UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO"

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE MATEMÁTICA

" Descifrado de Información Mediante Internet Usando el Teorema Chino de los Restos "

TESIS

Para optar el título profesional de Licenciado en Matemáticas

Presentado por:

Chero Custodio Yanina Emilia

García Llauce Rosa Magaly

Asesor

Lic. Mat. Dolores Sánchez García

LAMBAYEQUE - PERÚ

2016

UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO"
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
ESCUELA PROFESIONAL DE MATEMÁTICA

" Descifrado de Información Mediante Internet Usando el Teorema Chino de los Restos "

TESIS

Para optar el título profesional de Licenciado en Matemáticas

Presentado por:

Chero Custodio Yanina Emilia

Garcia Llauce Rosa Magaly

Asesor:

Lic.Mat. Dolores Sánchez García

LAMBAYEQUE – PERÚ

2016

UNIVERSIDAD NACIONAL" PEDRO RUIZ GALLO"

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE MATEMÁTICA

Los firmantes,por la presente certifican que han leído y recomiendan a la Facultad de Ciencias Físicas y Matemáticas la aceptación de la tesis titulada **"Descifrado de información mediante internet usando el teorema chino de los restos"**,presentada por las Bachilleres en Matemáticas,Chero Custodio Yanina Emilia y Garcia Llauce Rosa Magaly , en el cumplimiento parcial de los requisitos necesarios para la obtención del título profesional de Licenciado en Matemáticas.

Dr. Cárpena Velásquez Enrique Wilfredo
Presidente Jurado de Tesis

Mg. Malca Villalobos Amado
Secretario Jurado de Tesis

Mg. Cuti Gutiérrez Raúl Alcides
Vocal Jurado de Tesis

Fecha de Defensa: Marzo - 2016

UNIVERSIDAD NACIONAL" PEDRO RUIZ GALLO"
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
ESCUELA PROFESIONAL DE MATEMÁTICA

" Descifrado de Información Mediante Internet Usando el Teorema Chino de los Restos "

Bach. Mat. Chero Custodio Yanina Emilia
Autor

Bach. Mat. García Llauce Rosa Magaly
Autor

Lic.Mat. Dolores Sánchez García
Asesor

Lambayeque – Perú
Marzo - 2016

Agradecimiento

Son muchas las personas especiales a las que me gustaría agradecer su amistad, apoyo, ánimo y compañía en las diferentes etapas de mi vida. Algunas están aquí conmigo y algunas en mis recuerdos y en el corazón. Sin importar en donde estén o si alguna vez llegan a leer estas dedicatorias quiero darles las gracias por formar parte de mí, por todo lo que me han brindado y por todas sus bendiciones.

Magaly

Agradezco a Dios por protegerme durante todo mi camino y darme fuerzas para superar obstáculos y dificultades a lo largo de toda mi vida. A mis padres ANDREA y FELICIANO, mi tío (a) JUAN y BERTHA por darme la oportunidad de estudiar y guiarme como lo han hecho, hasta hora, a mis hermanos (a) por poyarme y estar presente para lo que necesito , a mi sobrinos ALESHKA JHANELLY, JESÚS FELICIANO que me da la alegría, la esperanza el deseo de salir adelante,a mis amigas SANDRA MIRELLA, ROSA MAGALY, LILIANA por su comprensión. Mil palabras no bastarían para agradecerles su apoyo, su comprensión y sus consejos en los momentos difíciles. A todos, espero no defraudarlos y contar siempre con su apoyo, sincero e incondicional

Yanina

Dedicatoria

Dedico esta tesis a DIOS quien con su gran misericordia y amor inspira día a día mi vida e hizo posible la conclusión de esta tesis.
A mis Padres: Rosa Emilia y Filomeno quienes me dieron vida, educación, apoyo y consejos.
A mis hermanos Edwin, Wiliam y Carlos Enrique por brindarme su amor.
A mis grandes amores:
Mi esposo Elmer quien con su apoyo incondicional me alentó para continuar en los momentos más difíciles y a mi hijo Nixon Enrique quien es y será siempre el motor de mi vida por el cual vale la pena seguir luchando.
A mis amigas de estudio Yanina, Liliana, Yesenia, Sandra, Yris y Rocío quienes fueron un gran apoyo emocional durante el tiempo en que escribía esta tesis.
A nuestro asesor de tesis Mg. Dolores Sánches Garcia quien nunca desistió al enseñarnos. Los quiero mucho ···

Magaly

Dedico esta tesis principalmente a Dios, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional.
A mis padres ANDREA y FELICIANO quienes con mucho cariño, amor y ejemplo han hecho de mí una persona con valores.
A mis tíos JUAN y BERTHA quienes han velado por mí durante este arduo camino.
A mis hermanos(a) que siempre ha estado junto a mí, brindándome su apoyo.
Agradezco también a mi asesor de tesis al Mg. Dolores Sánchez García por haber brindado la oportunidad de recurrir a su capacidad y conocimiento, así como también haber tenido toda la paciencia del mundo para guiarnos durante todo el desarrollo de la tesis.

Yanina Emilia

Resumen

El teorema chino de los restos tiene importantes aplicaciones, en diversas ciencias, como por ejemplo, en astronomía (se usa en la determinación del periodo en que ocurren la conjunción de los planetas y eclipses), en cronología (se usa para calcular el paso de los sistemas del año solar, año dorado y año de interdicción) y en criptografía (para reducir operaciones con números grandes mediante el paso a congruencias modulo n). Por esta razón este trabajo de investigación, se centra en el estudio del cifrado y descifrado de información mediante internet aplicando el teorema chino de los restos. Para ello, primero se presenta un estudio de la teoría de divisibilidad, el algoritmo de Euclides, la identidad de Bezout, el teorema fundamental de la aritmética, teoría de anillos y de los números primos, aritmética modular, congruencia modulo n. Estos resultados se usan para la demostración del teorema chino de los restos.

Luego se hace un breve recorrido sobre el sistema creado por Ronald Rivest, Adi Shamir y Leonard Adleman (RSA), a continuación para poner de manifiesto la utilidad práctica de la teoría desarrollada en este trabajo se presentan dos aplicaciones de la teoría estudiada, específicamente, se muestra una aplicación de la identidad de Bezout en el cifrado y descifrado de información para el sistema creado por Ronald Rivest, Adi Shamir y Leonard Adleman (RSA) así como también se muestra una aplicación del teorema chino de los restos en el cifrado y descifrado de imágenes digitales, mediante el uso de clave pública y clave privada usando números primos grandes. Mostrándose así la utilidad del trabajo en la seguridad del envío de información ya sea mediante mensajes o imágenes digitales.

Abstract

The Chinese remainder theorem has important applications in various sciences, such as astronomy (used in determining the period in which the conjunction of the planets and eclipses occur) in chronology (used to calculate the passage of systems of the solar year, dorado year and year ban) and cryptography (to reduce operations with large numbers by passage congruences modulo n). Therefore this research , focuses on the study of encryption and decryption of information through internet using the Chinese remainder theorem. For this, first a study of the theory of divisibility, the Euclidean algorithm, Bezout's identity, the fundamental theorem of arithmetic, theory of rings and prime numbers, modular arithmetic, congruence modulo n is presented. These results are used to show the Chinese remainder theorem.

A brief on the system created by Ronald Rivest, Adi Shamir and Leonard Adleman (RSA), then to highlight the practical utility of the theory developed in this paper is then made two applications of the theory are presented studied specifically an application of the Bezout identity in encryption and decryption shows information for the system created by Ronald Rivest, Adi Shamir and Leonard Adleman (RSA) as well as an application of the Chinese remainder theorem is also shown in encryption and decryption digital images, using public key and private key using large prime numbers. Thus showing the usefulness of labor safety delivery information either through messages or digital images.

Introducción

En esta tesis, se hace un estudio bibliográfico sobre la aplicación de la teoría de los anillos modulares para el cifrado y descifrado de mensajes, como por ejemplo: se estudia el encriptado y desencriptado de mensajes y de imágenes utilizando el teorema chino de los restos.

La tesis se divide en tres capítulos:

En el primer capítulo, revisamos el marco teórico y resultados de la teoría de divisibilidad. Además se enuncia y demuestra el teorema del Algoritmo de la división, en la sección 1.1, se revisan definiciones que permiten demostrar el algoritmo de la división, en la sección 1.2 se estudia la definición y propiedades de la Divisibilidad, en la sección 1.3 se estudia los Números Primos y sus propiedades, en la sección 1.4 se estudia el máximo común divisor y propiedades, 1.5 se enuncia y demuestra el algoritmo de Euclides, en la sección 1.6 se demuestra el teorema fundamental de la aritmética, en la sección 1.7 se estudia el mínimo común múltiplo y sus propiedades.

En el segundo capítulo, se revisa la definición y propiedades de la estructura de anillo, sobre la cual se realizan las operaciones aritméticas como adición, sustracción, multiplicación y división, en la sección 2.1, se estudian los preliminares, en la sección 2.2 se estudia el Producto Cartesiano, en la sección 2.3 se estudia Funciones, en la sección 2.4 se estudia Operaciones Binarias Internas, en la sección 2.5 se presentan las definiciones y propiedades de un anillo, en la sección 2.6 se estudia la definición y propiedades de un cuerpo, en la sección 2.7, se estudia los anillos modulares, específicamente se estudia la aritmética modular, en la sección 2.8 se demuestra el Teorema de los Restos Chinos.

En el tercer capítulo, se estudia el cifrado de información en el sistema RSA utilizando

el teorema chino de los restos, en la sección 3.1, se revisa la criptografía simétrica y asimétrica, en la sección 3.2 se hace un breve estudio del sistema RSA, en la sección 3.3 se estudia la función de Euler y sus propiedades , en la sección 3.4 se estudia el Encriptado y Desencriptado de la información, en la sección 3.5 se presentan dos aplicaciones del teorema chino de los restos en el cifrado de información para el sistema RSA.

Índice general

Capítulo 1:

Elementos de Teoría de Números

En este capítulo se revisan definiciones y resultado de la teoría de divisibilidad. Además se enuncia y demuestra el teorema del Algoritmo de la división, un resultado importante para el desarrollo del presente trabajo.

1.1 Algoritmo de la División

En esta sección revisamos el enunciado y la demostración del teorema del algoritmo de la división herramienta útil, para implementar la técnica de cifrado mediante el teorema chino de los restos. Iniciemos recordando el principio del buen orden.

Principio del Buen Orden:
Todo conjunto no vacío de números naturales contiene un elemento mínimo.

En particular, si $S \subset \mathbb{Z}$ y si S tiene al menos un elemento positivo, entonces S tiene un entero positivo mínimo.

Ejemplo 1.1. Si $a, b \in \mathbb{Z}$ con $b \geqslant 1$ entonces existe $q \in \mathbb{Z}$ tal que: $qb \leqslant a < (q+1)b$

Demostración.

Se usará el principio del buen orden para demostrar la existencia de $q \in \mathbb{Z}$, defínase:

$$S = \{a - nb : n \in \mathbb{Z} \ \ y \ \ a - nb \geq 0\}$$

Ahora se demuestra que $S \neq 0$

- Si $a \geq 0$,entonces se puede escribir $a = a - 0 \cdot b, \ 0 \in \mathbb{Z}$, de donde $a \in S$.
- Si $a < 0$, entonces se puede escribir $a - ab = a(1 - b)$, puesto que
  $b \geq 1 \longrightarrow 1 - b \leq 0$ y como $a < 0$ entonces $a - ab = a(1 - b) \geq 0$,
  de donde $a - ab \in S$
  De lo anterior se deduce que $S \neq 0$

  Luego de acuerdo con el principio del buen orden tiene S un elemento mínimo
  $a - qb \geq 0, \ q \in \mathbb{Z}$
  De otro lado como $q \leq q + 1 \rightarrow qb \leq (q + 1)b \rightarrow -qb \geq -(q + 1)b$

$$\longrightarrow a - qb \geq a - (q + 1)b \tag{1.1}$$

Si ocurriese $a - (q + 1)b \geq 0$, entonces como $(q + 1) \in \mathbb{Z}$ se tiene que $a - (q + 1)b \in S$, luego de acuerdo con la ecuación (1.1) se deduce que $a - qb$ no es el elemento mínimo de S , lo cual es una contradicción, de donde se deduce que $a - (q + 1)b < 0$
Ahora como:

- $a - qb \geq 0 \longrightarrow qb \leq a$
- $a - (q + 1)b < 0 \longrightarrow a < (q + 1)b$

De lo anterior se deduce que existe $q \in \mathbb{Z}$ tal que:

$$qb \leq a < (q + 1)b \quad \blacksquare$$

1.2 Divisibilidad

La siguiente definición es útil en la demostración del teorema del algoritmo de la división.

Definición 1.1. Sean a, b enteros con $b \neq 0$. Decimos que b divide a a si existe un entero c tal que $a = bc$.

Si b divide a a escribimos $\frac{b}{a}$.

Ejemplo 1.2. Sean $a = 15$; $b = 3$, entonces como $c = 5 \in \mathbb{Z}$ y además se cumple que: $a = bc$ puesto que $15 = (3)(5)$ se tiene que 3 *divide* a 15 .

El siguiente resultado proporciona propiedades sobre la divisibilidad de un número.

Teorema 1.1. *Sean $a, b, d, p, q \in \mathbb{Z}$ entonces:*

a) si $\frac{d}{a}$ *y* $\frac{d}{b}$ *entonces* $\frac{d}{ax+by}$ $\forall x, y \in \mathbb{Z}$

b) si $\frac{d}{p+q}$ *y* $\frac{d}{p}$ *entonces* $\frac{d}{q}$

Demostración.

a) Si $\frac{d}{a} \longrightarrow \exists\, n \in \mathbb{Z}$ tal que $a = nd$

Si $\frac{d}{b} \longrightarrow \exists\, m \in \mathbb{Z}$ tal que $b = md$

Luego $ax + by = ndx + mdy = (nx + my)d$, $nx + my \in \mathbb{Z}$ entonces $\frac{d}{ax+by}$

b) Si $\frac{d}{p+q} \longrightarrow \exists\, n \in \mathbb{Z}$ tal que $p + q = nd$

Si $\frac{d}{p} \longrightarrow \exists\, m \in \mathbb{Z}$ tal que $p = md$

Luego $p + q = md + q$ y como $p + q = nd$ entonces $md + q = nd$

Si $md + q = nd \longrightarrow q = (n - m)d$

Por lo tanto

$$\frac{d}{q} \blacksquare$$

Recordemos que si la división de a por b no es exacta, entonces podemos expresar esta división como un cociente más un resto.

Por ejemplo la división de 21 por 2 es 10 con resto $r = 1$, es decir: $21 = (10)(2)+1$

Formalmente se tiene el siguiente teorema.

Teorema 1.2. ***(Algoritmo de la división):***

Sean $a, b \in \mathbb{Z}$ *existen únicos* $q, r \in \mathbb{Z}$ *tales que:* $a = bq + r$*; con* $0 \leq r <\mid b \mid$

Demostración.

Primero se demuestra el resultado para $a, b \in \mathbb{Z}$ con $b > 0$, considérese la progresión aritmética.

$$\cdots - 3b, -2b, -b, 0, b, 2b, 3b, \cdots$$

Como consecuencia del principio del buen orden en el ejemplo 1 se demostró que existe $q \in \mathbb{Z}$ tal que

$$qb \leq a < (q + 1)b$$

Sea $r = a - qb \in \mathbb{Z}$ entonces $a = bq + r$; además $r = a - qb \geq 0$ y como $a < (q + 1)b$ entonces $r = a - qb < b =\mid b \mid$, es decir $r < b$

Por lo tanto existen $q, r \in \mathbb{Z}$ tales que:

$$a = bq + r; con\ 0 \leq r <\mid b \mid = b$$

La Unicidad: Se demuestra por contradicción.

Supóngase que existe $q_1, r_1 \in \mathbb{Z}$ tal que $a = bq_1 + r_1$; *con* $0 \leq r_1 < b$ y

$a = bq + r$; *con* $0 \leq r < b$

Supongamos que $r_1 \neq r$ y que $r > r_1$

Puesto que: $bq_1 + r_1 = a = bq + r \longrightarrow bq_1 - bq = r - r_1$

$$\longrightarrow b(q_1 - q) = r - r_1 \cdots (*)$$

De donde b divide a $r - r_1$

$$\longrightarrow r - r_1 \geq b \cdots (**)$$

De otro lado $r_1 > 0 \longrightarrow -r_1 < 0 \longrightarrow 0 < r - r_1 < r < b$

$\longrightarrow 0 < r - r_1 < b$ lo cual contradice (*)

$$Luego \;\; r = r_1$$

Puesto que por (*) se tiene que:

$b(q_1 - q) = r - r_1 \longrightarrow b(q_1 - q) = 0 \longrightarrow q_1 - q = 0 \longrightarrow q_1 = q$

Ahora se demuestra el resultado para $a, b \in \mathbb{Z}$ con $b < 0$, por el caso anterior existen únicos $q, r \in \mathbb{Z}$ tales que:

$$a = \mid b \mid q + r; con \; 0 \leq r < \mid b \mid$$

De donde:

$$a = b(-q) + r; con \; 0 \leq r < \mid b \mid, -q \in \mathbb{Z} \quad \blacksquare$$

1.3 Números Primos

En este trabajo los llamados **números primos** juegan un rol muy importante, razón por la cual en la siguiente sección revisamos su definición y algunas de sus propiedades que nos serán de utilidad.

Definición 1.2. Un entero **p>1** se dice **primo** si sus únicos divisores son **1** y **p**. Si **p** no es primo, se dice **compuesto.**

Ejemplo 1.3. Los primeros primos son $\{2, 3, 5, 7, 11, 13, 17, \cdots\}$

El siguiente resultado garantiza la existencia de números primos.

Teorema 1.3. *Todo entero positivo* ***n>1*** *tiene un divisor primo.*

Demostración.

Si n es primo, tiene un divisor primo (él mismo).

Supongamos que n es compuesto.

Por el principio del buen orden podemos suponer que existe un $d > 1$ que es el más pequeño divisor positivo de n .

Afirmación: d es primo.

En efecto, si d fuera compuesto, d tendría un divisor, digamos d_1 , de donde $1 < d_1 < d$. Pero si $\frac{d_1}{d}$ y $\frac{d}{n}$ entonces $\frac{d_1}{n}$, en contradicción con la suposición de que d era el más pequeño divisor de n mayor que 1. ■

Como consecuencia directa del teorema anterior se tiene el siguiente corolario.

Corolario 1.1. *Sea $n \in \mathbb{Z}, n > 1$. El más pequeño divisor positivo $d > 1$ de n es primo.*

Demostración.

Puesto $n \in \mathbb{Z}, n > 1$ entonces $n \in \mathbb{Z}^+$, luego por anterior existe un primo $d > 1$ que es el más pequeño divisor positivo de n . ■

El siguiente resultado nos dice que la cardinalidad de los números primos es infinita.

Teorema 1.4. ***(Teorema de Euclides):***

Hay un número infinito de primos.

Demostración.

La demostración se hará por contradicción.

Si $p_1, p_2, \cdots, p_n$ fueran todos los primos. El número $N = p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1$ es un nuevo primo o tiene un divisor primo diferente de cada $p_i, i = 1, 2, \cdots, n$

Si N es primo, $N > p_i, i = 1, 2, \cdots, n$ y entonces sería un nuevo primo, lo cual es contradicción.

Si N no es un nuevo primo, entonces N tiene un divisor primo p_j , pero entonces como $\frac{p_j}{p_1 p_2 \cdots p_{n+1}}$ y $\frac{p_j}{p_1 p_2 \cdots p_n}$ entonces $\frac{p_j}{1}$ lo cual es imposible pues $p_j > 1$. ■

1.4 Máximo Común Divisor

Definición 1.3. Sean a, b enteros con al menos uno de los dos diferente de cero.
El máximo común divisor de a y b, denotado $MCD\{a,b\}$, es el entero positivo d que satisface:

a) $\frac{d}{a}$ y $\frac{d}{b}$

b) $\frac{c}{a}$ y $\frac{c}{b}$ entonces $\frac{c}{d}$

Si $MCD\{a,b\} = 1$ se dice que a y b son relativamente primos o simplemente "coprimos".
A continuación se enuncian algunos resultados sobre el máximo común divisor de un número.

Teorema 1.5. *Si* $d = MCD\{a,b\}$, *entonces* $MCD\{a, b-na\} = d$ *con* $n \in \mathbb{Z}$

Demostración.

Sea $d_1 = MCD\{a, b-na\}$, puesto que por definición de máximo común divisor se tiene que $\frac{d}{a}$ y $\frac{d}{b}$, entonces por el teorema 1.1.a $\frac{d}{b-na}$, de donde se sigue que $d \leq d_1$.
Por otro lado como $\frac{d_1}{a}$ entonces $\frac{d_1}{na}$, así $\frac{d_1}{na}$ y también $\frac{d_1}{b-na}$, entonces por el teorema 1.1. b se tiene que $\frac{d_1}{b}$, entonces por la definición de máximo común divisor se tiene que $\frac{d_1}{d}$ de donde $d_1 \leq d$.
Luego tenemos que $d \leq d_1$ y $d_1 \leq d$, por lo tanto $d_1 = d$. ■

Teorema 1.6. *Sean* $a_1, a_2, \cdots, a_n \in \mathbb{Z}^+$, $n \geq 3$.
Entonces $MCD\{a_1, a_2, \cdots, a_n\} = MCD\{a_1, MCD\{a_2, \cdots, a_n\}\}$

Demostración.

Sea $d = MCD\{a_1, a_2, \cdots, a_n\}$ y $d_1 = MCD\{a_1, d_2\}$ con $d_2 = MCD\{a_2, \cdots, a_n\}$
Por definición se tiene que $\frac{d}{a_1}, \frac{d}{a_2}, \cdots, \frac{d}{a_n}$ de donde $\frac{d}{d_2}$ y por lo tanto $\frac{d}{d_1}$ $\cdots(1)$

De otro lado como $\frac{d_1}{a_1}$ y también $\frac{d_1}{d_2}$ entonces por transitividad $\frac{d_1}{a_2}, \cdots, \frac{d_1}{a_n}$,
por lo tanto $\frac{d_1}{d}$ $\cdots(2)$
De (1) y (2) se tiene que $\frac{d}{d_1}$ y también $\frac{d_1}{d}$ por lo tanto $d = d_1$. ■

En la siguiente sección revisamos el algoritmo de Euclides.

1.5 El Algoritmo de Euclides

La aplicación sucesiva del siguiente lema sirve como base para el algoritmo de Euclides.

Lema 1.1. Sean $a, b, q, r \in \mathbb{Z}$ tales que $a = bq + r$, con $b > 0$ y $0 \leq r < b$.
Entonces $MCD\{a, b\} = MCD\{b, r\}$

Demostración.

Según el teorema 1.5, se tiene que $MCD\{b, a\} = MCD\{b, a - bq\} = MCD\{b, r\}$
Y como $MCD\{a, b\} = MCD\{b, a\} \longrightarrow MCD\{a, b\} = MCD\{b, r\}$ ■

Teorema 1.7. ***(Algoritmo de Euclides)***
Sean a y b números naturales con $b \neq 0$. Aplicando el teorema 1.2 (algoritmo de la división) se obtiene una sucesión finita $a, r_0 = b, r_1, r_2, \cdots, r_n, 0$ definida por:

$$\begin{aligned}
a &= r_0 q_1 + r_1, 0 \leq r_1 \leq r_0 \\
r_0 &= r_1 q_2 + r_2, 0 \leq r_2 \leq r_1 \\
r_1 &= r_2 q_3 + r_3, 0 \leq r_3 \leq r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n, 0 \leq r_n \leq r_{n-1} \\
r_{n-1} &= r_n q_{n+1} + r_{n+1}, r_{n+1} = 0
\end{aligned}$$

El último término es $r_n = MCD\{a, b\}$

Demostración.

Si se aplica el teorema 1.2 se obtiene una sucesión decreciente de residuos $0 \leq \cdots < r_k \leq r_{k-1} < \cdots < r_1 < r_0 = b$, la sucesión es finita ya que entre 0 y $r_0 = b \neq 0$ solo hay un número finito de términos, ya que de no ser así se podría aplicar de manera indefinida y entonces entre 0 y b habría una sucesión de enteros lo cual es imposible. Si $\frac{b}{a}$ entonces $r_1 = 0$ y entonces r_0 sería el mínimo residuo positivo. En general debe haber un residuo mínimo $r_n > 0$ y $r_{n+1} = 0$

Usando el lema 1.1 se tiene que:

$$\begin{aligned} MCD\{a,b\} &= MCD\{a - r_0 q, r_0\} \\ &= MCD\{r_1, r_0\} \\ &= MCD\{r_1, r_0 - r_1 q_2\} \\ &= MCD\{r_1, r_2\} \\ &= MCD\{r_1 - r_2 q_2, r_2\} \\ &= MCD\{r_3, r_2\} \\ &\vdots \\ &= MCD\{r_{n-1}, r_n\} \\ &= MCD\{r_n, 0\} = r_n \end{aligned}$$

El siguiente resultado es un algoritmo extendido de Euclides, llamada **Identidad de Bezout**.

Teorema 1.8. ***(Identidad de Bezout)***

Si a y b son dos números enteros ambos no cero a la vez entonces existen $s, t \in \mathbb{Z}$ (posiblemente no únicos) tales que

$$sa + tb = MCD\{a,b\}$$

Demostración.

Sea A el conjunto de combinaciones lineales enteras de a y b , es decir $A = \{ua + vb : u, v \in \mathbb{Z}\}$. Este conjunto tiene números positivos, negativos y el cero. Sea $m = ax + by$ el más pequeño entero positivo en A .

Afirmación: $\frac{m}{a}$ y $\frac{m}{b}$

En efecto, supongamos que $a = mq + r$ con $0 \leq r < m$, entonces,

$$0 \leq r = a - mq = a - (ax + by)q = (1 - qx)a + (-qy)b$$

De donde $r \in A$, pero $0 \leq r < m$, así que la única posibilidad es que $r = 0$, ya que por construcción m es el mínimo entero positivo en A , de donde se sigue que $a = mq$, es decir $\frac{m}{a}$, con argumentos similares se demuestra que $\frac{m}{b}$

Sea $d = MCD\{a, b\}$, puesto que m es común divisor de a y b , entonces $m \leq d$ De otro lado, como $a = k_1 d$ y $b = k_2 d$ entonces $m = ax + by = (xk_1 + yk_2)d > 0$,

por lo tanto $d \leq m$. Luego se tiene que

$$m = d \quad \blacksquare$$

El siguiente corolario es consecuencia directa del teorema (1.8).

Corolario 1.2. *El* $MCD\{a, b\}$ *es el más pequeño entero positivo de la forma* $sa + tb, s, t \in \mathbb{Z}$. *En particular* $MCD\{a, b\} = 1$ *si y solamente si existen* $x, y \in \mathbb{Z}$ *tal que* $ax + by = 1$.

Corolario 1.3. *Si* $\frac{a}{bc}$ *y* $MCD\{a, b\} = 1$ *entonces* $\frac{a}{c}$

Demostración.

Puesto que $MCD\{a, b\} = 1$ entonces existen $x, y \in \mathbb{Z}$ tal que $ax + by = 1$

Si a la igualdad anterior se le multiplica por c ambos lados $acx + bcy = c$

Ahora como $\frac{a}{ac}$ y $\frac{a}{bc}$ entonces $\frac{a}{acx + bcy}$, por lo tanto $\frac{a}{c}$ $\blacksquare$

En la siguiente sección revisamos el teorema fundamental de la aritmética, muy útil en los siguientes dos capítulos.

1.6 Teorema Fundamental de la Aritmética

Para la demostración de este teorema se necesitan el siguiente lema.

Lema 1.2. (Lema de Euclides)
Si p es primo y $\frac{p}{ab}$ entonces $\frac{p}{a}$ o $\frac{p}{b}$

Demostración.

Supóngase que $\frac{p}{ab}$ pero p no divide a a , en este caso $MCD\{p,a\} = 1$ por ser p primo (el único factor común seria p o 1) entonces por el corolario 1.3 del teorema 1.8, se concluye que $\frac{p}{b}$ ■

Teorema 1.9. ***(Teorema fundamental de la Aritmética)***
Todo número natural $n > 1$ se puede factorizar de manera única:

$$n = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \dots p_k^{\beta_k}$$

Donde $p_1, p_2, p_3, \dots, p_k$ son primos distintos, y $\beta_1, \beta_2, \beta_3, \dots, \beta_k$ son enteros positivos. Esta factorización se llama ***factorización prima*** *de n .*

Demostración.

Primero se muestra la existencia, cuya prueba se hace por inducción.
El resultado es cierto para $n = 2$.
Supongamos ahora que el resultado es cierto para $n = 3, 4, \dots, k$
Ahora hay que probar que es cierto para $k + 1$.
Si $k + 1$ es primo está listo.
Si $k + 1$ es compuesto, entonces existen $a, b \in \mathbb{Z}, 1 < a \leq b < k + 1$, tal que $k+1 = ab$, pero por hipótesis inductiva a y b se factorizan como producto de primos, de donde se sigue que $k + 1$ también se factoriza como productos de primos, estos primos son justamente los factores de a y b .

Ahora se demuestra la unicidad.

La prueba se hace por contradicción

Supóngase que $n = r_1 r_2 \dots r_u = q_1 q_2 \dots q_v$, donde todos r_i y todos los q_j son primos además

$$r_1 \leq r_2 \leq \dots \leq r_u \;\; y \;\; q_1 \leq q_2 \leq \dots \leq q_v$$

Si se cancelan los primos iguales que hay en ambos lados queda

$$r_{i_1} r_{i_2} \dots r_{i_n} = q_{j_1} q_{j_2} \dots q_{j_m} \;\; (todos\ distintos)$$

Entonces

$$r_{i_1}(r_{i_2} \dots r_{i_n}) = q_{j_1} q_{j_2} \dots q_{j_m}$$

es decir

$$\frac{r_{i_1}}{q_{j_1} q_{j_2} \dots q_{j_m}}$$

De donde por el lema de Euclides r_{i_1} divide a algún q_{j_t} , por lo tanto $r_{i_1} = q_{j_t}$, lo cual es una contradicción pues se asumieron todos distintos.

1.7 Mínimo Común Múltiplo

Definición 1.4. Si $a, b \in \mathbb{Z}^+$ entonces el **mínimo común multiplo** de a y b es el mas pequeño entero $m > 0$ tal que $\frac{a}{m}$ y $\frac{b}{m}$,se escribe $mcm\{a, b\} = m$.

Nota 1.1. De la definición se deduce que si $\frac{a}{c}$ y $\frac{b}{c}$ con $c > 0$ entonces $m \leq c$, puesto que ningún múltiplo común puede ser menor que m .

Para el mínimo común múltiplo se tiene un teorema similar al teorema 1.5.

Teorema 1.10. *Sean* $a_1, a_2, \dots, a_n \in \mathbb{Z}^+, n \geq 3$. *Entonces*

$$mcm\{a_1, a_2, \dots, a_n\} = mcm\{a_1, \{a_2, \dots, a_n\}\}$$

Demostración.

Sea $m = mcm\{a_1, a_2, \ldots, a_n\}$ y $m_1 = \{a_1, m_2\}$ con $m_2 = mcm\{a_2, \ldots, a_n\}$. Puesto que por definición de mínimo común múltiplo se tiene que $\frac{a_2}{m_2}, \ldots, \frac{a_n}{m_2}$. Se tiene que $\frac{m_2}{m}$, y como también por definición de mínimo común múltiplo se tiene que $\frac{a_1}{m}$ por lo tanto de acuerdo con la nota 1.1.

$$m_1 \leq m \ldots (1)$$

Puesto que m es el menor múltiplo común de $\{a_1, a_2, \ldots, a_n\}$ se deduce que

$$m \leq m_1 \ldots (2)$$

De las ecuaciones (1) y (2) se sigue que $m = m_1$ ■

Nota 1.2. Si $a, b \in \mathbb{Z}^+$ con $d = MCD\{a, b\}$ y $m = mcm\{a, b\}$ entonces $dm = ab$

Corolario 1.4. *Si $m_1, m_2, \ldots, m_k$ son primos relativos dos a dos entonces*

$$mcm\{m_1, m_2, \ldots, m_k\} = m_1 m_2 \ldots m_k$$

Demostración.

Se hace por inducción

Si $k = 2$ entonces como m_1 y m_2 son primos relativos se tiene que $mcm\{m_1, m_2\} = 1$, usando la nota 2 se tiene que $mcm\{m_1, m_2\} = \frac{m_1 m_2}{MCD\{m_1, m_2\}}$ de donde

$$mcm\{m_1, m_2\} = m_1 m_2$$

Asúmase que el resultado es correcto para $1, 2, \ldots, t$. Es decir

$$mcm\{m_1, m_2, \ldots, m_t\} = m_1 m_2 \ldots m_t$$

Por teorema 1.10: $mcm\{m_1, m_2, \ldots, m_t, m_{t+1}\} = mcm\{\{m_1 m_2 \ldots m_t\}, m_{t+1}\}$ puesto que por hipótesis $m_1, m_2, ..., m_t, m_{t+1}$ son primos relativos dos a dos entonces $mcm\{m_1, m_2, \ldots, m_t\}$ y m_{t+1} Son primos entre si y de donde usando la hipótesis de inducción se obtiene

$$mcm\{m_1, m_2, \ldots, m_t, m_{t+1}\} = m_1 m_2 \ldots m_t m_{t+1}$$

Por lo tanto

$$mcm\{m_1, m_2, \ldots, m_k\} = m_1 m_2 \ldots m_k$$ ■

Corolario 1.5. *Si* $m_1, m_2, \ldots, m_k$, $a \in \mathbb{Z}^+$ *y si* $\frac{m_i}{a}$, $i = 1, 2, \ldots, k$ *entonces*

$$\frac{mcm\{m_1, m_2, \ldots, m_k\}}{a}$$

Demostración.

Se hace por inducción

Si $k = 2$ entonces como $\frac{m_1}{a}$ y $\frac{m_2}{a}$, de acuerdo a la nota 1.2. se tiene que $m = mcm\{m_1, m_2\} \leq a$, de donde se deduce que

$$\frac{mcm\{m_1, m_2\}}{a}$$

Asúmase que el resultado es correcto para $1, 2, \ldots, t$. Es decir

$$\frac{mcm\{m_1, m_2, \ldots, m_t\}}{a}$$

Supóngase que $\frac{m_i}{a}$ con $i = 1, 2, \ldots, t, t+1$, de donde por hipótesis inductiva se tiene que $\frac{mcm\{m_1, m_2, \ldots, m_t\}}{a}$. Y como también $\frac{m_{t+1}}{a}$ entonces por ser el resultado correcto para $k = 2$, se tiene que $\frac{mcm\{mcm\{m_1, m_2, \ldots, m_t\}, m_{t+1}\}}{a}$ luego de acuerdo con el teorema 1.10. se tiene que como

$$mcm\{m_1, m_2, \ldots, m_{t+1}\} = mcm\{mcm\{m_1, m_2, \ldots, m_t\}, m_{t+1}\}$$

Se deduce que $\frac{mcm\{m_1, m_2, \ldots, m_{t+1}\}}{a}$, por lo tanto $\frac{mcm\{m_1, m_2, \ldots, m_k\}}{a}$ ■

Capítulo 2:

Aritmética Modular

En esta capítulo se revisa la definición y propiedades de la estructura de anillo, sobre la cual se realizan las operaciones aritméticas como adición, sustracción, multiplicación y división.

2.1 Preliminares

La estructura de anillo se construye sobre la idea de conjunto, del cual no se tiene una definición formal de conjunto, se dice que un conjunto es una colección de objetos, los cuales son llamados elementos. Por lo general un conjunto será denotado por letras mayúsculas: $A, B, C, \ldots, X, Y, Z, \Gamma, \triangle, etc$ mientras que los elementos serán denotados empleando letras minúsculas: $a, b, c, \ldots, x, y, z, \alpha, \beta, etc$. La relación que existe entre elemento y conjunto es la de pertenencia. Es decir, dado un conjunto A , si el elemento x es uno de los que forma al conjunto A entonces se dice que x pertenece a A , lo cual será escrito como $x \in A$. En caso contrario simplemente se escribe $x \notin A$.

En el estudio de conjuntos se tiene los siguientes axiomas:

1. **Axioma de Unicidad:** Si los conjuntos A y B tienen los mismos elementos, entonces son idénticos, es decir, $A = B$ si y solamente si cada vez que $x \in A$

entonces $x \in B$ y recíprocamente.

Matemáticamente

$$A = B \leftrightarrow [\forall x \in A \rightarrow x \in B]$$

2. **Axioma de Unión:** Dados dos conjuntos A y B existe un conjunto que tiene todos los elementos de A ; todos los de B y ningún otro, lo representamos por $A \cup B$.

   Matemáticamente

   $$A \cup B \leftrightarrow [x \in A \vee x \in B]$$

3. **Axioma de Diferencia:** Para dos conjuntos cualesquiera A y B siempre existe otro que contiene los elementos de A que no están en B : Este conjunto seria representado por $A - B$.

   Matemáticamente

   $$A - B \leftrightarrow [x \in A \vee x \notin B]$$

4. **Axioma de Existencia:** Existe al menos un conjunto no vacío.

   Puesto que $A \cap B = A - (A - B)$, no hay necesidad de axiomatizar la existencia de la intersección de dos conjuntos A y B .

Ejemplo 2.1. En el quehacer diario los siguientes ejemplos de conjuntos siempre están presentes:

$\mathbb{N} = \{1, 2, 3, 4, \ldots\ldots\ldots\}$, llamado conjunto de números naturales, que es usado por ejemplo cuando nos referimos a la cantidad de páginas web que existe en el mundo virtual.

$\mathbb{Z} = \{\ldots\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\ldots\}$, llamado conjunto de los números enteros, el cual es útil por ejemplo cuando queremos determinar las ganancias y pérdidas en determinada inversión financiara.

$\mathbb{Q} = \{m/n : m, n \in \mathbb{Z}; n \neq 0\}$, conjunto de los números racionales, cuyos elementos son útiles en la repartición de terrenos, de pagos, etc.

$I = \{x \neq m/n : m, n \in \mathbb{Z}; n \neq 0\}$, conjunto de los números irracionales, aparecen sutilmente cuando se trata de ubicar determinada calle o avenida a través de google,

ya que este dispositivo se conecta con satélites cuyas distancias generalmente están relacionadas con el diámetro terrestre. $\mathbb{R} = \mathbb{Q} \cup I$, conjunto de los números reales, de donde podemos también escribir:

$$I = \mathbb{R} - \mathbb{Q}$$

Este conjunto se usa desde que se pone un pie fuera de la cama, ya que al mirar la hora se hace usos de ellos, cuando se prepara una taza de café, al calcular la cantidad de café se usan racionales y así por el estilo.

$\mathbb{C} = \{a + ib : a, b \in \mathbb{R}; i = \sqrt{-1}\}$, conjunto de los números complejos, estos conjuntos son útiles ya que permiten por ejemplo el desarrollo de los USB.

2.2 Producto Cartesiano

Definición: Dados dos conjuntos A y B no vacíos se llama producto cartesiano de los conjuntos A y B , a este producto cartesiano se le denota por $A \times B$ y es el conjunto de pares ordenados (a, b) con $a \in A$ y $b \in B$. Es decir:

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

Ejemplo 2.2. Si $A = B = \mathbb{N}$, entonces:

$$A \times B = \mathbb{N} \times \mathbb{N} = \{(a, b) : a \in \mathbb{N}, b \in \mathbb{N}\} = \mathbb{N}^2 \longrightarrow \mathbb{N} \times \mathbb{N} = \mathbb{N}^2$$

2.3 Función

Definición 2.1. Sean A y B dos conjuntos. Se llama función del conjunto A en el conjunto B a una regla en la que a cada elemento del conjunto A le asocia un único elemento de B . En símbolos, una función del conjunto A en el conjunto B es denotada por:

$$f : A \longrightarrow B$$
$$x \longrightarrow f(x)$$

Donde para cada $x \in A$, está asociado un único $y = f(x) \in B$, a través de la regla que define f . El conjunto A es llamado dominio de la función f , mientras que el conjunto B recibe el nombre de rango de la función f .

Llamaremos imagen de f al subconjunto de B formado por aquellos $y \in B$ para los que existe $x \in A$ tales que $f(x) = y$. Decimos que una función f es de A en B si su dominio es A y su imagen es subconjunto de B . Si la imagen de f es todo B decimos que f es una función sobreyectiva.

Ejemplo 2.3. Sean $A = B = \mathbb{N}$ se define f como la suma en el conjunto de los números naturales, es decir $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, definida por $f(a, b) = a + b$.

2.4 Operación Binaria Interna

Definición 2.2. Una operación binaria interna o ley de composición interna $*$ definida en un conjunto no vacío A , es una función que envía los elementos del producto cartesiano $A \times A$ hacia el conjunto A . Es decir:

$$* : A \times A \longrightarrow A$$
$$(a, b) \longrightarrow *(a, b) = a * b$$

Ejemplo 2.4. Las siguientes operaciones son ejemplos de operaciones binarias cerradas:

- La adición y el producto en el conjunto de números naturales.
  En efecto, para la adición

$$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$
$$(a, b) \longrightarrow +(a, b) = a + b$$

Por el axioma de la cerradura para la adición de números naturales se tiene que $a+b \in \mathbb{N}$, por lo tanto la adición de números naturales es una operación binaria interna o cerrada.

- El producto en el conjunto de números naturales.
  En efecto, para el producto

$$\begin{aligned} \cdot : \mathbb{N} \times \mathbb{N} &\longrightarrow \mathbb{N} \\ (a,b) &\longrightarrow \cdot(a,b) = a \cdot b \end{aligned}$$

Por el axioma de la cerradura para el producto de números naturales se tiene que $a \cdot b \in \mathbb{N}$, por lo tanto el producto de números naturales es una operación binaria interna o cerrada.

- La adición en el conjunto de números enteros.
  En efecto, para la adición

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (a,b) &\longrightarrow +(a,b) = a+b \end{aligned}$$

Por el axioma de la cerradura para la adición de números enteros se tiene que $a+b \in \mathbb{Z}$, por lo tanto la adición de números enteros es una operación binaria interna o cerrada.

- El producto en el conjunto de números enteros.
  En efecto, para el producto

$$\begin{aligned} \cdot : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (a,b) &\longrightarrow \cdot(a,b) = a \cdot b \end{aligned}$$

Por el axioma de la cerradura para el producto de números enteros se tiene que $a \cdot b \in \mathbb{Z}$, por lo tanto el producto de números enteros es una operación binaria interna o cerrada.

- La unión de conjuntos.

  En efecto, sea x un conjunto cualquiera distinto del vacío y definamos el conjunto potencia de X por $\mathcal{P}(X) = \{A : A \subset X\}$

$$\begin{aligned} \cup : \mathcal{P}(X) \times \mathcal{P}(X) &\longrightarrow \mathcal{P}(X) \\ (A, B) &\longrightarrow \cup(a, b) = A \cup B \end{aligned}$$

  Por el axioma de la unión de conjuntos se tiene que $A \cup B$ es también otro conjunto de donde $A \cup B \subset X$, entonces $A \cup B \in \mathcal{P}(X)$, por lo tanto la unión de conjuntos es una operación binaria interna o cerrada.

- La intersección de conjuntos

  En efecto, sea X un conjunto cualquiera distinto del vacío y definamos el conjunto potencia de X

$$\begin{aligned} \cap : \mathcal{P}(X) \times \mathcal{P}(X) &\longrightarrow \mathcal{P}(X) \\ (A, B) &\longrightarrow \cap(a, b) = A \cap B \end{aligned}$$

  Por el axioma de la unión de conjuntos se tiene que $A \cup B$ es también otro conjunto de donde $A \cap B \subset X$ entonces $A \cap B \in \mathcal{P}(X)$, por lo tanto la intersección de conjuntos es una operación binaria interna o cerrada.

- La adición de las matrices cuadradas.

  En efecto, sea A una matriz de orden $m \times n$, es decir $A = \left[a_{ij}\right]_{m \times n}$ y definamos al conjunto formado por estas matrices como sigue:

$$\mathcal{M}_{m \times n}(\mathbb{R}) = \left\{ A = \left[a_{ij}\right]_{m \times n} : a_{ij} \in \mathbb{R}; 1 \leq i \leq m; 1 \leq j \leq n \right\}$$

  De donde el conjunto de matrices cuadradas es un subconjunto de $\mathcal{M}_{m \times n}(\mathbb{R})$ cuando $m = n$. Sean $A, B \in \mathcal{M}_{m \times n}(\mathbb{R})$, entonces

$$A + B = \left[a_{ij}\right]_{n \times n} + \left[b_{ij}\right]_{n \times n} = \left[a_{ij} + b_{ij}\right]_{n \times n}$$

  De donde se sigue que $A + B \in \mathcal{M}_{m \times n}(\mathbb{R})$, por lo tanto la adición de las matrices cuadradas es una operación binaria interna o cerrada.

- El producto de las matrices cuadradas.

  En efecto, sean $A \cdot B \in \mathcal{M}_{m\times n}(\mathbb{R})$, entonces

$$A \cdot B = \left[a_{ij}\right]_{n\times n}\left[b_{ij}\right]_{n\times n} = \left[c_{ij}\right]_{n\times n}$$

  Con $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} : 1 \leq i \leq n : 1 \leq j \leq n$

  De donde se sigue que $AB \in \mathcal{M}_{n\times n}(\mathbb{R})$, por lo tanto la multiplicación de las matrices cuadradas es una operación binaria interna o cerrada.

2.5 Anillos

Definición 2.3. Sea A un conjunto no vacío con dos operaciones binarias cerradas, denotadas por $(+)$ y $(\cdot)$ (que pueden ser diferentes de la suma y producto usuales). Entonces $(A, +, \cdot)$ Es un anillo si para todo $a, b, c \in A$ se cumplen las siguientes condiciones:

1.	$a + b = b + a$	Ley conmutativa de $+$
2.	$a + (b + c) = (a + b) + c$	Ley asociativa de $+$
3.	Existe un $e \in A$ tal que	
	$a + e = e + a = a, \forall a \in A$	Existencia de unidad para $+$
4.	Para cada $a \in A$ existe un elemento	
	$b \in A : a + b = b + a = e$	Existencia de inversos bajo $+$
5.	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$	Ley asociativa de $\cdot$
6.	$a \cdot (b + c) = a \cdot b + a \cdot c$	Leyes distributivas
	$(b + c) \cdot a = b \cdot a + c \cdot a$	de $\cdot$ sobre $+$

Puesto que en un anillo $(A, +, \cdot)$, ambas operaciones son asociativas no hay ambigüedad si se escribe $a + b + c$ para $a + (b + c)$ o para $(a + b) + c$, o si se escribe $a \cdot b \cdot c$ para $a \cdot (b \cdot c)$ o para $(a \cdot b) \cdot c$.

Por conveniencia al trabajar sobre un anillo $(A, +, \cdot)$, se escribe ab para denotar $a \cdot b$

Ejemplo 2.5. $(\mathbb{Z}, +, \cdot)$ es un anillo, donde $(+)$ y $(\cdot)$ son las operaciones usuales de adición y producto en el conjunto numérico $\mathbb{Z}$ son anillos.

En efecto, de acuerdo al ejemplo (2.4), se tiene que tanto la suma como el producto de números enteros son operaciones binarias cerradas, además por los axiomas de conmutatividad y asociatividad de ambas operaciones se tiene que se cumplen las condiciones 1,2 y 5 de la definición de anillo, puesto que $z + 0 = 0 + z = 0 \ \forall z \in \mathbb{Z}$, entonces el cero es el neutro aditivo para la adición en $\mathbb{Z}$, es decir se cumple la condición 3, y como $-1 \cdot z = -z, \ \forall \ z \in \mathbb{Z}$ se puede definir al entero $-z$ como el inverso aditivo en $\mathbb{Z}$, con lo cual se cumple la condición 4 de la definición de anillo. Finalmente usando el axioma de la distributividad se tiene que:

$$a \cdot (b + c) = a \cdot b + a \cdot c; \ \forall \ a, b, c \in \mathbb{Z}$$

De otro lado como el producto en $\mathbb{Z}$ es conmutativo se tiene

$$a \cdot b + a \cdot c = b \cdot a + c \cdot a = (b + c) \cdot a$$

Es decir también se cumple

$$(b + c) \cdot a = b \cdot a + c \cdot a; \forall a, b, c \in \mathbb{Z}$$

Con lo cual se cumple la condición 6 de la definición de anillos, por lo tanto se concluye que es un anillo. ■

Ejemplo 2.6. En forma análoga al ejemplo (2.5) se comprueba que con las operaciones usuales de adición y producto también los conjuntos numéricos $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ son anillos.

En todos estos anillos, la identidad de la suma z es el entero cero y el inverso aditivo de cualquier número x es el conocido $-x$.

Definición 2.4. Sea $(A, +, \cdot)$ un anillo arbitrario.

a) Si $ab = ba; \ \forall a, b \in A$ entonces se dice que $(A, +, \cdot)$ es un **anillo conmutativo.**

b) El anillo $(A, +, \cdot)$ no tiene **divisores propios de cero** si para cualquiera

$$a, b \in A, ab = e \longrightarrow a = e \; o \; b = e$$

c) Si un elemento $u \in A$ es tal que $u \neq e$ y $au = ua = a$ para todo $a \in A$, se dice que u es un **elemento unidad, o identidad para el producto** de A , entonces $(A, +, \cdot)$ es llamado **anillo con unidad.**

Nótese que de la parte (c) de la definición anterior se sigue que si $(A, +, \cdot)$ es un anillo con unidad entonces A contiene al menos un elemento distinto de la identidad e.

Ejemplo 2.7. El anillo $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo, puesto que en $\mathbb{Z}$ el producto de enteros es conmutativo.

Además puesto que en $\mathbb{Z}$ siempre se cumple que:

- Si $ab = 0 \longrightarrow a = 0 \; \vee \; b = 0$ se deduce que el anillo $(\mathbb{Z}, +, \cdot)$ no tiene divisores propios de cero.
- $1 \in \mathbb{Z}$ y además $1 \cdot a = a \cdot 1 = a; \forall a \in \mathbb{Z}$, entonces $(\mathbb{Z}, +, \cdot)$ es un anillo con unidad.

Por lo tanto $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo, sin divisores propios de cero y con unidad 1.

Definición 2.5. Sea $(A, +, \cdot)$ un anillo con elemento unidad u .Si $a, b \in A$ y $ab = ba = u$, entonces b es un **inverso multiplicativo** del elemento a y a es una unidad de A (el elemento b también es una unidad de A).

Ejemplo 2.8. Como ya se dijo (siguiendo las ideas del ejemplo (2.1)) se puede comprobar que $(\mathbb{Q}, +, \cdot)$ es un anillo con elemento unidad 1, además por ejemplo si $a = 2$; $b = \frac{1}{2}$ entonces es claro que $ab = ba = 1$, de donde $b = \frac{1}{2}$ es inverso multiplicativo de $a = 2$ o $a = 2$ es inverso multiplicativo de $b = \frac{1}{2}$.

Definición 2.6. Sea $(A, +, \cdot)$ un anillo conmutativo con unidad entonces

a) A es un **dominio de integridad** si A no tiene divisores propios de cero.

b) A es un **cuerpo** si todo elemento distinto de cero en A es una unidad.

Ejemplo 2.9. De acuerdo al ejemplo (2.4) se sabe que $(\mathbb{Q}, +, \cdot)$ es un anillo conmutativo con elemento unidad 1, además en $\mathbb{Q}$ se cumple: Si $ab = 0 \longrightarrow a = 0 \quad \vee \quad b = 0$ para cualquiera $a, b \in \mathbb{Q}$, luego $\mathbb{Q}$ es un dominio de integridad.

2.5.1 Propiedades de los Anillos

En lo que sigue se revisan algunas propiedades que serán de utilidad en el desarrollo de este trabajo.

Teorema 2.1. *En cualquier anillo* $(A, +, \cdot)$

a) El elemento neutro aditivo e es único.

b) El elemento inverso aditivo de cada elemento del anillo es único.

Demostración.

a) Supóngase que $e_1 \neq e$ es otro elemento neutro aditivo, es decir $e_1 + e = e$, y como también e es un elemento neutro aditivo, se tiene que $e_1 + e = e_1$, de donde:

$$e_1 = e_1 + e = e \longrightarrow e_1 = e$$

Lo cual contradice el supuesto $e_1 \neq e$, por lo tanto e es único.

b) Para $a \in A$, supóngase que existen dos elementos $b, c \in A$, con $b \neq c$ tales que:

$$a + b = b + a = e; \quad a + c = c + a = e$$

De otro lado se puede escribir b del modo siguiente:

$$b = b + e = b + (a + c) = (b + a) + c = e + c = c \longrightarrow b = c$$

Lo cual contradice el supuesto $b \neq c$, por lo tanto el inverso aditivo es único. ■

Nota 2.1. Usando la parte (b) del teorema anterior se denotará el inverso aditivo de $a \in A$, como $-a$, y la resta en este anillo se define como $a - b = a + (-b)$

Teorema 2.2. *Para un anillo* $(A, +, \cdot)$

a) Si A tiene un elemento unidad, entonces es único, y

b) Si A tiene un elemento unidad y x es una unidad de A , entonces el inverso multiplicativo de x es único.

Demostración.

a) Supongamos que u_1, u_2 son elementos unidad en el anillo A ambos diferentes entre sí, entonces para cualquier $a \in A$ se cumple que:

$$au_1 = u_1a = a \qquad \ldots(1)$$

$$au_2 = u_2a = a \qquad \ldots(2)$$

Si en (1) se hace $a = u_2$, se tiene $u_2u_1 = u_1u_2 = u_2 \qquad \ldots(3)$

Analogamente Si en (2) se hace $a = u_1$, se tiene $u_1u_2 = u_2u_1 = u_1 \qquad \ldots(4)$
Usando las ecuaciones (3) y (4) se tiene:

$u_2 = u_1u_2 = u_1 \longrightarrow u_1 = u_2$,lo cual contradice el supuesto que ambos son diferentes, por lo tanto si existe el elemento unidad, este es único.

b) Sea x^{-1} un inverso multiplicativo del elemento unidad x , puesto que x es una unidad se tiene que para cualquier $a \in A$

$$xb = a \longrightarrow x^{-1}xa = x^{-1}a$$

$$\longrightarrow ea = x^{-1}a$$

$$\longrightarrow a = x^{-1}a$$

De la igualdad anterior se observa que también x^{-1} es una unidad del anillo A , luego de acuerdo con la parte (a) demostrada anteriormente se deduce que el inverso multiplicativo es único. ■

2.6 Cuerpo

Definición 2.7. Un **cuerpo** es un anillo conmutativo K con elemento unidad, tal que para todo

$$x \in K, x \neq e \longrightarrow x^{-1} \in K$$

Ejemplo 2.10. El anillo conmutativo $(\mathbb{Z}, +, \cdot)$ no es un cuerpo, puesto que por ejemplo el inverso multiplicativo de 2 es $\frac{1}{2} \notin \mathbb{Z}$.

Ejemplo 2.11. El anillo conmutativo $(\mathbb{Q}, +, \cdot)$ es un cuerpo, puesto que cualquier $0 \neq x \in \mathbb{Q}$, se puede escribir como:

$$x = \frac{m}{n}, m, n \in \mathbb{Z}, n \neq 0$$

Si se define:

$$x^{-1} = \frac{n}{m} \in \mathbb{Q}$$

Entonces

$x \cdot x^{-1} = \frac{m}{n}\frac{n}{m} = 1 = x^{-1} \cdot x \longrightarrow x^{-1}$. Es el inverso multiplicativo de x.
Además como por construcción se tiene $x^{-1} \in \mathbb{Q}$
se concluye que $(\mathbb{Q}, +, \cdot)$ es un cuerpo. ■

En la siguiente sección se estudia un cuerpo finito particular, el cual será de gran utilidad para este trabajo.

2.7 Enteros Módulo n

2.7.1 Aritmética Modular

Definición 2.8. Sea $n \in \mathbb{Z}^+$; $n > 1$. Para $a, b \in \mathbb{Z}$ se dice que a es congruente con b módulo n, lo que se denota por $a \equiv b(mod\ n)$, si $a = b + kn$ para algún $k \in \mathbb{Z}$

Nota 2.2. De la definición se deduce que todos los números son congruentes módulo $n = 1$. Si se usa $n = 2$, los pares son congruentes con los pares (resto 0 módulo 2) y los impares con los impares (resto 1 módulo 2). En general, la idea es "agrupar"los números según el residuo que dejan al dividir por n . Estos subconjuntos constituyen una partición de $\mathbb{Z}$ de tal manera que podemos trabajar no con todo $\mathbb{Z}$ sino con un grupo de representantes.

Ejemplo 2.12. $14 \equiv 2(mod\ 3)$ puesto que existe $k = 4 \in \mathbb{Z}$ tal que $14 = 2 + (4)(3)$

Teorema 2.3. *La congruencia módulo n es una relación de equivalencia sobre* $\mathbb{Z}$

Demostración.

Por definición se sabe que una relación de equivalencia es una relación:

1. **Reflexiva:** $a \equiv a(mod\ n)$
2. **Simétrica:** $a \equiv b(mod\ n)$, entonces $b \equiv a(mod\ n)$
3. **Transitiva:** Si $a \equiv b(mod\ n)$ y $b \equiv c(mod\ n)$ entonces $a \equiv c(mod\ n)$

   - La congruencia módulo n es una relación reflexiva, puesto que para cualquier $a \in \mathbb{Z}$, existe $k = 0 \in \mathbb{Z}$ tal que $a = a + (0)n = a$, de donde, $a \equiv a(mod\ n)$.

- La congruencia módulo n es una relación simétrica, puesto que si para $a, b \in \mathbb{Z}$ se tiene $a \equiv b(mod\, n)$, existe $k \in \mathbb{Z}$ tal que $a = b+kn$, de donde $b = a+(-k)n$, y como $-k \in \mathbb{Z}$ se deduce que $b \equiv a(mod\, n)$.
- La congruencia módulo n es una relación transitiva, sean $a, b, c \in \mathbb{Z}$ tales que:$a \equiv b(mod\, n)$ y $b \equiv c(mod\, n)$,debemos comprobar que $a \equiv c(mod\, n)$, por hipótesis existen $k_1, k_2 \in \mathbb{Z}$:

$$a = b + k_1 n \longrightarrow b = a - k_1 n \tag{2.1}$$

$$b = c + k_2 n \tag{2.2}$$

Si se sustituye la ecuación (2.1) en la ecuación (2.2) se tiene

$$a - k_1 n = c + k_2 n \longrightarrow a = c + k_1 n + k_2 n$$

$$\longrightarrow a = c + (k_1 + k_2)n$$

Usando la cerradura para la adición en $\mathbb{Z}$ se deduce que $(k_1 + k_2) \in \mathbb{Z}$, de donde se obtiene que $a \equiv c(mod\, n)$.

Por lo tanto la relación congruencia módulo es una relación de equivalencia.

Usando la relación congruencia módulo n se resuelven ecuaciones como se muestra en el siguiente ejemplo:

Ejemplo 2.13. Resolver $4x \equiv 8(mod\ 12)$ con $x \in \{0, 1, 2, \ldots, 11\}$

Solución 2.1.

Puesto que $4x \equiv 8(mod\ 12) \longrightarrow 4(x) \equiv 4(2(mod\ 3))$

$$\longrightarrow x \equiv 2(mod\ 3)$$

Luego los $x \in \{0, 1, 2, \ldots, 11\}$ que dejan resto 2 al dividir por 3 son $x = 2, 5, 8\ y\ 11$ ■

Nota 2.3. Como una relación de equivalencia sobre un conjunto induce una partición de éste, para $n \geq 2$, la congruencia módulo n divide a $\mathbb{Z}$ en las n clases de equivalencia.

$$[0] = \{\ldots, -2n, -n, 0, n, 2n, \ldots\} = \{0 + nx : x \in \mathbb{Z}\}$$
$$[1] = \{\ldots, -2n+1, -n+1, 1, n+1, 2n+1, \ldots\} = \{1 + nx : x \in \mathbb{Z}\}$$
$$[2] = \{\ldots, -2n+2, -n+2, 2, n+2, 2n+2, \ldots\} = \{2 + nx : x \in \mathbb{Z}\}$$
$$[3] = \{\ldots, -2n+3, -n+3, 3, n+3, 2n+3, \ldots\} = \{3 + nx : x \in \mathbb{Z}\}$$
$$\vdots$$
$$[n-1] = \{\ldots, -n-1, -1, n-1, 2n-1, 3n-1, \ldots\} = \{(n-1) + nx : x \in \mathbb{Z}\}$$

Para cualquier $t \in \mathbb{Z}$, por el algoritmo de Euclides de la división se puede escribir $t = qn + r;\ 0 \leq r < n$, de donde $t \in [r]$, o $[t] = [r]$. Es decir al dividir por n solo hay posibilidad de n residuos $0, 1, 2, \ldots, n-1$.

En este contexto se usa la notación $\mathbb{Z}_n$ para referirse al conjunto de las clases de equivalencia de la relación congruencia módulo n , es decir:

$$\mathbb{Z}_n = \Big\{[0], [1], [2], \ldots, [n-1]\Big\}$$

Cuando no haya peligro de confusión se escribirá simplemente:

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

Si n es impar, la representación simétrica de $\mathbb{Z}_n$ es

$$\mathbb{Z}_n = \Big\{-\frac{n-1}{2}, \ldots, -1, 0, 1, 2, \ldots, \frac{n-1}{2}\Big\}$$

Si p es primo, existe $b \in \mathbb{Z}$ tal que

$$\mathbb{Z}_n = \{0, b, b^2, \ldots, b^{p-1}\}$$

2.7.2 El Anillo $\mathbb{Z}_n$

El siguiente objetivo es definir operaciones binarias cerradas de adición y producto sobre el conjunto de clases de equivalencia $\mathbb{Z}_n$, de modo que con estas operaciones $\mathbb{Z}_n$ sea un anillo.

Para $[a], [b] \in \mathbb{Z}_n$, se definen

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$

Definición 2.9. Para $[a], [b] \in \mathbb{Z}_n$, se definen

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$

$$([a], [b]) \longrightarrow [a] + [b] = [a + b]$$

Afirmación: Esta operación está bien definida, es decir es independiente del representante de la clase de equivalencia.

Demostración.

sean: $[a] = [b]$ y $[c] = [d]$. Se debe demostrar que $[a] + [c] = [b] + [d]$, en efecto:

Como $[a] = [b]$, entonces existe $k_1 \in \mathbb{Z} : a = b + k_1 n$.

Como $[c] = [d]$, entonces existe $k_2 \in \mathbb{Z} : c = d + k_2 n$.

De donde:

$a + c = (b + k_1 n) + (d + k_2 n) = (b + d) + (k_1 + k_2)n$.

Es decir $(a + c) \equiv (b + d)(mod\ n) \longrightarrow [a + c] = [b + d]$

Por lo tanto $[a] + [c] = [b] + [d]$ ■

Ejemplo 2.14. En $\mathbb{Z}_5$, se tiene que $[1] + [4] = [5] = [0]$

Definición 2.10. Para $[a], [b] \in \mathbb{Z}_n$, se definen

$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$

$$([a], [b]) \longrightarrow [a] \cdot [b] = [a \cdot b]$$

Afirmación: Esta operación está bien definida, es decir es independiente del representante de la clase de equivalencia.

Demostración.

$[a] = [b]$ y $[c] = [d]$. Se debe demostrar que $[a][c] = [b][d]$, en efecto:
Como $[a] = [b]$, entonces existe $k_1 \in \mathbb{Z} : a = b + k_1 n$
Como $[c] = [d]$, entonces existe $k_2 \in \mathbb{Z} : c = d + k_2 n$
De donde:
$ac = (b + k_1 n)(d + k_2 n) = (bd) + (bk_2 + dk_1 + k_1 k_2 n)n$
Es decir $(ac) \equiv (bd)(mod\ n) \longrightarrow [ac] = [bd]$
Por lo tanto $[a][c] = [b][d]$ ■

Ejemplo 2.15. En $\mathbb{Z}_5$, se tiene que $[1][4] = [1 \cdot 4] = [4]$

Teorema 2.4. *Para $n \in \mathbb{Z}^+, n > 1$, $(\mathbb{Z}_n, +, \cdot)$ es una anillo conmutativo con elemento unidad igual a* $[1]$.

Demostración.

Sean $[a], [b]$ *y* $[c] \in \mathbb{Z}_n$

1. $[a] + [b] = [a + b] = [b + a] = [b] + [a] \longrightarrow [a] + [b] = [b] + [a]$.
   Ley conmutativa de $+$

2. $[a] + ([b] + [c]) = [a + (b + c)] = [(a + b) + c] = ([a + b]) + [c]$
   $\longrightarrow [a] + ([b] + [c]) = ([a + b]) + [c]$ Ley asociativa de $+$

3. Existe un $[0] \in \mathbb{Z}_n$ tal que $[a] + [0] = [a + 0] = [a]$, $\forall\ [a] \in \mathbb{Z}_n$
   Existencia de unidad para $+$

4. Para cada $[a] \in \mathbb{Z}_n$ existe un elemento
   $[b] = [-a] \in \mathbb{Z}_n : [a] + [b] = [a + b] = [a + (-a)] = [0]$.
   Existencia de inversos bajo $+$

5. $[a]([b][c]) = [a(bc)] = [(ab)c] = [(ab)][c] \longrightarrow [a]([bc]) = ([ab])[c]$
   Ley asociativa de $\cdot$

6. $[a]([b+c]) = [a(b+c)] = [ab+ac] = [ab] + [ac] \longrightarrow [a]([b+c]) = [ab] + [ac]$

   Además:

   $[b+c][a] = [(b+c)a] = [ba+ca] = [ba] + [ca] \longrightarrow [b+c][a] = [ba] + [ca]$

   Es decir se cumplen las Leyes distributivas del producto sobre la adición.

   De otro lado

   $$[a][b] = [ab] = [ba] = [b][a] \longrightarrow [a][b] = [b][a]$$

   $[a] = [a \cdot 1] = [a] \cdot [1] \longrightarrow [a], \forall [a] \in \mathbb{Z}_n$, entonces [1] es la unidad $(\mathbb{Z}_n, +, \cdot)$

   Por lo tanto $(\mathbb{Z}_n, +, \cdot)$ es un anillo conmutativo con unidad igual a [1] ■

Teorema 2.5. *Para $n \in \mathbb{Z}^+, n > 1$, $(\mathbb{Z}_n, +, \cdot)$ es un cuerpo si y solo sí n es primo.*

Demostración.

- **Condición necesaria:** Si $\mathbb{Z}_n$ es un cuerpo entonces n es primo.

  Si $\mathbb{Z}_n$ es un cuerpo, razonemos por el absurdo y supóngase que n no es primo entonces $n = n_1 n_2$, donde $0 < n_1 n_2 < n$, de donde $[n_1] \neq [0]$ y $[n_2] \neq [0]$, sin embargo $[n] = [n_1][n_2] \rightarrow [n_1][n_2] = [0]$, luego $\mathbb{Z}_n$ tiene divisores de cero, por lo tanto $\mathbb{Z}_n$ no es cuerpo, lo cual es una contradicción, por lo tanto n es primo.

- **Condición suficiente:** Sea n un primo entonces $\mathbb{Z}_n$ es un cuerpo.

  Sea n un primo y supongamos que $0 < a < n$.

  Entonces $MCD\{a, n\} = 1$,

  luego existen enteros k,l:$ak + ln = 1 \rightarrow ak = 1 + (-l)n \rightarrow ak \equiv 1 (mod\ n)$, de donde $[ak] = [a][k] = [1]$, entonces $[a]$ es una unidad de $\mathbb{Z}_n$.

  Por lo tanto $\mathbb{Z}_n$ es un cuerpo. ■

Teorema 2.6. *En $\mathbb{Z}_n$, $[a]$ es una **unidad** si y solo sí $MCD\{a, n\} = 1$*

Demostración.

- **Condición necesaria:** Sea $[a] \in \mathbb{Z}_n$ una unidad entonces $MCD\{a, n\} = 1$

  Sea $[a] \in \mathbb{Z}_n$ una unidad y $[a]^{-1} = [s]$, entonces:

  $[as] = [a][s] = [a][a]^{-1} = [1] \rightarrow [as] = [1] \rightarrow as \equiv 1 (mod\ n)$

  $\rightarrow \exists t \in \mathbb{Z} : as = 1 + tn \rightarrow 1 = as + (-t)n \rightarrow MCD\{a, n\} = 1$

- **Condición suficiente:** Si $MCD\{a,n\} = 1$ entonces, sea $[a] \in \mathbb{Z}_n$ una unidad. Supongamos que $0 < a < n$. Entonces como por hipótesis se tiene que: $MCD\{a,n\} = 1$, luego existen enteros $k, l : ak + ln = 1 \rightarrow ak \equiv 1(mod\ n)$, de donde $[ak] = [a][k] = [1]$, entonces $[a]$ es una unidad de $\mathbb{Z}_n$ ■

En la siguiente sección estudiamos el resultado más importante de este capítulo, el cual usaremos para el cifrado de mensajes.

2.8 Teorema Chino de los Restos

Teorema chino de los restos: Consideremos el sistema lineal de congruencias

$$\begin{aligned} x &\equiv a_1(mod\ m_1) \\ x &\equiv a_2(mod\ m_2) \\ &\vdots \quad\quad \vdots \\ x &\equiv a_k(mod\ m_k) \end{aligned}$$

Con $MCD\{m_i, m_j\} = 1; 1 \leq i,\ j \leq k$.
Entonces $M = m_1 m_2 \ldots m_k$ y $M_i = \dfrac{M}{m_i}$, entonces el sistema tiene solución única

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_k M_k y_k \quad \text{módulo M.}$$

Demostración.

La prueba se hará en dos partes, en la primera parte de la prueba se muestra una solución explícita y en la segunda parte se muestra que dicha solución es única.

- **Primera Parte**
  Sean $M = m_1 m_2 \ldots m_k$ y $M_i = \dfrac{M}{m_i}$, $\quad 1 \leq i \leq k$, puesto que los módulos son primos relativos dos a dos, entonces el$MCD\{M_i, m_i\} = 1$ para cada i , además también se tiene que $M_i \equiv 0(mod\ m_j)$, $\quad j \neq i$
  Puesto que $MCD\{M_i, m_i\} = 1$ entonces $M_i y_i \equiv 1(mod\ m_i)$ tiene única solución

$y_i \equiv M_i^{-1}(mod\ m_i)$ Sea $x = a_1M_1y_1 + a_2M_2y_2 + \ldots + a_kM_ky_k$ demostraremos que x es solución del sistema de congruencias.

En efecto

$$x = \sum_{\substack{i=1 \\ j\neq i}}^{k} a_iM_iy_i + a_jM_jy_j$$

Puesto que $M_iy_i \equiv 1(mod\ m_i)$ entonces

$$x = \sum_{\substack{i=1 \\ j\neq i}}^{k} a_i \cdot 0 \cdot y_i + a_j \cdot 1 \cdot (mod\ m_j)$$

$$\rightarrow \quad x \equiv 0 + a_j(mod\ m_j)$$

$$\rightarrow \quad x \equiv a_j(mod\ m_j), \quad 1 \leq j \leq k$$

De lo cual se deduce que x satisface todas las congruencias del sistema, es decir, es una solución del sistema.

- **Segunda parte**

  Para probar la unicidad modulo M supongamos que x_1 y x_2 son soluciones del sistema, entonces demostraremos que $x_1 \equiv x_2(mod\ M)$.

  Puesto que $x_1 \equiv a_j(mod\ m_j)$ y $x_2 \equiv a_j(mod\ m_j)$ para $1 \leq j \leq k$ De donde $x_1 - x_2 \equiv 0(mod\ m_j)$ entonces $\dfrac{m_j}{x_1 - x_2}$.

  Por otra parte, como $m_1, m_2, \ldots, m_k$ son primos relativos dos a dos entonces por el corolario 1.4 del teorema 1.10 del capítulo 1 $M = MCD\{m_1, m_2, \ldots, m_k\} = m_1m_2 \ldots m_k$, y como además , $m_1, m_2, \ldots, m_k$, $x_1 - x_2 \in \mathbb{Z}^+$, $\dfrac{m_i}{x_1 - x_2}$ con $1 \leq i \leq k$ entonces por el corolario 1.5 del teorema 1.10 del capítulo 1 se tiene que $M = \dfrac{MCD\{m_1, m_2, \ldots, m_k\}}{x_1 - x_2}$, de lo que se sigue que $x_1 - x_2 \equiv 0(mod\ M)$

  Por lo tanto $x_1 \equiv x_2(mod\ M) \cdot$ ■

Nota 2.4. De la demostración del teorema chino de los restos se obtiene que:

$$y_i \equiv M_i^{-1}(mod\ m_i)$$

Ejemplo 2.16. Resolver

$x \equiv 2(mod\ 3)$

$x \equiv 3(mod\ 5)$

$x \equiv 2(mod\ 7)$

Solución

Puesto que $3, 5, 7$ son coprimos, es decir $MCD\{3,5\} = 1$; $MCD\{3,7\} = 1$ $MCD\{5,7\} = 1$ de acuerdo con el teorema chino de los restos, el sistema tiene una única solución dada por

$$x = (2M_1y_1 + 3M_2y_2 + 2M_3y_3)(mod\ M)$$

Con $M = (3)(5)(7) = 105$; $M_1 = \frac{105}{3} = 35$; $M_2 = \dfrac{105}{5} = 21$; $M_3 = \dfrac{105}{7} = 15$
Además de acuerdo con la nota anterior

$y_1 \equiv M_1^{-1}(mod\ 3)$; $y_2 \equiv M_2^{-1}(mod\ 5)$; $y_3 \equiv M_3^{-1}(mod\ 7)$
De donde

$y_1 \equiv 35^{-1}(mod\ 3) = 2$ ya que $\frac{35}{3} = 11(3) + 2$
$y_2 \equiv 21^{-1}(mod\ 5) = 1$ ya que $\frac{21}{5} = 4(5) + 1$
$y_3 \equiv 15^{-1}(mod\ 7) = 1$ ya que $\frac{15}{7} = 2(7) + 1$
Usando los resultados anteriores se tiene

$$x = (2(35)(2) + 3(21)(1) + 2(15)(1))(mod\ 105)$$

$$\rightarrow x = (233)(mod\ 105)$$

Y como $\dfrac{233}{105} = (2)105 + 23$ se concluye que $x = (23)(mod\ 105)$.
Es la única solución del sistema. ■

Capítulo 3:

Cifrado de Información en el Sistema RSA

3.1 Criptografía

Las raíces etimológicas de la palabra Criptografía son **criptos** (oculto), y **graphos** (escritura). Una definición clásica de **Criptografía** es la siguiente:**Arte de escribir mensajes en clave secreta o enigmáticamente**.
Es decir, anteriormente la Criptografía era considerada como un arte pero en la actualidad se considera una ciencia gracias a su relación con la estadística, la teoría de la información, la teoría de los números y la teoría de la complejidad computacional. Lo cual origina la siguiente definición.

Definición 3.1. La Criptografía es la ciencia que se encarga del estudio de técnicas para transformar la información a una forma que no pueda entenderse a simple vista; sin embargo, el objetivo de la Criptografía no es sólo mantener los datos secretos, sino también protegerlos contra modificación y comprobar la fuente de los mismos.

Otros conceptos relacionados son los siguientes.

El Criptoanálisis es la ciencia que se ocupa del análisis de un texto cifrado para obtener la información original sin conocimiento de la clave secreta, esto es, de forma ilícita rompiendo así los procedimientos de cifrado establecidos por la Criptografía, por lo que se dice que Criptoanálisis y Criptografía son ciencias complementarias pero contrarias.

La Esteganografía por su parte, estudia la forma de ocultar la existencia de un mensaje. Esta ciencia consiste en esconder en el interior de un mensaje, otro mensaje secreto, el cual sólo podrá ser entendido por el emisor y el receptor y pasará inadvertido para todos los demás.

La Criptografía se subdivide en **Criptografía Simétrica** (Clave secreta) y **Criptografía Asimétrica** (Clave pública).

3.1.1 Criptografía Simétrica

Utiliza una clave secreta para la encriptación y desencriptación del mensaje. Esta clave se debe intercambiar entre los equipos por medio de un canal seguro. Ambos equipos deben tener la misma clave para cumplir con el proceso. Los algoritmos de encriptación simétricos mezclan la trasposición y la permutación, los sistemas de clave simétrica ofrecen confidencialidad sin embargo no ofrecen: autenticidad, integridad, confidencialidad en el envío y no repudio si van asociados a una firma digital.
Para que un algoritmo de este tipo sea considerado fiable debe cumplir algunos requisitos básicos:

- Conocido el criptograma (texto cifrado) no se pueden obtener de él ni el texto en claro ni la clave.
- Conocidos el texto en claro y el texto cifrado debe resultar más caro en tiempo o dinero descifrar la clave que el valor posible de la información obtenida por terceros.

Todos los sistemas criptográficos clásicos se pueden considerar simétricos, y los principales algoritmos simétricos actuales son DES, IDEA y RC5. Las principales desventajas de los métodos simétricos son la distribución de las claves, el peligro de que muchas personas deban conocer una misma clave y la dificultad de almacenar y proteger muchas claves diferentes.

DES: El Algoritmo de encriptación DES trabaja con claves simétrica, fue desarrollado en 1977 por la empresa IBM, se basa en un sistema mono alfabético, con un algoritmo descifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones.

Inicialmente el texto a cifrar se somete a una permutación, con bloque de entrada de 64 bits (o múltiplo de 64), para posteriormente ser sometido a la acción de dos funciones principales, una función de permutación con entrada de 8 bits y otra de sustitución con entrada de 5 bits, en un proceso que consta de 16 etapas de cifrado.

En general, DES utiliza una clave simétrica de 64 bits, de los cuales 56 son usados para la encriptación, mientras que los 8 restantes son de paridad, y se usan para la detección de errores en el proceso.

DES ya no es estándar y fue crackeado en Enero de 1999 con un poder de cómputo que efectuaba aproximadamente 250 mil millones de ensayos en un segundo Actualmente se utiliza el Triple DES con una clave de 128 bits y que es compatible con el DES visto anteriormente. Este nuevo algoritmo toma una clave de 128 bits y la divide en dos de 64 bits cada una, de la siguiente forma:

- Se le aplica al documento a cifrar un primer cifrado mediante la primera clave, C1.
- Al resultado (denominado ANTIDES) se le aplica un segundo cifrado con la segunda clave, C2.
- Y al resultado se le vuelve a aplicar un tercer cifrado con la primera clave, C1.

RC5: Este sistema es el sucesor de RC4, que consistía en hacer un XOR al mensaje con un vector que se supone aleatorio y que se desprende de la clave, mientras que RC5 usa

otra operación, llamada dependencia de datos, que aplica sifths a los datos para obtener así el mensaje cifrado.
IDEA: Trabaja con bloques de texto de 64 bits, operando siempre con números de 16 bits usando operaciones como XOR y suma y multiplicación de enteros.

El algoritmo de desencriptación es muy parecido al de encriptación, por lo que resulta muy fácil y rápido de programar, y hasta ahora no ha sido roto nunca, aportando su longitud de clave una seguridad fuerte ante los ataques por fuerza bruta (prueba y ensayo o diccionarios).

Este algoritmo es de libre difusión y no está sometido a ningún tipo de restricciones o permisos nacionales, por lo que se ha difundido ampliamente, utilizándose en sistemas como UNIX y en programas de cifrado de correo como PGP.

3.1.2 Criptografía Asimétrica

Utiliza dos claves diferentes, que poseen una propiedad fundamental: una clave puede desencriptar lo que la otra a encriptado. Una de las claves, llamada clave pública, es usada por su propietario para encriptar los mensajes, mientras que la otra clave, llamada clave privada, es usada para la desencriptación del mensaje.
Las claves pública y privada tienen características matemáticas especiales, por ejemplo se generan siempre a la vez, por parejas, estando cada una de ellas ligada intrínsecamente a la otra.
Mientras que la **clave privada** debe mantenerla en secreto su propietario, ya que es la base de la seguridad del sistema, la **clave pública** (de allí porque a la criptografía asimétrica también se le llama criptografía de clave pública) es difundida, para que esté al alcance del mayor número posible de personas, existiendo servidores que guardan, administran y difunden dichas claves.

Para que un algoritmo de clave pública sea considerado seguro debe cumplir con los siguientes puntos:

- Conocido el texto cifrado no debe ser posible encontrar el texto en claro ni la clave privada.
- Conocido el texto cifrado (criptograma) y el texto en claro debe resultar más caro en tiempo o dinero descifrar la clave que el valor posible de la información obtenida por terceros.
- Conocida la clave pública y el texto en claro no se puede generar un criptograma correcto encriptado con la clave privada.
- Dado un texto encriptado con una clave pública sólo existe una clave privada capaz de desencriptarlo, y viceversa.

Dentro de los sistemas asimétricos destacan el de Diffie-Hellman, el cual apareció en 1976, y fue la base para el desarrollo de los que después aparecieron, entre los que cabe destacar el RSA.

Diffie-Hellman: Este algoritmo de encriptación de Whitfield Diffie y Martin Hellman fue el punto de partida para los sistemas asimétricos, basados en claves pública y la privada.

Su importancia se debe sobre todo al hecho de ser el inicio de los sistemas asimétricos, ya que en la práctica sólo es válido para el intercambio de claves simétricas, y con esta funcionalidad es muy usado en los diferentes sistemas seguros implementados en Internet, como SSL (Secure Socket Layer) y VPN (Virtual Private Network).

Matemáticamente se basa en las potencias de los números y en la función mod (módulo discreto). Uniendo estos dos conceptos se define la potencia discreta de un número como $y = x^a (mod\ q)$. Si bien el cálculo de potencias discretas es fácil, la obtención de su fun-

ción inversa, el logaritmo discreto, no tiene una solución analítica para números grandes.

El sistema RSA será tratado en la siguiente sección.

3.2 Sistema RSA

Debe su nombre a sus tres inventores, los matemáticos: Ronald Rivest, Adi Shamir y Leonard Adleman, de allí el nombre RSA, es el más conocido y usado de los sistemas de clave pública, y también el más rápido de ellos. Este sistema emplea la doble clave: Pública y Privada. Las claves pública y privada se calculan a partir de un número que se obtiene como producto de dos primos grandes. Un atacante que quiere recuperar un texto claro a partir del criptograma y de la clave pública, tiene que enfrentarse a dicho problema de factorización. Este sistema presenta todas las ventajas de los sistemas asimétricos, incluyendo la firma digital, aunque resulta más útil a la hora de implementar la confidencialidad el uso de sistemas simétricos, por ser más rápidos. Se suele usar también en los sistemas mixtos para encriptar y enviar la clave simétrica que se usará posteriormente en la comunicación cifrada.

DETERMINACIÓN DE LOS PARÁMETROS DEL SISTEMA RSA

Antes se revisa una definición y resultados muy útiles para el desarrollo de esta sección.

3.3 Función Phi de Euler

Definición 3.2. Para cada $n \geq 1$, se denota por $\varphi(n)$ a la cantidad de enteros menores que n y coprimos con n . A esta función se le llama **función phi de Euler**.

Ejemplo 3.1. $\varphi(24) = 8$ pues $1, 5, 11, 13, 17, 19$ y 23 son coprimos con 24 inferiores a 24

Nota 3.1. Recordemos que $a \in \mathbb{Z}_n$ tiene inverso si $MCD\{a, n\} = 1$, de donde se sigue que $\varphi(n)$ calcula la cantidad de **unidades** en $\mathbb{Z}_n$. Por lo tanto si p es primo entonces $\varphi(P) = p - 1$.

Ejemplo 3.2. Sea $\mathbb{Z}_9$ luego de acuerdo con la siguiente tabla

a	1	2	3	4	5	6	7	8
$MCD\{a, 9\}$	1	1	3	1	1	3	1	1

Luego hay 9 unidades en $\mathbb{Z}_9$ es decir $\varphi(9) = 6$

Teorema 3.1. *Si p es primo si y solamente si $\varphi(p) = p - 1$*

Demostración.

- **Condición necesaria:** Si p es primo entonces $\varphi(p) = p - 1$.
  Se sigue de la nota anterior, puesto que si p es primo entonces $\mathbb{Z}_p = \{1, 2, \ldots, p-1\}$ es decir $MCD\{p, a\} = 1$ para todo $a = 1, 2, \ldots, p - 1$ de donde por el teorema 2.4 cada $a \in \mathbb{Z}_p$ es una unidad y por definición se sigue que $\varphi(p) = p - 1$.

- **Condición suficiente:** Si $\varphi(p) = p - 1$ entonces p es primo.
  Si $\varphi(p) = p - 1$ significa que hay exactamente $p - 1$ enteros positivos menores que p puesto que $\varphi(p) = p - 1$, ninguno de estos $p - 1$ enteros divide al número primo p , por lo tanto p es primo. ■

3.3.1 Propiedades de la Función Euler

A continuación enumeramos algunas propiedades importantes de la función de Euler.

1. Si $MCD\{n, m\} = 1$ entonces $\varphi(nm) = \varphi(n)\varphi(m)$

2. Si n es compuesto entonces $\varphi(n) < n - 1$

3. Si $n > 1$ entonces $a^{\varphi(n)} \equiv 1(mod\, p)$ para todo elemento del subgrupo multiplicativo $\mathbb{Z}_n$.

4. Si p y q son primos relativos entonces $\varphi(pq) = (p-1)(q-1)$

Los parámetros del sistema RSA serán denotados por n, p, q, e, d a continuación se describe como obtener cada uno de ellos.

Dados dos números primos p, q ambos muy grandes, escogidos de manera aleatoria, se define el parámetro n por la igualdad

$$n = pq$$

A este número se le llamará **módulo.**
Nótese que la seguridad del sistema depende de que los números primos p y q una vez que se ha generado el módulo n , deban ser guardados en secreto, puesto que si son conocidos por cualquier persona, esta podría eventualmente obtener la **clave privada**, y por lo tanto podría acceder al mensaje cifrado.

El parámetro d llamado **exponente privado** del sistema, se elige de modo que sea menor que n y que además sea primo relativo con la función de Euler evaluada en n , es decir de acuerdo con la propiedad 4 de la función Euler, debe ser primo relativo con el número $(p-1)(q-1)$, que ocurre cuando por la identidad de Bezout existen $s, t \in \mathbb{Z}$ tales que:

$$s(p-1) + t(q-1) = 1$$

El parámetro e llamado **exponente público** del sistema, se elige de modo que satisfaga la ecuación:
$ed \equiv 1(mod(p-1)(q-1))$ y además $1 \leq e \leq (p-1)(q-1)$
La relación entre e y d asegura una correcta reconstrucción de los mensajes encriptados.

La clave pública está formada por el par ordenado (n, e) mientras que la **clave privada** está dada por el par ordenado (n, d) , como ya se dijo con la clave pública se encripta el mensaje, y con la clave privada se desencripta dicho mensaje cifrado.

3.4 Encriptado y Desencritado de la Información

Para encriptar un mensaje m se divide el mensaje en bloques del mismo tamaño M, y se siguen los siguientes pasos:

1. Se escogen de manera aleatoria dos números primos p y q , ambos muy grandes.
2. Se halla n mediante la ecuación $n = pq$.
3. Se calcula d de modo que $d < n$, el cual debe ser coprimo con el número $\varphi(n) = (p-1)(q-1)$, para lo cual se elige d en el intervalo $[Max\{p, q\}] + 1,\ n-1]$
4. Se determina e de la siguiente relación $ed \equiv 1(mod(p-1)(q-1))$ con $1 \leq e \leq (p-1)(q-1)$
5. Se determina la clave privada dada por el par ordenado (n, d).
6. Se determina la clave pública dada por el par ordenado (n, e).
7. Asociamos a cada carácter del alfabeto un valor numérico con lo cual se cifra el mensaje m en bloques del mismo tamaño M . Este valor numérico está comprendido en un cierto rango $1, 2, 3, \ldots, n$.
8. Se cifra cada uno de los bloques de tamaño M se usa la clave pública (n, e) mediante la siguiente relación
$$C = M^e (mod\ n)$$
9. Para descifrar C y así obtener el mensaje m se usa la clave privada mediante la relación.
$$M = C^d (mod\ n)$$

Antes de mostrar un ejemplo ilustrativo para el encriptado y desencriptado de un mensaje se necesita implementar un método que nos permite calcular potencias en el anillo modular $\mathbb{Z}_n$

3.4.1 Método Para Calcular $n^{\alpha}(mod\ m)$

Para calcular $n^{\alpha}(mod\ m)$ se procede como sigue:

1. Se expresa la potencia α en el sistema binario, es decir se escribe α como sigue:

$$\alpha = 2^r + \alpha_{r-1}2^{r-1} + \ldots + \alpha_1 2 + \alpha_0; \quad \alpha_i = 1; \quad 0 \leq i \leq r-1$$

2. En el número binario obtenido intercalamos C entre cada dos cifra consecutivas.

3. Sustituimos los UNOS por M y eliminamos los ceros.

4. Empezando por 1 se tiene que M equivale a multiplicar por n mientras que C equivale a elevar al cuadrado.

Este método nos asegura que, para cualquier α el número de multiplicaciones que requiere el cálculo de n^{α} es como máximo el doble del número de dígitos de la expresión binaria de α es decir como máximo $2(1 + log(\alpha))$.

Ejemplo 3.3. Calcular $1305^{17}(mod\ 2773)$

Solución

Sigamos el método descrito anteriormente.

1. Se expresa la potencia $\alpha = 17$ en el sistema binario, es decir se escribe α como sigue:

$$17{=}1.2^4{+}0.2^3{+}0.2^2{+}0.2^1{+}1.2^0$$

$$\rightarrow 17{=}\ 10001_{(2)}$$

2. En el número binario obtenido intercalamos C entre cada dos cifra consecutivas, es decir:

$$1C0C0C0C1$$

3. Sustituimos los UNOS por M y eliminamos los ceros. Es decir:

$$MCCCCM$$

4. Empezando por 1 se tiene que M equivale a multiplicar por n mientras que C equivale a elevar al cuadrado. Es decir:

$$1 \xrightarrow{M} 1305 \xrightarrow{C} 1305^2 \xrightarrow{C} [[1305]^2]^2 \xrightarrow{C} \left[[[1305]^2]^2\right]^2 \xrightarrow{C} \left[\left[[[1305]^2]^2\right]^2\right]^2 \xrightarrow{M} \left[\left[[[11305305]^2]^2\right]^2\right]^2$$

De donde:

$$1305^{17}(mod\ 2773) = \left[\left[[[1305]^2]^2\right]^2\right]^2 (1305)(mod\ 2773)$$

$$\rightarrow 1305^{17}(mod\ 2773) \equiv \left[\left[[1703025]^2\right]^2\right]^2 (1305)(mod\ 2773)$$

Puesto que $1703025 \equiv 403(mod\ 2773)$ entonces $[1703025]^2 = [403]^2 = 162409$

$$\rightarrow 1305^{17}(mod\ 2773) \equiv \left[\left[162409\right]^2\right]^2 (1305)(mod\ 2773)$$

$$\rightarrow 1305^{17}(mod\ 2773) \equiv \left[26376683281\right]^2 (1305)(mod\ 2773)$$

Puesto que $26376683281 \equiv (1563)(mod\ 2773)$ entonces

$$\rightarrow 1305^{17}(mod\ 2773) \equiv [1563]^2 (1305)(mod\ 2773)$$

$$\rightarrow 1305^{17}(mod\ 2773) \equiv 2442969\ (1305)(mod\ 2773)$$

$$\rightarrow 1305^{17}(mod\ 2773) \equiv 3188074545(mod\ 2773)$$

Puesto que $3188074545 \equiv 813(mod\ 2773)$ entonces

$$\rightarrow 1305^{17}(mod\ 2773) \equiv 813(mod\ 2773)$$

Por lo tanto $1305^{17}(mod\ 2773) \equiv 813(mod\ 2773)$ ■

En la última sección mostramos aplicaciones del teorema chino de los restos en el envío de mensajes y de imágenes.

3.5 Envío de Información Usando Teorema Chino de los Restos

EJEMPLO ILUSTRATIVO DE ENCRIPTADO DE UN MENSAJE

Para el envío de un mensaje de texto usaremos el siguiente alfabeto para implementar el sistema de envío del mensaje.

01	02	03	04	05
A	B	C	D	5
06	07	08	09	10
F	G	H	I	J
11	12	13	14	15
K	L	M	N	O
16	17	18	19	20
P	Q	R	S	T
21	22	23	24	25
U	V	W	X	Y
26				
Z				

Tabla 01

De acuerdo con la Real Academia española (REA), la única letra que no se ha considerado en el sistema anterior es la ñ. Nuestro mensaje a enviar será la conocida cita latina **"MENS SANA IN CORPORE SANO"** (sátiras de Juvenal), que como sabemos traducida al castellano significa "Mente sana en un cuerpo sano".

Para lo cual dividiremos el mensaje en bloques iguales de tamaño dos, es decir $M = 2$.

Ahora desarrollaremos cada uno de los pasos para encriptar y desencriptar un mensaje.

1. Elegimos de manera aleatoria los dos números primos $p = 47$ y $q = 59$.

2. De donde se tiene que $n = (47)(59)$, es decir $n = 2773$.

3. Se calcula $d \in [Max\{p, q\} + 1;\ \ n - 1] \rightarrow d \in [59, 2772]$ de modo que $d < 2772$, el cual debe ser coprimo con el número $\varphi(2773) = (p-1)(q-1) = (46)(58)$, es decir d debe ser coprimo con 2668, de donde $d = 157$

4. Se determina e de la siguiente relación

$$ed \equiv 1(mod\ (p-1)(q-1)) \rightarrow e(157) \equiv 1(mod\ 2668)$$

Puesto que $(157)(17) = 2669$ entonces $2669 \div 2668 = 2668 + 1$, es decir

$$(157)(17) \equiv 1(mod\ 2668)$$

Por lo tanto $e = 17$

5. Se determina la clave privada dada por el par ordenado (n, d) , que en este caso viene dado por $(n, d) = 2773, 157$. Es decir:
La clave privada es $(2773, 157)$

6. Se determina la clave pública dada por el par ordenado $(n, e) = (2773, 17)$. Es decir:
La clave pública es $(2773, 17)$

7. Asociamos a cada carácter del alfabeto un valor numérico con lo cual se cifra el mensaje m en bloques del mismo tamaño $M = 2$. Este valor numérico está comprendido en un cierto rango $1, 2, 3, \ldots, 2773$.
Usando $\phi = 00$ y la tabla 01 se tiene

M	E		N	S		S	A		N	A		I	N		C	O		R	P
13	05		14	19		19	01		14	01		09	14		03	15		18	16

O	R		E	ϕ		S	A		N	O	
15	18		05	00		19	01		14	15	

Formándose así los siguientes bloques

$M_0 = 1305$; $M_1 = 1419$; $M_2 = 1901$; $M_3 = 1401$; $M_4 = 0914$; $M_5 = 0315$;

$M_6 = 1816$; $M_7 = 1518$; $M_8 = 0500$;$M_9 = 1901$; $M_{10} = 1415$

8. Se cifra cada uno de los bloques de tamaño M se usa la clave pública $(2773, 17)$ mediante la siguiente relación

$$C_i \equiv M_i^{17}(mod\ 2773);\quad 0 \leq i \leq 10$$

de donde se tiene:

$$C_0 \equiv M_0^{17}(mod\ 2773) \rightarrow C_0 = (1305)^{17}(mod\ 2773)$$

Luego, de acuerdo con el ejemplo se tiene que $C_0 \equiv 813(mod\ 2773)$

Es decir $C_0 = 813$ es el primer bloque del mensaje cifrado.

CÁLCULO DEL SEGUNDO BLOQUE DEL MENSAJE CIFRADO $C_1 = M_1^{17}(mod\ 2773) \rightarrow C_1 = (1419)^{17}(mod2773)$

$$\rightarrow C_1 = (1419)^{17}(mod2773) = \left[\left[\left[[1419]^2\right]^2\right]^2\right]^2 (1419)(mod\ 2773)$$

$$\rightarrow C_1 = \left[\left[\left[2013561\right]^2\right]^2\right]^2 (mod\ 2773)$$

Puesto que $2013561 \equiv 363(mod\ 2773)$ entonces

$$\rightarrow C_1 = \left[\left[\left[363\right]^2\right]^2\right]^2 (1419)(mod\ 2773)$$

$$\rightarrow C_1 = \left[\left[131769\right]^2\right]^2 (1419)(mod\ 2773)$$

$$\rightarrow C_1 = \left[17363069361\right]^2 (1419)(mod\ 2773)$$

Puesto que $17363069361 \equiv 1959(mod\ 2773)$ entonces

$$\rightarrow C_1 = \left[1959\right]^2 (1419)(mod\ 2773)$$

$$\rightarrow C_1 = 3837681\ (1419)(mod\ 2773)$$

Puesto que $3837681 \equiv 2622(mod\ 2773)$ entonces

$$\rightarrow C_1 = 2622\ (1419)(mod\ 2773)$$

$$\rightarrow C_1 = 3720618(mod\ 2773)$$

Puesto que $3720618 \equiv 2622(mod\ 2773)$ entonces

$$\rightarrow C_1 = 2025(mod\ 2773)$$

CÁLCULO DEL TERCER BLOQUE DEL MENSAJE CIFRADO

$C_2 = M_2^{17}(mod\ 2773) \rightarrow C_2 = (1901)^{17}(mod2773)$

$$\rightarrow C_2 = \left[\left[\left[[1901]^2\right]^2\right]^2\right]^2 (1901)(mod\ 2773)$$

$$\rightarrow C_2 = \left[\left[\left[3613801\right]^2\right]^2\right]^2 (1901)(mod\ 2773)$$

Puesto que $3613801 \equiv 582(mod\ 2773)$ entonces

$$\rightarrow C_2 = \left[\left[\left[582\right]^2\right]^2\right]^2 (1901)(mod\ 2773)$$

$$\rightarrow C_2 = \left[\left[338724\right]^2\right]^2 (1901)(mod\ 2773)$$

Puesto que $338724 \equiv 418(mod\ 2773)$ entonces

$$\rightarrow C_2 = \left[\left[418\right]^2\right]^2 (1901)(mod\ 2773)$$

$$\rightarrow C_2 = \left[174724\right]^2 (1901)(mod\ 2773)$$

Puesto que $30528476176 \equiv 625(mod\ 2773)$ entonces

$\rightarrow C_2 = 625(1901)(mod\ 2773)$

$\rightarrow C_2 = 1188125(mod\ 2773)$

Puesto que $1188125 \equiv 1281(mod\ 2773)$ entonces

$\rightarrow C_2 = 1281(mod\ 2773)$

CÁLCULO DEL CUARTO BLOQUE DEL MENSAJE CIFRADO

$C_3 = M_3^{17}(mod\ 2773) \rightarrow C_3 = (1401)^{17}(mod 2773)$

$$\rightarrow C_3 = \left[\left[\left[1401\right]^2\right]^2\right]^2 (1401)(mod\ 2773)$$

$$\rightarrow C_3 = \left[\left[\left[1962801\right]^2\right]^2\right]^2 (1401)(mod\ 2773)$$

Puesto que $1962801 \equiv 2290(mod\ 2773)$ entonces

$$\rightarrow C_3 = \left[\left[\left[2290\right]^2\right]^2\right]^2 (1401)(mod\ 2773)$$

$$\rightarrow C_3 = \left[\left[5244100\right]^2\right]^2 (1401)(mod\ 2773)$$

Puesto que $5244100 \equiv 357(mod\ 2773)$ entonces

$$\rightarrow C_3 = \left[\left[357\right]^2\right]^2 (1401)(mod\ 2773)$$

$$\rightarrow C_3 = \left[127449\right]^2 (1401)(mod\ 2773)$$

Puesto que $127449 \equiv 2664(mod\ 2773)$ entonces

$\rightarrow C_3 = [2664]^2\ (1401)(mod\ 2773)$

$\rightarrow C_3 = (7096896)(1401)(mod\ 2773)$

Puesto que $7096896 \equiv 789(mod\ 2773)$ entonces

$\rightarrow C_3 = 789(1401)(mod\ 2773)$

$\rightarrow C_3 = 1105389(mod\ 2773)$

Puesto que $1105389 \equiv 1735(mod\ 2773)$ entonces

$\rightarrow C_3 = 1735(mod\ 2773)$

CÁLCULO DEL QUINTO BLOQUE DEL MENSAJE CIFRADO

$C_4 = M_4^{17}(mod\ 2773) \rightarrow C_4 = (914)^{17}(mod 2773)$

$$\rightarrow C_4 = \left[\left[\left[[914]^2\right]^2\right]^2\right]^2 (914)(mod\ 2773)$$

$$\rightarrow C_4 = \left[\left[\left[835396\right]^2\right]^2\right]^2 (914)(mod\ 2773)$$

Puesto que $835396 \equiv 723(mod\ 2773)$ entonces

$$\rightarrow C_4 = \left[\left[\left[723\right]^2\right]^2\right]^2 (914)(mod\ 2773)$$

$$\rightarrow C_4 = \left[\left[522729\right]^2\right]^2 (914)(mod\ 2773)$$

Puesto que $522729 \equiv 1405(mod\ 2773)$ entonces

$$\rightarrow C_4 = \left[\left[1405\right]^2\right]^2 (914)(mod\ 2773)$$

$\rightarrow C_4 = \left[1974025\right]^2 (914)(mod\ 2773)$

Puesto que $1974025 \equiv 2422(mod\ 2773)$ entonces

$\rightarrow C_4 = [2422]^2\ (914)(mod\ 2773)$

$\rightarrow C_4 = (5866084)(914)(mod\ 2773)$

Puesto que $5866084 \equiv 1189(mod\ 2773)$ entonces

$\rightarrow C_4 = 1189(914)(mod\ 2773)$

$\rightarrow C_4 = 1086746(mod\ 2773)$

Puesto que $1086746 \equiv 2503(mod\ 2773)$ entonces

$\rightarrow C_4 = 2503(mod\ 2773)$

CÁLCULO DEL SEXTO BLOQUE DEL MENSAJE CIFRADO

$C_5 = M_5^{17}(mod\ 2773) \rightarrow C_5 = (315)^{17}(mod 2773)$

$$\rightarrow C_5 = \left[\left[\left[[315]^2\right]^2\right]^2\right]^2 (315)(mod\ 2773)$$

$$\rightarrow C_5 = \left[\left[\left[99225\right]^2\right]^2\right]^2 (315)(mod\ 2773)$$

$$\rightarrow C_5 = \left[\left[9845600625\right]^2\right]^2 (315)(mod\ 2773)$$

Puesto que $9845600625 \equiv 346(mod\ 2773)$ entonces

$$\rightarrow C_5 = \left[\left[346\right]^2\right]^2 (315)(mod\ 2773)$$

$$\rightarrow C_5 = \left[119716\right]^2 (315)(mod\ 2773)$$

Puesto que $119716 \equiv 477(mod\ 2773)$ entonces

$$\rightarrow C_5 = \left[\left[346\right]^2\right]^2 (315)(mod\ 2773)$$

$$\rightarrow C_5 = \left[477\right]^2 (315)(mod\ 2773)$$

$\rightarrow C_5 = 227529(315)(mod\ 2773)$

Puesto que $227529 \equiv 143(mod\ 2773)$ entonces

$\rightarrow C_5 = 143(315)(mod\ 2773)$

$\rightarrow C_5 = 45045(mod\ 2773)$

Puesto que $45045 \equiv 677(mod\ 2773)$ entonces

$\rightarrow C_5 = 677(mod\ 2773)$

Puesto que $1086746 \equiv 2503(mod\ 2773)$ entonces

$\rightarrow C_5 = 2503(mod\ 2773)$

CÁLCULO DEL SÉPTIMO BLOQUE DEL MENSAJE CIFRADO

$C_6 = M_6^{17}(mod\ 2773) \rightarrow C_6 = (1816)^{17}(mod 2773)$

$$\rightarrow C_6 = \left[\left[\left[[1816]^2\right]^2\right]^2\right]^2 (1816)(mod\ 2773)$$

$$\rightarrow C_6 = \left[\left[\left[3297856\right]^2\right]^2\right]^2 (1816)(mod\ 2773)$$

Puesto que $3297856 \equiv 759(mod\ 2773)$ entonces

$$\rightarrow C_6 = \left[\left[[759]^2\right]^2\right]^2 (1816)(mod\ 2773)$$

$$\rightarrow C_6 = \left[\left[576081\right]^2\right]^2 (1816)(mod\ 2773)$$

$$\rightarrow C_6 = \left[331869318561\right]^2 (1816)(mod\ 2773)$$

Puesto que $331869318561 \equiv 615(mod\ 2773)$ entonces

$$\rightarrow C_6 = \left[615\right]^2 (1816)(mod\ 2773)$$

$\rightarrow C_6 = 378225(1816)(mod\ 2773)$

Puesto que $378225 \equiv 1097(mod\ 2773)$ entonces

$\rightarrow C_6 = 1097(1816)(mod\ 2773)$

$\rightarrow C_6 = 1992152(mod\ 2773)$

Puesto que $1992152 \equiv 1138(mod\ 2773)$ entonces

$\rightarrow C_6 = 1138(mod\ 2773)$

CÁLCULO DEL OCTAVO BLOQUE DEL MENSAJE CIFRADO

$C_7 = M_7^{17}(mod\ 2773) \rightarrow C_7 = (1518)^{17}(mod 2773)$

$$\rightarrow C_7 = \left[\left[\left[[1518]^2\right]^2\right]^2\right]^2 (1518)(mod\ 2773)$$

$$\rightarrow C_7 = \left[\left[\left[2304324\right]^2\right]^2\right]^2 (1518)(mod\ 2773)$$

Puesto que $2304324 \equiv 2734(mod\ 2773)$ entonces

$$\rightarrow C_7 = \left[\left[[2734]^2\right]^2\right]^2 (1518)(mod\ 2773)$$

$$\rightarrow C_7 = \left[[7474756]^2\right]^2 (1518)(mod\ 2773)$$

Puesto que $7474756 \equiv 1521(mod\ 2773)$ entonces

$$\rightarrow C_7 = \left[[1521]^2\right]^2 (1518)(mod\ 2773)$$

$\rightarrow C_7 = [2313441]^2(1518)(mod\ 2773)$

Puesto que $2313441 \equiv 759(mod\ 2773)$ entonces

$\rightarrow C_7 = 759(1518)(mod\ 2773)$

$\rightarrow C_7 = 1152162(mod\ 2773)$

Puesto que $1152162 \equiv 1367(mod\ 2773)$ entonces

$\rightarrow C_7 = 1367(mod\ 2773)$

CÁLCULO DEL NOVENO BLOQUE DEL MENSAJE CIFRADO

$C_8 = M_8^{17}(mod\ 2773) \rightarrow C_8 = (500)^{17}(mod 2773)$

$$\rightarrow C_8 = \left[\left[\left[[500]^2\right]^2\right]^2\right]^2 (500)(mod\ 2773)$$

$$\rightarrow C_8 = \left[\left[\left[250000\right]^2\right]^2\right]^2 (500)(mod\ 2773)$$

Puesto que $250000 \equiv 430(mod\ 2773)$ entonces

$$\rightarrow C_8 = \left[\left[[430]^2\right]^2\right]^2 (500)(mod\ 2773)$$

$$\rightarrow C_8 = \left[[184900]^2\right]^2 (500)(mod\ 2773)$$

Puesto que $184900 \equiv 1882(mod\ 2773)$ entonces

$$\rightarrow C_8 = \left[[1882]^2\right]^2 (500)(mod\ 2773)$$

$\rightarrow C_8 = [3541924]^2(500)(mod\ 2773)$

Puesto que $3541924 \equiv 803(mod\ 2773)$ entonces

$\rightarrow C_8 = [803]^2(500)(mod\ 2773)$

$\rightarrow C_8 = 644809(500)(mod\ 2773)$

Puesto que $644809 \equiv 1473(mod\ 2773)$ entonces

$\rightarrow C_8 = 1473(500)(mod\ 2773)$

$\rightarrow C_8 = 736500(mod\ 2773)$

Puesto que $736500 \equiv 1655(mod\ 2773)$ entonces

$\rightarrow C_8 = 1655(mod\ 2773)$

CÁLCULO DEL DÉCIMO BLOQUE DEL MENSAJE CIFRADO

$C_9 = M_9^{17}(mod\ 2773) \rightarrow C_9 = (1901)^{17}(mod 2773)$

$$\rightarrow C_9 = \left[\left[\left[[1901]^2\right]^2\right]^2\right]^2 (1901)(mod\ 2773)$$

$$\rightarrow C_9 = \left[\left[\left[3613801\right]^2\right]^2\right]^2 (1901)(mod\ 2773)$$

Puesto que $3613801 \equiv 582(mod\ 2773)$ entonces

$$\rightarrow C_9 = \left[\left[[582]^2\right]^2\right]^2 (1901)(mod\ 2773)$$

$$\rightarrow C_9 = \left[[338724]^2\right]^2 (1901)(mod\ 2773)$$

Puesto que $338724 \equiv 418(mod\ 2773)$ entonces

$$\rightarrow C_9 = \left[[418]^2\right]^2 (1901)(mod\ 2773)$$

$\rightarrow C_9 = [174724]^2(1901)(mod\ 2773)$

$\rightarrow C_9 = 30528476176(1901)(mod\ 2773)$

Puesto que $30528476176 \equiv 625(mod\ 2773)$ entonces

$\rightarrow C_9 = 625(1901)(mod\ 2773)$

$\rightarrow C_9 = 1188125(mod\ 2773)$

Puesto que $1188125 \equiv 1281(mod\ 2773)$ entonces

$\rightarrow C_9 = 1281(mod\ 2773)$

CÁLCULO DEL UN DÉCIMO BLOQUE DEL MENSAJE CIFRADO

$C_{10} = M_{10}^{17}(mod\ 2773) \rightarrow C_{10} = (1415)^{17}(mod 2773)$

$$\rightarrow C_{10} = \left[\left[\left[[1415]^2\right]^2\right]^2\right]^2 (1415)(mod\ 2773)$$

$$\rightarrow C_{10} = \left[\left[\left[2002225\right]^2\right]^2\right]^2 (1415)(mod\ 2773)$$

Puesto que $2002225 \equiv 119(mod\ 2773)$ entonces

$\rightarrow C_{10} = \left[\left[[119]^2\right]^2\right]^2 (1415)(mod\ 2773)$

$\rightarrow C_{10} = \left[[14161]^2\right]^2 (1415)(mod\ 2773)$

$\rightarrow C_{10} = \left[200533921\right]^2 (1415)(mod\ 2773)$

Puesto que $200533921 \equiv 1653(mod\ 2773)$ entonces

$\rightarrow C_{10} = \left[1653\right]^2 (1415)(mod\ 2773)$

$\rightarrow C_{10} = 2732409(mod\ 2773)$

Puesto que $2732409 \equiv 1004(mod\ 2773)$ entonces

$\rightarrow C_{10} = 1004(mod\ 2773)$

Recordemos que los bloques son de tamaño dos, luego hay que completar con ceros en la primera cifra tanto C_0 como C_5 luego el mensaje cifrado es:

C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}
0813	2025	1281	1735	2503	0677	1138	1367	1655	1281	1004

9. Para descifrar C y así obtener el mensaje m se usa la clave privada mediante la relación.

$$M_i = C_i^{157}(mod\ 2773),\ 0 \leq i \leq 10$$

El procedimiento es análogo al explicado en el paso (8).

Por ejemplo: $M_0 = C_0^{157}(mod\ 2773) \longrightarrow M_0 = 813^{157}(mod\ 2773)$

$157 \equiv 10011101_2$

De donde:

$$M_0 = (813)^{157} = [813]^{156}(813) = \left[\left[\left[\left[[[[813]^2]^2]^2(813)\right]^2(813)\right]^2\right]^2\right]^2 (813)$$

$$M_0 = \left[\left[\left[[436880018961]^2(813)\right]^2(813)\right]^2(813)\right]^2(813)(mod\ 2773)$$

Puesto que $436880018961 \equiv 64(mod\ 2773)$ entonces:

$$M_0 = \left[\left[\left[[64]^2(813)\right]^2(813)\right]^2(813)\right]^2(813)(mod\ 2773)$$

$$M_0 = \left[\left[\left[[4096(813)]^2(813)\right]^2(813)\right]^2(813)(mod\ 2773)$$

$$M_0 = \left[\left[\left[3330048\right]^2(813)\right]^2\right]^2(813)(mod\ 2773)$$

Puesto que $3330048 \equiv 2448(mod\ 2773)$ entonces

$$M_0 = \left[\left[\left[[2448]^2(813)\right]^2(813)\right]^2\right]^2(813)(mod\ 2773)$$

$$M_0 = \left[\left[\left[(5992704)(813)\right]^2(813)\right]^2\right]^2(813)(mod\ 2773)$$

Puesto que $5992704 \equiv 251(mod\ 2773)$ entonces

$$M_0 = \left[\left[\left[(251)(813)\right]^2(813)\right]^2\right]^2(813)(mod\ 2773)$$

$$M_0 = \left[\left[\left[204063\right]^2(813)\right]^2\right]^2(813)(mod\ 2773)$$

$$M_0 = \left[\left[41641707969(813)\right]^2\right]^2(813)(mod\ 2773)$$

Puesto que $41641707969 \equiv 2330(mod\ 2773)$ entonces

$$M_0 = \left[\left[2330(813)\right]^2\right]^2(813)(mod\ 2773)$$

$$M_0 = \left[\left[1894290\right]^2\right]^2(813)(mod\ 2773)$$

$$M_0 = \left[349098704100\right]^2(813)(mod\ 2773)$$

Puesto que $349098704100 \equiv 2309(mod\ 2773)$ entonces

$$M_0 = \Big[2309\Big]^2(813)(mod\ 2773)$$

$$M_0 = (5331481)(813)(mod\ 2773)$$

Puesto que $5331481 \equiv 1775(mod\ 2773)$ entonces

$$M_0 = (1775)(813)(mod\ 2773) = 1305(mod\ 2773)$$

$M_1 = 2025^{157}(mod\ 2773)$

$M_1 = (2025)^{157}$

$M_1 = (2025)^{156}(2025)$

$$M_1 = \Big[\Big[\Big[[[[[2025]^2]^2]^2(2025)]^2(2025)\Big]^2(2025)\Big]^2\Big]^2(2025)$$

$$M_1 = \Big[\Big[\Big[[[4100625]^2]^2(2025)]^2(2025)\Big]^2(2025)\Big]^2\Big]^2(2025)$$

Puesto que $4100625 \equiv 2131 mod(2773)$

$$M_1 = \Big[\Big[\Big[[[2131]^2]^2(2025)]^2(2025)\Big]^2(2025)\Big]^2\Big]^2(2025)$$

$$M_1 = \Big[\Big[\Big[[4541161]^2(2025)]^2(2025)\Big]^2(2025)\Big]^2\Big]^2(2025)$$

Puesto que $4541161 \equiv 1760 mod(2773)$

$$M_1 = \Big[\Big[\Big[[1760]^2(2025)]^2(2025)\Big]^2(2025)\Big]^2\Big]^2(2025)$$

$$M_1 = \Big[\Big[\Big[[3097600](2025)]^2(2025)\Big]^2(2025)\Big]^2\Big]^2(2025)$$

Puesto que $3097600 \equiv 159 mod(2773)$

$$M_1 = \left[\left[\left[(159)(2025)\right]^2(2025)\right]^2(2025)\right]^2(2025)$$

$$M_1 = \left[\left[\left[321975\right]^2(2025)\right]^2(2025)\right]^2(2025)$$

Puesto que $321975 \equiv 307 mod(2773)$

$$M_1 = \left[\left[\left[307\right]^2(205)\right]^2(2025)\right]^2(2025)$$

$$M_1 = \left[\left[\left[190854225\right]^2(2025)\right]^2\right]^2(2025)$$

Puesto que $190854225 \equiv 2500 mod(2773)$

$$M_1 = \left[\left[\left[6250000(2025)\right]^2\right]^2(2025)\right]$$

Puesto que $6250000 \equiv 2431 mod(2773)$

$$M_1 = \left[\left[2431(2025)\right]^2\right]^2(2025)$$

$$M_1 = \left[\left[4922775\right]^2\right]^2(2025)$$

Puesto que $4922775 \equiv 700 mod(2773)$

$$M_1 = \left[\left[700\right]^2\right]^2(2025)$$

$$M_1 = \left[490000\right]^2(2025)$$

$M_1 = (1952)^2(2025)$

$M_1 = 3810304(2025)$

Puesto que $3810304 \equiv 202 mod(2773)$

$M_1 = 202(2025)$

$M_1 = 409050$

Puesto que $409050 \equiv 1419 mod(2773)$

Entonces $M_1 = 1419$

$M_2 = 1281^{157}(mod\ 2773)$

$M_2 = (1281)^{156}(1281)$

$$M_2 = \left[\left[\left[\left[\left[[[[1281]^2]^2]^2(1281)\right]^2(1281)\right]^2(1281)\right]^2\right]^2\right](1281)$$

$$M_2 = \left[\left[\left[\left[[[1640961]^2]^2(1281)\right]^2(1281)\right]^2(1281)\right]^2\right]^2(1281)$$

Puesto que $1640961 \equiv 2118 mod(2773)$

$$M_2 = \left[\left[\left[\left[[[2118]^2]^2(1281)\right]^2(1281)\right]^2(1281)\right]^2\right]^2(1281)$$

$$M_2 = \left[\left[\left[\left[[[4485924]^2(1281)\right]^2(1281)\right]^2(1281)\right]^2\right]^2(1281)$$

Puesto que $4485924 \equiv 1983 mod(2773)$

$$M_2 = \left[\left[\left[\left[[[1983]^2(1281)\right]^2(1281)\right]^2(1281)\right]^2\right]^2(1281)$$

$$M_2 = \left[\left[\left[\left[[[3932289]^2(1281)\right]^2(1281)\right]^2(1281)\right]^2\right]^2(1281)$$

Puesto que $3932289 \equiv 175 mod(2773)$

$$M_2 = \left[\left[\left[\left[(175)(1281)\right]^2(1281)\right]^2(1281)\right]^2\right]^2(1281)$$

$$M_2 = \left[\left[\left[224175\right]^2(1281)\right]^2(1281)\right]^2\right]^2(1281)$$

Puesto que $224175 \equiv 2335 mod(2773)$

$$M_2 = \left[\left[\left[\left[2335\right]^2(1281)\right]^2(1281)\right]^2\right]^2(1281)$$

$$M_2 = \left[\left[\left[5452225(1281)\right]^2(1281)\right]^2\right]^2(1281)$$

Puesto que $5452225 \equiv 507 mod(2773)$

$$M_2 = \left[\left[\left[\left[(507)(1281)\right]^2(1281)\right]^2\right]^2\right]^2(1281)$$

$$M_2 = \left[\left[\left[649467\right]^2(1281)\right]^2\right]^2(1281)$$

$$M_2 = \left[\left[\left[585\right]^2(1281)\right]^2\right]^2(1281)$$

$$M_2 = \left[\left[438390225\right]^2\right]^2(1281)$$

$$M_2 = \left[\left[1109\right]^2\right]^2(1281)$$

$$M_2 = \left[1229881\right]^2(1281)$$

Puesto que $1229881 \equiv 1442 mod(2773)$

$$M_2 = \left[1447\right]^2(1281)$$

$$M_2 = 2079364(1281)$$

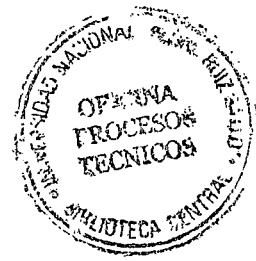
Puesto que 2079364

$M_2 = 2387(1281)$

$M_2 = 3057747$

Puesto que $3057747 \equiv 1901 mod(2773)$

Entonces $M_2 = 1901$



$M_3 = 1735^{157}(mod\ 2773)$

$M_3 = (1735)^{156}(1735)$

$$M_3 = \Big[\Big[\Big[\Big[[[[[1735]^2]^2]^2(1735)]^2(1735)\Big]^2(1281)\Big]^2\Big]^2(1735)$$

$$M_3 = \Big[\Big[\Big[[[3010225]^2]^2(1735)\Big]^2(1735)\Big]^2(1735)\Big]^2(1735)$$

Puesto que $3010225 \equiv 1520 mod(2773)$

$$M_3 = \Big[\Big[\Big[[[[1520]^2]^2(1735)]^2(1735)\Big]^2(1735)\Big]^2\Big]^2(1735)$$

$$M_3 = \Big[\Big[\Big[[[2310400]^2(1735)]^2(1735)\Big]^2(1735)\Big]^2\Big]^2(1735)$$

Puesto que $2310400 \equiv 491 mod(2773)$

$$M_3 = \Big[\Big[\Big[[[491]^2(1735)]^2(1735)\Big]^2(1735)\Big]^2\Big]^2(1735)$$

$$M_3 = \Big[\Big[\Big[[[241081](1735)]^2(1735)\Big]^2(1735)\Big]^2\Big]^2(1735)$$

Puesto que $241081 \equiv 2603 mod(2773)$

$$M_3 = \left[\left[\left[\left[(2603)(1735)\right]^2(1735)\right]^2(1735)\right]^2\right]^2(1735)$$

$$M_3 = \left[\left[\left[4516205\right]^2(1735)\right]^2(1735)\right]^2\right]^2(1735)$$

Puesto que $4516205 \equiv 1761 mod(2773)$

$$M_3 = \left[\left[\left[\left[1761\right]^2(1735)\right]^2(1735)\right]^2\right]^2(1735)$$

$$M_3 = \left[\left[\left[3101121(1735)\right]^2(1735)\right]^2\right]^2(1735)$$

Puesto que $3101121 \equiv 907 mod(2773)$

$$M_3 = \left[\left[\left[(907)(1735)\right]^2(1735)\right]^2\right]^2(1735)$$

$$M_3 = \left[\left[\left[1573645\right]^2(1735)\right]^2\right]^2(1735)$$

Puesto que $1573645 \equiv 1354 mod(2773)$

$$M_3 = \left[\left[\left[1354\right]^2(1735)\right]^2\right]^2(1735)$$

$$M_3 = \left[\left[1833316(1735)\right]^2\right]^2(1735)$$

Puesto que $1833316 \equiv 363 mod(2773)$

$$M_3 = \left[\left[(363)(1735)\right]^2\right]^2(1735)$$

$$M_3 = \left[\left[629805\right]^2\right]^2(1735)$$

Puesto que $629805 \equiv 334 mod(2773)$

$$M_3 = \left[\left[334\right]^2\right]^2(1735)$$

$$M_3 = \left[111556\right]^2(1735)$$

Puesto que $111556 \equiv 636 mod(2773)$

$M_3 = \Big[636\Big]^2(1735)$

$M_3 = 404496(1735)$

Puesto que $404496 \equiv 2411 mod(2773)$

$M_3 = 2411(1735)$

$M_3 = 4183085$

Puesto que $4183085 \equiv 1401 mod(2773)$

Entonces $M_3 = 1401$

$M_4 = 2503^{157}(mod\ 2773)$

$M_4 = (2503)^{156}(2503)$

$$M_4 = \Big[\Big[\Big[\Big[[[[[2503]^2]^2]^2(2503)]^2(2503)\Big]^2(2503)\Big]^2\Big]^2(2503)$$

$$M_4 = \Big[\Big[\Big[[[6265009]^2]^2(2503)\Big]^2(2503)\Big]^2(2503)\Big]^2(2503)$$

Puesto que $6265009 \equiv 802 mod(2773)$

$$M_4 = \Big[\Big[\Big[[[[802]^2]^2(2503)]^2(2503)\Big]^2(2503)\Big]^2\Big]^2(2503)$$

$$M_4 = \Big[\Big[\Big[[[643204]^2(2503)]^2(2503)\Big]^2(2503)\Big]^2\Big]^2(2503)$$

Puesto que $643204 \equiv 2641 mod(2773)$

$$M_4 = \Big[\Big[\Big[[[2641]^2(2503)]^2(2503)\Big]^2(2503)\Big]^2\Big]^2(2503)$$

$$M_4 = \left[\left[\left[\left[[6974881]^2(2503)\right]^2(2503)\right]^2(2503)\right]^2\right]^2(2503)$$

Puesto que $6974881 \equiv 786 mod(2773)$

$$M_4 = \left[\left[\left[\left[(786)(2503)\right]^2(2503)\right]^2(2503)\right]^2\right]^2(2503)$$

$$M_4 = \left[\left[\left[1967358\right]^2(2503)\right]^2(2503)\right]^2\right]^2(2503)$$

Puesto que $1967358 \equiv 1301 mod(2773)$

$$M_4 = \left[\left[\left[\left[1301]^2(2503)\right]^2(2503)\right]^2\right]^2\right]^2(2503)$$

$$M_4 = \left[\left[\left[\left[1692601(2503)\right]^2(2503)\right]^2\right]^2\right]^2(2503)$$

Puesto que $1692601 \equiv 1071 mod(2773)$

$$M_4 = \left[\left[\left[\left[(1071)(2503)\right]^2(2503)\right]^2\right]^2\right]^2(2503)$$

$$M_4 = \left[\left[\left[\left[2680713\right]^2(2503)\right]^2\right]^2\right]^2(2503)$$

Puesto que $2680713 \equiv 1995 mod(2773)$

$$M_4 = \left[\left[\left[\left[1995\right]^2(2503)\right]^2\right]^2\right]^2(2503)$$

$$M_4 = \left[\left[\left[\left[3980025(2503)\right]^2\right]^2\right]^2\right]^2(2503)$$

Puesto que $3980025 \equiv 770 mod(2773)$

$$M_4 = \left[\left[\left[\left[(770)(2503)\right]^2\right]^2\right]^2\right]^2(2503)$$

$$M_4 = \left[\left[1927310\right]^2\right]^2 (2503)$$

Puesto que $1927310 \equiv 75 mod(2773)$

$$M_4 = \left[\left[75\right]^2\right]^2 (2503)$$

$$M_4 = (31640625)(2503)$$

Puesto que $31640625 \equiv 695 mod(2773)$

$$M_4 = 695(2503)$$

$$M_4 = 1739585$$

Puesto que $1739585 \equiv 914 mod(2773)$

Entonces $M_4 = 914$

$$M_5 = 677^{157} (mod\ 2773)$$

$$M_5 = (677)^{156}(677)$$

$$M_5 = \left[\left[\left[\left[\left[\left[[[[677]^2]^2]^2(677)\right]^2(677)\right]^2(677)\right]^2\right]^2\right]^2 (677)$$

$$M_5 = \left[\left[\left[\left[\left[[[458329]^2]^2(677)\right]^2(677)\right]^2(677)\right]^2\right]^2\right]^2 (677)$$

Puesto que $458329 \equiv 784 mod(2773)$

$$M_5 = \left[\left[\left[\left[\left[[[784]^2]^2(677)\right]^2(677)\right]^2(677)\right]^2\right]^2\right]^2 (677)$$

$$M_5 = \left[\left[\left[\left[\left[[614656]^2(677)\right]^2(677)\right]^2(677)\right]^2\right]^2\right]^2 (677)$$

Puesto que $614656 \equiv 1823 mod(2773)$

$$M_5 = \left[\left[\left[\left[[1823]^2(677)\right]^2(677)\right]^2(677)\right]^2\right]^2(677)$$

$$M_5 = \left[\left[\left[\left[[3323329]^2(677)\right]^2(677)\right]^2(677)\right]^2\right]^2(677)$$

Puesto que $3323329 \equiv 1275 mod(2773)$

$$M_5 = \left[\left[\left[\left[(1275)(677)\right]^2(677)\right]^2(677)\right]^2\right]^2(677)$$

$$M_5 = \left[\left[\left[863175\right]^2(677)\right]^2(677)\right]^2\right]^2(677)$$

Puesto que $863175 \equiv 772 mod(2773)$

$$M_5 = \left[\left[\left[\left[772]^2(677)\right]^2(677)\right]^2\right]^2(677)$$

$$M_5 = \left[\left[\left[595984(677)\right]^2(677)\right]^2\right]^2(6773)$$

Puesto que $595984 \equiv 2562 mod(2773)$

$$M_5 = \left[\left[\left[(2562)(677)\right]^2(677)\right]^2\right]^2(677)$$

$$M_5 = \left[\left[\left[1734474\right]^2(677)\right]^2\right]^2(677)$$

Puesto que $1734474 \equiv 1349 mod(2773)$

$$M_5 = \left[\left[\left[1349\right]^2(677)\right]^2\right]^2(677)$$

$$M_5 = \left[\left[1819801(677)\right]^2\right]^2(677)$$

Puesto que $1819801 \equiv 713 mod(2773)$

$$M_5 = \left[\left[(713)(677)\right]^2\right]^2 (677)$$

$$M_5 = \left[\left[482701\right]^2\right]^2 (677)$$

Puesto que $482701 \equiv 199 mod(2773)$

$$M_5 = \left[\left[199\right]^2\right]^2 (677)$$

$$M_5 = (1568239201)(677)$$

Puesto que $1568239201 \equiv 2327 mod(2773)$

$$M_5 = 2327(677)$$

$$M_5 = 1575379$$

Puesto que $1575379 \equiv 315 mod(2773)$

Entonces $M_5 = 315$

$$M_6 = 1138^{157} (mod\ 2773)$$

$$M_6 = (1138)^{156}(1138)$$

$$M_6 = \left[\left[\left[\left[\left[[[[1138]^2]^2]^2(1138)\right]^2(1138)\right]^2(1138)\right]^2\right]^2 (1138)$$

$$M_6 = \left[\left[\left[\left[\left[[[1295044]^2]^2(1138)\right]^2(1138)\right]^2(1138)\right]^2\right]^2 (1138)$$

$$M_6 = \left[\left[\left[\left[\left[[1677138961936]^2(1138)\right]^2(1138)\right]^2(1138)\right]^2\right]^2 (1138)$$

Puesto que $1677138961936 \equiv 36 mod(2773)$

$$M_6 = \left[\left[\left[\left[\left[[[36]^2](1138)\right]^2(1138)\right]^2(1138)\right]^2\right]^2 (1138)$$

$$M_6 = \left[\left[\left[\left[\left[1296(1138)\right]^2(1138)\right]^2(1138)\right]^2\right]^2 (1138)$$

$$M_6 = \left[\left[\left[\left[1474848\right]^2(1138)\right]^2(1138)\right]^2\right]^2(1138)$$

Puesto que $1474848 \equiv 2385 mod(2773)$

$$M_6 = \left[\left[\left[\left[2385\right]^2(1138)\right]^2(1138)\right]^2\right]^2(1138)$$

$$M_6 = \left[\left[\left[\left[5688225(1138)\right]^2(1138)\right]^2\right]^2\right]^2(1138)$$

Puesto que $5688225 \equiv 802 mod(2773)$

$$M_6 = \left[\left[\left[\left[(802)(1138)\right]^2(1138)\right]^2\right]^2\right]^2(1138)$$

$$M_6 = \left[\left[\left[\left[912676\right]^2(1138)\right]^2\right]^2\right]^2(1138)$$

Puesto que $912676 \equiv 359 mod(2773)$

$$M_6 = \left[\left[\left[\left[359\right]^2(1138)\right]^2\right]^2\right]^2(1138)$$

$$M_6 = \left[\left[\left[\left[12881(1138)\right]^2\right]^2\right]^2\right]^2(1138)$$

$$M_6 = \left[\left[\left[\left[146666578\right]^2\right]^2\right]^2\right]^2(1138)$$

Puesto que $146666578 \equiv 2608 mod(2773)$

$$M_6 = \left[\left[\left[\left[2608\right]^2\right]^2\right]^2\right]^2(1138)$$

$$M_6 = \left[\left[6801664\right]^2\right]^2(1138)$$

Puesto que $6801664 \equiv 2268 mod(2773)$

$M_6 = \left[2268\right]^2(1138)$

$M_6 = 5143824(1138)$

Puesto que $5143824 \equiv 2682 mod(2773)$

$M_6 = 2682(1138)$

$M_6 = 3052116$

Puesto que $3052116 \equiv 1816 mod(2773)$

Entonces $M_6 = 1816$

En forma análoga se recuperan

$M_7 = 1367^{157}(mod\ 2773) \rightarrow M_7 = 1518$

$M_8 = 1655^{157}(mod\ 2773) \rightarrow M_8 = 0500$

$M_9 = 1281^{157}(mod\ 2773) \rightarrow M_9 = 1901$

$M_{10} = 1004^{157}(mod\ 2773) \rightarrow M_{10} = 1415$

Con lo cual recuperamos el mensaje cifrado: " **MENS SANA IN CORPORE SANO**".

En la siguiente sección mostraremos como cifrar una imagen utilizando el teorema chino de los restos.

3.6 Cifrado de Imágenes Digitales

Para cifrar una imagen digital se siguen los siguientes pasos:

1. Se calcula el número de bloque a enviar, en nuestro caso cada uno formado por 4 pixeles, de modo que, como la imagen que se quiere enviar es de tamaño 256 *pixeles*$\times$ 256 *pixeles* entonces el número de bloques es igual a:

$$\frac{256 \times 256}{4} = 16384$$

   Luego se deben enviar 16384 bloques.

2. Se envía un número x por cada bloque, es decir se deben enviar 16384 números x. Los valores de x varían entre 0 y $M-1$, es decir los posibles restos módulo M, en nuestro ejemplo $M-1 = 4447473407$ el cual tiene exactamente 33 bits.
   Para determinar el número x por cada bloque se procede como sigue:

   i) Se escogen un conjunto de k módulos $\{m_1, m_2, \ldots, m_k\}$ tal que $m_i \geq l$, $1 \leq i \leq k$ donde l es el tamaño de la imagen original, y además los m_i son primos entre sí. Los números m_i serán secretos y solo serán conocidos por el emisor y el receptor.

   ii) Se divide la imagen en bloques de tamaño k, se toma un bloque de k niveles de gris de la imagen original que se indicarán por $\{a_1, a_2, \ldots, a_k\}$.

   iii) Se define $M = m_1.m_2 \cdots m_k$ y se forma el siguiente sistema de ecuaciones en congruencias:

$$\begin{aligned} x &\equiv a_1 (mod\ m_1) \\ x &\equiv a_2 (mod\ m_2) \\ &\vdots \\ x &\equiv a_k (mod\ m_k) \end{aligned}$$

iv) Se aplica el teorema chino de los restos al sistema de ecuaciones en congruencias y se obtiene la solución

$$x = a_1 x_1 M_1 + a_2 x_2 M_2 + \cdots + a_k x_k M_k$$

3. De acuerdo con el paso 2 hay que enviar $16384 \times 33 = 540672$ *bits*, se agrupan de ocho en ocho. Estos grupos de 8 bits se pasa a decimal, obteniendo un número comprendido entre 0 y 255 que se interpretan como los niveles de gris. Es decir hay una lista de 67584 de elementos donde cada elemento es un número entre 0 y 255

4. Puesto que la imagen original es de tamaño 65536 resulta insuficiente para la lista de 67584 de elementos obtenidos. Así que se debe construir una matriz B de tamaño $264 \times 256 = 67584$ para tener espacio suficiente, se rellenan los elementos de la matriz B empezando en la esquina superior izquierda y moviéndose de izquierda a derecha y de arriba hacia abajo.

5. La matriz B se puede mostrar como una imagen y será la imagen codificada que se envía al receptor.

6. Para decodificar la imagen el receptor resuelve el sistema

$$\begin{aligned} x(mod\ m_1) &\equiv a_1 \\ x(mod\ m_2) &\equiv a_2 \\ &\vdots \\ x(mod\ m_k) &\equiv a_k \end{aligned}$$

Los valores $\{a_1, a_2, \ldots, a_k\}$ son los niveles de gris originales de cada bloque de la matriz B

EJEMPLO ILUSTRATIVO DE ENCRIPTADO DE UNA IMAGEN DIGITAL

Supongamos que queremos enviar la siguiente imagen en escala de grises, los cuales varían entre 0 y 255 , la imagen original tiene un tamaño de 256×256

Figura 3.1: Imagen a Encriptar.

Por ejemplo tomemos bloques de tamaño cuatro, tomándolos empezando en la esquina superior izquierda y moviéndonos de izquierda a derecha y de arriba hacia abajo. Si denotamos por I la imagen original, el primer bloque será denotado por $\{a_{11}, a_{12}, a_{13}, a_{14}\}$, y así sucesivamente. Sigamos los pasos dados por el método descrito anteriormente:

1. Elijamos $m_1 = 256$; $m_2 = 257$; $m_3 = 259$; $m_4 = 261$, los cuales son mayores o iguales que 256 , y además primos entre sí.

2. Se divide la imagen en bloques de tamaño $k = 4$, se toma un bloque de 4 niveles de gris de la imagen original que se indicaran por $\{a_{11}, a_{12}, a_{13}, a_{14}\}$.

3. Se define $M = (256)(257)(259)(261) = 4447473408$ y se forma el siguiente sistema de ecuaciones en congruencias:

$$x \equiv a_{11}(mod\ 256)$$
$$x \equiv a_{12}(mod\ 257)$$

$$x \equiv a_{13}(mod\ 259)$$
$$x \equiv a_{14}(mod\ 261)$$

4. Se aplica el teorema chino de los restos al sistema de ecuaciones en congruencias y se obtiene la solución

$$x = a_{11}x_1M_1 + a_{12}x_2M_2 + a_{13}x_3M_3 + a_{14}x_4M_4$$
$$M_1 = \frac{M}{m_1} = \frac{4447473408}{256} \rightarrow M_1 = 17372943$$
$$M_2 = \frac{M}{m_2} = \frac{4447473408}{257} \rightarrow M_1 = 17305344$$
$$M_3 = \frac{M}{m_3} = \frac{4447473408}{259} \rightarrow M_3 = 17171712$$
$$M_4 = \frac{M}{m_4} = \frac{4447473408}{261} \rightarrow M_4 = 17040128$$

Además

$$x_1 = 17372943^{-1}(mod\ 256) \rightarrow x_1 = 15$$
$$x_2 = 17305344^{-1}(mod\ 257) \rightarrow x_2 = 249$$
$$x_3 = 17171712^{-1}(mod\ 259) \rightarrow x_3 = 13$$
$$x_4 = 17040128^{-1}(mod\ 261) \rightarrow x_4 = 221$$

Supongamos que el bloque de 4 pixeles que nos toca elegir es

$a_{11} = 152;\ a_{12} = 153;\ a_{13} = 152;\ a_{14} = 155;$

Luego:

$$x = a_1x_1M_1 + a_2x_2M_2 + \ldots + a_kx_kM_k$$

$x = (152)(15)(17372943) + (153)(249)(17305344) + (154)(13)(17171712) +$
$(155)(221)(17040128)$
$\rightarrow x = 3109790360(mod\ 4447473408)$

Detallemos como se envían los números x , que como dijimos se envía un x por cada bloque de 4 pixeles. Los valores de x varían entre 0 y $M-1$, es decir los posibles restos modulo M , en nuestro ejemplo $M-1 = 4447473407$ tiene exactamente 33 bits.

Como la imagen tiene tamaño 256×256 luego el número de bloques es igual a

$$\frac{256 \times 256}{4} = 16384$$

Por lo tanto hay que enviar 16384 números y cada uno de ellos ocupa 33 bits, por lo tanto, el número de bits a enviar es de $16384 \times 33 = 540672$ los cuales se agrupan de ocho en ocho.

Luego cada grupo de 8 bits se pasa a decimal, obteniendo un número comprendido entre 0 y 255 que se interpretan como los niveles de gris. Es decir hay una lista de 67584 de elementos donde cada elemento es un número entre 0 y 255 .

Puesto que la imagen original es de tamaño 65536 resulta insuficiente para la lista de 67584 de elementos obtenidos. Así que se debe construir una matriz B de tamaño $264 \times 256 = 67584$ para tener espacio suficiente se rellenan los elementos de la matriz B empezando en la esquina superior izquierda y moviéndose de izquierda a derecha y de arriba hacia abajo.

La matriz B se puede mostrar como una imagen y será la imagen codificada que se envía al receptor.

5. Se envía al receptor de la imagen cifrada

Es decir los valores de x obtenidos en el paso 4, uno por cada bloque. El receptor resuelve el sistema

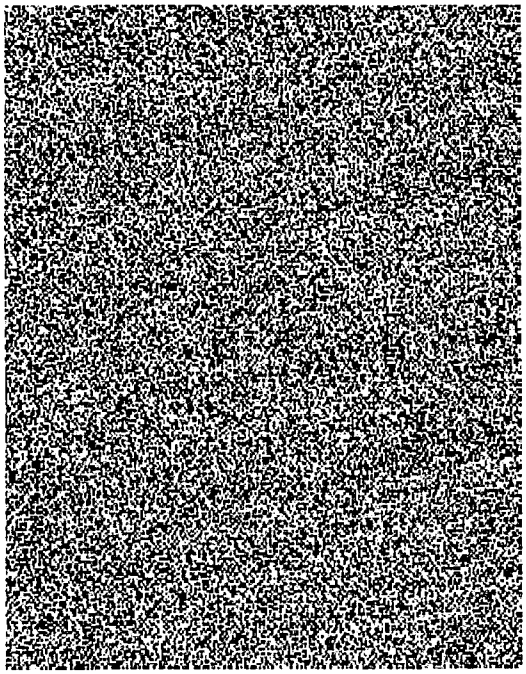


Figura 3.2: Imagen cifrada enviada.

$$3109790360(mod\ 256) \equiv 152$$
$$3109790360(mod\ 257) \equiv 153$$
$$3109790360(mod\ 259) \equiv 152$$
$$3109790360(mod\ 261) \equiv 155$$

Es decir se han recuperado los niveles de gris originales, recuperándose así la imagen original.

Figura 3.3: Imagen recuperada

Conclusiones

1. El Sistema RSA es uno de los más seguros para el envío de mensajes cifrados.
2. El algoritmo extendido de Euclides o Identidad de Bezout es la base para el envío de mensajes cifrados en el sistema RSA.
3. Usando aritmética modular es posible encriptar y desencriptar un mensaje en el sistema RSA.
4. Usando el teorema chino de los restos es posible encriptar y desencriptar una imagen digital.
5. Este trabajo sirve como punto de partida para estudiantes de Matemática e Ingeniería.

Bibliografía

[1] Ciet, M., Neve, M., Peeters, E., & Quisquater, J. (2003, December). Parallel FPGA implementation of RSA with residue number systems-can side-channel threats be avoided. In Circuits and Systems, 2003 IEEE 46th Midwest Symposium on (Vol. 2, pp. 806-810). IEEE.

[2] Coutinho, S. C. The Mathematics of Ciphers: Number Theory and RSA Cryptography. Wellesley, MA: A K Peters, 1999.

[3] Flannery, S. and Flannery, D. In Code: A Mathematical Journey. Profile Books, 2000.

[4] Galindo, A. El arte de disfrazar la información. Revista Real Académica de Ciencias Exactas Físicas Naturales.Vol.101 n°2, p.307-320, 2007.

[5] Hungerford, T.W. (1990) Abstract Algebra. An Introduction. Saunders College Publishing.

[6] Li-Jun, J. I. N. (2011). System in the RSA asymmetric encryption algorithm [J].Electronic Design Engineering, 11, 010.

[7] Mora, W. Introducción a la teoría de números, ejemplos y algoritmos. Revista Digital Matemática Educación e Internet. Instituto Tecnológico de Costa Rica 2014.

[8] Thomas, T., Emmanuel, S., Zhang, P., Kankanhalli,M.S, M.S, "An Authentication Mechanism Using Chinese Remainder Theorem for Efficient Sur-

veillance Video Transmission", Seventh IEEE International Conference on Advanced Video and Signal Based Surveillance), Boston, 2010.