ bits}$

Total de espacio de memoria en la computadora de Bernardo: $2(6L_p) \text{ bits} = 12 L_p \text{ bits}$

Nuevamente, si se tiene en cuenta que “ p ” es un número primo muy grande y por lo tanto, tiene numerosos dígitos binarios, el Algoritmo de Diffie-Hellman empleando cuaterniones necesita mucho menos espacio de memoria que el Diffie-Hellman clásico.

La seguridad criptográfica del algoritmo radica en la dificultad para hallar la función $f(x)$ ó $h(x)$. Más precisamente, el “intruso” conoce q_A , q_B , m , n , r_A y r_B . Entonces podría ir probando cuál es la función $f(x)$ o $h(x)$ que verifica una de las ecuaciones:

$$r_A = [f_N(q_A)]^m \cdot q_B \cdot [f_N(q_A)]^n \text{ ó } r_B = [h_N(q_A)]^m \cdot q_B \cdot [h_N(q_A)]^n$$

De este modo, conociendo $f(x)$ o bien $h(x)$, el intruso descubriría la clave, ya que

$$k_A = [f_N(q_A)]^m \cdot r_B \cdot [f_N(q_A)]^n \text{ y } k_B = [h_N(q_A)]^m \cdot r_A \cdot [h_N(q_A)]^n$$

Pero ¿qué tan difícil es hallar $f(x)$ o $h(x)$? La siguiente Proposición prueba que si se emplea la “fuerza bruta” es muy difícil encontrarla, ya que la cantidad de funciones que verifican las hipótesis del algoritmo es sorprendentemente numerosa. Este hecho pone de manifiesto la seguridad criptográfica del algoritmo.

Proposición 4.5.9

Sea $q = a + b.i + c.j + d.k$ un cuaternión unitario, cuya forma trigonométrica es

$$q = \cos(\theta) + \sin(\theta) \cdot v'$$

Donde

$$\theta = \arccos(a), \quad 0 \leq \theta \leq \pi$$

$$v' = \begin{cases} 0 & \text{si } b = c = d = 0 \\ \frac{b.i + c.j + d.k}{|b.i + c.j + d.k|} & \text{en otro caso} \end{cases}$$

Entonces la cantidad total de los polinomios no nulos $f(x)$ a coeficientes y exponentes en $\mathbf{Z}_{16}$ que verifican que $f(q) \neq 0$ es:

$$\begin{cases} 16^{16} - 1 - 16^{14} & \text{si } v' \neq 0 \\ 16^{16} - 1 - 16^{15} & \text{si } v' = 0 \end{cases}$$

Demostración

Sea $\mathbf{Z}_{16}[x]$ el conjunto de polinomios a coeficientes en $\mathbf{Z}_{16}$ de grado menor o igual que 15. Es decir,

$$\mathbf{Z}_{16}[x] = \{a_0 + a_1.x + a_2.x^2 + \dots + a_{15}.x^{15} / a_i \in \mathbf{Z}_{16} \quad \forall i = 0, \dots, 15\}$$

Entonces, $\text{card}(\mathbf{Z}_{16}[x]) = 16^{16}$ pues los posibles valores de a_i son 16 con $i = 0, \dots, 15$.

Por lo tanto, por el Principio de la Multiplicación, el total de polinomios es 16^{16} .

Entonces, el total de polinomios no nulos en $\mathbf{Z}_{16}[x]$ es $16^{16} - 1$.

A continuación se determinará cuántos polinomios no nulos en $\mathbf{Z}_{16}[x]$ tienen a “ q ” como raíz. Sea $g(x) = a_0 + a_1 \cdot x + \dots + a_{15} \cdot x^{15} \in \mathbf{Z}_{16}[x]$ tal que $g(q) = 0$.

De la fórmula de De Moivre se tiene que:

$$q^n = (\cos(n\theta) + \text{sen}(n\theta) \cdot v')$$

Entonces, como $g(q) = 0$ resulta

$$\begin{aligned} a_0 + a_1 \cdot q + a_2 \cdot q^2 + \dots + a_{15} \cdot q^{15} &= 0 \Rightarrow \\ a_0 + a_1 \cdot (\cos(\theta) + \text{sen}(\theta) \cdot v') + a_2 \cdot (\cos(2\theta) + \text{sen}(2\theta) \cdot v') + \dots + \\ + a_{15} \cdot (\cos(15\theta) + \text{sen}(15\theta) \cdot v') &= 0 \end{aligned}$$

Al aplicar la propiedad distributiva y asociando convenientemente resulta:

$$\begin{aligned} [a_0 + a_1 \cdot \cos(\theta) + a_2 \cdot \cos(2\theta) + \dots + a_{15} \cdot \cos(15\theta)] + [a_1 \cdot \text{sen}(\theta) + a_2 \cdot \text{sen}(2\theta) + \dots + \\ + a_{15} \cdot \text{sen}(15\theta)] \cdot v' &= 0 \end{aligned}$$

Por igualdad de cuaterniones, se tiene:

$$\begin{cases} a_0 + a_1 \cdot \cos(\theta) + a_2 \cdot \cos(2\theta) + \dots + a_{15} \cdot \cos(15\theta) = 0 \\ [a_1 \cdot \text{sen}(\theta) + a_2 \cdot \text{sen}(2\theta) + \dots + a_{15} \cdot \text{sen}(15\theta)] \cdot v' = 0 \end{cases} \quad [1]$$

Se presentan dos casos:

Primer Caso: $v' \neq 0$

De [1] se obtiene

$$\begin{cases} a_0 + a_1 \cdot \cos(\theta) + a_2 \cdot \cos(2\theta) + \dots + a_{15} \cdot \cos(15\theta) = 0 \\ [a_1 \cdot \text{sen}(\theta) + a_2 \cdot \text{sen}(2\theta) + \dots + a_{15} \cdot \text{sen}(15\theta)] = 0 \end{cases} \quad [2]$$

Pero $\text{sen}(\theta) \neq 0$ pues si se supone por el absurdo que $\text{sen}(\theta) = 0$ entonces

$$\theta = 0 \text{ ó } \theta = \pi$$

Como

$$\begin{aligned} \theta = \arccos(a) \Rightarrow 0 = \arccos(a) \vee \pi = \arccos(a) \Rightarrow \cos(0) = a \vee \cos(\pi) = a \\ \Rightarrow 1 = a \vee -1 = a \end{aligned}$$

Por otro lado, como

$$|q| = 1 \Rightarrow \sqrt{a^2 + b^2 + c^2 + d^2} = 1 \Rightarrow a^2 + b^2 + c^2 + d^2 = 1 \Rightarrow$$

$\Rightarrow 1+b^2+c^2+d^2=1 \Rightarrow b^2+c^2+d^2=0 \Rightarrow b=c=d=0$, lo cual es una contradicción pues $v' \neq 0$.

Luego, como $\text{sen}(\theta) \neq 0$, de [2] resulta:

$$a_0 = -a_1 \cdot \cos(\theta) - a_2 \cdot \cos(2\theta) - \dots - a_{15} \cdot \cos(15\theta)$$

$$a_1 = \frac{-a_2 \cdot \text{sen}(2\theta) - a_3 \cdot \text{sen}(3\theta) - \dots - a_{15} \cdot \text{sen}(15\theta)}{\text{sen}(\theta)}$$

Por lo tanto, si $g(q)=0$ entonces sus coeficientes pueden tomar la siguiente cantidad de valores:

Para a_0 : 1

Para a_1 : 1

Para a_i : 16, con $i=2, \dots, 15$.

De este modo, el total de polinomios que tienen como raíz a “ q ” es 16^{14} . En consecuencia, si se considera el conjunto A definido por

$$A = \{ f(x) \in \mathbb{Z}_{16}[x] : f(x) \neq 0 \wedge f(q) \neq 0 \wedge v' \neq 0 \}$$

Entonces $\text{card}(A) = 16^{16} - 1 - 16^{14}$.

Segundo Caso: $v' = 0$

En este caso sólo se considera la primera ecuación del sistema [1], ya que la segunda de ellas es trivial. Es decir,

$$a_0 + a_1 \cdot \cos(\theta) + a_2 \cdot \cos(2\theta) + \dots + a_{15} \cdot \cos(15\theta) = 0.$$

Por lo tanto,

$$a_0 = -a_1 \cdot \cos(\theta) - a_2 \cdot \cos(2\theta) - \dots - a_{15} \cdot \cos(15\theta).$$

Luego, si $g(q)=0$ entonces sus coeficientes pueden tomar la siguiente cantidad de valores:

Para a_0 : 1

Para a_i : 16, con $i=1, \dots, 15$.

Así, el total de polinomios que tienen como raíz a “ q ” es 16^{15} . En consecuencia, si se considera el conjunto B definido por

$$B = \{ f(x) \in \mathbb{Z}_{16}[x] : f(x) \neq 0 \wedge f(q) \neq 0 \wedge v' = 0 \}$$

Entonces $\text{card}(B) = 16^{16} - 1 - 16^{15}$. ■

Se finaliza este capítulo mostrando el código fuente del programa que implementa el Algoritmo de Diffie-Hellman aplicando cuaterniones. El mismo fue diseñado mediante el software Wolfram Mathematica 10.0.

Programa que implementa el Algoritmo de Diffie-Hellman aplicado a cuaterniones.

```

Interpretation[{m = 0, n = 0, a = 0, b = 0, c = 0, d = 0, e = 0,
f = 0, g = 0, h = 0, f0 = 0, f1 = 0, f2 = 0, f3 = 0, f4 = 0, f5 = 0,
f6 = 0, f7 = 0, f8 = 0, f9 = 0, f10 = 0, f11 = 0, f12 = 0, f13 = 0,
f14 = 0, f15 = 0, h0 = 0, h1 = 0, h2 = 0, h3 = 0, h4 = 0, h5 = 0,
h6 = 0, h7 = 0, h8 = 0, h9 = 0, h10 = 0, h11 = 0, h12 = 0, h13 = 0,
h14 = 0, h15 = 0},
Panel[Grid[{
{Style[
"Ingresa dos números enteros positivos pertenecientes a \
 $\mathbb{Z}_{16}$  :", Bold], SpanFromLeft}, {"m=",
InputField[Dynamic[m], FieldSize -> 2]},
{"n=", InputField[Dynamic[n], FieldSize -> 2]},
{Style[
"Ingresa el cuaternión no nulo A, a coeficientes en \
 $\mathbb{Z}_{256}$  :", Bold], SpanFromLeft}, {"A=",
MatrixForm[{ {InputField[Dynamic[a], FieldSize -> 2], ",",
InputField[Dynamic[b], FieldSize -> 2], ",",
InputField[Dynamic[c], FieldSize -> 2], ",",
InputField[Dynamic[d], FieldSize -> 2]}]}],
{Style[
"Ingresa el cuaternión no nulo B, a coeficientes en \
 $\mathbb{Z}_{256}(\mathbb{Z}_{16})$  :", Bold],
SpanFromLeft}, {"B=",
MatrixForm[{ {InputField[Dynamic[e], FieldSize -> 2], ",",
InputField[Dynamic[f], FieldSize -> 2], ",",
InputField[Dynamic[g], FieldSize -> 2], ",",
InputField[Dynamic[h], FieldSize -> 2]}]}],
{Style[
"Ingresa los coeficientes del polinomio f(x)  $\mathbb{Z}_{16}[x]$  de Alice:", Bold],
SpanFromLeft}, {"f(x)=",
MatrixForm[{ {InputField[Dynamic[f0], FieldSize -> 2], "+",
InputField[Dynamic[f1], FieldSize -> 2], "x +",
InputField[Dynamic[f2], FieldSize -> 2],
 $x^2$  +",
InputField[Dynamic[f3], FieldSize -> 2],
 $x^3$  +",
InputField[Dynamic[f4], FieldSize -> 2],
 $x^4$  +",
InputField[Dynamic[f5], FieldSize -> 2],
 $x^5$  +",
InputField[Dynamic[f6], FieldSize -> 2],
 $x^6$  +",
InputField[Dynamic[f7], FieldSize -> 2],

```

```

"!\(\(*SuperscriptBox[\(x\), \((7)\)]\) +",
InputField[Dynamic[f8], FieldSize -> 2],
"!\(\(*SuperscriptBox[\(x\), \((8)\)]\) +",
InputField[Dynamic[f9], FieldSize -> 2],
"!\(\(*SuperscriptBox[\(x\), \((9)\)]\) +",
InputField[Dynamic[f10], FieldSize -> 2],
"!\(\(*SuperscriptBox[\(x\), \((10)\)]\) +",
InputField[Dynamic[f11], FieldSize -> 2],
"!\(\(*SuperscriptBox[\(x\), \((11)\)]\) +",
InputField[Dynamic[f12], FieldSize -> 2],
"!\(\(*SuperscriptBox[\(x\), \((12)\)]\) +",
InputField[Dynamic[f13], FieldSize -> 2],
"!\(\(*SuperscriptBox[\(x\), \((13)\)]\) +",
InputField[Dynamic[f14], FieldSize -> 2],
"!\(\(*SuperscriptBox[\(x\), \((14)\)]\) +",
InputField[Dynamic[f15], FieldSize -> 2],
"!\(\(*SuperscriptBox[\(x\), \((15)\)]\)")}},
TableSpacing -> {None, 0.1}}},

{Style[
  "Ingrese los coeficientes del polinomio h(x) \[Epsilon] \
!\(\(*SubscriptBox[\(Z\), \((16)\)]\) ) [x] de Bob:", Bold,
SpanFromLeft}, {"h(x)=",
MatrixForm[{ { InputField[Dynamic[h0], FieldSize -> 2], "+",
  InputField[Dynamic[h1], FieldSize -> 2], "x +",
  InputField[Dynamic[h2], FieldSize -> 2],
  "!\(\(*SuperscriptBox[\(x\), \((2)\)]\) +",
  InputField[Dynamic[h3], FieldSize -> 2],
  "!\(\(*SuperscriptBox[\(x\), \((3)\)]\) +",
  InputField[Dynamic[h4], FieldSize -> 2],
  "!\(\(*SuperscriptBox[\(x\), \((4)\)]\) +",
  InputField[Dynamic[h5], FieldSize -> 2],
  "!\(\(*SuperscriptBox[\(x\), \((5)\)]\) +",
  InputField[Dynamic[h6], FieldSize -> 2],
  "!\(\(*SuperscriptBox[\(x\), \((6)\)]\) +",
  InputField[Dynamic[h7], FieldSize -> 2],
  "!\(\(*SuperscriptBox[\(x\), \((7)\)]\) +",
  InputField[Dynamic[h8], FieldSize -> 2],
  "!\(\(*SuperscriptBox[\(x\), \((8)\)]\) +",
  InputField[Dynamic[h9], FieldSize -> 2],
  "!\(\(*SuperscriptBox[\(x\), \((9)\)]\) +",
  InputField[Dynamic[h10], FieldSize -> 2],
  "!\(\(*SuperscriptBox[\(x\), \((10)\)]\) +",
  InputField[Dynamic[h11], FieldSize -> 2],
  "!\(\(*SuperscriptBox[\(x\), \((11)\)]\) +",
  InputField[Dynamic[h12], FieldSize -> 2],
  "!\(\(*SuperscriptBox[\(x\), \((12)\)]\) +",
  InputField[Dynamic[h13], FieldSize -> 2],
  "!\(\(*SuperscriptBox[\(x\), \((13)\)]\) +",
  InputField[Dynamic[h14], FieldSize -> 2],
  "!\(\(*SuperscriptBox[\(x\), \((14)\)]\) +",
  InputField[Dynamic[h15], FieldSize -> 2],

```

```

"!\\(*SuperscriptBox[(x\\), (15\\)])")}},
  TableSpacing -> {None, 0.1}}
}, Spacings -> {0, 1}]],
(*Guardamos los coeficientes de f(x) y h(x) en los vectores ff y hh \
respectivamente *)

ff = {f0, f1, f2, f3, f4, f5, f6, f7, f8, f9, f10, f11, f12, f13,
  f14, f15};
hh = {h0, h1, h2, h3, h4, h5, h6, h7, h8, h9, h10, h11, h12, h13,
  h14, h15};

qA = {a, b, c, d}/Sqrt[a^2 + b^2 + c^2 + d^2];
qB = {e, f, g, h}/Sqrt[e^2 + f^2 + g^2 + h^2];

Print["La normalización del cuaternión A es:"];
Print["!\\(*SubscriptBox[(q\\), (A\\)])")= ", qA // MatrixForm, "=",
  N[qA] // MatrixForm];
Print["La normalización del cuaternión B es:"];
Print["!\\(*SubscriptBox[(q\\), (B\\)])")= ", qB // MatrixForm, "=",
  N[qB] // MatrixForm];

(*Expresamos qA en forma trigonométrica*)

angA = ArcCos[qA[[1]]];
If[b == 0 && c == 0 && d == 0,
  qAT = {Cos[angA], 0, 0, 0},
  qAT = {Cos[angA],
    Sin[angA] qA[[2]]/Sqrt[(qA[[2]])^2 + (qA[[3]])^2 + (qA[[4]])^2],
    Sin[angA] qA[[3]]/Sqrt[(qA[[2]])^2 + (qA[[3]])^2 + (qA[[4]])^2],
    Sin[angA] qA[[4]]/Sqrt[(qA[[2]])^2 + (qA[[3]])^2 + (qA[[4]])^2]}
];

(*Calculamos f(qA) *)

fqA = {f0, 0, 0, 0};

For[ k = 2, k <= 16, k++,

  If[ff[[k]] != 0,
    fqA =
      fqA + ff[[k]]*{Cos[(k - 1) angA],
        Sin[(k - 1) angA] qA[[2]]/
          Sqrt[(qA[[2]])^2 + (qA[[3]])^2 + (qA[[4]])^2],
        Sin[(k - 1) angA] qA[[3]]/
          Sqrt[(qA[[2]])^2 + (qA[[3]])^2 + (qA[[4]])^2],
        Sin[(k - 1) angA] qA[[4]]/
          Sqrt[(qA[[2]])^2 + (qA[[3]])^2 + (qA[[4]])^2]}

  ]
]
Print["f\\(*SubscriptBox[(q\\), (A\\)])")= ",
  N[fqA] // MatrixForm];

```

```

(*Normalizamos f(qA) *)

fqANorm = fqA/Norm[fqA];
Print["f(\(*SubscriptBox[\(q\), \(\A\)])\) normalizado es:"];
Print["!(\(*SubscriptBox[\(f\), \(\n\)])\)(!\(*SubscriptBox[\(q\), \(\A\)])\)]=", N[fqANorm] // MatrixForm];

(*Expresamos f(qA) normalizado en forma trigonométrica*)

angfqANorm = ArcCos[fqANorm[[1]]];
fqANormT = {Cos[angfqANorm],
Sin[angfqANorm] fqANorm[[2]]/
Sqrt[(fqANorm[[2]])^2 + (fqANorm[[3]])^2 + (fqANorm[[4]])^2],
Sin[angfqANorm] fqANorm[[3]]/
Sqrt[(fqANorm[[2]])^2 + (fqANorm[[3]])^2 + (fqANorm[[4]])^2],
Sin[angfqANorm] fqANorm[[4]]/
Sqrt[(fqANorm[[2]])^2 + (fqANorm[[3]])^2 + (fqANorm[[4]])^2]};

(*Calculamos (fn(qA))^m *)

fqAm = {Cos[m *angfqANorm],
Sin[m *angfqANorm] fqANorm[[2]]/
Sqrt[(fqANorm[[2]])^2 + (fqANorm[[3]])^2 + (fqANorm[[4]])^2],
Sin[m *angfqANorm] fqANorm[[3]]/
Sqrt[(fqANorm[[2]])^2 + (fqANorm[[3]])^2 + (fqANorm[[4]])^2],
Sin[m *angfqANorm] fqANorm[[4]]/
Sqrt[(fqANorm[[2]])^2 + (fqANorm[[3]])^2 + (fqANorm[[4]])^2]};

(*Calculamos (fn(qA))^n *)

fqAn = {Cos[n *angfqANorm],
Sin[n *angfqANorm] fqANorm[[2]]/
Sqrt[(fqANorm[[2]])^2 + (fqANorm[[3]])^2 + (fqANorm[[4]])^2],
Sin[n *angfqANorm] fqANorm[[3]]/
Sqrt[(fqANorm[[2]])^2 + (fqANorm[[3]])^2 + (fqANorm[[4]])^2],
Sin[n *angfqANorm] fqANorm[[4]]/
Sqrt[(fqANorm[[2]])^2 + (fqANorm[[3]])^2 + (fqANorm[[4]])^2]};

(* Cálculo de rA. En este caso, AuxProd=(fn(Subscript[q, \
A]))^mSubscript[q, B] *)

AuxProd = {fqAm[[1]]*qB[[1]] - fqAm[[2]]*qB[[2]] -
fqAm[[3]]*qB[[3]] - fqAm[[4]]*qB[[4]],
fqAm[[1]]*qB[[2]] + fqAm[[2]]*qB[[1]] + fqAm[[3]]*qB[[4]] -
fqAm[[4]]*qB[[3]],
fqAm[[1]]*qB[[3]] - fqAm[[2]]*qB[[4]] + fqAm[[3]]*qB[[1]] +
fqAm[[4]]*qB[[2]],
fqAm[[1]]*qB[[4]] + fqAm[[2]]*qB[[3]] - fqAm[[3]]*qB[[2]] +
fqAm[[4]]*qB[[1]]};

```

```

rA = {AuxProd[[1]]*fqAn[[1]] - AuxProd[[2]]*fqAn[[2]] -
      AuxProd[[3]]*fqAn[[3]] - AuxProd[[4]]*fqAn[[4]],
      AuxProd[[1]]*fqAn[[2]] + AuxProd[[2]]*fqAn[[1]] +
      AuxProd[[3]]*fqAn[[4]] - AuxProd[[4]]*fqAn[[3]],
      AuxProd[[1]]*fqAn[[3]] - AuxProd[[2]]*fqAn[[4]] +
      AuxProd[[3]]*fqAn[[1]] + AuxProd[[4]]*fqAn[[2]],
      AuxProd[[1]]*fqAn[[4]] + AuxProd[[2]]*fqAn[[3]] -
      AuxProd[[3]]*fqAn[[2]] + AuxProd[[4]]*fqAn[[1]]};

Print["!\(\\(*SubscriptBox[\\(r\\), \\(A\\)])\\)=", N[rA] // MatrixForm];

(*Calculamos h(qA) *)

hqA = {h0, 0, 0, 0};

For[ k = 2, k <= 16, k++,

  If[h0[[k]] != 0,
    hqA =
      hqA + hh[[k]]*{Cos[(k - 1) angA],
        Sin[(k - 1) angA] qA[[2]]/
        Sqrt[(qA[[2]]^2 + (qA[[3]]^2 + (qA[[4]]^2),
        Sin[(k - 1) angA] qA[[3]]/
        Sqrt[(qA[[2]]^2 + (qA[[3]]^2 + (qA[[4]]^2),
        Sin[(k - 1) angA] qA[[4]]/
        Sqrt[(qA[[2]]^2 + (qA[[3]]^2 + (qA[[4]]^2)}

  ]
]

Print["h!\(\\(*SubscriptBox[\\(q\\), \\(A\\)])\\)=",
      N[hqA] // MatrixForm];

(*Normalizamos h(qA) *)
hqANorm = hqA/Norm[hqA];
Print["h!\(\\(*SubscriptBox[\\(q\\), \\(A\\)])\\) normalizado es:"];
Print["!\(\\(*SubscriptBox[\\(h\\), \\(n\\)])\\)!\(\\(*SubscriptBox[\\(q\\), \\(A\\)])\\)=", N[hqANorm] // MatrixForm];

(*Expresamos h(qA) normalizado en forma trigonométrica*)

anghqANorm = ArcCos[hqANorm[[1]]];
hqANormT = {Cos[anghqANorm],
  Sin[anghqANorm] hqANorm[[2]]/
  Sqrt[(hqANorm[[2]]^2 + (hqANorm[[3]]^2 + (hqANorm[[4]]^2),
  Sin[anghqANorm] hqANorm[[3]]/
  Sqrt[(hqANorm[[2]]^2 + (hqANorm[[3]]^2 + (hqANorm[[4]]^2),
  Sin[anghqANorm] hqANorm[[4]]/
  Sqrt[(hqANorm[[2]]^2 + (hqANorm[[3]]^2 + (hqANorm[[4]]^2)}];

(*Calculamos (hn(qA))^m *)

```

```

hqAm = {Cos[m * anghqANorm],
Sin[m * anghqANorm] hqANorm[[2]]/
Sqrt[(hqANorm[[2]])^2 + (hqANorm[[3]])^2 + (hqANorm[[4]])^2],
Sin[m * anghqANorm] hqANorm[[3]]/
Sqrt[(hqANorm[[2]])^2 + (hqANorm[[3]])^2 + (hqANorm[[4]])^2],
Sin[m * anghqANorm] hqANorm[[4]]/
Sqrt[(hqANorm[[2]])^2 + (hqANorm[[3]])^2 + (hqANorm[[4]])^2]};

```

(*Calculamos (hn(qA))^n *)

```

hqAn = {Cos[n * anghqANorm],
Sin[n * anghqANorm] hqANorm[[2]]/
Sqrt[(hqANorm[[2]])^2 + (hqANorm[[3]])^2 + (hqANorm[[4]])^2],
Sin[n * anghqANorm] hqANorm[[3]]/
Sqrt[(hqANorm[[2]])^2 + (hqANorm[[3]])^2 + (hqANorm[[4]])^2],
Sin[n * anghqANorm] hqANorm[[4]]/
Sqrt[(hqANorm[[2]])^2 + (hqANorm[[3]])^2 + (hqANorm[[4]])^2]};

```

(* Cálculo de rB. En este caso, AuxProd=(hn(Subscript[q, \
A]))^mSubscript[q, B]*)

```

AuxProd = {hqAm[[1]]*qB[[1]] - hqAm[[2]]*qB[[2]] -
hqAm[[3]]*qB[[3]] - hqAm[[4]]*qB[[4]],
hqAm[[1]]*qB[[2]] + hqAm[[2]]*qB[[1]] + hqAm[[3]]*qB[[4]] -
hqAm[[4]]*qB[[3]],
hqAm[[1]]*qB[[3]] - hqAm[[2]]*qB[[4]] + hqAm[[3]]*qB[[1]] +
hqAm[[4]]*qB[[2]],
hqAm[[1]]*qB[[4]] + hqAm[[2]]*qB[[3]] - hqAm[[3]]*qB[[2]] +
hqAm[[4]]*qB[[1]]};

```

```

rB = {AuxProd[[1]]*hqAn[[1]] - AuxProd[[2]]*hqAn[[2]] -
AuxProd[[3]]*hqAn[[3]] - AuxProd[[4]]*hqAn[[4]],
AuxProd[[1]]*hqAn[[2]] + AuxProd[[2]]*hqAn[[1]] +
AuxProd[[3]]*hqAn[[4]] - AuxProd[[4]]*hqAn[[3]],
AuxProd[[1]]*hqAn[[3]] - AuxProd[[2]]*hqAn[[4]] +
AuxProd[[3]]*hqAn[[1]] + AuxProd[[4]]*hqAn[[2]],
AuxProd[[1]]*hqAn[[4]] + AuxProd[[2]]*hqAn[[3]] -
AuxProd[[3]]*hqAn[[2]] + AuxProd[[4]]*hqAn[[1]]};

```

```
Print["!\(\\(*SubscriptBox[\\(r\\), \\(B\\)]\\)=", N[rB] // MatrixForm];
```

(* Cálculo de kA. En este caso, AuxProd=(fn(Subscript[q, \
A]))^mSubscript[r, B] *)

```

AuxProd = {fqAm[[1]]*rB[[1]] - fqAm[[2]]*rB[[2]] -
fqAm[[3]]*rB[[3]] - fqAm[[4]]*rB[[4]],
fqAm[[1]]*rB[[2]] + fqAm[[2]]*rB[[1]] + fqAm[[3]]*rB[[4]] -
fqAm[[4]]*rB[[3]],
fqAm[[1]]*rB[[3]] - fqAm[[2]]*rB[[4]] + fqAm[[3]]*rB[[1]] +
fqAm[[4]]*rB[[2]],
fqAm[[1]]*rB[[4]] + fqAm[[2]]*rB[[3]] - fqAm[[3]]*rB[[2]] +
fqAm[[4]]*rB[[1]]};

```

```
kA = {AuxProd[[1]]*fqAn[[1]] - AuxProd[[2]]*fqAn[[2]] -
```

```

AuxProd[[3]]*fqAn[[3]] - AuxProd[[4]]*fqAn[[4]],
AuxProd[[1]]*fqAn[[2]] + AuxProd[[2]]*fqAn[[1]] +
AuxProd[[3]]*fqAn[[4]] - AuxProd[[4]]*fqAn[[3]],
AuxProd[[1]]*fqAn[[3]] - AuxProd[[2]]*fqAn[[4]] +
AuxProd[[3]]*fqAn[[1]] + AuxProd[[4]]*fqAn[[2]],
AuxProd[[1]]*fqAn[[4]] + AuxProd[[2]]*fqAn[[3]] -
AuxProd[[3]]*fqAn[[2]] + AuxProd[[4]]*fqAn[[1]]};

Print["\\(\\(*SubscriptBox[\\(k\\), \\(A\\)]\\)=", N[kA] // MatrixForm];

(* Cálculo de kB. En este caso, AuxProd=(hn(Subscript[q, \\
A]))^mSubscript[r, A] *)

AuxProd = {hqAm[[1]]*rA[[1]] - hqAm[[2]]*rA[[2]] -
hqAm[[3]]*rA[[3]] - hqAm[[4]]*rA[[4]],
hqAm[[1]]*rA[[2]] + hqAm[[2]]*rA[[1]] + hqAm[[3]]*rA[[4]] -
hqAm[[4]]*rA[[3]],
hqAm[[1]]*rA[[3]] - hqAm[[2]]*rA[[4]] + hqAm[[3]]*rA[[1]] +
hqAm[[4]]*rA[[2]],
hqAm[[1]]*rA[[4]] + hqAm[[2]]*rA[[3]] - hqAm[[3]]*rA[[2]] +
hqAm[[4]]*rA[[1]]};

kB = {AuxProd[[1]]*hqAn[[1]] - AuxProd[[2]]*hqAn[[2]] -
AuxProd[[3]]*hqAn[[3]] - AuxProd[[4]]*hqAn[[4]],
AuxProd[[1]]*hqAn[[2]] + AuxProd[[2]]*hqAn[[1]] +
AuxProd[[3]]*hqAn[[4]] - AuxProd[[4]]*hqAn[[3]],
AuxProd[[1]]*hqAn[[3]] - AuxProd[[2]]*hqAn[[4]] +
AuxProd[[3]]*hqAn[[1]] + AuxProd[[4]]*hqAn[[2]],
AuxProd[[1]]*hqAn[[4]] + AuxProd[[2]]*hqAn[[3]] -
AuxProd[[3]]*hqAn[[2]] + AuxProd[[4]]*hqAn[[1]]};
Print["\\(\\(*SubscriptBox[\\(k\\), \\(B\\)]\\)=", N[kB] // MatrixForm];

(* Ahora calculamos las claves Subscript[k, A] y Subscript[K, B] *)

KA = Mod[IntegerPart[kA * 256], 256];
Print["La clave de Alice es:"];
Print["\\(\\(*SubscriptBox[\\(K\\), \\(A\\)]\\)=", KA // MatrixForm];

KB = Mod[IntegerPart[kB * 256], 256];
Print["La clave de Bob es:"];
Print["\\(\\(*SubscriptBox[\\(K\\), \\(B\\)]\\)=", KB // MatrixForm];

]

```

Conclusiones

El Algoritmo de Diffie-Hellman aplicado a cuaterniones, desarrollado en la presente tesis, permite generar claves en plataformas de porte reducido. Por otro lado, en relación al Algoritmo de Diffie-Hellman clásico, disminuye significativamente el tiempo de ejecución y el espacio de memoria requerido para generar dichas claves, sin sacrificar la seguridad criptográfica.

Además, se lo ha caracterizado como “compacto” porque no requiere el uso de bibliotecas de precisión extendida y por ende es aplicable a entornos de bajo poder computacional y memoria RAM escasa, como por ejemplo smartcards y firma digital.

Una vez más se pone de manifiesto que la Matemática está siempre presente, ya que conceptos matemáticos tan abstractos como los cuaterniones, pueden ser aplicados a situaciones de la vida real.

Bibliografía

- [1] Diffie, W. & Hellman, M.E. “*New Directions in Cryptography*”. IEE Transactions on Information Theory 22. Pp. 644-654, 1976.
- [2] Kamlofsky, J. & Hecht, P. “*A Diffie-Hellman Compact Model over Non-Commutative Rings using quaternions*”. VIII Congreso de Seguridad Informática CIBSI. Quito (Ecuador), 2015.
- [3] Xifré Solana, P. “*Antecedentes y perspectivas de estudio en historia de la Criptografía*”. Trabajo Final de Ingeniería Técnica en Informática de Gestión. Universidad Carlos III de Madrid (España), 2009.
- [4] Magliveras S., Stinson D.R. & Van Trung, T. “*New approaches to designing public key cryptosystems one-way functions and trapdoors in finite groups*”. Technical Report CORR. Pp. 200-2049, 2000.
- [5] Shor, P. “*Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*”. SIAM J. Comput. Pp 1484-1509, 1997.
- [6] Sánchez Fernández, P. “*Sistema de Gestión de la Ciberseguridad Industrial*”. Trabajo Final de Maestría en Ingeniería Informática. Escuela Politécnica de Ingeniería de Gijón. Universidad de Oviedo (España), 2013.
- [7] Granado Peralta, S. “*Matemática Discreta*”. Ed. CEIT. Buenos Aires, 2002.
- [8] Rojo, Armando. “*Álgebra I*”. Ed. El Ateneo. Buenos Aires, 1982.
- [9] Dorronsoro, J. & Fernández, E. “*Números, Grupos y Anillos*”. Ed. Addison Wesley Iberoamericana. Madrid, 1997.
- [10] https://es.wikipedia.org/wiki/Peque%C3%B1o_teorema_de_Fermat
- [11] Somma, Francisco Javier. “*Cuaterniones y rotaciones en el espacio tridimensional*”. Tesis de Licenciatura en Matemática. Directora: Bergamini, María Lorena. Universidad Abierta Interamericana. Buenos Aires, 2018.
- [12] Oviedo, Pablo Andrés. “*Fundamentos Matemáticos de Computación Cuántica en el Algoritmo de Shor, para la factorización prima de números enteros*”. Tesis de Licenciatura en Matemática. Directora: Abdel Masih, Samira. Universidad Abierta Interamericana. Buenos Aires, 2017.