Revista Electrónica de Conocimientos, Saberes y Prácticas

e-ISSN: 2616-8294 / http://recsp.org
DOI: https://doi.org/10.5377/recsp.v3i1.9791
Año 3, Volumen 3, No. 1, Enero-Junio, 2020

Estudio de la Teoría de Números Aplicada a Algunos Métodos Criptográficos haciendo uso de las TIC

German Camilo Fontecha Moreno[1]
Erika Alejandra Vacca Díaz[2]

INFORMACIÓN DEL ARTÍCULO

Recibido: 20.03.2020
Aprobado: 30.04.2020

Palabras claves:
Seguridad Informática,
Algoritmos,
Teoría de los Números,
Teoría de la Información,
Aprendizaje,
Criptografía.

RESUMEN

Dentro de las ciencias, la criptografía es una rama de las matemáticas denominada Teoría de la Información, esta rama se divide en Teoría de Códigos y en Criptología; que a su vez se divide en Criptoanálisis y Criptografía, que trata de las leyes de la codificación de la información. Al tener fundamentos matemáticos, como la estadística, la Teoría de Números, la Teoría de la Complejidad Algorítmica y la Teoría de la Comunicación, es importante comprender de qué manera la matemática interviene en los procesos de encriptación y desencriptación de un mensaje realizando un estudio para visualizar el momento en que se aplican en un criptosistema. Al enfatizar el uso de programas computacionales, es posible integrar dos áreas que siempre han estado ligadas en los avances tecnológicos. Encontrando así, que los fundamentos matemáticos ayudan a la eficiencia y seguridad de estos sistemas de seguridad, adicionando el programa Cryptool que favorece el desarrollo de la criptografía.

Keyword:
Computer Security,
Algorithms,
Number Theory,
Information Theory,
Learning,
Cryptography.

Study of the theory of numbers applied to some cryptographic methods using TIC

ABSTRACT

A In sciences, cryptography is a branch of math called “The Theory of Information”. This branch is divided in theory of coding and cryptology, which at the same time is divided in cryptanalysis and cryptography, that is about the laws of information coding. By having mathematical grounds, like statistics, number’s theory, algorithmic complexity theory and communication theory, it is simpler to understand the mathematical way that they intervene in the processes of encryption and decryption of a message by performing a study to visualize the moment when they are applied in a cryptosystem. Emphasizing the use of computer programs, it is possible to integrate two areas that have always been linked in technological advances. Finding the way that these mathematical

[1] Licenciado en Informática y Tecnología. Profesor del Colegio Gimnasio Santander Tunja. Email: German.7350@gmail.com : https://orcid.org/0000-0003-3169-4933
[2] Licenciada en Matemáticas. Profesora del Colegio Cristiano Filadelfia. Email: alejitavacca@gmail.com : https://orcid.org/0000-0001-9425-0649

Fontecha Moreno, G., & Vacca Díaz, E. (2020). Estudio de la teoría de números aplicada a algunos métodos criptografícos haciendo uso de las TIC. ***Revista Electrónica de Conocimientos, Saberes y Prácticas*****, 3(1), 49-71. DOI: https://doi.org/10.5377/recsp.v3i1.9791**

foundations help to the efficiency and security of these systems, by adding programs such as Cryptool that favors the development of cryptography.

1. Introducción

El presente artículo es producto de la monografía titulada Estudio de la Teoría de números aplicada a algunos métodos criptográficos, que tiene como propósito describir los contenidos matemáticos que han permitido el avance de algunos métodos de encriptación, investigando como interviene la teoría de números en los algoritmos criptográficos de tal forma que los estudiantes de la Licenciatura en Matemáticas puedan complementar su formación conociendo sus aplicaciones en otras áreas de conocimiento. Enfocandonos en la estructura general de un criptosistema aplicando los conceptos matemáticos que son necesarios para realizar las operaciones de cifrado y descifrado de mensajes en los diferentes sistemas criptograficos, haciendo uso del programa computacional Cryptool donde se aplicaran los algoritmos de los sistemas criptográficos de Julio Cesar y RSA.

2. Literatura

2.1 Referentes y fundamentos teóricos de la criptografía

El termino criptografía según Gómez (2011) proviene del griego "Kriptos" (oculto) y "Grafos" (escritura) convirtiéndose en el arte de escribir de un modo secreto o enigmático, ya que con esta es posible garantizar la confidencialidad y autenticidad de los mensajes que se guardan en un sistema informático. Al profundizar en los métodos de encriptación es evidente notar que cada uno es más sofisticado que el otro debido a que guardar la información es complicado y por ende es una prioridad; por tal razón la criptografía es la ciencia que se encarga de estudiar las distintas técnicas empleadas para transformar la información y hacerla irreconocible a todos aquellos usuarios no autorizados.

La criptografía surgió a raíz de una necesidad que el hombre tuvo y tiene de guardar información, por eso es importante resaltar los aportes que culturas como los Griegos, Mesopotámicos, Romanos y Egipcios le dieron para ser lo que es hoy en día. Uno de los primeros registros sobre Criptografía fue en el año 3000 a.c. en la civilización egipcia con la escritura jeroglífica que según Xifre (2009) es una escritura fonética que incluye sema-gramas, pero más que hacer criptografía era para obtener intriga y misterio. la civilización Mesopotámica que en el año 3300 a.c. utilizaba la escritura cuneiforme donde cambiaban los signos de la escritura por otros con el fin de alterar la misma, pero que a diferencia de los egipcios los escribas sí querían ocultar el significado de la escritura. Otra cultura que intentó realizar criptografía fue la Griega en el año 500 a.c. enrollando una tira de cuero alrededor de un cilindro para escribir el mensaje sobre el cuero conocido como la "scytale"; por otro lado, están los Romanos que le dieron un

giro a la forma de hacer criptografía, ya que con las constantes batallas el emperador Julio César inventó un sistema criptográfico que consiste en sustituir cada letra por la que se encuentra tres posiciones adelante en el orden del alfabeto. Lo anterior son algunos descubrimientos que hacen de la criptografía algo fascinante pues los pocos avances que se tienen siempre han sido bajo una situación en particular.

Para Lucena (2001), la criptografía moderna nace al mismo tiempo que las computadoras, durante la segunda guerra mundial en un lugar llamado Bletchley Park, donde un grupo de científicos trataban de descifrar los mensajes enviados por el ejército alemán con la máquina Enigma, hoy en día considerado el primer computador. Por las consideraciones anteriores es importante aclarar que hasta entonces la criptografía era considerada un arte difícil y entretenido de realizar pero que gracias a matemáticos y científicos se convirtió en una ciencia cuya finalidad básica es la seguridad informática, uno de los padres de la criptografía científica es el matemático Claude Elwood Shannon quien fue el pionero de la era de la información a raíz de haber demostrado en su artículo "A Mathematical Theory of Communication" (1948) que la información podía definirse y medirse como noción científica, creando la Teoría de la Información que según Granados (2006) se divide en Teoría de Códigos y en Criptología y que a su vez la Criptología se divide Criptografía y Criptoanálisis, por supuesto todo a raíz de las matemáticas como se muestra en siguiente figura.

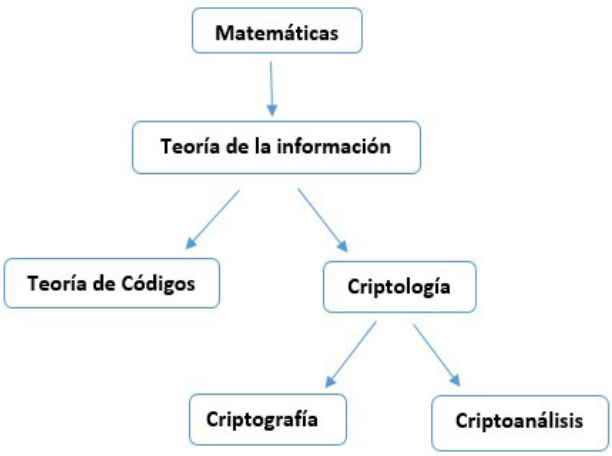


Figura 1. Origen de la criptografía

Nota: Tomado de introducción a la criptografía, Granados (2006).

Entonces, es importante tener claro el proceso general que se utiliza a la hora de cifrar un mensaje, ya que de esta forma es más fácil comprender el momento en que son necesarias las matemáticas, en especial la Teoría de Números para cada proceso. De acuerdo con Gómez (2011) un sistema criptográfico está constituido por un conjunto

de algoritmos y técnicas que permiten ofrecer una serie de servicios de seguridad de la información, es decir realizar unas transformaciones sobre el texto original para obtener un texto modificado, como se puede observar en la siguiente figura.

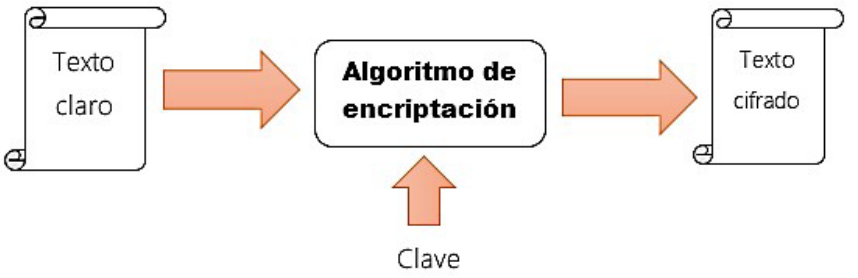


Figura 2. Esquema del cifrado de un mensaje.

Nota: Tomado y adaptado del libro Enciclopedia de la seguridad informática, Gómez (2011).

¿Pero en qué momento y con ayuda de qué se realizan tales transformaciones?, para eso es necesario conocer la importancia de cada elemento en el esquema del proceso de cifrado; cómo se puede observar en la figura 2, se inicia con el texto claro que es aquél que no oculta su información o al que no se le ha aplicado un procedimiento criptográfico o en efecto el que se ha reconstruido mediante la clave, enseguida se realiza una combinación llamada algoritmo de encriptación que es una función matemática que trabaja en combinación con una llave (un número, palabra, frase o contraseña) usada en los procesos de encriptación y des encriptación, el algoritmo de encriptación se ejecuta de acuerdo con una clave que trabaja como un código de signos convenidos para la transmisión de mensajes secretos o privados llegando a la fase final que es el texto cifrado. Hay que aclarar que dependiendo del sistema criptográfico el esquema de cifrado puede variar y eso depende en muchos casos del algoritmo de cifrado que se utiliza.

Por otra parte, durante muchos años la matemática ha estado involucrada en el desarrollo de la humanidad, aunque en ocasiones parezca un tanto complicado de entender, en especial por los campos en que se profundiza. Siendo importante para diferentes áreas de la tecnología en la actualidad, sobre todo para la criptografía ya que ha permitido crear sofisticados algoritmos informáticos que ayudan a la seguridad de redes.

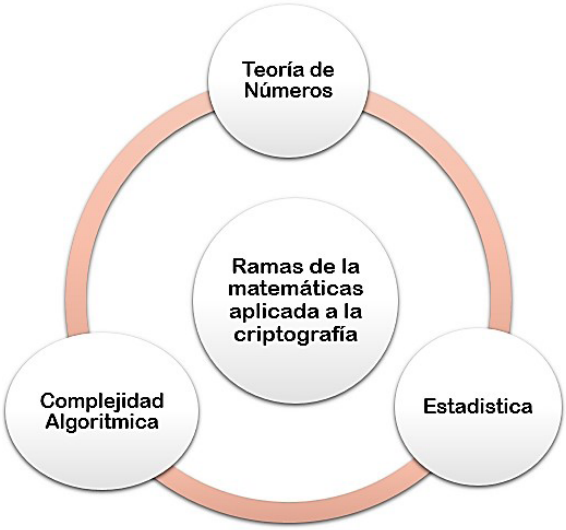


Figura 3. Ramas de las Matemáticas Aplicadas a la Criptografía

Nota: Estudio de la teoría de números aplicada a algunos métodos criptograficos, Vacca (2016).

En la Figura 3, se puede observar que la criptografía se complementa de varias ramas de las matemáticas que hacen más fácil su funcionalidad, las cuales son la Complejidad Algorítmica, la Estadística y la Teoría de Números, importantes para desarrollar computacionalmente un proceso criptográfico. Es importante definir de qué forma se puede expresar la estructura de un criptosistema matemáticamente y esto es posible por medio de un proceso conocido como función, donde, M es el mensaje original y el mensaje cifrado es C:

Se denotará el cifrado de un criptosistema como una función E:

$$M \xrightarrow{E} C,$$

tal que:

$$E(M) = C$$

Siguiendo el proceso anterior el algoritmo de descifrado se expresa mediante una función como:

$$C \xrightarrow{D} M,$$

donde D es una función tal que:

$$D(C) = M$$

Obteniendo la siguiente correspondencia:

$$D(E(M))= M, \qquad E(D(C))= C.$$

Para expresar matemáticamente un criptosistema es necesario adaptar la notación para cada parte del cifrado y descifrado, es por eso que se define un sistema criptográfico como una quíntupla (M, C, K, E, D) donde:

1. M es el conjunto finito de posibles textos claro.

2. C es el conjunto finito de posibles mensajes cifrados.

3. k es el conjunto finito de posibles claves.

4. E es el conjunto de transformaciones de cifrado.

5. D es el conjunto de transformaciones de descifrado.

Para todo K en k, existe una regla de cifrado $e_K \in E$ y una regla de descifrado D; cada una definidas $e_K: M \to C \; y \; d_K: C \to D \;\; tal \; que$:

$$d_K \; (e_K(x)) = x \text{ para todo } x \text{ en } M$$

Es decir que, si se tiene un mensaje x, se cifra empleando la clave k y luego se descifra empleando la misma clave, obteniendo de nuevo el mensaje original x (Ibáñez, 2012).

2.2 Sistemas Criptográficos

Ahora se resaltarán los algoritmos matemáticos y se describirá las operaciones de cifrado y descifrado de cada método de encriptación que se estudiaron.

Cifrado del César

El primer método para estudiar es el Cifrado de Julio César que le debe su nombre al emperador Julio César quien inventó un sencillo método para mantener algunos de sus escritos en secreto y para comunicarse con los generales en las batallas, aunque es uno de los más simples en cuanto al proceso de cifrado para aquellos tiempos no era tan común que las personas supieran leer por lo cual tuvo gran efectividad en un comienzo, pasando a la historia como el Cifrado del César.

Este tipo de cifrado se conoce con el nombre de cifrados monográficos, es decir aquellos que están basados en la sustitución de cada símbolo del alfabeto por otro (Lucena, 2001). Para este método el proceso de cifrado consiste en sustituir cada letra

por la que se encuentra tres posiciones más adelante en el orden alfabético, para el alfabeto castellano formado por 27 letras donde se excluye las letras CH y LL quedaría de la siguiente manera para cifrar un mensaje claro.

Tabla 1. Desplazamiento de letras para el cifrado del César

A	B	C	D	E	F	G	H	I	J	K	L	M	N
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P

Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Nota: Tomado de Libro Diseño e Implementación de un Software Multimedia para el Aprendizaje de la Criptografía, Chaves (2008).

A pesar de ser uno de los cifrados más sencillos en la actualidad matemáticamente es necesario aplicar una parte de la Teoría de Números conocida como la Aritmética Modular mediante una relación de congruencias, ya que la transformación realiza un desplazamiento que introduce a esta teoría conocida como la Aritmética del reloj. Para estudiar la estructura matemática de este algoritmo criptográfico también son necesarias algunas nociones sobre divisibilidad, porque estos facilitan el análisis de algunos procesos de encriptación de un mensaje.

Algoritmo Matemático del cifrado del cesar

ste se encuentra determinado por: Definición 1. Sean $\mathbb{K} = \mathbb{Z}_{27}$, para $0 \leq 26$, se define:

$e_K(x) \equiv x + K \ m\acute{o}d\ 27$,para el cifrado

$d_K(y) \equiv y - K \ m\acute{o}d\ 27$, para el descifrado,

Donde x y y pertenecen a $\mathbb{Z}_{27.}$

Si la clave *K*=3, entonces se tiene el código de cifrado y descifrado del método del Cesar (Ibáñez, 2012).

Para realizar el procedimiento para cifrar un mensaje es necesario asignar a cada letra un número denominado equivalente numérico, quedando el alfabeto de la siguiente manera.

Tabla 2. Equivalentes numéricos para el cifrado del César

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Nota: Tomado del Libro Teoría de Números para Principiantes, Rubiano (2004).

Criptosistemas de clave pública

En el mundo de la seguridad informática así como hay métodos de encriptación que tienen un algoritmo básico, existen otros en la actualidad que son más sofisticados gracias a los métodos matemáticos que utilizan para diseñar el algoritmo de cifrado, este tipo de criptosistemas se conoce con el nombre de cifrado asimétricos o cifrado con clave pública que apareció en 1976, con la publicación de un trabajo sobre criptografía por Whitfeld Diffie y Martin Hellman que sugirieron usar problemas computacionalmente irresolubles para el diseño de criptosistemas seguros. Lucena (2001), dice que esta clase de criptosistemas posee dos claves diferentes denominadas clave privada y clave pública, donde una de ellas se emplea para codificar mientras que la otra se usa para decodificar.

Un criptosistema de clave pública es una familia de funciones unidireccionales tramposas $\{f_k\}$, para cada clave k de K de modo que la trampa $t\ (k)$ sea fácil de obtener. Además, para cada k de K se debe poder describir un algoritmo eficiente que permita calcular $\{f_k\}$, ; de modo que sea intratable la determinación de k y $t\ (k)$. Para implementar un criptosistema de clave pública dada una familia de funciones unidireccionales tramposas, cada usuario U elige una clave aleatoria u de k y pública E_u que permite calcular f_u; donde E_u es la clave pública mientras que la trampa $t\ (u)$ es necesaria para invertir f_u que es la clave privada. Pero si un usuario desea enviar un mensaje m a otro usuario B, mira la clave pública del usuario B, E_b y transmite $f_b(m) = c$ a B : Como el usuario B es el único capaz de invertir f_b es el único que puede recuperar el mensaje m: $f_b^{-1}(c) = f_b^{-1}(f_b(m)) = m$ (Fuster, 2001). En general los sistemas asimétricos vienen dados por el esquema representado en la figura 5.

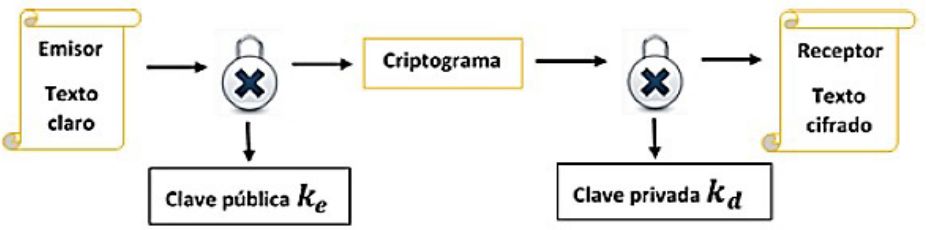


Figura no. 4: Esquema general de los criptosistemas asimétricos.

Nota: Tomado de Artículo Introducción a la criptografía, Granados (2006).

Sistema RSA

Este sistema fue desarrollado en 1978 por Ronald Riverst, Adi Shamir y Leonard Adleman, de ahí el nombre RSA, que corresponde a las iniciales de los apellidos de sus autores. La seguridad del sistema RSA se basa en el hecho de que no existe una forma eficiente de factorizar números que sean productos de dos grandes números primos, por lo que requiere aplicaciones de la aritmética modular, complejidad algorítmica y exponenciación rápida.

Algoritmo matemático del cifrado del RSA.

Definición 3. Sea p,q dos números primos elegidos aleatoriamente, e un número primo relativo con $(p-1)$ y $(q-1)$, el inverso de e mód $(p-1)(q-1)$, y el producto de p y q; la codificación de un mensaje con el cifrado RSA se lleva a cabo por medio de la siguiente expresión:

$$c \equiv m^e \,(\text{mód } n); \qquad (1)$$

la clave pública está dada por (e,n).

Y la decodificación se hará de la siguiente manera:

$$c \equiv m^d \,(\text{mód } n); \qquad (2)$$

Donde la clave privada es la letra d (Lucena, 2001).

3. Metodología

El trabajo que se desarrolló, tiene como objetivo describir la importancia que tiene la matemática en la criptografía por medio del estudio de documentos y la observación directa , se propone un enfoque de tipo cualitativo ya que por sus características de investigación es el más apropiado para tener en cuenta, por eso se tomará como referencia para orientar esta idea a Hernández & Fernández & Baptista (2010), quien dice que este tipo de investigación es un análisis dirigido a la descripción detallada de los fenómenos estudiados, donde la mayoría de estas investigaciones pone el acento en la utilización práctica de la investigación. Lo anterior porque lo que se desarrolló durante todo el proceso es un estudio detallado de las aplicaciones de la teoría de números en los métodos de encriptación, describiendo cada uno de estos y a su vez resaltando una de las muchas aplicaciones de las matemáticas.

Al ser un tema que poco se ha trabajado este proyecto también lo sustenta un tipo de investigación exploratorio donde se va tomar como referencia a Hernández & Fernández & Baptista (2010), donde ha decidido los estudios de este tipo se efectúan

cuando el objetivo es examinar un problema de investigación poco estudiado o que no ha sido abordado antes, por tal motivo es que se ha decidido profundizar más en el tema de la criptografía por que el amplio campo de aprendizaje y aplicación de las matemáticas ha sido poco estudiado. Estos mismos autores resaltan que esta clase de estudio exploratorio sirve para aumentar el grado de familiaridad con fenómenos relativamente desconocidos y a obtener información sobre la posibilidad de llevar a cabo una investigación más completa sobre un contexto particular de la vida real.

Con este tipo de pensamiento es que se caracteriza la segunda parte de este trabajo, porque lo que se pretende con el estudio teórico de la criptografía es llegar a la aplicación de algunos métodos de encriptación e implementarlos como una herramienta de estudio que ayude a los estudiantes de la Licenciatura en Matemáticas de la UPTC a fortalecer los temas vistos en el área de teoría de grupos.

Para investigar y comprender de qué forma interviene la teoría de números en los algoritmos criptográficos utilizados en los métodos de encriptación, se va a iniciar con una búsqueda referencial para posteriormente seleccionar documentos matemáticos que contengan la información necesaria sobre este tema y así profundizar en la estructura matemática que complementa la teoría de números; logrando con esto que se facilite el estudio de algunas técnicas de encriptación que hay en la actualidad. Adicionalmente se va a utilizar un programa computacional que permita ver la aplicación de la matemática en la vida real. Para lograr este objetivo se propone profundizar más sobre la criptografía clásica y la criptografía moderna desde una perspectiva matemática viendo las técnicas que utiliza cada uno para cifrar mensajes y así poder realizar aplicaciones sencillas de algunos métodos haciendo uso de un programa computacional llamado CRYPTOOL desarrollado por el profesor Bernhard Esslinge, de software libre que ilustra conceptos criptográficos y permite desarrollar ejercicios donde se puede mostrar lo útil que es la matemática en otras áreas del conocimiento.

4. Resultados

A continuación, se describirá un ejemplo de cifrado y descifrado por el método del César y RSA, se mostrará el procedimiento matemático para la primera letra, y para las demás letras del mensaje el proceso de cifrado y descifrado es el mismo.

Ejemplo 1. Cifrado del Mensaje:

Mensaje: “SI BUSCAS RESULTADOS DISTINTOS NO HAGAS SIEMPRE LO MISMO” Albert Einstein.

1. Se organiza el texto en bloques de 4 letras, para enviarlo y así hacer más difícil la comprensión de este.

SIBU	SCAS	RESU	LTAD	OSDI	STIN
TOSN	OHAG	ASSI	EMPR	ELOM	ISMO

2. Se le asigna a cada letra del mensaje un equivalente numérico, utilizando la tabla 2.

198121	192019	1841921	112003	151938	1920813
20151913	15706	019198	4121618	4111512	8191215

3. Se aplica la transformación $e_K(x) \equiv x + K \ mód\ 27$, si $K=3$ entonces $e_K(x) \equiv x + 3 \ mód\ 27$, donde x corresponde al equivalente numérico de cada letra del mensaje cifrado a enviar, quedando:

$S = 19$

Se reemplaza en:

$$e_K(x) \equiv x + K \ mód\ 27$$
$$e_K(19) \equiv 19 + 3 \ mód\ 27$$
$$e_K(19) \equiv 22 \ mód\ 27$$

La primera letra cifrada es $c_1 = 22$, que corresponde a la letra V.

Realizando un procedimiento igual al anterior se cifra cada letra del mensaje quedando los bloques de la siguiente manera:

2211424	225322	2172224	142336	1822711	22231116
VLEX	VFDV	UHVX	ÑWDG	RVGL	VWLP

23182216	181039	3222211	7151921	7141815	11221518
WRVP	RKDJ	DVVL	HOSU	HÑRO	LVOR

Quedando el mensaje a enviar: VLEX VVFDV UHVX ÑWDG RVGL VWLP WRVP RKDJ DVVL HOSU HÑRO LVOR.

Descifrado del mensaje:

Mensaje: VLEX VVFDV UHVX ÑWDG RVGL VWLP WRVP RKDJ DVVL HOSU HÑRO LVOR.

1. Se pasa el mensaje a sus respectivos equivalentes numéricos.

VLEX	VFDV	UHVX	ÑWDG	RVGL	VWLP
2211424	225322	2172224	142336	1822711	22231116

WRVP	RKDJ	DVVL	HOSU	HÑRO	LVOR
23182216	181039	3222211	7151921	7141815	11221518

2. Se aplica al mensaje cifrado la transformación $d_k(y) \equiv y - 3 \; m\acute{o}d \; 27$ para volver al mensaje original.

$V = 22$

Se reemplaza en:

$d_k(y) \equiv y - 3 \; m\acute{o}d \; 27$
$d_k(22) \equiv 22 - 3 \; m\acute{o}d \; 27$
$d_k(22) \equiv 19 \; m\acute{o}d \; 27.$

La primera letra descifrada es $d_1 = 19$, que corresponde a la letra S.

Realizando un procedimiento igual al anterior se cifra cada letra del mensaje quedando los bloques de la siguiente manera:

198121	182018	1841921	112003	141938	1920813
SIBU	SCAS	RESU	LTAD	OSDI	STIN

20151913	15706	019198	4121618	4111512	8191215
TOSN	OHAG	ASSI	EMPR	ELOM	ISMO

Se organiza la frase para tener el mensaje original: SI BUSCAS RESULTADOS DISTINTOS NO HAGAS SIEMPRE LO MISMO.

Ejemplo 2. Cifrar el siguiente mensaje el cifrado RSA.

Mensaje: "ES IMPOSIBLE SER MATEMÁTICO SIN SER UN POETA DEL ALMA" de Sofía Kovalévakaya.

1. Se escogen dos números primos p y q, para aplicaciones en software de seguridad se recomienda que los números sean mayores de 200 dígitos no obstante para este caso se van a tomar números primos de solo tres dígitos:

$$p = 227, \; q = 251$$

Para estos dos números primos se comprobó su primalidad mediante la relación del símbolo de Legendre y Jacobi, para números primos impares de tal manera $\left(\frac{a}{b}\right) \equiv a^{\frac{(p-1)}{2}}$ y se cumpla que $r \equiv a^{\frac{n-1}{2}} \; mod \; n$ y se compruebe que $r = n-1$.

2. Se determina el grupo en el que se va a trabajar, es decir el valor $n=pq$.

$$n=227 \cdot 251$$

$$n=56977,$$

Se obtiene que se va a trabajar en el grupo $\mathbb{Z}_{56977.}$

3. Se determina el orden de grupo $\Phi(n)=(p-1)(q-1)$

$\Phi(n)=(227-1)(251-1)$

$\Phi(n)=226 \cdot 250$

$\Phi(n)=56500.$

4. Se escoge el valor de e de tal manera que el $m.c.d(\Phi(n),e)=1$ Se selecciona $e=21$ y se comprueba que aplicando el algoritmo de la división: $m.c.d(\Phi(56500),21)=1$ y, además

$$56500=2690 \cdot 21+10$$

$$21=2 \cdot 10+1,$$

Es decir, $e = 21$ es coprimo con $\Phi(n)=56500$. Por lo tanto, la clave pública es $(e,n=(21,56977)$.

5. Se determina el tamaño del bloque a cifrar.

N=Tamaño del alfato (27 letras)

(j−1, j) Tamaño del bloque de entrada y salida.

$$N^{j-1} < n < N^{j}$$

$$27^{3} < 56977 < 27^{4},$$

Los bloques que se van a formar para cifrar el mensaje son de 3 cifras.

6. Se expresa $e=21$ como suma de potencias de 2, esto se puede conseguir a partir de la expresión binaria de un número.

$$21 = 10101_{2} = 16 + 4 + 1.$$

7. Se expresa el mensaje a su respectivo equivalente numérico.

ESoo	IMP	OSI	BLE	ooSE	RooM	ATE	MAT	ICO
51900	91316	15199	2125	00195	180013	1205	13120	9315

ooSI	NooS	ERoo	UNoo	POE	TAoo	DEL	ooAL	MA
00199	180019	51800	211400	16155	20100	4512	00112	1301

El número cero representa el espacio entre las palabras del mensaje a cifrar, por lo que el equivalente numérico se corre una unidad.

8. Utilizando la ecuación $c \equiv m^e \ (mód\ n)$ se reemplaza para cifrar cada uno de los bloques.

- $c_1 = ES00 = 51900$

Se expresa en base 27 para que el mensaje sea un elemento del grupo $\mathbb{Z}^*_{56977}$.

$$ES = 5\times 27^2 + 19 \times 27^1 + 0\times 27^0 = 4158 = 4158\ (mód\ 56977).$$

Quedando $c_1 = 4158^{21}\ mód(56977)$, ahora se encripta c_1 con la clave pública $(21,56977)$, aplicando la exponenciación rápida el proceso de cifrado se realiza mediante: $a^{2i} = (a^{2i-1})^2$

$c^1 = 4158^{16+4+1}\ (mód\ 56977).$

$$4158^{16} = 4158^{24} = (4158^{23}) \cdot (4158^{23})\ (mód\ 56977)$$

$$= (4158^{2^2})^2 \cdot (4158^{2^2})^2 \cdot (mód\ 56977)$$

$$= ((4158)^{2^1})^2)^2 \cdot ((4158)^{2^1})^2)^2\ (mód\ 56977)$$

$$= ((4158)^2)^2 \cdot (4158^2)^2\ (mód\ 56977)$$

$$= (4158)^2 \cdot (4158)^2\ (mód\ 56977)$$

$$= 42952 \cdot 42952\ (mód\ 56977)$$

$$= 16021\ (mód\ 56977).$$

Ahora se trabaja con

$$4158^4 = 4158^{2^2} = (4158^{2^1}) \cdot (4158^{2^1}) \ (mód\ 56977)$$

$$= 24933 \cdot 24933 \ (mód\ 56977) = 35419 \ (mód\ 56977).$$

$$4158^1 = 4158^1 = 4158 \ (mód\ 56977).$$

Por lo tanto

$$c_1 = 4158^{16+4+1} \ (mód\ 56977) = 16021 \cdot 35419 \ (mód\ 56977)$$

$$= 9501 \ (mód\ 56977).$$

Se decodifica c_1 a base 27, para saber a qué letras equivale.

$$c_1 = 9501 \rightarrow 13\ 0\ 24.$$

El primer bloque para enviar es: 13 0 24, donde el número 13 equivale a la letra M, el cero es el espacio y el número 24 se reemplaza por la letra X; es decir, el mensaje codificado es M X. Realizando el procedimiento del punto 8 se codifica los otros bloques de letras que pertenecen al mensaje: MXC UOB YDB KHA RKT BMI JQB CZU ABS BGH MJE LBG TDBQ GYX WZU CID ZUB KIH NRS.

Descifrado del mensaje por el sistema RSA:

Quien recibe el mensaje debe conocer la clave privada y utilizar el siguiente proceso para descifrar el mensaje: MXC UOB YDB KHA RKT BMI JQB CZU ABS BGMJE LBG TDBQ GYX WZU CID ZUB KIH NRS.

1. Hallar el inverso (d) de $e=21$, para esto se utiliza el algoritmo extendido de Euclides y se determina el inverso d

$$1 = 21 - 2 \cdot 10$$

$$1 = 21 - 2(56500 - 2690 \cdot 21)$$

$$1 = 5381 \cdot 21 - 2 \cdot (56500),$$

Se obtiene que el inverso de $e=21$ es $d=5381$.

2. Se expresa el inverso $d=5381$ como potencia de 2.

$$5381= 1010100000101_2= 4096 + 1024 + 256 + 4 + 1.$$

3. Para recuperar el mensaje original, se va a decodificar cada bloque con la ecuación $m= c^d \ (mód\ n)$.

$$D_1= M00X = 130024$$

$$D_1= 130024^{5381} \ (mód\ 56977)$$

Se expresa en base 27 el bloque $M00X$

$$MOOX=13\times 27^2 + 0 \times 27^1 + 24 \times 27^0= 9477 + 0 + 24 = 9501 \ (mód\ 56977).$$

Por lo que queda expresado como $D_1= 9501^{5381} \ (mód\ 56977)$.

Haciendo uso del algoritmo de exponenciación rápida $a^{2i}= (a^{2i-1})^2$, con cada elemento del inverso d, se procede a recuperar el mensaje original.

$D_1= 9501^{4096+1024+256+4+1} \ (mód\ 56977)$, obteniendo:

$$9501^{4096}= 39866 \ (mód\ 56977)$$

$$9501^{1024}= 13582 \ (mód\ 56977)$$

$$9501^{256}= 35282 \ (mód\ 56977)$$

$$9501^{4}= 51148 \ (mód\ 56977)$$

$$9501^{1}= 9501 \ (mód\ 56977).$$

Por lo tanto, se tiene que:

$$D_1= 9501^{4096+1024+256+4+1} \ (mód\ 56977),$$

$$D_1=39866 \cdot 35282 \cdot 13582 \cdot 51148 \cdot 9501 \ (mód\ 56977)$$

$$D_1=4158 \ (56977).$$

Decodificamos D_1 en base 27.

$D_1 = 4158 \rightarrow 0519$

El primer bloque del mensaje original que se recupera es 05 19, donde 05 corresponde a la letra E y el número 19 equivale a la letra S, es decir el primer bloque de letras del mensaje es ES. Siguiendo el procedimiento anterior se descifra cada bloque obteniendo el mensaje: ES IMPOSIBLE SER MATEMÁTICO, SIN SER UN POETA DEL ALMA.

Herramientas Informáticas

Como se comprobó en el capítulo anterior, dentro de los procesos de seguridad de la información se involucran algoritmos que se basan en cálculos matemáticos de una sola vía, es decir son muy fáciles de realizar, pero difíciles de revertir (Córdoba & Méndez, 2017). Convirtiendo así, la criptografía en la base de cualquier mecanismo de seguridad informática, debido a que, con la aparición del internet, el correo electrónico y el comercio on-line entre otros programas informáticos, el ser humano se ha visto obligado a actualizar y desarrollar sistemas criptográficos más sofisticados y seguros para proteger la información, siendo la seguridad informática una de las áreas que más ha evolucionado en los últimos años (Jonquera, 2004).

El principal motivo para que esta área evolucionara significativamente, fue el interés por crear funciones criptográficas más seguras, que inició a finales de 1990 con la técnica de cifrado y autenticidad de datos de una sola clave (Bos, Naehrig & Van de Pol, 2017). Iniciando un sin fin de algoritmos uno más sofisticado que el otro.

Hay que destacar algunos procedimientos matemáticos mediante aplicaciones criptográficas, permite involucrar programas computacionales resaltando en primer lugar la evolución que la criptografía ha tenido a través de los años gracias a fundamentos computacionales y matemáticos que se han desarrollado para la seguridad informática de datos en redes (Clear & McGoldrick, 2017). Ofreciendo una aplicación completa que apoya cálculos básicos y abstractos de algunos métodos de encriptación, resaltando las fortalezas y debilidades de cada uno.

Involucrar la criptografía en el aprendizaje de temas matemáticos en la licenciatura en matemáticas, puede despertar un interés por investigar y aprender mediante aplicaciones de la vida real. Que de acuerdo con Higuera (2018) involucrar programas en un contexto educativo motiva y facilita la comprensión de conceptos con alta dificultad y abstracción, lo cual se quiere resaltar.

Como parte de la dinámica del estudio realizado, se hace uso de un programa computacional, esto con el objetivo de comprobar y resaltar aplicaciones de las matemáticas a la informática presente en la criptografía.

Programa CRYPTOOL

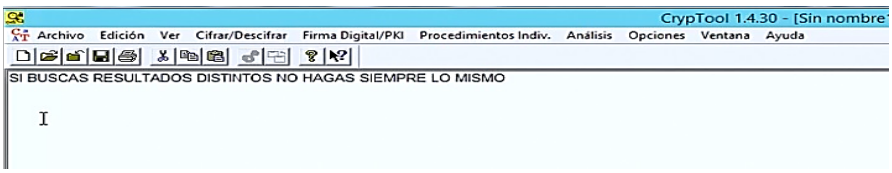
El programa se empezó a desarrollar en 1998 por patrocinio de compañías y universidades alemanas como un programa de aprendizaje para el área de la criptología el cual corre bajo un sistema operativo de Microsoft Windows y es de libre uso. La versión más actual del Cryptool es la 1.4.30 publicada en el año 2010, que estuvo a cargo del ingeniero de sistemas Raphael Labaca Castro. El papel principal de este programa consiste en hacer que los usuarios tomen conciencia de las amenazas de seguridad de la red, el cual se diseñó como una herramienta de aprendizaje electrónica o productiva (Adamo vi, Sarac, Stamenkovic & Radovanovic, 2018).

Figura 5: Logo del programa Cryptool.

Nota: Tomado del programa Cryptool.

Se presentará los ejemplos explicados matemáticamente en la sección anterior en el programa computacional Cryptool. Para el cifrado del Cesar se codificó el mensaje "SI BUSCAS RESULTADOS DISTINTOS NO HAGAS SIEMPRE LO MISMO" Albert Einstein en el programa Cryptool, escribiendo el mensaje en la pantalla principal (figura 6) y seleccionando el método de cifrado a usar en la pestaña Cifrar/Descifrar (figura 7) obteniendo por último el mensaje a enviar: VLEX VFDV UHVX ÑWDG RVGL VWLP WRVP RKDJ DVVL HOSU HÑRO LVPR (figura 8).

Figura 6. Pantalla principal programa Cryptool. Cifrado del Julio César.



Nota: Desde la figura 6 a la figura 10, fueron tomadas del programa Cryptool.

Figura 7: Selección del cifrado del Julio César.

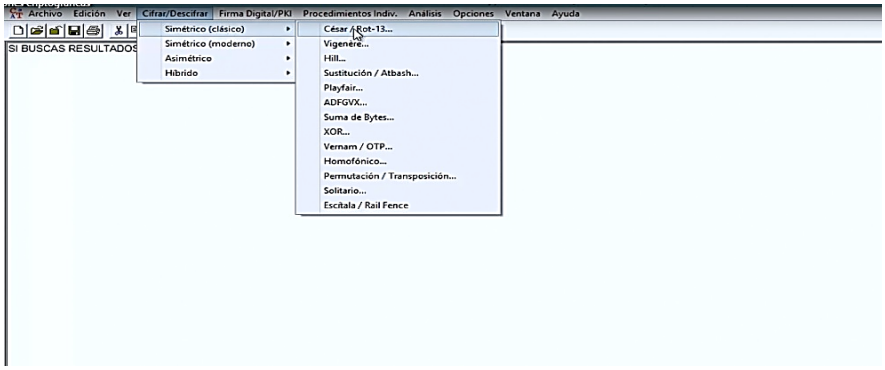
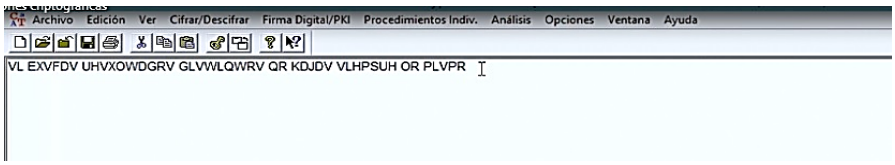


Figura 8: Mensaje cifrado por el método del Julio César.



El cifrado explicado y comprobado con el programa Cryptool es un cifrado simétrico clásico, por lo que realizar la comprobación con el programa es algo sencillo, sin embargo, al cifrar con el método del RSA en este programa es necesario realizar otros pasos adicionales para obtener el mensaje correcto. Primero se selecciona en la pestaña Cifra/Descifrar la subpestaña Asimétrico y RSA cifrar (figura 9), apareciendo una pestaña de demostración de RSA (figura 10) donde se especifica cada una de las claves privadas y públicas, y el grupo en el que se operó la comprobación matemática para que al cifrar se obtenga los mismos resultados al escribir el mensaje "ES IMPOSIBLE SER MATEMÁTICO SIN SER UN POETA DEL ALMA" de Sofía Kovalévakaya, en la pantalla principal como se muestra.

Figura 9: Selección del cifrado del RSA en el programa Cryptool.

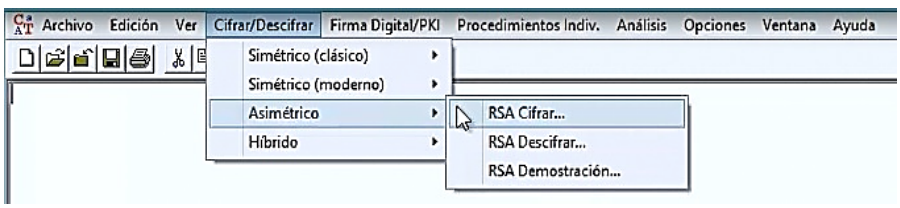
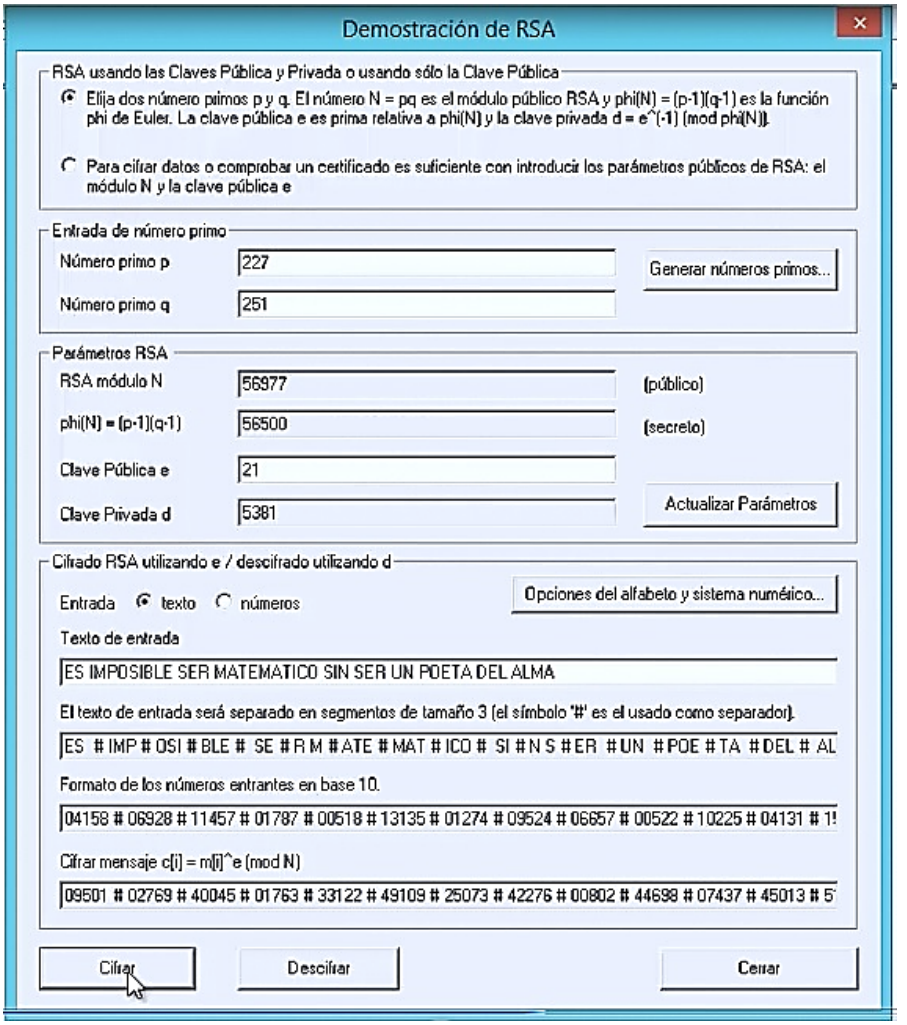


Figura 10: Ventana de demostración del RSA.



Cabe resaltar que, en la descripción del uso de los programas Cryptool se explica el proceso de cifrado ya que el de descifrado se realiza de la misma manera, a diferencia que se debe seleccionar la pestaña de "Descifrar". Conviene subrayar, que el uso de estos softwares de criptografía motiva el aprendizaje del fundamento matemático, necesario para el cifrado y descifrado de un mensaje. Los cuales, ayudan al proceso de abstracción de los contenidos de una forma eficiente e interactiva. De acuerdo con Adamo vi, Sarac, Stamenkovic y Radovanovic (2018) estos softwares sirven como laboratorios donde el estudiante resuelve problemas de instrucción básica, que requiere el uso de operaciones matemáticas complejas, lo que permite que el estudiante se involucre más en la solución del problema y pueda aprender mediante la criptografía. Considerando

que esta investigación tiene como objetivo comprender la teoría de números mediante algunas aplicaciones criptográficas, se pudo comprobar de manera eficaz con Cryptool el amplio uso de esta área de la matemática en los procesos de codificación en estos programas, el cual afirma que mediante aplicaciones es posible facilitar el aprendizaje de las matemáticas en los estudiantes de la licenciatura en matemáticas.

5. Discusión y conclusiones

Después de realizar el estudio de la teoría de números aplicada al desarrollo de algunos sistemas criptográficos se puede resaltar que:

El cifrado de Julio César al ser uno de los primeros métodos con escritura secreta, para su época era efectivo ya que quien lo utilizaba tenía la ventaja de que no todos sabían leer o escribir por lo que fue eficiente para la época, pero al estudiar su algoritmo se observa que es el más simple hablando en términos matemáticos, ya que es una sustitución basada en la aritmética modular por lo que actualmente la seguridad del sistema puede ser intervenida tanto computacionalmente como matemáticamente con facilidad.

Respecto al sistema RSA se resalta el hecho de que no existe una forma eficiente de factorizar números que sean producto de dos números primos grandes, por lo que distinguir conceptos específicos de la Teoría de Grupos y Factorización es interesante, ya que aplicados al algoritmo lo vuelve uno de los criptosistemas más seguros en la actualidad.

En los métodos criptográficos trabajados intervienen fundamentos matemáticos que necesitan de un sistema computacional para mejorar su eficacia, pues se necesita trabajar con algoritmos que utilizan números primos muy grandes, por eso, programas computacionales como Cryptool favorecen el desarrollo de la criptografía. Se quiso mostrar el manejo de este programa, realizando los procedimientos de cifrado de cada sistema estudiado, obteniendo resultados en poco tiempo; también se trabajaron estos programas con el propósito de darlos a conocer para que se puedan utilizar en las asignaturas de Álgebra Lineal, Teoría de Grupos y Teoría de Anillos que se dan en la Licenciatura en Matemáticas, pues se pueden descargar fácilmente ya que son de uso libre.

6. Lista de referencias

Adamovic, S., Stamenkovic, D., Sarac, M. & Radovanovic, D. (2018). The importance of the using software tools for learning modern cryptography. *International Journal of Engineering Education,* 34(1), 256-262. Recuperado de https://www.researchgate.net/publication/322578255.

Beltran, E. (2012). *Análisis comparativo de algoritmos criptográficos de clave pública.* (tesis de maestría). Instituto Politécnico Nacional.

Bos, J., Naehrig, M., Van de Pol, J. (2017). Sieving for shortest vectors in ideal lattices: a practical perspective. *International Journal of Applied Cryptography* 3 (4). DOI: 10.1504 / IJACT.2017.10010312

Chaves, H. (2008). Diseño e implementación de un software multimedia para el aprendizaje de la criptografía. (tesis de pregrado). Universidad San Buenaventura.

Clear, M., McGoldrick, C. (2017). Attribute-Based fully homomorphic encryption with a bounded number of inputs. *International Journal of Applied cryptography* 3(4). DOI: 10.1504/IJACT.2017.10010329

Cordoba , D., & Méndez, M. (2017). *Criptografía Post Cuántica. Consejo nacional de investigaciones científicas y técnicas CONICET.* Red de universidades con carreras en informática. 1038-1042. Recuperado de http://sedici.unlp.edu.ar/handle/10915/61343.

Fúster, A., Montoya, F., De la Guia Martinez, D., & Hernández, L. (2001). *Técnicas Criptográficas de Protección de Datos.* México: RA-MA.

Gómez, A. (2011). *Enciclopedia de la Seguridad Informática.* México: Alfa-omega RA-MA.

Gómez, M. (2011). *La Aritmética Modular y Algunas de sus Aplicaciones.* (tesis de maestría) Universidad Nacional de Colombia.

Granados, G. (2006). Introducción a la Criptografía. *Revista Digital Universitaria,* 7(7). Recuperado de http://www.revista.unam.mx/vol.7/num7/art55/int55.htm. ISSN: 1067-6079.

Hernández, R., Fernández, C. & Baptista P. (2010). *Metodológia de la Investigación.* Mexico: Mc Grand Gill Educación.

Higuera, F. (2018). *Gamificación para la enseñanza de la computación, criptografía e información cuántica.* (tesis pregrado). Escuela técnica superior de ingenieros informáticos.

Ibañez, F. (2012). *La enseñanza de la Criptografía en los Curso de Educación Media.* (tesis de maestría). Universidad Nacional de Colombia.

Jonquera, M. (2004). Criptografía. *SUMA*, (46), 27-30. Recuperado de http://revistasuma.es.

Lucena, M. (2001). *Criptografía y seguridad en computación.* Recuperado de http://index-of.co.uk/Tmp/Criptografia.pdf

Rubiano, G. (2004). *Teoría de Números para Principiantes.* Bogotá: Universidad Nacional de Colombia.

Vacca, E. (2016). *Estudio de la Teoría de Números Aplicada a Algunos Métodos Criptográficos.* (tesis pregrado). Universidad Pedagógica y Tecnológica de Colombia.

Xifre, P. (2009). *Antecedentes y Perpestivas de Estudio en Historia de la Criptografía.* (tesis de pregrado). Universidad de Madrid Carlos III.