UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

Técnicas de criptografía en las comunicaciones modernas. Empleo del método de curvas elípticas.

AUTOR:

Ing. Proaño Andrade, Juan Carlos

Trabajo de Titulación previo a la obtención del Grado Académico de

MAGÍSTER EN TELECOMUNICACIONES

TUTOR:

MSc. Romero Paz, Manuel de Jesús

Guayaquil, Ecuador

26 de octubre del año 2018

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Magíster **Proaño Andrade, Juan Carlos** como requerimiento parcial para la obtención del Grado Académico de **MAGÍSTER EN TELECOMUNICACIONES.**

TUTOR

_____

M. Sc. Romero Paz, Manuel de Jesús

DIRECTOR DEL PROGRAMA

_____

M. Sc. Romero Paz, Manuel de Jesús

Guayaquil, 26 de octubre del año 2018

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Proaño Andrade, Juan Carlos**

DECLARÓ QUE:

El trabajo de titulación **"Técnicas de criptografía en las comunicaciones modernas. Empleo del método de curvas elípticas"**, previa a la obtención del grado académico de **Magíster en Telecomunicaciones**, ha sido desarrollado, respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del trabajo de titulación del Grado Académico en mención.

Guayaquil, 26 de octubre del año 2018

EL AUTOR

_____

Ing. Proaño Andrade, Juan Carlos

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Proaño Andrade, Juan Carlos**

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del trabajo de titulación de Maestría titulada: **"Técnicas de criptografía en las comunicaciones modernas. Empleo del método de curvas elípticas"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

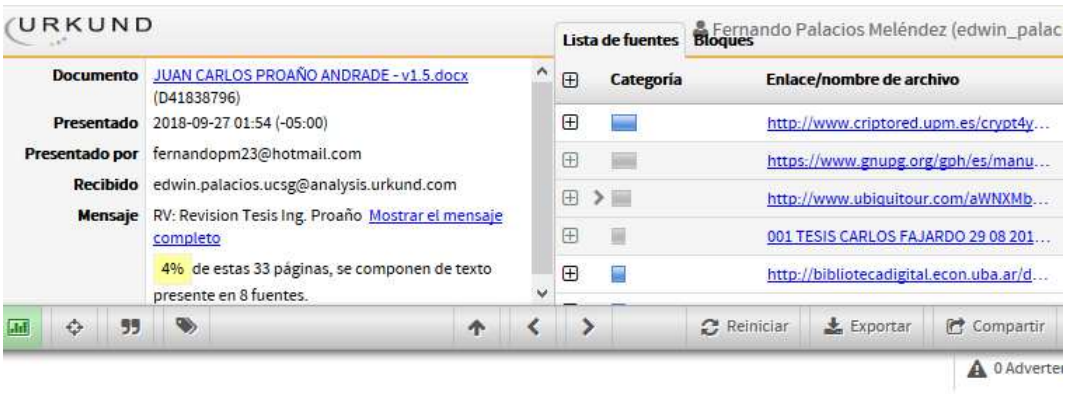
Guayaquil, 26 de octubre del año 2018

EL AUTOR

_____

Ing. Proaño Andrade, Juan Carlos

REPORTE DE URKUND



SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

Técnicas de criptografía en las comunicaciones modernas. Empleo del método de curvas elípticas.

Trabajo de Titulación previo a la obtención del Grado Académico de Magíster en Telecomunicaciones

ELABORADO POR: Ing. JUAN CARLOS PROAÑO ANDRADE

TUTOR: MSc. Manuel Romero Paz

Dedicatoria

Todo mi esfuerzo, cariño y amor en el presente trabajo va dedicado de manera especial:

A mis padres, que, con su ejemplo de vida, serán siempre mis fuentes de inspiración para alcanzar nuevas metas.

A mi hijo “Paquito”, que día a día con su inocencia y ternura es mi mejor maestro de vida.

Gracias a Dios, por ponerlos en mi vida.

Agradecimientos

Agradezco a mi Director de Tesis, Ing. Manuel Jesús Romero Paz, que, junto a los revisores; aportaron con sus conocimientos y experiencias para la ejecución de este trabajo investigativo.

Al prestigioso cuerpo docente de la Maestría de Telecomunicaciones de la Universidad Católica Santiago de Guayaquil, quienes nos dieron la oportunidad de enriquecer mi conocimiento.

Mi agradecimiento a todos: mis padres, Paquito y amigos que de una u otra forma estuvieron acompañándome y apoyándome en el transcurso de la Maestría.

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

M. SC. ROMERO PAZ MANUEL DE JESÚS

TUTOR

f. _____

M. SC. CÓRDOVA RIVADENEIRA, LUIS SILVIO

REVISOR

f. _____

M. SC. PALACIOS MELÉNDEZ, EDWIN FERNANDO

REVISOR

f. _____

M. SC. ROMERO PAZ MANUEL DE JESÚS

DIRECTOR DEL PROGRAMA

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

Capítulo 1: Descripción del proyecto de intervención.

Capítulo 2: Estado del Arte de la Criptografía.

Capítulo 3: Modelamiento de Algoritmos Criptográficos utilizando Curvas Elípticas.

ÍNDICE DE TABLAS

Resumen

El presente proyecto de titulación está orientado a realizar una simulación de un algoritmo criptográfico asimétrico de clave corte utilizando el método de curvas elípticas; este trabajo de investigación está estructurado de tres capítulos. En el capítulo uno, se efectúa la descripción del presente trabajo de titulación, tales como: la justificación, antecedentes, definición del problema, objetivo general, objetivos específicos, hipótesis y, la metodología a seguir. En el capítulo dos, se desarrolla la fundamentación teórica de la Criptografía, la cual explica los orígenes de la Criptografía y, sus principales definiciones empleadas; luego se describe la Criptografía Simétrica y, el desarrollo de la Criptografía Asimétrica; se ha tratado, en cada tipo de Criptografía especificar lo más relevante de los algoritmos más empleados, lo cual no deja ser temas menos importantes de destacar. Se hace una breve referencia, al Criptoanálisis, tanto, para Sistemas Simétricos como para Asimétricos y, finalmente se hace una breve descripción en cuanto al Cifrado y, Criptoanálisis cuántico. En el capítulo tres, se realiza toda la parte teórica relacionada con la Criptografía con Curvas Elípticas; con estas bases, se hace una propuesta de modelamiento de un algoritmo asimétrico por medio de una herramienta de código abierto, finalmente, se muestran las conclusiones y, recomendaciones.

Palabras Claves: Criptografía, Seguridad, Simétrico, Asimétrico, Curvas Elípticas.

Abstract

The present project of study is oriented to realize a simulation of an asymmetric cryptographic algorithm of key cut using the method of elliptic curves; this research work is structured in three chapters. In chapter one, the description of the present titration work is carried out, such as: justification, background, problem definition, general objective, specific objectives, hypothesis and, the methodology to be followed. In chapter two, the theoretical foundation of Cryptography is developed, which explains the origins of Cryptography and its main definitions used; then the Symmetric Cryptography and the development of Asymmetric Cryptography are described; it has been tried, in each type of Cryptography, to specify the most relevant of the most used algorithms, which does not stop being less important subjects to highlight. A brief reference is made to Cryptanalysis, both for Symmetric and Asymmetric Systems and, finally, a brief description is made regarding Ciphering and Quantum Cryptanalysis. In chapter three, all the theoretical part related to Cryptography with Elliptical Curves is done; With these bases, a proposal of modeling an asymmetric algorithm is made by means of an open source tool, finally, conclusions and recommendations are shown.

Key Words: Cryptography, Security, Symmetric, Asymmetric, Elliptical Curves.

Capítulo 1: Descripción del proyecto de intervención.

Este trabajo está motivado, por el interés investigativo relacionado con las técnicas criptográficas, tanto simétrico como asimétrico implementado en las comunicaciones modernas que han sido desarrollados con la finalidad de asegurar el contenido de la información en los mensajes transmitidos en una comunicación. De la misma forma que se han perfeccionado múltiples técnicas para asegurar la información como contraparte, han sido florecientes las técnicas para vulnerar estos mecanismos; por esta razón, se expone una propuesta en el ámbito de la investigación de estas técnicas criptográficas y sus atributos, empleando el método de curvas elípticas. El efecto de aprovechar los atributos del método que brinda las curvas elípticas en las técnicas criptográficas es empleado en múltiples aplicaciones que no solo ofrecen seguridad sino, además una longitud corta en el tamaño de sus claves.

1.1. Justificación del Problema a Investigar.

El continuo desarrollo de las tecnologías de las comunicaciones ha sido de forma acelerada, pero de igual forma, este avance ha ido en conjunto con la aparición de técnicas que tienen como finalidad vulnerar la seguridad en las comunicaciones y utilizarlas de forma malintencionada, por citar algunas de estas técnicas se tiene: falsificación de peticiones en sitios cruzados, inclusión de ficheros remotos, inyección CRLF, dominios fantasmas y ataques de denegación de servicio, entre otros.

En la figura 1.1 se muestra los elementos de la Arquitectura de Seguridad, según la Rec. UIT-T X.805; en la cual, se observa las amenazas, los ataques y las vulnerabilidades a las que están expuestas las diferentes capas de seguridad: en las aplicaciones, de los servicios y en la infraestructura.

En este sentido, la criptografía moderna tiene como objetivo garantizar la seguridad en las capas referidas fortaleciendo los algoritmos propios de su materia.

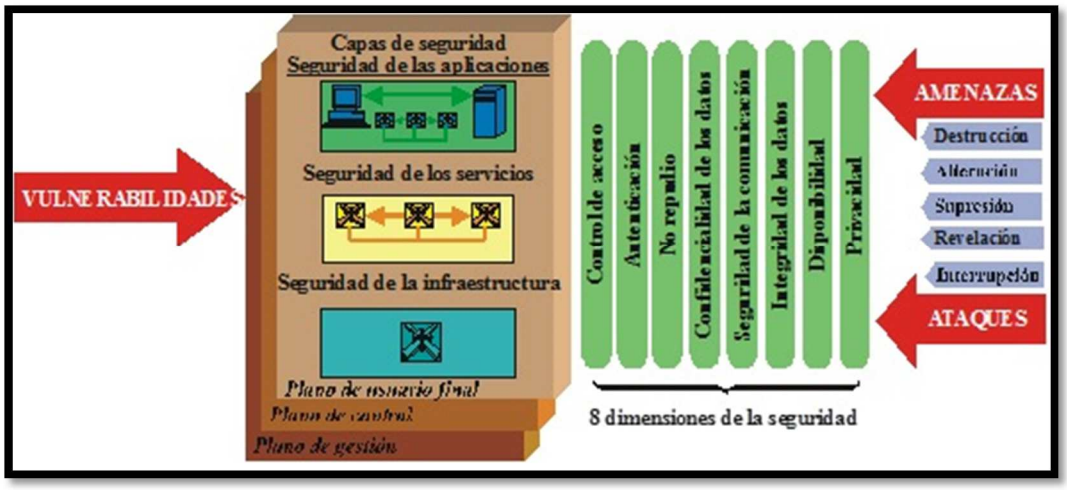


Figura 1. 1: Elementos de la arquitectura de seguridad de la Rec. UIT-T X.805.
Fuente: (UIT-T-X.805).

Con este argumento, es necesario modelar un algoritmo con características que garanticen la seguridad y, de esta manera reducir la inseguridad a la que son expuestos los sistemas de comunicaciones.

1.2. Antecedentes.

El continuo incremento de incidentes relacionados con la seguridad de la información conlleva al crecimiento de un problema de seguridad tanto para los usuarios como para las empresas al ser expuestas a posibles intrusiones en sus sistemas de información. Como referencia CISCO, en su 2018 Annual Cybersecurity Report, en sus investigaciones realizadas a cabo en los últimos meses, concluye que cada vez, los ciberataques, técnicamente son más sofisticados, sobre todo empleando técnicas de malware oculto en tráfico cifrado.

En la tabla 1.1 se muestra un reporte de CISCO, en el cual se observa los avisos críticos de vulnerabilidades, reportados entre noviembre de 2016 y mayo de 2017. Estadísticas de este tipo, conllevan a motivar el estudio más detallado en buscar modelos de algoritmos criptográficos, que sean seguros y, computacionalmente eficientes, de tal forma que garanticen la seguridad en la información en las comunicaciones.

Tabla 1. 1: Avisos críticos de vulnerabilidades ente noviembre de 2016 y mayo de 2017.

Date	Activity	Date	Activity
05/24/17	Samba Insecure Library Loading CVE-2017-7494	03/06/17	Apache Struts2 Remote Code Execution Vulnerability CVE-2017-5638
04/11/17	Microsoft Office CVE-2017-0199 (Dridex Exploiting)	02/06/17	OpenSSL Vulnerabilities CVE-2017-3733
04/08/17	Shadow Brokers Group Disclosure of Equation Group Exploits	01/26/17	OpenSSL Vulnerabilities
04/06/17	Operation Cloud Hopper Sustained Global Campaigns	01/18/17	Oracle CPU Oracle OIT Vulnerabilities (Talos)
03/29/17	Microsoft Internet Information Services (IIS) WebDav CVE-2017-7269	01/03/17	PHPMailer Arbitrary Command Injection CVE-2016-10033 CVE-2016-10045
03/21/17	Network Time Protocol	11/22/16	Network Time Protocol
03/14/17	Microsoft Windows Graphics CVE-2017-0108	11/10/16	BlackNurse - ICMP DOS
03/07/17	WikiLeaks Vault 7 Release	11/04/16	Mobile OAuth 2.0 Implementation Issues

Source: Cisco Security Research

Fuente: (CISCO, 2017).

1.3. Definición del problema.

El perfeccionamiento de diversas técnicas para quebrantar sistemas de comunicaciones ha conllevado a los investigadores especializados en el campo de la Criptografía y, a los fabricantes de tecnología de comunicaciones a desarrollar diferentes métodos para reducir las vulnerabilidades como las anteriormente descritas. La falta de simulación de algoritmos criptográficos conlleva a la necesidad de experimentar, mediante el modelamiento, algoritmos criptográficos de cifrado asimétrico, empleando buenas curvas elípticas sobre campos finitos, de tal forma que estos algoritmos sean seguros por defecto y, computacionalmente óptimos.

1.4. Objetivos.

Los objetivos que se plantean en este trabajo de investigación se detallan a continuación:

1.4.1. Objetivo General:

Modelar un algoritmo criptográfico asimétrico, con buenas curvas elípticas sobre campos finitos con característica n=2, empleando una aritmética eficiente y que sea práctico.

1.4.2 Objetivos específicos:

- Investigar los fundamentos teóricos de la criptografía tanto clásica como moderna, aplicados a los sistemas de comunicaciones.
- Profundizar, el estudio de las curvas elípticas en el campo de la criptografía.
- Simular métodos y, algoritmos que permitan modelar un algoritmo criptográfico asimétrico, con buenas curvas elípticas sobre campos finitos y que sean eficientes en aplicaciones prácticas.

1.5. Hipótesis.

El modelamiento de un algoritmo criptográfico asimétrico, con curvas elípticas aplicado sobre campos finitos con característica n=2, permitirá una aritmética eficiente. Este modelamiento demuestra la seguridad del criptosistema, utilizando claves reducidas; lo que conlleva a desarrollar múltiples aplicaciones que requieren seguridad empleando claves de longitud corta.

1.6. Metodología de investigación.

El enfoque de investigación es cuantitativo, método empírico analítico. Alcance de la investigación: descriptivo, explicativo, exploratorio o correlacional.

- Alcance descriptivo, se refiere a la recopilación de información para cumplir con el objetivo principal de este trabajo que es *"Modelar un algoritmo criptográfico asimétrico, con la característica de una curva elíptica buena sobre campos finitos".*
- Alcance explicativo, analizar y proponer aplicaciones de sistemas criptográficos implementados con curvas elípticas en ambientes donde, no solo brinden seguridad, sino además el uso de claves mínimas.

Capítulo 2: Estado del Arte de la Criptografía.

En el Capítulo 2, se desarrollará todo lo relacionado con la fundamentación teórica del presente trabajo.

2.1. Criptografía. Definiciones y origen.

El termino criptografía, nace de dos palabras de origen griego: krypto (ocultar) y graphos (escribir); a continuación, se citan algunas definiciones de autores reconocidos en esta materia con relación a su definición:

García (2013), define lo siguiente: “La criptografía es una ciencia que estudia los métodos para transmitir con seguridad Información entre dos partes, haciendo que el mensaje sea ininteligible para cualquier Terceros no autorizados”. (García, 2013).

Pacheco (2014) afirma: “Conjunto de técnicas basadas en la matemática y aplicadas por medio de la informática que utilizan distintos métodos con el objetivo de ocultar datos ante observaciones no autorizados, mediante el uso de un algoritmo y al menos una clave”. (Pacheco, 2014).

Hernández (2015) manifiesta: “Tradicionalmente, la criptografía se ha ocupado de este problema con el fin de garantizar la confidencialidad, integridad y autenticidad de la información mediante diferentes técnicas y algoritmos, denominados criptosistemas” (Hernández F. , 2015).

Se puede definir entonces a la criptografía, como la ciencia que tiene como objetivo certificar la confidencialidad, integridad y, autenticidad de la información que se transpone entre un emisor y un receptor a través de un medio, empleando diferentes algoritmos matemáticos y, al menos una clave.

2.1.1 Criptógrafo.

Ramio (2006) define: “Maquina diseñada o artilugio para cifrar información”. (Ramió, 2006).

2.1.2 Criptología.

Este término (del griego krypto y logos, se refiere al estudio de lo escondido), según Fernández (2011) lo define como: ‘’la ciencia que trata los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en

clave entre un emisor y un receptor a través de un canal de comunicaciones". (Fernández, 2011).

2.1.3 Criptólogo.

Ramió (2006) lo define como: "Persona que trabaja de forma legítima para proteger información creando algoritmos criptográficos". (Ramió, 2006).

2.1.4 Criptosistema.

Pacheco (2014) define a un criptosistema como un ''conjunto completo de elementos de un sistema criptográfico, de tal forma que pueda ser utilizado para cumplir con sus funciones''. (Pacheco, 2014).

2.1.5 Criptoanálisis.

Es la ciencia que, por medio de diferentes métodos, tiene como objetivo descifrar los mensajes en clave, de tal forma que pueda vulnerar un criptosistema.

Lucena (2010) describe en relación con la criptografía y al criptoanálisis: "Conviene hacer notar que la palabra criptografía sólo hace referencia al uso de códigos, por lo que no engloba a las técnicas que se usan para romper dichos códigos, conocidas en su conjunto como criptoanálisis. En cualquier caso, ambas disciplinas están íntimamente ligadas; no debe olvidarse que cuando se diseña un sistema para cifrar información, hay que tener muy presente su posible criptoanálisis". (Lucena, 2010).

2.1.6 Criptoanalista.

Ramió (2006) puntualiza: "Persona cuya función es romper algoritmos de cifrado en busca de debilidades, la clave o del texto en claro". (Ramió, 2006).

2.1.7 Estenografía.

Esta es una técnica de escritura, la cual tiene como objetivo esconder un mensaje con información privada por medio de un canal inseguro, de tal forma que el mensaje no sea descubierto. Regularmente, el mensaje con la información escondida se encuentra dentro con otros formatos, por ejemplo: vídeo, imágenes, audio o mensajes de texto.

2.1.8 Estegoanálisis.

Al contrario de la Estenografía, esta es una técnica que tiene como finalidad detectar mensajes ocultos con técnicas estenográficas. Teóricamente, el estegoanálisis, pretende explotar técnicas para encontrar las vulnerabilidades de la estenografía, las cuales pueden reducir o eliminar la seguridad que teóricamente aportaba la técnica estenográfica.

2.2 Seguridad de la Información.

La seguridad de la Información es un tema, que cada vez las empresas, las organizaciones y, los usuarios de diferentes sistemas de información en forma general han tomado conciencia y, por lo tanto, le han dado la importancia al buen uso de la información, que es el activo más valorado por una organización o un usuario. Por esta razón, la Seguridad de la Información, en los últimos años ha tenido un desarrollo y, en los actuales momentos, se la puede catalogar como un tema relevante y de vital importancia para todos los campos que abarca las tecnologías de la información y evidentemente las telecomunicaciones en todos sus ámbitos no están exentas de este tema.

La seguridad de la información abarca una extensa terminología, pero de forma general existen tres principios, sobre los cuales se sienta las bases fundamentales de la seguridad de la información que son:

- Confidencialidad.
- Disponibilidad.
- Autenticidad.

2.2.1 Confidencialidad.

Este primer elemento, básicamente tiene como objetivo principal, que la información que fluye a través de un canal entre un emisor y un receptor sea leída por la persona o sistema autorizado. Costas (2011) define lo siguiente: “Se trata de la cualidad que debe poseer un documento o archivo para que este solo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado. De esta manera se dice que un documento (o archivo o mensaje) es confidencial si y solo si puede ser comprendido por la persona o entidad a quien va dirigida o esté autorizada. En el caso de un

mensaje esto evita que exista una intercepción de este y que pueda ser leído por una persona no autorizada". (Costas, 2011).

2.2.2 Integridad.

Este segundo elemento, tiene como objetivo que la información en una comunicación entre un emisor y, un receptor por medio de un canal no sea alterada. Ramió (2006) define lo siguiente: "Los componentes del sistema sólo pueden ser creados y modificados por los usuarios autorizados". (Ramió, 2006).

2.2.3 Disponibilidad.

Por último, para el tercer elemento, su objetivo es que la información entre en un emisor y, un receptor a través de una canal de comunicación este siempre disponible. Ramió (2006) define: "Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen". (Ramió, 2006).

En los últimos años, se ha introducido en el ámbito de la seguridad de la información un nuevo elemento que es el "No repudio", a continuación, su definición:

2.2.4 No repudio.

Este elemento, es adicionado como una característica de los elementos que componen la seguridad de la información, Ramió (2006), al respecto define: "Está asociado a la aceptación de un protocolo de comunicación entre emisor y receptor (cliente y servidor) normalmente a través del intercambio de sendos certificados digitales de autenticación. Se habla entonces de No Repudio de Origen y No Repudio de Destino, forzando a que se cumplan todas las operaciones por ambas partes en una comunicación". (Ramió, 2006).

2.3 Origen de la criptografía.

Para narrar el origen de la criptografía, hay que retroceder en el tiempo y, mencionar que las antiguas civilizaciones ya tenían la necesidad de esconder su información y, no precisamente estas civilizaciones,

desarrollaron métodos criptográficos, pero sí, aplicaron procedimientos de forma empírica. Por citar algunas civilizaciones: los griegos desarrollaron en el siglo V A.C. el escítalo espartano, el cual consistía en una cinta de cuero enrollado en un bastón de mando, sobre el cual se escribía de forma longitudinal el mensaje, por así decirlo era una manera cifrar el mensaje. Procedimiento contrario, para descifrar el mensaje, la cinta debía ser enrollada en un bastón de diámetro adecuado. En la figura 2.1 se muestra un escítalo espartano.

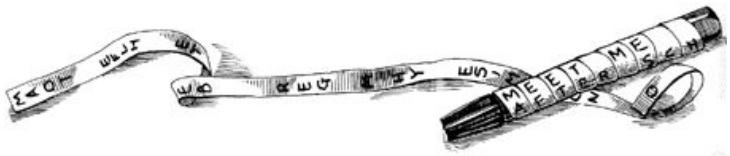


Figura 2. 1: Escítalo espartano.
Fuente: (Tabara, 2014)

En cambio, el historiador griego Polybios en el Siglo II A.C., elaboró una tabla formada por filas y, columnas sobre la cual, se hacía corresponder a cada letra del alfabeto un par de letras según su posición; es decir, el criptograma era el conjunto de pares de letras. En la figura 2.2 se muestra una representación del Cifrado de Polybios, por citar un ejemplo la letra A, está representada por AA y la letra Z es la combinación de EE.

Por otro lado, los romanos inventaron el Cifrario de Cesar; esto en honor al Emperador Julio Cesar en el Siglo I a.C. En la figura 2.3 se muestra una representación del Cifrario de Cesar, el cual consistía en escribir el mensaje en un alfabeto latino desplazado con tres posiciones hacia la derecha; por ejemplo, la letra D es equivalente a la letra A.

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I/J	K
C	L	M	N/Ñ	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Figura 2. 2: Tabla de Polybios.
Fuente: (Pacheco, 2014)

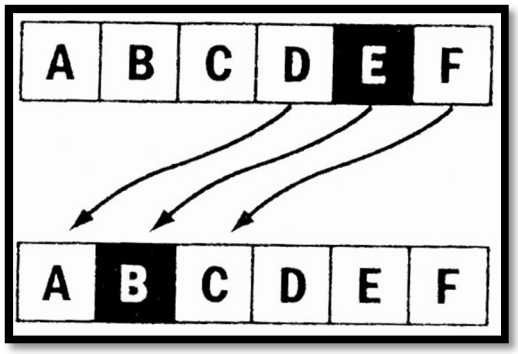


Figura 2. 3: Cifrario de Cesar.
Fuente: (Pacheco, 2014).

2.4 Surgimiento y desarrollo de los encriptadores de datos.

Como se mencionó, el hombre, desde las primeras civilizaciones ha tenido la necesidad de ocultar mensajes por diferentes mecanismos; esta necesidad, acompañada del desarrollo del campo de las matemáticas y, la informática, la criptografía y, sus diferentes técnicas de cifrado, no han sido exoneradas de este desarrollo; por esta razón, la mayoría de autores de criptografía, clasifican dos épocas en relación a la evolución de los encriptadores de datos: la criptografía clásica y, la criptografía moderna. A continuación, se hace una breve descripción de algunos sistemas desarrollados en orden cronológico.

2.4.1 Técnicas clásicas de cifrado.

Acerca de las técnicas clásicas de cifrado Pacheco (2014), cita lo siguiente: "Las técnicas utilizadas en esta primera etapa de la Criptografía, se basaban en la transposición y sustitución de caracteres, y en el uso de claves, aunque no necesariamente" (Pacheco, 2014).

Las técnicas clásicas de cifrado tenían básicamente dos características:

- Técnicas de Cifrado basadas en letras de un determinado alfabeto y,
- Secreto del mecanismo del cifrado.

En la llamada criptografía clásica, esta se basó en dos tipos de algoritmos: los de transposición y sustitución; los cuales asentaron los principios para el desarrollo de la criptografía moderna. Los algoritmos desarrollados por

sustitución fueron de dos tipos: por sustitución monoalfabética y, sustitución polialfabética.

Los algoritmos por sustitución monoalfabética o también simple, se basa en el uso de un solo alfabeto con una sola llave para realizar la sustitución. Pacheco (2014), define: ‘’Un cifrado por sustitución es monoalfabético cuando utiliza una sustitución fija para todo el mensaje. Por ejemplo, si la letra A del texto plano se la empareja con la letra H del texto cifrado, se sustituirá siempre la misma forma’’. (Pacheco, 2014).

Los algoritmos desarrollados por sustitución monoalfabética fueron: El Cifrado de Atbash, La escítala, Cifrado de Polybios, Cifrado del Cesar, el disco de Wheatstone, el disco de Bazeries, Cifrado Playfair y, el Cifrado de Hill.

Especial atención se debe prestar a la máquina Bombe, inventada por el británico Alan Turing (1912-1954), diseñada con la intención de descifrar los mensajes de la maquina Enigma, la cual fue desarrollada por los criptólogos alemanes con el objetivo de cifrar y, descifrar información de forma polialfabética durante el transcurso de la Segunda Guerra Mundial. Bombe, fue una invención de Turing, la cual se basó en el método de análisis bayesiano; la implementación de esta máquina, se la puede catalogar como el portaestandarte de la época del cifrado clásico.

Ángel (2012) al respecto se refiere: “Turing usó diferentes caminos para criptoanalizar a enigma, desde ingeniería en reversa hasta el desarrollo de un complejo análisis estadístico. Con la ayuda de todo el conocimiento del equipo polaco y los mensajes que eran interceptados, poco a poco lograron afinar ciertas técnicas que finalmente lograron descifrar mensajes. Se ayudaban con una maquina llamada Bombe que el grupo polaco ya había probado. La Bombe de Turing usaba una técnica llamada cribs, pequeños fragmentos de texto plano y cifrado que se podían conocer de las intercepciones hechas por los alemanes” (Ángel, 2012). En la figura 2.4, se observa la maquina Bombe.

Por otra parte, los algoritmos desarrollados por sustitución polialfabética, se basaron en reemplazar cada carácter que varía en función de la posición que ocupe dentro del mensaje; las técnicas desarrolladas bajo este tipo de

sustitución fueron: Cifrado de Alberti, Cifrado de Vigenére y, el Cifrado de Vernam.

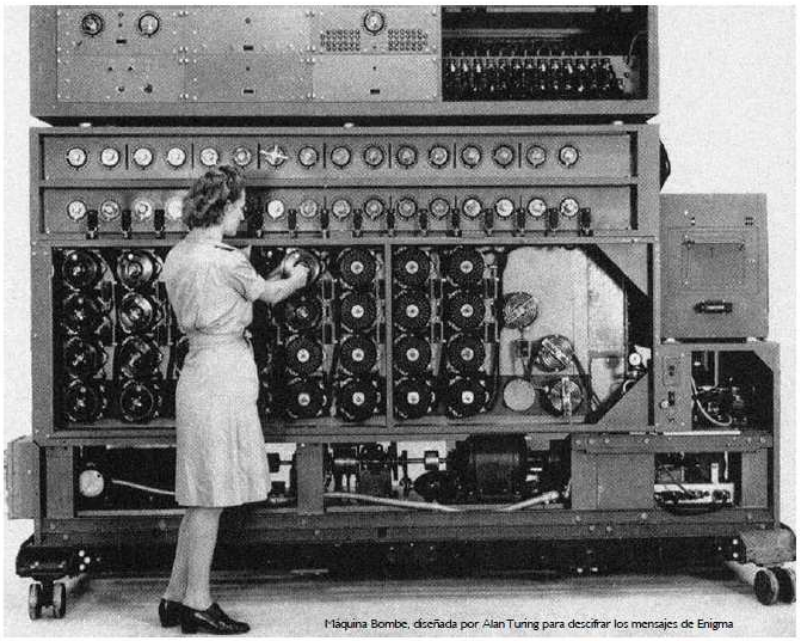


Figura 2. 4: Maquina Bombe.
Fuente: (Ángel, 2012)

Carrasco (2015) comenta lo siguiente: “La criptografía ha existido desde hace varios miles de años y el propósito básico siempre ha sido alterar un mensaje mediante codificación o cifrado para hacerlo ininteligible ante los intrusos y conservar la confidencialidad del mensaje original con el objetivo de que solo las partes autorizadas puedan acceder a él. Las técnicas criptográficas han ido evolucionando a la par que los ataques a su seguridad (criptoanálisis), aumentando de forma creciente la complejidad, pero en general se puede hablar de un texto plano que es necesario cifrar con algún algoritmo y una clave para transformarlo en un criptograma que más tarde pueda ser descifrado para recuperar el texto plano original mediante otro algoritmo y una clave. Si bien la confidencialidad ha sido el principal objetivo de esta disciplina a lo largo de la historia, con el tiempo han ido surgiendo nuevas propiedades, como la autenticación, integridad y el no repudio. Con el aumento de la capacidad de computación, las técnicas criptográficas han ido aumentando en complejidad, principalmente debido a la creciente facilidad para vulnerar esta seguridad, precisamente propiciada por esta mayor capacidad computacional” (Carrasco, 2015).

2.4.2 Técnicas Modernas de cifrado.

Las técnicas de cifrado clásico anteriormente expuestas tuvieron un quebrante significativo con la evolución de las matemáticas y de la tecnología, específicamente de la electrónica y la computación. Se puede definir, que este quiebre entre la criptografía clásica y la moderna, fue a partir de 1949, cuando Claude Shannon hizo la publicación de su artículo: Communication Theory of Secrecy Systems (Teoría de la Comunicación de Sistemas Secretos) y junto a Warren Weaver, publicaron el libro Theory of Communication (Teoría de la Comunicación). La base de la Criptografía Moderna está basada en:

- Teoría de la Información.
- Teoría de los números.
- Teoría de la Complejidad Numérica.

Las técnicas de cifrado de criptografía moderna en relación a la criptografía clásica se caracterizan por:

- Cifrado con representación en códigos, generalmente binarios.
- Uso de técnicas matemáticas.
- Procesamiento por tecnologías informáticas.

Estas tres características, dieron origen a nuevos conceptos dentro de la criptografía que son: llave pública y privada, utilizadas para cifrar y descifrar mensajes; al igual que nuevos conceptos de criptografía simétrica y asimétrica.

2.4.3 Empleo de técnicas de criptografía en trasmisión de datos.

Como se indicó en un principio, la humanidad desde las primeras civilizaciones hasta nuestros días ha tenido la necesidad de ocultar su información con finalidades distintas. Hoy en día, por el acelerado desarrollo de las tecnologías de la información, la criptografía como ciencia, está obligada a certificar que los principios de Seguridad de la información: confidencialidad, disponibilidad, autenticidad y no repudio, se cumplan en la

transmisión de información a través de un canal entre un emisor y un receptor.

Cesaratto y Fuentes (2015) describen lo siguiente: “Un protocolo criptográfico o criptosistema es un procedimiento que permite intercambiar información de forma segura entre dos personas, que se llamará **C** y **M**, si ambas o alguna de ellas conoce la clave que el protocolo establece. Se entiende por seguridad que, si esta información circula por un canal público y es interceptada por un tercero, este no pueda acceder a la misma. Para describir las etapas básicas de un protocolo criptográfico, se comienza suponiendo que **M** quiere enviar información a **C** de forma segura y que la misma está escrita en un texto en idioma español. Al texto original se lo llama texto plano. Para que la transmisión de la información sea segura es necesario encriptar el texto. El primer paso para encriptarlo es transformar al texto plano en una tira de números que sea susceptible de ser manipulada matemáticamente. Este procedimiento se suele llamar codificación y su resultado, texto codificado. Al texto codificado se lo encripta, es decir, se lo modifica de acuerdo con lo estipulado por el protocolo que se esté usando, dando lugar a una nueva tira de números que se llama mensaje. El mensaje es recibido por **C** quien, conociendo el protocolo y las claves necesarias, puede recuperar el texto codificado, decodificarlo y recuperar la información” (Cesaratto & Fuentes, 2015). En la figura 2.5 se ilustra un esquema de comunicaciones utilizando un protocolo criptográfico.

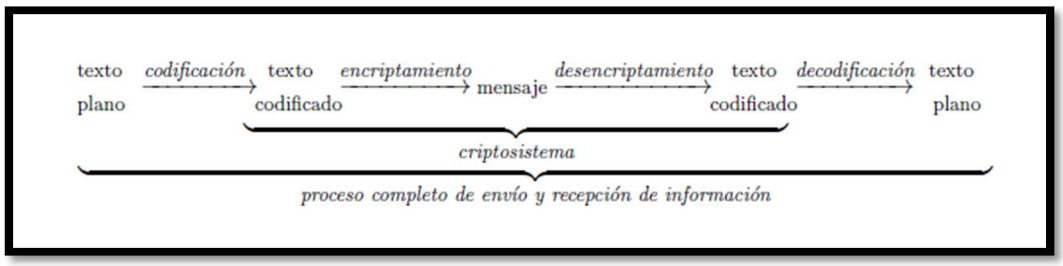


Figura 2. 5: Esquema Protocolo Criptográfico.
Fuente: (Cesaratto & Fuentes, 2015).

Con la descripción de este modelo de comunicaciones, las técnicas de criptografía en la trasmisión de datos tienen múltiples aplicaciones en diferentes campos; los cuales se enuncia a continuación:

- Banca electrónica.

- Internet de las cosas o Internet-of-Things (IoT).
- Ciudades inteligentes (Smart Cities).
- Dispositivos móviles inteligentes (Smartphones).
- Dispositivos de recursos limitados (Sistemas embebidos).
- Gestión Digital de Derechos o Digital Rights Management (DRM).
- Critpomonedas.
- Videojuegos en línea (Wii).
- Voto electrónico.
- Suite documental.

Finalmente, se debe mencionar que las diferentes técnicas de criptografía son aplicables tanto en el Modelo de Interconexión Abierto (Open Systems Interconnection) como en el TCP-IP (Transmission Control Protocol / Internet Protocol) en todas las capas que componen los modelos referidos, a excepción de la Capa Física.

2.5 Cifrado Simétrico.

El cifrado simétrico, según García (2013), define lo siguiente: “En este tipo de criptografía el emisor cifra el mensaje con una clave y el receptor para poder descifrar el mensaje recibido tendrá que usar la misma clave que uso el emisor”’. En la figura 2.6 se ilustra una representación esquemática elemental de un criptosistema simétrico con todos sus componentes. (García, 2013).

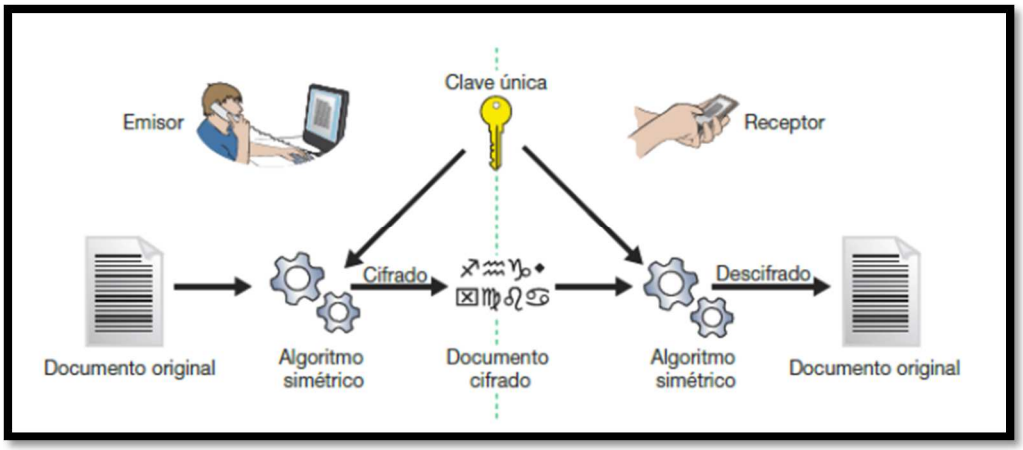


Figura 2. 6: Esquema de un algoritmo simétrico.
Fuente: (Roe Buendia , 2013).

2.5.1 Características del cifrado simétrico.

- Es rápido.
- Es seguro.
- El texto cifrado que resulta de un cifrado es compacto.
- Dado que la clave simétrica debe llegar al receptor, el cifrado simétrico está sujeto a la intercepción.
- La criptografía simétrica requiere una administración compleja de claves.
- No se ajusta a las firmas digitales o a la aceptación (Garcia, 2016).

2.5.2 Algoritmos Simétricos.

Los algoritmos criptográficos construidos bajo el esquema Simétrico son: DES (Data Encryption Standard) con tamaño de clave de 56 bits, Triple-DES con tamaño de clave de 128 bits a 256 bits, IDEA (International Data Encryption Algorithm) con 64 bits, pero utiliza clave de 128 bits y, AES (Advanced Encryption Estándar) con tamaño de clave de 128, 192 o 256 bits. A continuación, se detalla una descripción de cada uno de ellos.

2.5.3 DES y 3DES.

DES es un algoritmo producto de un concurso público citado por NIST (National Institute of Standards and Technology) en el año de 1973, el cual tenía el propósito de seleccionar un algoritmo criptográfico a nivel nacional de forma estandarizada. El algoritmo fue discutido al principio, sobre todo se debatía sus elementos de diseño, la longitud de la clave, y las continuas dudas sobre la existencia de alguna puerta trasera para la NSA (National Security Agency). Subsiguientemente, este algoritmo fue sometido a un amplio debate académico; el resultado de este debate fue el desarrollo de conceptos modernos, tales como el cifrado por bloques y su criptoanálisis. En el año de 1976, se reconoce a este algoritmo, como uno criptográfico estandarizado y, por lo tanto, se autoriza su utilización. En la actualidad, este algoritmo se lo considera inseguro en el uso de algunas aplicaciones, principalmente por el tamaño de la clave de 56 bits; ya que estas claves, han sido ‘’rotas’’ en un tiempo menor a 24 horas.

En el algoritmo simétrico DES el tamaño del bloque está compuesto por 64 bits, el algoritmo emplea además una clave criptográfica para modificar la transformación, de tal forma que el descifrado es posible siempre y cuando se conozca la clave. De los 64 bits que contiene el algoritmo solo son utilizados 56, los 8 bits restantes son empleados para comprobar la paridad, luego de este proceso, estos bits son anulados. Este algoritmo toma el texto del emisor mediante el cifrado por bloques, con una longitud fija, lo transmuta en otro texto cifrado con la misma longitud. La evolución de DES, es 3DES; este algoritmo simétrico se considera más seguro en relación a DES. En la figura 2.7 se muestra un esquema del cifrado utilizando un algoritmo DES, el cual inicia con una permutación inicial, luego 16 vueltas y, finalmente una permutación final, trabaja alternadamente con cada sub-bloque de 32 bits a partir de la entrada de 64 bits.

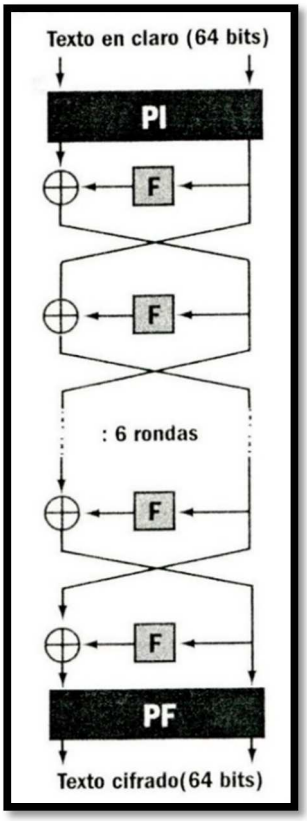


Figura 2. 7: Esquema Cifrado DES.
Fuente: (Pacheco, 2014).

El algoritmo simétrico 3DES, fue desarrollado por IBM en 1998; Pacheco (2014) al respecto afirma: “3DES opera aplicando tres veces el DES. Si bien podría suponerse que aplicándolo dos veces se duplicaría el tamaño de la

clave, esto no es así, sino que solo aumenta en 1 bit su longitud efectiva" (Pacheco, 2014). Según el proceso de implementación, surgen tres variantes de este algoritmo, que se describe a continuación:

- **DES-EEE3:** se cifra tres veces con una clave diferente cada vez.
- **DES-EDE3:** primero se aplica la operación de cifrado, luego se aplica de del descifrado y finalmente la del cifrado otra vez, todas con distintas claves**.**
- **DES-EEE2/DES-EDE2:** similares a las anteriores, pero usando la misma clave en el primero y último paso.

En la figura 2.8 se ilustra el proceso del algoritmo 3DES.

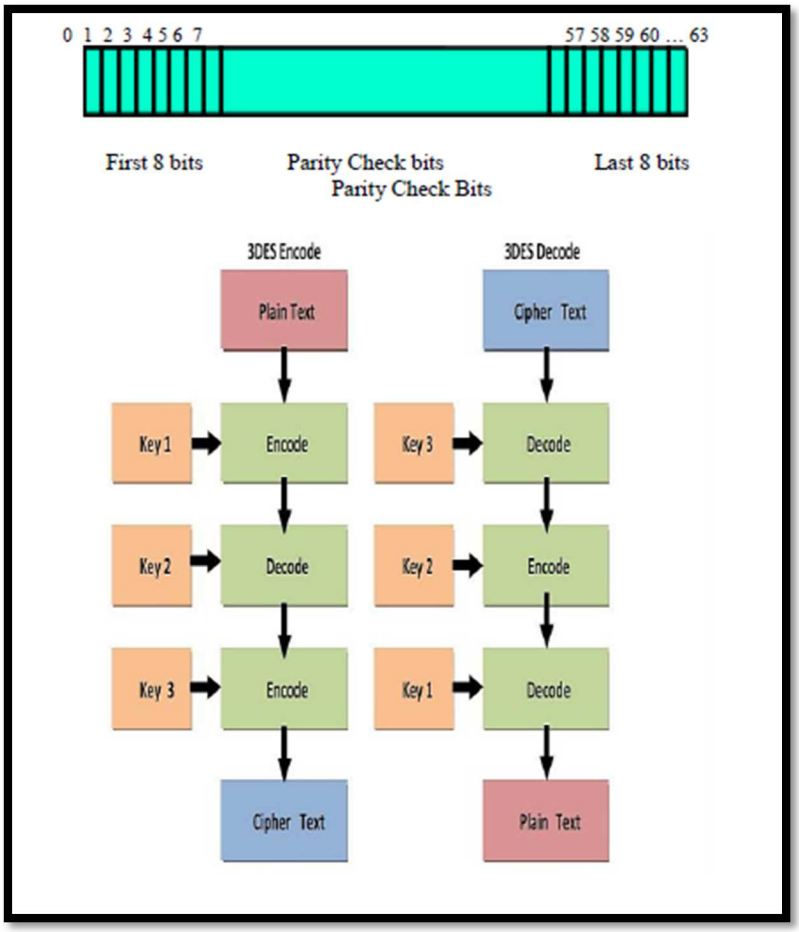


Figura 2. 8: Estructura 3DES.
Fuente: (Joseph , 2015).

2.5.4 IDEA.

IDEA es un algoritmo simétrico, producto de la creación de James Massey y Xuejia en el año 1991, su funcionamiento se basa en bloques compuestos de 64 bits, pero utiliza una clave de 128 bits, lo cual garantiza un espacio

total de posibles combinaciones de claves. La figura 2.9 ilustra un esquema de la implementación del algoritmo IDEA, el cual realiza ocho vueltas, más media vuelta al final del proceso.

El bloque de entrada lo divide en cuatro de 16 bits, de lo cual se genera 5 subclaves de 16 bits, de las cuales utiliza seis por vuelta, en cuanto a los subbloques, estos se procesan con claves implementadas de ocho vueltas, para finalmente aplicar la transformación lineal con cuatro subclaves que se invierten en la operación inicial, de esta forma se obtiene el criptograma de salida.

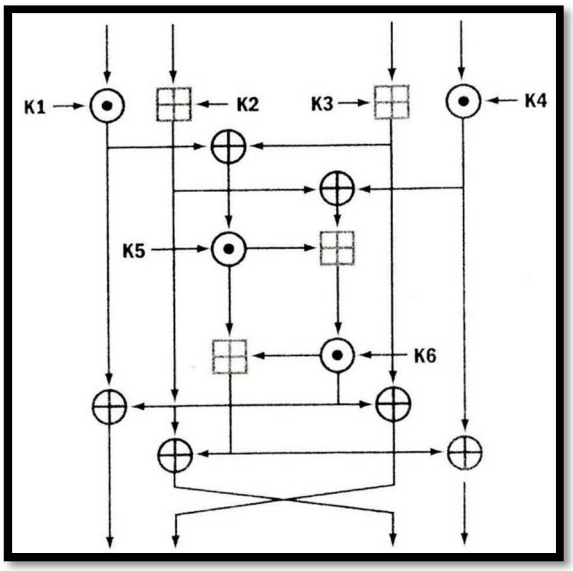


Figura 2. 9: Esquema de una vuelta en IDEA.
Fuente: (Pacheco, 2014).

2.5.5 AES.

AES es un algoritmo simétrico, producto de un concurso impulsado en 1997 por la FIPS (Federal Information Proccessing Standars), desarrollado por los criptologos Joan Daemen y Vincent Rijmen, por esta razón el algoritmo desarrollado se lo conoce también con el nombre de Rijndael. AES, fue reconocido como estándar en el año 2003; por el diseño de este algoritmo, comparativamente no es tan compleja su implementación y es rápido; otra característica es que su proceso de cifrado es diferente al descifrado. Su funcionamiento, básicamente es una matriz de 4 x 4 bytes denominada state, la cual implementa una red de sustitución – permutación (no utiliza red Feistel). AES, cifra y descifra la información dividiendo los datos a procesar en bloques de 128 bits. El algoritmo AES es capaz de cifrar información con

claves de 128, 192 y 256 bits, lo cual lo convierte en un algoritmo fácilmente adaptable a las necesidades de seguridad del sistema donde vaya a ser utilizado. Las funciones internas de este algoritmo son:

- **AddRoundKey:** combina un byte con una clave derivada.
- **SubBytes:** sustitución no lineal.
- **ShiftRows:** transposición por rotación cíclica.
- **MixColumns:** transformación lineal sobre las columnas.
- **SubBytes:** sustitución de bits.
- **ShiftRows**: rotación cíclica de filas.

A continuación, en las figuras 2.10 y 2.11 se ilustran la estructura de AES y sus componentes.

Figura 2. 10: Tres etapas de la implementación AES.
Fuente: (Pacheco, 2014).

2.6 Cifrado Asimétrico.

El cifrado asimétrico fue propuesto en el año de 1976, por Diffie y Hellman (1976); basa sus algoritmos en funciones matemáticas y no con operaciones con patrones de bits, como es el caso del cifrado simétrico. El cifrado asimétrico, conceptualiza el termino de ‘’un solo sentido’’, que significa la

implementación del algoritmo basados en funciones matemáticas simples en un solo sentido, mientras que, en sentido inverso, su resolución es compleja. Navarro define lo siguiente: “La criptografía de clave pública utiliza dos claves: una privada y otra pública. Cada usuario tiene una clave privada que debe mantener en secreto y otra clave pública que debe difundir entre sus receptores. En una comunicación entre dos usuarios, el emisor cifra los datos con la clave pública del receptor, quien a su vez utiliza su clave privada para descifrar el mensaje recibido” (Navarro, 2013)

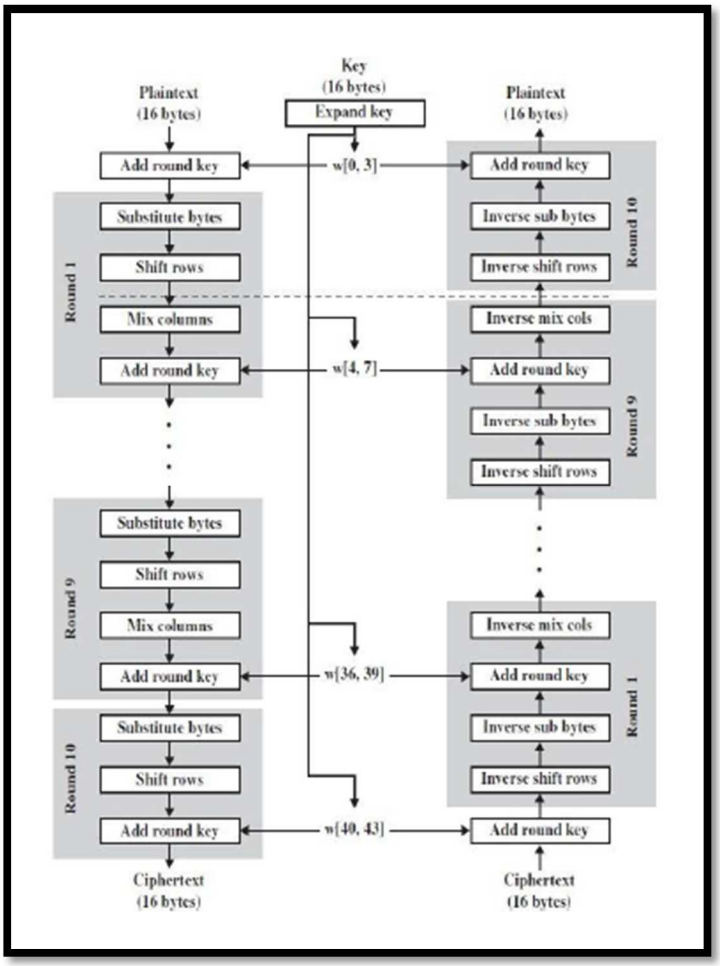


Figura 2. 11: Estructura de AES.
Fuente: (Joseph , 2015).

Paguay (2015) define lo siguiente, en relación a la conceptualización de cifrado asimétrico: “Debido a que en la utilización de cifrados simétricos se presentan dificultades con el intercambio de claves dentro de una comunicación segura entre el remitente y destinatario, se han desarrollado los algoritmos asimétricos, los cuales responden muy bien ante el problema de las claves. Es así que los sistemas de cifrados de clave pública

implementan para su funcionamiento dos claves, una pública que puede ser de conocimiento general, y una clave privada que es conocida solamente por una persona, por lo cual debe ser celosamente guardada" (Paguay, 2015).

A continuación, en las figuras 2.12 y 2.13 se muestra, básicamente dos esquemas elementales acerca del cifrado asimétrico.

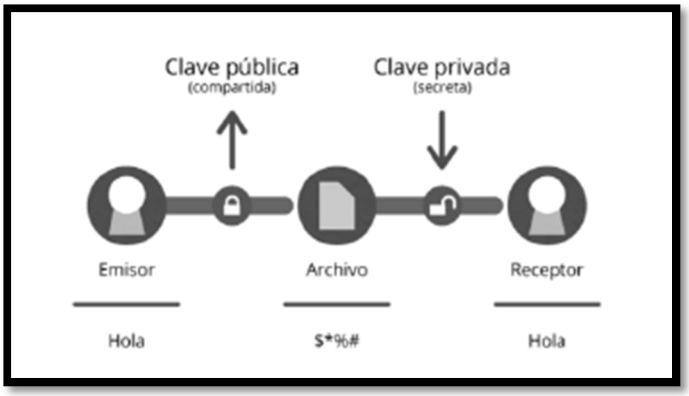


Figura 2. 12: Esquema Básico de cifrado asimétrico.

Fuente: (Méndez Naranjo , 2015).

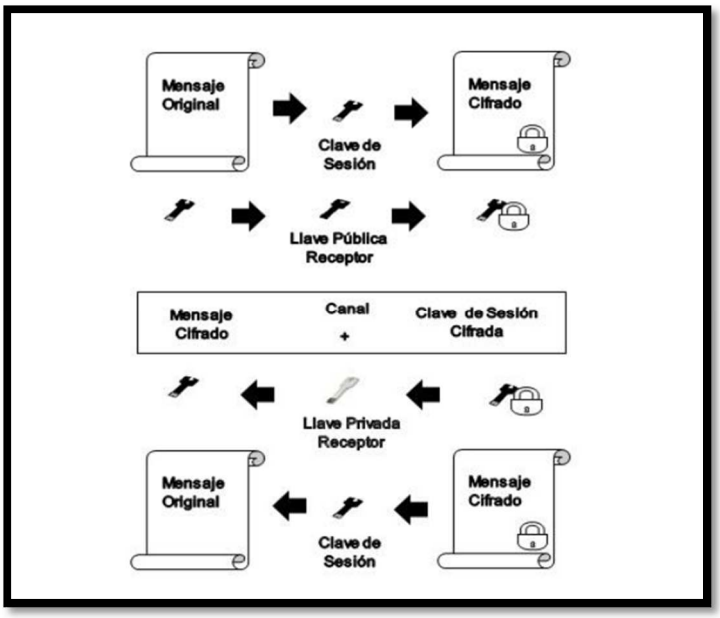


Figura 2. 13: Proceso Criptográfico Asimétrico.

Fuente: (Garcia Belmont , 2016).

2.6.1 Algoritmos asimétricos.

En cuanto a los algoritmos asimétricos Sánchez y González (2016), resumen lo siguiente: "El nacimiento de la criptografía asimétrica llegó a ser la búsqueda de una forma más práctica para el intercambio de claves simétricas, Diffie y Hellman (1976) proponen una manera de hacer esto, sin

embargo, no fue hasta el método popular de Rivest, Shamir y Adleman (RSA), publicado en 1978, cuando se toma la forma de criptografía asimétrica, su funcionamiento se basa en la imposibilidad computacional de factorizar enteros grandes. Actualmente la criptografía asimétrica se utiliza ampliamente, sus dos aplicaciones principales son, precisamente, el intercambio de claves privadas (ANSI X9.42,1995) y la firma digital, la cual se puede definir como una cadena de caracteres en un archivo digital, añadiendo el mismo rol que la firma convencional cuando se escribe en un documento de papel ordinario". (Sánchez & González, 2016).

2.6.2. Factorización de enteros (IF).

Pacheco (2014), define: "la factorización de enteros busca descomponer un número no primo en divisores no triviales, que al multiplicarse resultan el numero original"; en la figura 2.14 se muestra la clasificación global de los números. El teorema fundamental de la aritmética afirma que todo número entero positivo puede descomponerse de una única manera en factores primos. (Pacheco, 2014).

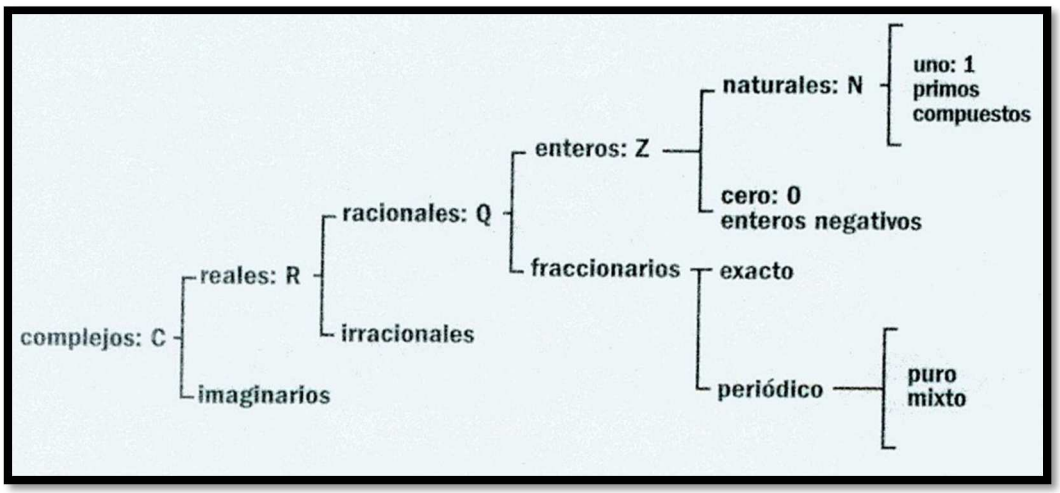


Figura 2. 14: Clasificación global de los números.

Fuente: (Pacheco, 2014).

Brotons Molinero (2016), define**:** "La factorización (IF) de enteros fue presentada en 1978 como método de implementación de la criptografía de clave pública con la introducción del algoritmo RSA. Los algoritmos de factorización de enteros emplean el subgrupo multiplicativo formado por los enteros en Módulo **N**, donde **N** es un entero más grade compuesto por **n**

dígitos formado por el producto de dos números aleatorios **p** y **q** de tamaño **n/2**'' (Brotons, 2016).

2.6.3. Logaritmos discretos (Discrete Logarithm).

Un numero con un exponente elevado a una base, se lo conoce como un logaritmo y, su operación inversa se la denomina exponenciación; este mismo principio del logaritmo es utilizado en criptografía, ya que computacionalmente toma mucho tiempo calcular el logaritmo. Según Pacheco, en relación al logaritmo discreto define: "Algunos algoritmos más sofisticados corren en tiempo lineal a la raíz cuadrada del tamaño del grupo, por ende, exponencial a la mitad de los dígitos del tamaño, pero ninguno corre en tiempo polinomial (en el número de dígitos en el tamaño del grupo)" (Pacheco, 2014).

En la figura 2.15, se muestra un esquema de un sistema de cifrado asimétrico, en el cual se emplean claves para intercambiar de forma segura a partir de parámetros públicos.

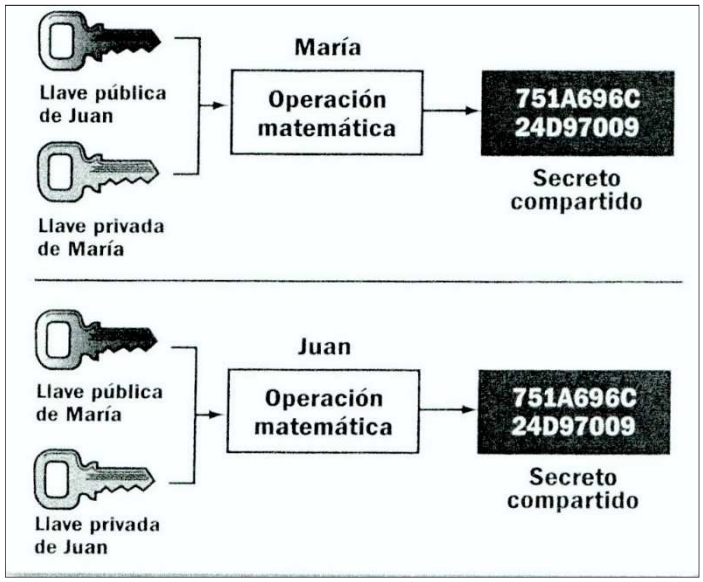


Figura 2. 15: Esquema Cifrado Asimétrico.

Fuente: (Pacheco, 2014).

2.6.4. Diffie Hellman (D-H).

Este algoritmo asimétrico fue desarrollado por los criptógrafos Whitfield Diffie y Martin Hellman en 1976, y su funcionamiento está basado en un protocolo de intercambio de claves. Zapata Valdez (2014) afirma: "En 1976, Whitfield

Diffie y Martin Hellman, presentaron una manera de resolver las necesidades de seguridad de aquel momento a través del concepto de criptografía de clave pública. La propuesta se conoció como Protocolo de establecimiento o acuerdo de clave Diffie-Hellman, consiste en un mecanismo por el que dos entidades intercambian pequeñas cantidades de información a través de un canal inseguro, de modo que al terminar el proceso únicamente ellos conozcan la clave secreta compartida. El protocolo de acuerdo de clave Diffie-Hellman originalmente no fue planteado como un criptosistema, ya que no realiza el cifrado y descifrado de información, sino que sólo permite el intercambio de información con el objetivo de conseguir una clave secreta". (Zapata, 2014).

En la figura 2.16 se muestra un esquema práctico del cifrado asimétrico Diffie Hellman.

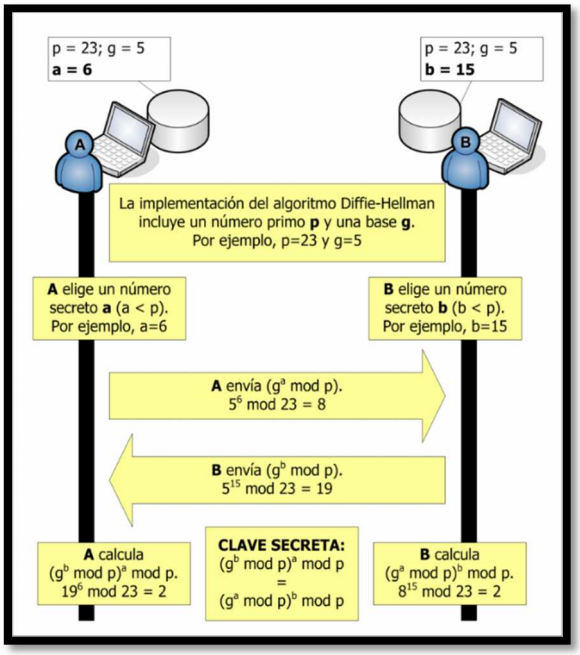


Figura 2. 16: Cifrado Asimétrico Diffie Hellman.

Fuente: (Javier Campos Blog , 2011).

2.6.5. RSA.

Este cifrado asimétrico desarrollado en 1977 por los criptógrafos del Massachusetts Institute of Technology (MIT - Instituto Tecnológico de Massachusetts): Ron Rivest, Adi Shamir y, Leonard Adleman, por esta razón se lo denomina RSA (iniciales de sus apellidos). Este cifrado fue la primera materialización del algoritmo Diffie y Hellman para criptografía de clave

pública. Este algoritmo, es el más reconocido dentro de los cifrados que tiene como principio la factorización de números enteros; su fortificación, se halla en la dificultad matemática de factorizar números grandes; por lo tanto, RSA, ofrece seguridad en su cifrado dependiendo de la dificultad matemática relacionada a la factorización de números enteros grandes.

En la figura 2.17 se muestra un esquema del cifrado utilizando el algoritmo RSA.

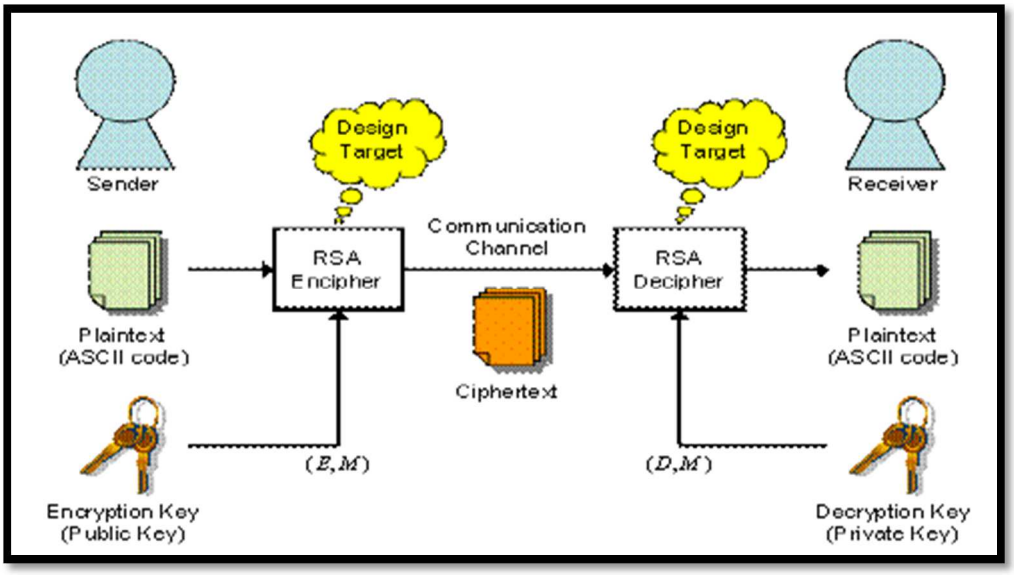


Figura 2. 17: Esquema RSA.

Fuente: (Joseph , 2015).

2.6.6. El Gamal.

El criptógrafo egipcio Taher Elgamal, en 1985 publicó su artículo: “A public key cryptosystem and a signature scheme based on discrete Logarithms”, en dicha publicación su autor propone un sistema de criptografía de clave pública basado en el problema del logaritmo discreto (PLD); este sistema ha demostrado ser flexible y muchos de los sistemas actuales de criptografía están basados en este algoritmo, por ejemplo, las firmas digitales. La seguridad que ofrece este método avala en la dificultad de resolver el problema del algoritmo discreto.

Navarro (2013) define: “El conocido protocolo El Gamal y todas sus numerosas variantes basan su fortaleza en el problema DLP (Discrete Logarithm Problem). Fue descrito y desarrollado por Taher EL Gamal en 1984 y siempre ha sido de uso libre. La seguridad del mismo radica en la

dificultad que ofrece el cálculo del logaritmo discreto en grupos cíclicos de tamaño muy grande. Tanto los esquemas RSA como El Gamal se basan en la resolución de ecuaciones exponenciales en aritmética modular. Sim embargo, en EL Gamal, el secreto está incrustado en el exponente, mientras que la base y el resultado son conocidos. En el esquema RSA, el exponente es público y es la base la que constituye el objetivo del atacante, lo que representa la gran diferencia entre ambos protocolos". (Navarro, 2013).

2.6.7. Curvas Elípticas.

La asociación del concepto de curvas elípticas con la criptografía inicia con la publicación de dos trabajos: Use of elliptic curves in cryptography, Math. Comp. De V. Miller en 1985 y Elliptic Curve Cryptography, Math. Comp., en 1987. En ambos casos, los dos autores proponen implementar el Problema del Algoritmo Discreto (PLD Discrete Logarithm Problem), en el grupo de puntos de una curva elíptica definida sobe un cuerpo finito, en lugar de un grupo multiplicativo, la motivación de esta asociación es por la razón que el grupo de puntos de una curva elíptica resulta inmune ante ataques criptoanaliticos, por citar un ejemplo el Index-Calculus, el cual permite una seguridad equivalente con longitudes de clave mucho menor.

Según Miret y Valera (2015) afirman: "En las últimas décadas, la criptografía con curvas elípticas ha adquirido una creciente importancia, llegando a formar parte de los estándares industriales. Su principal logro se ha conseguido en los criptosistemas basados en el problema del logaritmo discreto, como los de tipo El Gamal. Estos criptosistemas planteados en el grupo de puntos de una curva elíptica garantizan la misma seguridad que los construidos sobre el grupo multiplicativo de un cuerpo finito, pero con longitudes de clave mucho menores. La criptografía con curvas elípticas aparece como una alternativa a los criptosistemas de clave pública clásicos como el RSA y El Gamal, tanto por la disminución del tamaño de las claves que se requieren como por el abanico de grupos que ofrecen en el mismo cuerpo base. Su implantación en algunos sistemas de comunicaciones es un hecho constatable y su uso aumenta día a día debido a sus ventajas. Por ejemplo, se usa en tarjetas inteligentes, sistemas de identificación por radio frecuencia, sistemas de votación electrónica, etc." (Miret & Valera, 2015).

En el Capítulo 3, se hace un análisis más detallado en relación con la criptografía empleando las curvas elípticas.

2.7. Algoritmo de Firma Digital (DSA - Digital Signature Algorithm).

La criptografía de cifrado asimétrico, tiene dos aplicaciones fundamentales que son:

- el intercambio de claves privadas.
- firma digital.

En SSL247 se afirma lo siguiente: “El algoritmo de firma digital DSA (Digital Signature Algorithm), lo propuso el National Institute of Standards and Technology (NIST) en 1991 y fue adoptado por los estándares FIPS (Federal Information Processing Standards) en 1993, este algoritmo sirve para firmar y no para cifrar información. Desde entonces se ha revisado cuatro veces” (SSL247, s.f.).

En GNUPG se describe lo siguiente: “Una firma digital en un documento es el resultado de aplicar una función `hash' al mismo. Para que ésta sea de utilidad, necesita satisfacer dos propiedades importantes. Primero, debería ser difícil encontrar dos documentos cuyo valor para una función `hash' sea el mismo. Segundo, dado un valor `hash' debería ser difícil de recuperar el documento que produjo ese valor. Algunos sistemas de cifrado de clave pública se pueden usar para firmar documentos. La firmante cifra el documento con su clave privada. Cualquiera que quiera comprobar la firma y ver el documento, no tiene más que usar la clave pública del firmante para descifrarla. Este algoritmo satisface las dos propiedades necesarias para una buena función de `hash', pero en la práctica este algoritmo es demasiado lento para que sea de utilidad. Como alternativa está el uso de funciones `hash' designadas para satisfacer estas dos importantes propiedades. SHA y MD5 son dos ejemplos de este tipo de algoritmos. Al usar uno de ellos, un documento se firma con una función `hash', y el valor del `hash' es la firma. Otra persona puede comprobar la firma aplicando también una función `hash' a su copia del documento y comparando el valor `hash' resultante con el del documento original. Si concuerdan, es casi seguro que los documentos son idénticos”. (GNUPG, s.f.)

En la figura 2.18 se muestra un esquema de firma digital y la comprobación de la firma.

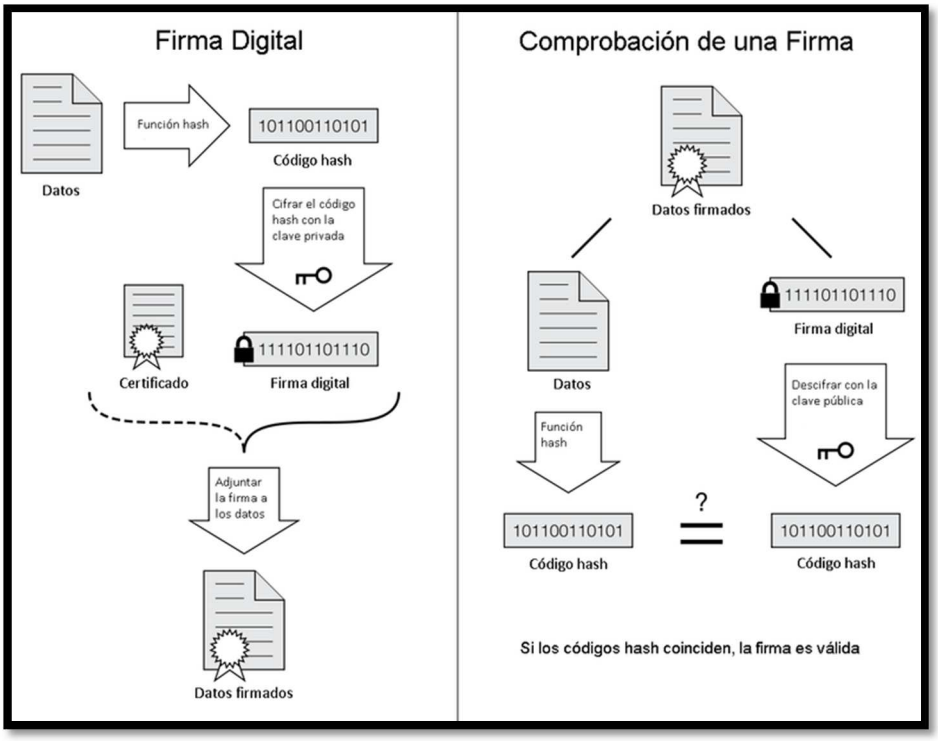


Figura 2. 18: Firma Digital.
Fuente: (FirmaDigitalUAP, 2010).

2.8. Diferencia entre cifrado simétrico y asimétrico.

Con conocimiento tanto del cifrado simétrico como del asimétrico, se determina a continuación las diferencias entre ambos cifrados, los cuales se expone a continuación:

- **Cifrado Simétrico.** Según Ubiquitour (2015)**: "**En el cifrado simétrico, también conocido como compartida cifrado, el remitente y el destinatario de una parte de mensaje una contraseña común, pasar frase o clave. En otras palabras, los datos se codifican y descifran utilizando la misma clave. Algoritmos de cifrado simétrico son más simples, más rápidos y requieren menos recursos de la computadora, tales como el procesamiento de energía y memoria, que los algoritmos de cifrado asimétrico. Sin embargo, no se pueden usar a menos que el remitente y el destinatario ya han intercambiado claves de cifrado." (Ubiquitour, 2015).

- **Cifrado Asimétrico.** Según Ubiquitour (2015): **"**En el cifrado asimétrico, también conocido como una encriptación pública/privada, dos relacionados con teclas, conocidas como claves públicas y privadas, se utilizan para cifrar y descifrar datos. La clave pública se distribuye libremente a cualquier persona que quiera enviar un mensaje, pero la clave privada se mantiene en secreto y nunca distribuidos. Algoritmos de cifrado asimétricos son más complejos y más lentos, de hecho, hasta 1.000 veces más lentos, que los algoritmos de cifrado simétrico, pero significativamente más seguros". (Ubiquitour, 2015).

En la Tabla 2.1 se resume la diferencia entre el cifrado Simétrico y el Asimétrico.

Tabla 2. 1: Diferencia Cifrado simétrico y asimétrico.

CARACTERÍSTICA	CIFRADO	
	SIMETRICO	ASIMETRICO
CONFIDENCIALIDAD	SI	SI
AUTENTIFICACIÓN	PARCIAL	COMPLETA
FIRMA DIGITAL	NO	SI
LONGÍTUD DE CLAVE	PEQUEÑA	GRANDE
VIDA DE CLAVE	CORTA (SESIÓN)	LARGA
CANTIDAD DE CLAVES	n(n-1)/2	n*2
VELOCIDAD	ALTA	BAJA
APLICACIONES	CIFRADO DE MUCHA INFORMACIÓN	FIRMA E INTERCAMBIO DE CLAVES

Fuente: (Pacheco, 2014).

2.9. Ataques Criptoanalíticos.

Como se expuso anteriormente, el criptoanálisis es una ciencia, la cual, por medio de diferentes métodos, tiene como objetivo descifrar los mensajes en clave, de tal forma que pueda vulnerar un sistema criptográfico; para llevar a cabo este objetivo, el criptoanálisis primero encuentra las debilidades de los sistemas criptográficos y, en base a las debilidades encontradas, se diseña un ataque que permita romper la seguridad del sistema criptográfico; a todo este proceso, se denomina *ataques criptoanalíticos*. Cabe mencionar, que no todos los ataques criptoanalíticos, tienen como objetivo vulnerar el

sistema criptográfico, sino recabar información acerca del sistema que permita ir atenuando el sistema criptográfico.

La clasificación de los ataques de criptoanálisis es amplia, según el tipo de ataque; los cuales se describe a continuación: por la actitud del atacante, por el conocimiento previo, por el objetivo en criptoanálisis, por el tipo de criptografía y, por el coste. Por la amplitud y, extensión de este tema, el presente trabajo se limita en describir únicamente los ataques por el tipo de criptografía.

2.9.1. Criptoanálisis de Sistemas Simétricos.

Como se describió en párrafos anteriores del presente trabajo, la Criptografía Simétrica, son algoritmos basados en una función invertible, es decir, que tanto su cifrado como descifrado son invertibles con la utilización de una llave secreta; por ende, existen criptoanálisis para los cifrados simétricos que tienen como fin desarrollar técnicas para descifrar estos algoritmos. A continuación, se exponen los dos tipos de criptoanálisis para algoritmos simétricos.

2.9.1.1. Criptoanálisis lineal.

El Criptoanálisis lineal es una técnica de tipo estadístico, es decir, realiza suposiciones sobre la distribución del texto cifrado (monogramas, diagramas, trigramas, etc.) Esta técnica, se aplica a los algoritmos criptográficos tipo DES. Su implementación, está basada en realizar operaciones binarias OR EXCLUSIVO. Sanchez Acosta define lo siguiente: “perar o-exclusivo dos bits del texto en claro, hacer lo mismo con otros dos del texto cifrado y volver a operar o-exclusivo los dos bits obtenidos. Se obtiene un bit que es el resultado de componer con la misma operación dos bits de la clave. Si se usan textos en claro recopilados y los correspondientes textos cifrados, se pueden conjeturar los bits de la clave. Cuantos más datos se tengan más fiable será el resultado”. (Sánchez Acosta).

2.9.1.2. Criptoanálisis diferencial.

Esta técnica es similar a la técnica de tipo lineal, en el sentido que también es de tipo estadístico y se aplica a algoritmos criptográficos tipo DES.

Sanchez Acosta, define lo siguiente: “técnica en cifrar parejas de texto en claro escogidas con la condición de que su producto o-exclusivo obedezca a un patrón definido previamente. Los patrones de los correspondientes textos cifrados suministran información con la que conjeturar la clave criptográfica’’. (Sánchez Acosta).

2.9.2. Criptoanálisis de Sistemas Asimétricos.

Partiendo del concepto de criptografía asimétrica; en la cual, la característica más relevante es el empleo de dos claves (o llaves): una publica y una privada. Por ende, los criptoanálisis para sistemas asimétricos se benefician del conocimiento de la llave pública; por lo tanto, los métodos de criptoanálisis asimétrico se enfocan en el desarrollo matemático de la llave privada. A continuación, se detalla los métodos sobre los cuales están basados estos criptoanálisis:

2.9.2.1. Factorización.

Los métodos de criptoanálisis desarrollados para criptografía asimétrica por factorización son: Trial Division, Pollard’s rho, Polllard’s p-1, Lenstra’s Elliptic Curve Method, Factorización por diferencia de cuadrados, Quadratic Sieve y, Number Field Sieve.

2.9.2.2. Cálculo del Logaritmo Discreto.

Al igual que en el caso de Factorización, existen otros métodos implementados para criptoanálisis de sistemas criptográficos asimétricos que están basados en el Cálculo del Logaritmo Discreto, los cuales se detallan a continuación: Fuerza Bruta, Algoritmo Shanks, Algoritmo Pohlig-Hellman, Pollard’s rho y, Index Calculus.

2.9.2.3. Ataques de Canal Lateral.

Lumbiarres-López, López Garcia, & Cantó-Navarro hacen referencia en relación a los ataques de Canal Lareal lo siguiente: “A finales de la década de los 90, Paul C. Kocher, Joshua Jaffe y Benjamin Jun publican un artículo que describe cómo obtener la clave de un algoritmo criptográfico analizando el consumo de corriente del dispositivo hardware que lo implementa. La información de la

clave, que se filtra a través de este consumo, se utiliza para realizar los denominados ataques por canal lateral (Side Channel Attacks). Estos ataques, además de ser conceptualmente muy sencillos, necesitan de equipos de captura y procesado relativamente baratos. Si bien los autores demostraron su teoría aplicándola sobre el algoritmo de encriptado DES (Data Encryption Standard), en la actualidad el mismo procedimiento se ha aplicado con éxito sobre otros algoritmos criptográficos de clave privada. Sin embargo, y probablemente debido a su elevada seguridad, la mayoría de los artículos se han centrado en el algoritmo de cifrado por bloques AES (Advanced Encryption Standard) adopción como estándar por parte del NIST, este algoritmo ha experimentado una creciente popularidad, siendo utilizado como base para el encriptado de documentos oficiales tanto por parte de la National Security Agency (NSA) como por el propio gobierno de los EUA.'' (Lumbiarres-López, López Garcia, & Cantó-Navarro).

2.9.3. Cifrado y Criptoanálisis Cuánticos.

Los matemáticos Deutsh y Feymann, en la época de los ochenta, proponen el modelo de la computación cuántica, como una alternativa de herramienta de cálculo; esta alternativa, tiene como unidad elemental el qubit o también denominado bit cuántico, el cual se define como el estado básico representado entre 0> y 1>. Dicho de otra forma, un sistema cuántico de dos estados del spin de un electrón. Este sistema cuántico, se representa el spin -1/2 por el estado |0> y el spin ½ por el estado |1>. Sin embargo, el estado cuántico puede ser una trasposición de los dos estados básicos. Esta última característica, es la que difiere de la computación clásica.

En la actualidad, son los canales de comunicación empleados en computación cuántica esta implementada mediante la polarización de un fotón, empleando este estado físico como un estado cuántico.

Entre los logros de la computación cuántica, son los algoritmos polimoniales para la factorización de los números enteros y, el cálculo de logaritmos discretos, modelo propuesto por P. Shor, este trabajo, permitió que los computadores cuánticos puedan descifrar criptosistemas de clave pública.

Un criterio comparativo en relación a la criptografía aplicada con ordenadores convencionales y, cuánticos, según Cordova & Méndez-Garabetti, según: "La criptografía es la base de cualquier mecanismo de

seguridad informática. Se utiliza habitualmente en un login web, en el envío de correos electrónicos, o incluso cuando se produce la sincronización de archivos en la nube, entre otros. Todos los protocolos de comunicación que utilizan SSL/TLS en TCP/IP hacen uso de criptografía asimétrica para autenticación y firma digital. Estos algoritmos se basan en complejos cálculos matemáticos de una sola vía, es decir, son fáciles de realizar, pero muy difíciles de revertir. Si bien los ordenadores actuales no son capaces de romper estos algoritmos en periodos de tiempo aceptables, las computadoras cuánticas, hoy en sus albores de desarrollo, sí podrán hacerlo fácilmente. Es aquí donde surge la necesidad de algoritmos de cifrado que sean resistentes a ataques cuánticos. Estos algoritmos, denominados post cuánticos, si bien están en sus primeras etapas de investigación, resultarán de suma utilidad en un futuro cercano, en el que las técnicas de cifrado asimétrico actuales no puedan brindar la privacidad, autenticación e integridad de los datos en Internet. El algoritmo de Shor fue el primer algoritmo cuántico no trivial que demostró un potencial de crecimiento exponencial de velocidad sobre los algoritmos clásicos. Es un algoritmo cuántico para descomponer en factores un número N en un tiempo O ((log N)^3), y debe su nombre al profesor de matemáticas aplicadas del MIT Peter Shor. Por otro lado, el algoritmo de Shor, como todos los algoritmos de computación cuántica, da su resultado en forma probabilística con un determinado grado de acierto, por lo que se requieren ejecuciones sucesivas del mismo para aumentar el porcentaje de exactitud del resultado. En la actualidad casi la totalidad del tráfico web en Internet corre sobre SSL/TLS. El intercambio de datos de autenticación o números de tarjetas de crédito suelen protegerse mediante HTTPS. Debido a esto, surgió la necesidad de comenzar a pensar e implementar algoritmos post cuánticos para proteger este tipo de tráfico en Internet. Con el fin de nuclear el desarrollo de implementaciones prototípicas de algoritmos criptográficos post cuánticos, vio la luz el proyecto Open Quantum Safe (OQS)” (Cordova & Méndez-Garabetti, 2017).

A continuación, se exponen algunos protocolos basados en Criptografía Cuántica:

- Criptografía basada en hash (hash-based).
- Criptografía basada en código (code-based).
- Criptografía basada en sistemas de ecuaciones multi variable.
- Criptografía basada en enrejado (lattice based).
- Cifrado simétrico basado en clave secreta de Rijndael.
- Protocolo BB84. Basado en 4 estados cuánticos.
- Protocolo B92. Basado en 2 estados cuánticos no ortogonales.
- Estados trampa.
- Protocolo SARG04
- Protocolo E91. Basado en pares entrelazados
- Corrección de errores. Cascade.
- Corrección de errores. Búsqueda binaria
- Amplificación de la privacidad.
- Intercambio a 3 bandas.
- Proceso de certificación utilizando un sistema QKD.

Capítulo 3: Modelamiento de Algoritmos Criptográficos utilizando Curvas Elípticas.

3.1. Fundamentos de Campos Finitos y, Curvas Elípticas.

Para profundizar el estudio de los algoritmos criptográficos basados en curvas elípticas, se debe abordar determinados fundamentos de Algebra Abstracta; principalmente, conceptos teóricos relacionados a los Campos Finitos y Curvas Elípticas. En el presente Capítulo, se detalla los conceptos más relevantes y necesarios para el modelamiento de algoritmos criptográficos empleando curvas elípticas.

3.1.1. Conceptos básicos de Campos Finitos.

Los campos finitos, también conocidos como campos de Galois (Galois Field), en honor al matemático francés Évariste Galois, desde el principio de su aparición, este concepto teórico, ha sido fuente de constantes investigaciones para fines prácticos, sobre todo en el desarrollo de aplicaciones basadas en algoritmos para Criptografía; a continuación, el detalle de los conceptos de: Grupo, Anillo y, Campo en referencia a los campos finitos.

3.1.1.1. Grupo.

Sobre un plano proyectivo, Hernández define lo siguiente: ‘’Un grupo ***G***, es un conjunto elementos con una operación binaria que asocia a cada par ordenado (a,b) de elementos en ***G*** un elemento (a,b) ‘’ (Hernández G. , 2010) . Un grupo debe cumplir las siguientes cuatro propiedades:

1. **Asociativa.**

   $a.(b.c) = (a.b).c$ Para toda, a,b,c *en* ***G****.*

2. **Elemento de Identidad.**

   Existe un elemento e en ***G***, tal que $a.e = e.a = a$ para toda ***a*** en ***G***.

3. **Cerradura.**

   Si ***a*** y ***b*** pertenecen a ***G***, entonces $a.b$ también se encuentra en ***G.***

4. **Elemento Inverso.**

Para cada ***a*** en ***G***, existe un elemento a' en ***G*** tal que: $a \cdot a' = a' \cdot a = e$

3.1.1.2. Anillo.

Un anillo ***A*** es un conjunto de elementos $\{a, b, c\}$ con dos operaciones binarias, llamadas adición y, multiplicación, de tal forma que para todas $\{a, b, c\} \in A$. Un anillo debe cumplir las siguientes cuatro propiedades:

1. ***A* es un grupo abeliano.**

   En el caso de un grupo aditivo, el elemento identidad es **0** y la inversa de ***a*** es ***–a.***

2. **Ley distributiva.**

   $a(b + c) = ab + ac$ para toda $a, b, c \in A$ y, $(a + b)c = ac + bc$ para toda $a, b, c \in A$

3. **Ley Asociativa para la multiplicación.**

   $a(bc) = (ab)c$ para toda $a, b, c \in A$

Cerradura bajo multiplicación.

Si ***a*** y ***b*** pertenecen a ***A***, entonces ab también están en ***A***.

3.1.1.3. Campo.

Hernández define lo siguiente: ‘’Un campo ***F*** es un anillo conmutativo con elemento unidad en el que todo elemento distinto de cero tiene inverso multiplicativo. A veces denotado como $\{F\}$ el conjunto de elementos con dos operaciones binarias, llamadas adición y multiplicación, de tal forma para todas $a, b, c \in F$ los siguientes axiomas se cumplen’’: (Hernández G. , 2010).

3.1.1.4. Características de un campo.

“Sea Z_m al anillo de clases residuales módulo el número entero ***m***, en efecto para

$$m = 3, Z_3 = \{0,1,2\}$$

todo número natural tiene como representación en $\mathbb{Z}_3$ su resto al dividirlo por 3 como elemento representativo del anillo. El siguiente teorema establece cuando el anillo de clases residuales es un campo, siendo este un importante resultado en la teoría de números". (Martínez Rodríguez & Borges Trenard).

Teorema 3.1

$\mathbb{Z}_m$es un campo si, y solo si, ***m*** es un numero primo.

''Los campos $\mathbb{Z}_p$ (tan poco parecidos al campo de los números racionales) han ido ocupando, por su valor practico, un lugar cada vez más relevante; en particular, en los procesos de codificación y descodificación de la información''. (Martínez Rodríguez & Borges Trenard).

Del teorema 3.1, se origina la siguiente definición: ''Un campo que no tiene ningún subcampo propio se denomina primo'' (Martínez Rodríguez & Borges Trenard).

Teorema 3.2.

Cada campo ***K*** contiene un, y solo un, campo primo. Este campo primo es isomorfo a $\mathbb{Q}$, o bien, a $\mathbb{Z}_p$, para algún ***p.***

Nota:

La estructura de un campo tiene un morfismo, los cuales pueden ser:

- **Monoformismo**: cuando el campo tiene propiedad inyectiva.
- **Epimorfismo:** cuando el campo tiene propiedad sobreyectiva.
- **Isomorfismo**: cuando el campo tiene propiedad inyectiva.
- **Endomorfismo**: cuando el campo es un morfismo del grupo en sí mismo.
- **Automorfismo**: cuando el campo es un isomorfismo del grupo en sí mismo.

Del Teorema 3.2, da origen a las siguientes definiciones:

Definición 3.1. ''Se dice que el campo ***K*** tiene características cero, si su campo primo es isomorfo a $\mathbb{Q}$, o bien, a $\mathbb{Z}_p$, para algún ***p.''*** (Martínez Rodríguez & Borges Trenard)***.***

Definición 3.2. ‘’Un campo ***K*** es finito si contiene un numero finito de elementos. El orden de ***K*** es el número de elementos de este campo”. (Martínez Rodríguez & Borges Trenard).

3.2. Campos Finitos.

La existencia y, unicidad de los campos finitos, son isomorfos; basado en las siguientes definiciones 3.3 y, 3.4 de Martínez y Borges.

Definición 3.3.

‘’Sea ***K*** un campo finito. Entonces, existen números enteros positivos ***p*** y ***m***, donde ***p*** es primo, tales que el orden de ***K*** es igual a p^m”. (Martínez Rodríguez & Borges Trenard).

Definición 3.4.

‘’Recíprocamente, para todo número de la forma p^m, donde m y p son enteros positivos y p es primo, existe un único campo finito (hasta el isomorfismo) de orden p^m. Este campo se denomina por Fp^m (también GF(p^m))’’. (Martínez Rodríguez & Borges Trenard).

Para el entendimiento teórico acerca de las curvas elípticas, se debe considerar tres conceptos importantes de: grupo abeliano, Teorema de Bezout y, el Teorema de Unidades de Hasse.

3.2.1. Grupo Abeliano

En Algebra Abstracta, un Grupo es abeliano cuando cumple con la propiedad Conmutativa para todo elemento ***a*** y ***b***, es decir: $a.b = b.a$.

Teorema 3.3. Teorema de Bezout.

“Sean dos polinomios $P, Q \in \mathbb{Z}[x]$ y $d \in m.c.d(P, Q)$ entonces, existe otros dos polinomios $u, v \in \mathbb{Z}[x]$ de modo que:” (Departamento de Análisis Matemático, Facultad de Matemáticas de la universidad Complutense de Madrid). Ver Ecuación Nro. 3.1.

$$d(x) = u(x)P(x) + v(x)Q(x) \qquad \textbf{(3.1)}$$

La ecuación 3.1 prueba, que el máximo común divisor de dos polinomios no es vacío.

Teorema 3.4. Teorema de las Unidades de Hasse.

"Sea ***K*** un cuerpo numérico y ***E*** un conjunto de primos de ***K*** que contenga a todos los primos arquimedianos. Entonces el grupo $\overset{k}{e}$ es un grupo abeliano finitamente generado cuya parte de torsión es el grupo (finito) de las raíces de la unidad contenidas en ***K*** y cuya parte libre tiene rango ***s-1***, donde ***s***, es el número de elementos de ***E***". (Ivorra).

3.3. Curvas Elípticas.

Como toda ciencia y tecnología ha tenido sus inconvenientes en su desarrollo; la Criptografía no ha sido exenta de este escenario; y uno de estos inconvenientes es la distribución de la clave compartida, en el caso de los algoritmos asimétricos. Es decir, los usuarios que emplean de alguna forma, los diferentes métodos criptográficos para asegurar su información deben de alguna forma establecer previamente la clave compartida para cifrar la información.

El trabajo de Diffie y Hellman, proponen para excluir este inconveniente, realizando un intercambio seguro de las claves, este concepto originó la criptografía de clave pública. Miret Biosca, afirma lo siguiente: "La seguridad de un criptosistema de clave pública reside entonces en problemas matemáticos subyacentes que se conjeturan computacionalmente difíciles, es decir problemas para los que no se conocen algoritmos eficientes para resolverlos" (Miret Biosca).

Con el surgimiento de este concepto de clave pública, se originaron otros criptosistemas, entre los cuales se destaca: RSA, basado en el problema de factorización de enteros, y el ElGamal, basado en el problema del logaritmo discreto sobre el grupo multiplicativo de un cuerpo finito. Según Miret Biosca, afirma: ''la eficiencia de nuevos algoritmos de factorización, como en el criptoanálisis del problema del logaritmo discreto han provocado la necesidad de aumentar el tamaño de las claves". (Miret Biosca).

Aparece como solución a esta necesidad, los criptosistemas basados en curvas elípticas, por la ventaja de la disminución del tamaño de las claves, y conservando la seguridad computacional. Esta ventaja, ha sido ventajosa para el desarrollo de sistemas de telecomunicaciones y, de tarjetas inteligentes. A continuación, se expone el desarrollo teórico relacionado con las curvas elípticas en Criptografía.

Definición 3.5

Una curva elíptica ***E*** que está definida sobre un cuerpo ***k,*** es una curva proyectiva, de tipo no singular, admitiendo una ecuación, definida sobre ***k***, en la denominada *Forma Normal de Weierstrass,* que cumple con la siguiente condición: ***k*** (números complejos C, reales R, un cuerpo finito F_q) bien dada por: Ver Ecuación Nro.3.2

$$E: y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 a, ai \in k \qquad \textbf{(3.2)}$$

Una curva que admite un único punto en el infinito, con las siguientes condiciones, siempre y cuando:

- 1.- $0 = (0:1:0)$
- 2.- Punto del infinito en la direccion del eje *y* .

Si $Car(k) \neq 2,3$

La Forma Normal de Weiertrass se reduce a la ecuacion mas simple; ver Ecuación Nro. 3.3:

$$E: y^2 = x^3 + Ax + B, A, B \in k \qquad \textbf{(3.3)}$$

La grafica rusultante de esta curva de la Forma Normal de Weirtrass para el cuerpo ***R*** de los numeros reales, puede adoptar una de las siguientes formas. Ver figuras 3.1 y 3.2.

Se mostrará con ***E(k)*** al conjunto de puntos de la curva ***E*** con coordenadas en el cuerpo ***k,*** comprendido el punto en el infinito 0. Una de las utilidades de la criptografía de las curvas elípticas procede con la posibilidad de conferir a ***E(k)*** de una estructura de un conjunto de grupo abeliano, teniendo 0 como un elemento neutro. La ley de grupo puede definirse geométricamente descrita con la Ecuación Nro. 3.6:

$$Car(k) \neq 2,3 \text{ y } E: y^2 = x^3 + Ax + B \qquad \textbf{(3.6)}$$

Considerando el *Teorema de Bezout*, una recta ***L*** corta a ***E*** en tres puntos.

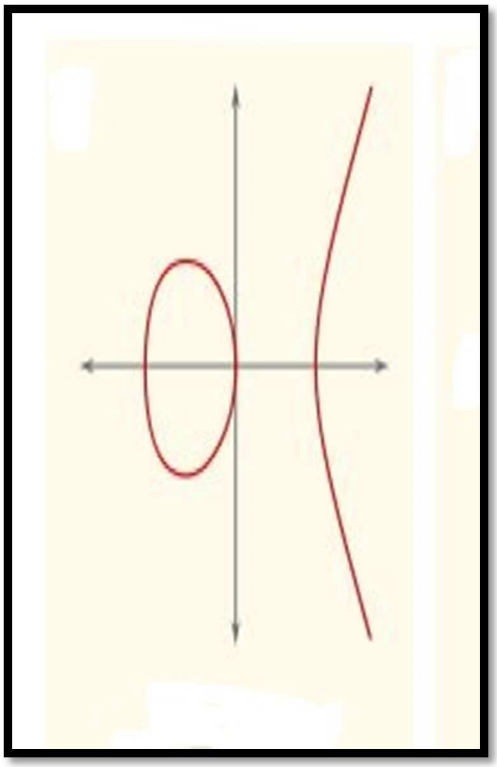


Figura 3. 1: (Ecuación 3.4)

$$y^2 = x^3 - x$$

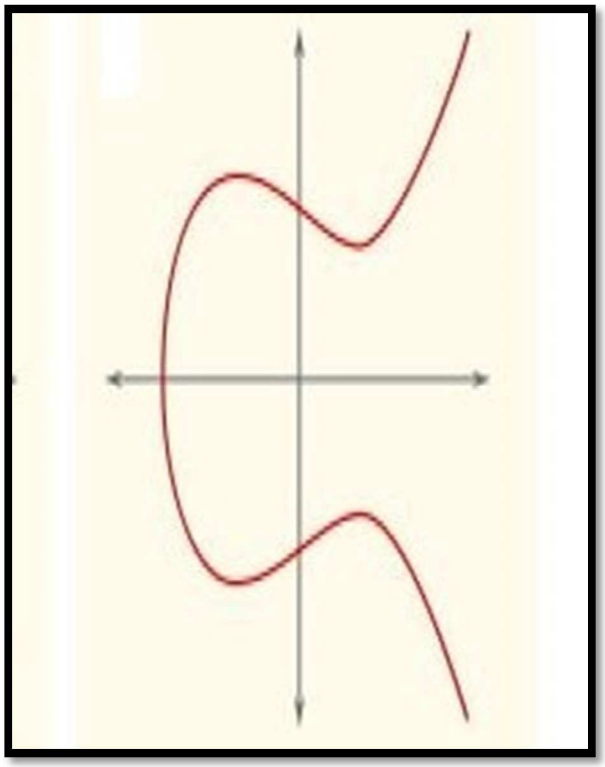


Figura 3. 2: (Ecuación 3.5)

$$y^2 = x^3 - x + 1$$

Fuente: (Tena, 2014).

Definición 3.6

La suma de dos puntos en una curva, tal que:

$$P, Q \in E(k)$$

Es el punto simétrico, respecto al eje ***x***, del tercer punto de intersección con la cúbica de la recta que une ***P*** y ***Q***. Si se cumple ***P = Q***, en este caso se habla de doblado del punto y se sustituye una cuerda por tangente.

A continuación, en las figuras Nro.3.3 y Nro.3.4 se ilustra gráficamente las operaciones referidas de suma y doblado de puntos:

Considerando, el caso particular de un cuerpo base finito, de tal forma que:

$$k = F_q; \; q = p^m$$

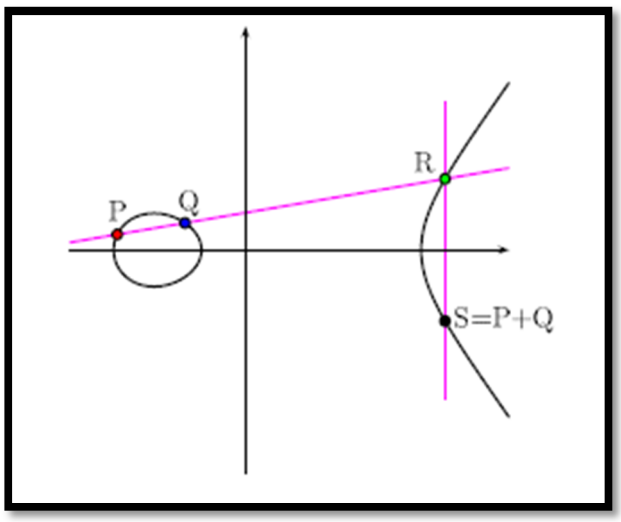


Figura 3. 3: Suma de Puntos en Curva Elíptica.

Fuente: (Tena, 2014).

Entonces se tiene:

Teorema 3.5:

Si ***E*** en una curva elíptica definida sobre F_q, entonces:

1. Sea $N = \#\left(E\left(F_q\right)\right)$ el cardinal de la curva. Se verifica el *Teorema de Hasse*, entonces se tiene la ecuación Nro. 3.7

$$q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q} \qquad \textbf{(3.7)}$$

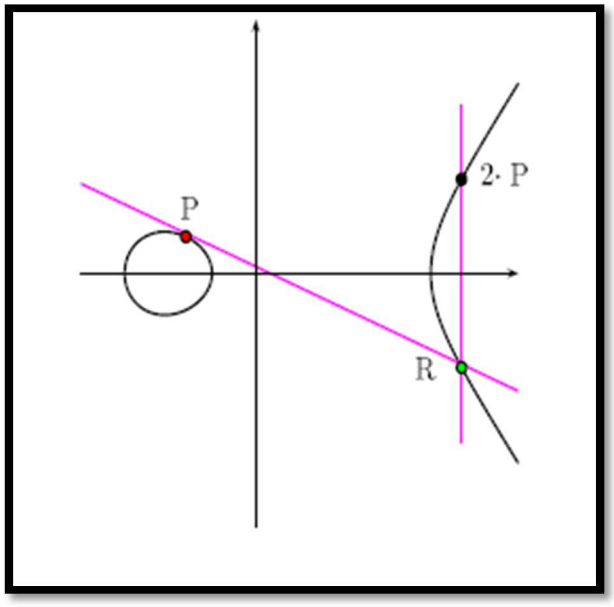


Figura 3. 4: Doblado de Punto en Curva Elíptica.

Fuente: (Tena, 2014).

Siempre y cuando se cumpla:

$$N = q + 1 - t_{\text{con:}} \left| t \right| \leq \sqrt{q}$$

2. El grupo abeliano finito con la siguiente estructura de la Ecuación Nro. 3.8

$$E(Fq) \simeq \left(\frac{Z}{n_1}\right) ZX \left(\frac{Z}{n_2}\right) Z \qquad \textbf{(3.8)}$$

En la cual, (Ecuación Nro.3.9)

$$N = n_1 n_2, n_2 \left| n_1, n_2 \right| q - 1 \qquad \textbf{(3.9)}$$

N, resulta una curva elíptica supersingular, lo cual se define:

Definición 3.7

Una curva elíptica ***E*** definida sobre el cuerpo finito de la Ecuación Nro.3.10.

$$Fq, q = p^m \qquad \textbf{(3.10)}$$

Se llama supersingular si ***p*** divide a ***t.***

3.4. Problema del Logaritmo Discreto Elíptico.

Definición 3.8

Si, se cumple, la ecuación 3.11:

$$G = < g > \qquad \textbf{(3.11)}$$

En un grupo cíclico finito con cardinal ***N***, en el cual el grupo ***G*** considerado es (Ecuación Nro.3.12)

$$F_q = F_q - \{0\} \qquad \textbf{(3.12)}$$

Con cardinal:

$$N = q - 1 \qquad \textbf{(3.13)}$$

Si:

$$x \in G \qquad \textbf{(3.14)}$$

Se denomina logaritmo discreto de ***x*** en la base ***g*** al entero natural:

$$n \leq N \qquad \textbf{(3.15)}$$

De tal forma que:

$$g^n = x \qquad \textbf{(3.16)}$$

Conocidos los valores de ***g*** y ***n*** es computacionalmente cómodo calcular el valor de ***x***. Sin embargo, conocidos los valores de ***g*** y ***x***, es computacionalmente muy difícil determinar ***n*** (**PLD**, Problema del Logaritmo Discreto).

Se clasifica los algoritmos para resolver el Problema del Algoritmo Discreto en las siguientes clases:

1. Algoritmos validos en cualquier grupo Rho de J. M. Pollard, Baby Steps Giant Steps (BSGS), etc., los cuales tienen un coste exponencial elevado.
2. Algoritmo de R. Silver– G. C. Pohlig–M.E. Hellman: Eficientes para grupos cuyo cardinal tiene todos sus factores primos pequeños. Por lo tanto, el cardinal del grupo deberá poseer un factor primo grande para ser un algoritmo criptográficamente seguro.
3. Algoritmos de tipo Index Calculus.

En el caso de del método del Index Calculus se ha aplicado con éxito a los cuerpos finitos de la forma: ***Fq***, en particular los binarios: F_{2^m}.

En la actualidad, se considera necesario un tamaño mínimo para el cardinal de estos cuerpos de 1024 bits, por lo que es necesario, aumentar el tamaño de las claves y, por lo tanto, todos los recursos computacionales necesarios.

Una posibilidad alternativa es substituir el grupo:

$$G = F_q \qquad \textbf{(3.17)}$$

Por otros inmunes al logaritmo Index Calculus. Esta fue la motivación de los criptógrafos Miller y Koblitz para su propuesta en relación con el Problema del Logaritmo Discreto Elíptico (PLDE), el cual se enuncia:

Dada una curva elíptica ***E*** sobre F_q y puntos ***P*** y $Q = nP$ en $E(F_q)$ encontrar ***n.***

El **PLDE** ofrece las siguientes ventajas sobre el **PLD** clásico:

4. **Flexibilidad:** Fijado el cuerpo F_q existen muchas curvas elípticas sobre él, lo que ofrece la posibilidad de cambiar periódicamente la curva, manteniendo la aritmética F_q
5. El grupo $E(F_q)$ es inmune al Index Calculus, lo que lo hace más seguro que el grupo F_q:
    1. El ataque al **PLDE** para una curva elíptica sobre F_p, ***p*** primo de 160 bits, se necesita aproximadamente 10^{24} operaciones elementales.
    2. El ataque al DLP, utilizando el método del Index Calculus para F_p, ***p*** primo de 160 bits, es necesario 10^9 operaciones.

La posibilidad de implementar claves más cortas hace eficaz a la Criptografía con curvas elípticas para su uso en plataformas con capacidad computacional reducida como en tarjetas inteligentes, redes de sensores, sistemas embebidos. etc.

Ataques al **Problema del Logaritmo Discreto Elíptico**, como el método MOV, favorecieron la búsqueda de otras alternativas como base del logaritmo discreto. Es el caso de las Curvas Hiperelípticas, la generalización de las curvas elípticas. Estas curvas vienen dadas por una ecuación del tipo: (Ecuación 3.18)

$$C: y^2 + h(x)y = f(x) \,|\, gr(h) \le g,\ gr(f) = 2g + 1 \qquad \textbf{(3.18)}$$

Las curvas elípticas corresponden al caso ***g***=1.

Sin embargo, el **PLD** sobre las curvas hiperelípticas se ha mostrado vulnerable, para ***g > 2***, frente a variantes del Index Calculus.

3.5. Curvas elípticas criptográficamente útiles.

Presentemente el PLDE se considera un algoritmo criptográfico seguro, pero es necesario algunas precauciones en la elección de la curva elíptica de base ***E***, a continuación, se les expone:

1. El cardinal de ***E*** debe ser adecuado, primo o con un factor primo grande para evitar el ataque de Silver- Pohlig-Hellman.
2. Con grado de inmersión en particular, no supersingulares para evitar el ataque de tipo MOV.
3. Evitar las denominadas curvas Anómalas, curvas sobre F_p (p primo), y con cardinal ***p***.
4. ***E*** debe ser inmune al ataque por Descenso de Weil.

Dos vías, pero computacionalmente elevadas, se pueden utilizarse para elegir una curva elíptica buena:

5. Tomar curvas aleatoriamente, calcular su cardinal y comprobar si es adecuado.
6. Construcción de curva elíptica con cardinal adecuado prefijado.

Una tercera vía consiste en el empleo de isogenias; dos curvas isogenias tienen igual cardinal; por lo tanto, partiendo de una curva criptográficamente buena con cardinal adecuado ***N***, todas las curvas obtenidas a partir de ellas como imágenes por isogenias serán también buenas.

Considerando el conjunto de todas las curvas elípticas, definidas salvo isomorfa; sobre un cuerpo finito dado (Ecuación 3.19):

$$F_q, q = p^m \qquad \textbf{(3.19)}$$

Y con cardinal ***N.*** Sea l un número primo diferente de característica ***p*** del cuerpo y, considerando las posibles isogenias de grado l entre tales curvas; tal conjunto puede considerarse como un grafo dirigido (Ecuación 3.20):

$$G(N, l) \qquad \textbf{(3.20)}$$

Con aristas l- isogenias; es posible asignar a estas aristas un cierto sentido (horizontal, ascendente o descendente) y, por lo tanto, estratificar a:

$G(N, l)$ en pisos o niveles. **(3.21)**

Cada componente conexa de (Ecuación Nro.3.21):

$$G(N, l) \qquad \textbf{(3.22)}$$

Se denomina un l - volcán.

El nombre de volcán responde a su similitud con un cono volcánico, en un l volcán se habla de cráter, ladera y suelo. El grafo total $G(N, l)$ está formado por varios l - volcanes y puede denominarse una l - cordillera. En la figura Nro. 3.5 se ilustra la estructura de un volcán.

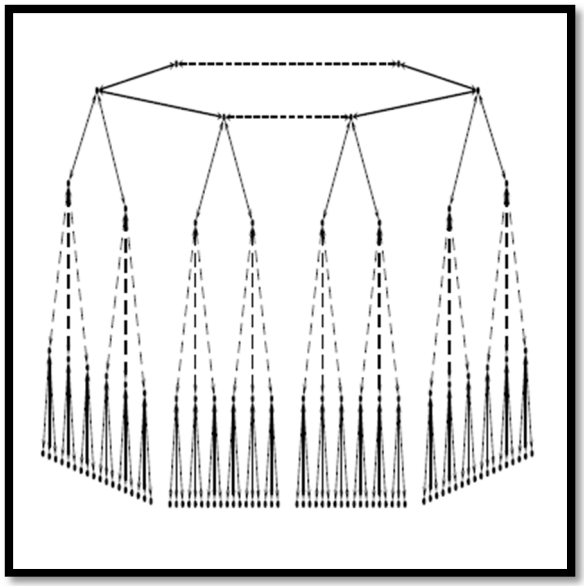


Figura 3. 5: Volcán de Isogenias.
Fuente: (Tena, 2014).

Biosca, en cuanto al Volcán de Isogenias, manifiesta: ‘’No obstante, resultados experimentales indican que mientras la altura de estos volcanes es más bien pequeña, el tamaño del cráter puede ser enorme: el volcán de la curva $y^2 = x(x-1)(x-2017156814720162)$ sobre el cuerpo F_p con $p = 8010956020551503$ tiene altura 1 y longitud de cráter 74638817. Con estas técnicas parece, pues, probable que dada una curva criptográficamente buena se pueda construir muchas más curvas isógenas y por tanto útiles”. (Miret Biosca).

Nota aclaratoria:

Existe múltiple bibliografía acera de los campos finitos, en algunos casos, se utiliza ***p*** en lugar de ***m*** y, F_p en vez de $\mathbb{Z}_p$.

3.6. Estándares.

Las continuas investigaciones y, trabajos realizados en relación a la aplicación de la criptografía con curvas elípticas, no se ha quedado como un aspecto teórico - práctico, más bien como parte de su evolución y, con la finalidad de mejorar los diferentes esquemas propuestos inicialmente y para que exista una mejor interoperabilidad con las aplicaciones que emplea criptografía con curvas elípticas, se han realizado esfuerzos para estandarizar este tipo de criptografía; a continuación, se enlista los principales estándares que se han desarrollado:

- ANSI X9.62, X9.63.
- IEEE P1363 y P1363A.
- ISO 14888, 9796-4, 15946.
- FIPS 186-2.
- SEC 1, SEC 2, SEC 3 y SEC 4.
- RSA.
- NSA.

Producto del esfuerzo de estandarizar la criptografía con curvas elípticas, se han desarrollado otras iniciativas de criptosistemas de clave pública, implementaciones con otros esquemas, de tal forma, que el algoritmo cifrado a manejar cumpla con determinadas propiedades. En este sentido, se han desarrollado estándares de aplicación de criptografía con curvas elípticas, sobre todo en ambientes donde se requiere el cumplimiento de los atributos de la seguridad de la información (integridad, disponibilidad, confidencialidad y, no repudio) y que requieran, tamaños mínimos de clave.

A continuación, se enlista los principales estándares de aplicación desarrollados:

- IETF (IPSec, TLS, S/MIME, SSH, DNSSEC)
- WAP WTLS
- ATM

El estándar FIPS 186-2, especifica cinco rangos para el valor de n (número de bits) Para cada rango, también se especifica un tamaño de cofactor h

máximo. Se debe considerar que la especificación de un cofactor h en un conjunto de parámetros de dominio es opcional en el estándar ANS X9.62; mientras que las implementaciones que cumplen con esta Norma, deberán especificar el cofactor h en el conjunto de parámetros de dominio. A continuación, en la Tabla 3.1 se proporciona los tamaños máximos para el cofactor h.

Tabla 3. 1: Tabla de Cofactores FIPS 186-2.

Bit length of n	Maximum Cofactor (h)
160 - 223	2^{10}
224 - 255	2^{14}
256 - 383	2^{16}
384 - 511	2^{24}
≥ 512	2^{32}

Fuente: (NIST, 2013)

La fortaleza de la seguridad para los cinco rangos de la longitud n (número de bits), lo proporcionan SP 800-57 (NIST Special Publication 800-57 Part 1 Revised 2007). Para el campo $GF(p)$, la fuerza de seguridad depende de la longitud de la expansión binaria de p. Para el campo $GF(2m)$, la fuerza de seguridad depende del valor de m. La Tabla 3.2 proporciona las longitudes de bits de los diversos campos subyacentes de las curvas proporcionadas en el Anexo D: ‘’Recommended Elliptic Curves for Federal Government Use’’ del documento NIST.FIPS PUB 186-4. En la tabla referida, la columna 1 enumera los rangos para la longitud de bit de n; la columna 2 identifica el valor de p usado para las curvas sobre los campos principales, donde $len(p)$ es la longitud de la expansión binaria del entero p y, la columna 3 proporciona el valor de m para las curvas sobre campos binarios.

Tabla 3. 2: Numero de Bits para curvas recomendadas.

Bit Length of n	Prime Field	Binary Field
161 – 223	$\text{len}(p) = 192$	$m = 163$
224 – 255	$\text{len}(p) = 224$	$m = 233$
256 – 383	$\text{len}(p) = 256$	$m = 283$
384 – 511	$\text{len}(p) = 384$	$m = 409$
≥ 512	$\text{len}(p) = 521$	$m = 571$

Fuente: (NIST, 2013).

Se incluye en este trabajo, el Anexo D: ‘’Recommended Elliptic Curves for Federal Government Use’’ del documento **NIST.FIPS PUB 186-4.**

3.7. Descripción de la propuesta de Modelamiento del Sistema Criptográfico.

Con el propósito de cumplir uno de los objetivos del presente trabajo de investigación, en el cual se propone realizar el modelamiento de un criptosistema implementado con criptografía asimétrica mediante de curvas elípticas, se propone utilizar el algoritmo de ElGamal, por el motivo que su seguridad está basada en el Problema del Logaritmo Discreto (PLD) y los cálculos tanto de cifrado como de descifrado se realiza sobre un grupo cíclico, lo cual hace que la seguridad de este algoritmo es proporcional a la dificultad en el cálculo del logaritmo discreto en el grupo en referencia.

A continuación, se enlista la metodología en cuanto a la parte teórica del modelamiento propuesto:

- Configuración del Criptosistema.
- Algoritmo de Cifrado del Criptosistema.
- Algoritmo de Descifrado del Criptosistema.

La idea principal del modelamiento propuesto es enviar un mensaje cifrado, suponiendo el escenario de dos usuarios que se comunican entre sí; es decir, un emisor y, un receptor del mensaje cifrado a través de un canal.

El usuario emisor enviara al receptor un mensaje cifrado bajo el esquema ElGamal, cada usuario, tiene un par de claves asociadas, una clave pública y, una clave privada; la implementación de este criptosistema es mediante curvas elípticas.

En la figura 3.6 se ilustra el esquema propuesto para el modelamiento del criptosistema y, sus elementos intervinientes.

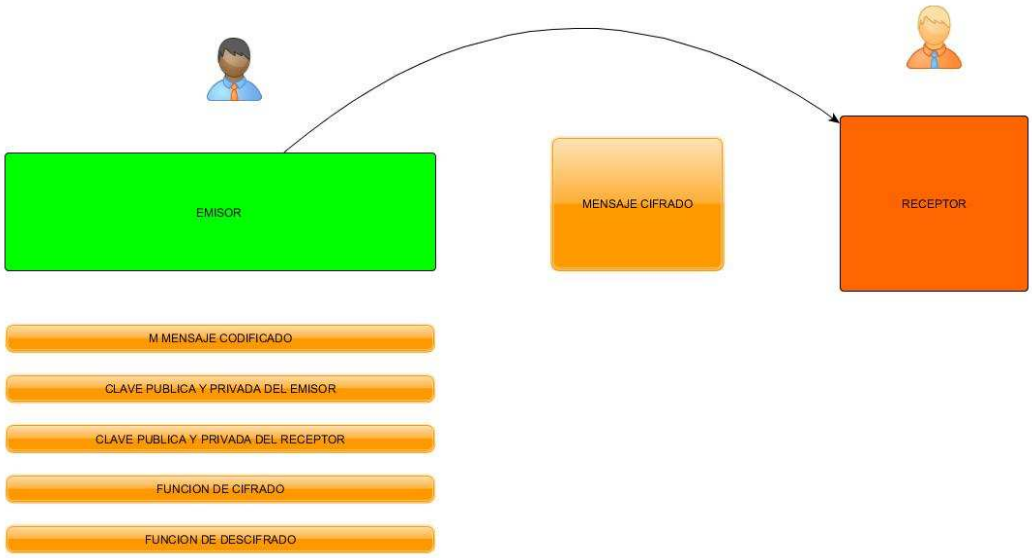


Figura 3. 6: Esquema del Criptosistema.
Fuente: (Propia)

Para el modelamiento del criptosistema en mención, se decidió utilizar el programa: SAGE; este es un proyecto de Software Libre y, de Código Abierto, que surgió como una alternativa a otros Sistemas de Algebra Computacional (CAS) como Matlab y Maple. Esta herramienta seleccionada tiene la capacidad de analizar curvas elípticas, lo cual fue una de las razones por las que se decidió modelar el criptosistema propuesto.

3.7.1. Configuración del Criptosistema.

a. Generar un número primo para definir el cuerpo finito.

b. Seleccionar los parámetros a y b de la curva elíptica E sobre F_p.

c. Seleccionar un punto P de la curva elíptica, en la cual el orden debe ser un numero entero n que contenga un factor primo del tamaño de p

d. Clave privada: es un numero entero d que se encuentra en el intervalo $[1, n-1]$

e. Clave pública: El punto $Q = d.P$ de la curva elíptica seleccionada. (Ver Figura Nro. 3.9).

f. Mensaje; El mansaje que se quiere cifrar se supone que se ha convertido en un numero natural $m, 0 < m < p$.

3.7.2. Algoritmo de Cifrado del Criptosistema ElGamal Elíptico.

a. Seleccionar el Algoritmo para el Cifrado aplicando en este caso, el Criptosistema de ElGamal Elíptico.

b. Clasificar los elementos, tanto de Entrada como de Salida.

- Entrada: definir los parámetros (p, a, b, P, n), la clave pública Q y el mensaje a transmitir m.
- Salida: el mensaje cifrado $(\alpha_1, \alpha_2, \gamma)$

c. Escoger un entero aleatorio r en $[1, n-1]$

d. Calcular: $r \cdot P = (\alpha_1, \alpha_2) yr \cdot Q = (\beta_1, \beta_2) en E_a, b(F_p)$

e. Calcular: $\gamma = m \cdot \beta_1 en F_p$

f. Devolver m $(\alpha_1, \alpha_2, \gamma)$. (Ver Figura Nro. 3.10).

3.7.3. Algoritmo de Descifrado del Criptosistema El Gamal Elíptico.

a. Clasificar los elementos, tanto de Entrada como de Salida:

- Entrada: Los parámetros (p, a, b, P, n), la clave privada d.
- Salida: El mensaje cifrado m.

b. Calcular el punto $d \cdot (\alpha_1, \alpha_2) = d \cdot r \cdot P = r \cdot Q = (\beta_1, \beta_2)$ en $E_a, b(F_p)$.

c. Obtener el mensaje cifrado $m = \gamma \cdot \beta^{-1}$ en F_p.

d. Devolver el menaje descifrado m. (Ver Figura Nro. 11)

3.7.4. Modelamiento del Criptosistema de ElGamal Elíptico utilizando SAGE.

Dada una curva elíptica E sobre un cuerpo F_p, un generador P de un subgrupo cíclico G de puntos de $E(F_p)$ y un punto Q de G, se debe encontrar el entero n de tal forma que: $Q = n \cdot P$

Curva: $E: y^2 = x^3 + 102x + 2005$ (Ver Figura 3.7)

Cuerpo: $F_p = 314159265359$

Cardinal: $\#\, E(F_p) = 314159228780 = 2^2 \cdot 5 \cdot 15707961439$

Se selecciona sobre la curva elíptica un valor de x aleatorio, y este valor se comprueba si $x^3 + ax + b$ es un cuadrado de F_p, de tal forma se obtiene el punto:

$$P = (217516809093, 126715600995)$$

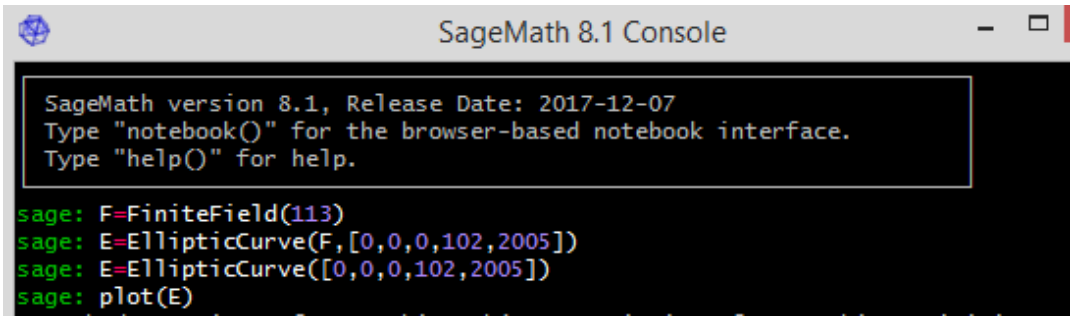


Figura 3. 7: Configuración de la Cueva Elíptica en el plano proyectivo.

Fuente: (Propia).

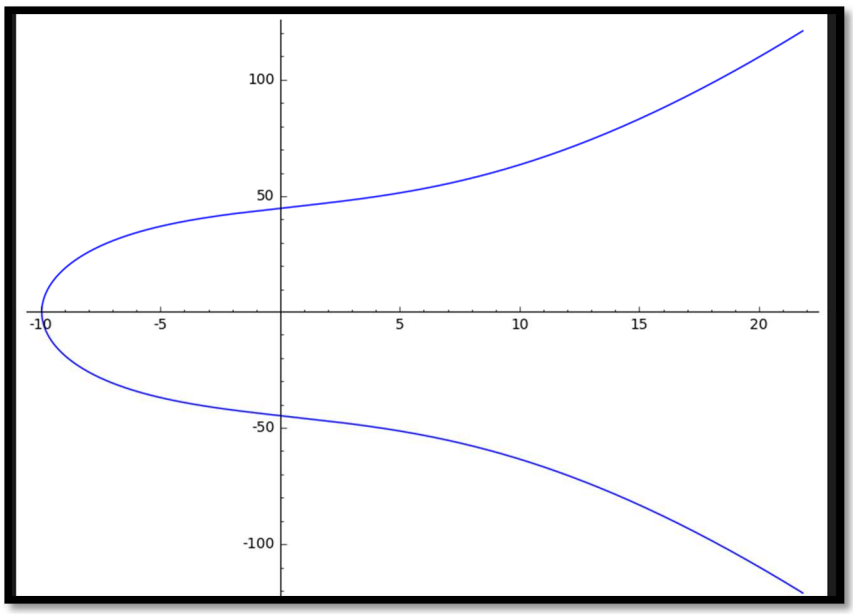


Figura 3. 8: Curva Elíptica modelada con SAGE en el plano proyectivo.

Fuente: (Propia).

- **Configuración del Criptosistema.**
  - $p = 123456789011$
  - $a = 72349835377$
  - $b = 102213907268$
  - $P = (104450850632,89206086037)$
  - $n = 1234456319379$
  - $d = 987654321$
  - Clave Publica: $Q = dP$ (Ver figura 3.9)

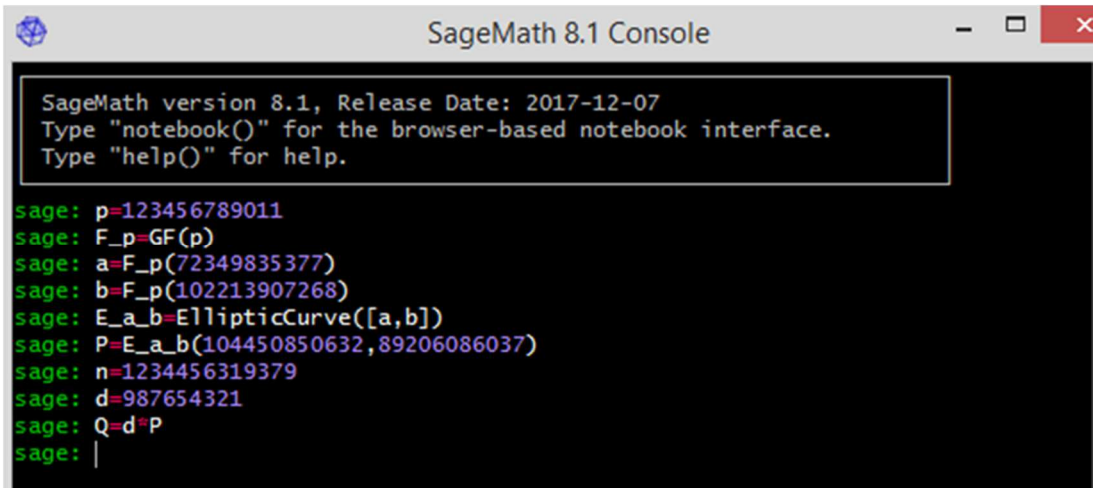


Figura 3. 9: Configuración del Criptosistema ElGamal Elíptico.

Fuente: (Propia).

- **Cifrado Criptosistema ElGamal Elíptico.**

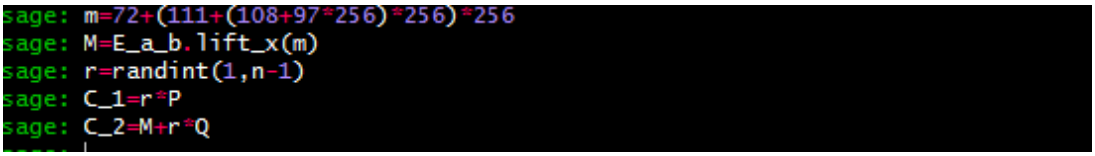


Figura 3. 10: Cifrado Criptosistema ElGamal Elíptico.

Fuente: (Propia).

- **Descifrado Criptosistema ElGamal Elíptico.**

Figura 3. 11: Descifrado Criptosistema ElGamal Elíptico.

Fuente: (Propia).

En la Figura Nro. 3.11, se observa que, en ambos casos, tanto el mensaje cifrado con curvas elípticas como el mensaje descifrado bajo el mismo esquema, al ser comparados son entre sí, son iguales; por lo tanto, el criptosistema es válido. Se debe considerar en este modelamiento, el tamaño mínimo de las claves utilizadas por los dos usuarios, que finalmente, convierte a este criptosistema seguro y, óptimo.

Conclusiones.

1. La realización del Estado del Arte del presente trabajo de investigación inicia con el origen de la Criptografía hasta la Criptografía Cuántica, incluyendo la descripción de los Criptosistemas tanto Simétricos como Asimétricos.

2. Por medio de la elaboración del Estado del Arte, se determina que la implementación de los Criptosistemas de tipo Asimétricos es más compleja; lo cual otorga a estos que sean portadores de atributos que brindan más seguridad, sobre todo en aplicaciones, como es el caso de las firmas digitales, implementación de seguridad de tarjetas electrónicas, entre otras aplicaciones.

3. El modelamiento del criptosistema propuesto empleando Curvas Elípticas por medio del software de uso libre SAGE, es netamente teórico; sin embargo, se demuestra que es posible construir criptosistemas utilizando claves de tamaño mínimo para implementar sistemas criptográficos asimétricos de clave pública, como es el caso de ElGamal Elíptico.

4. Se demuestra, que la implementación de criptosistemas con curvas elípticas con claves de tamaño mínimo concede seguridad para aplicaciones en firmas digitales, tarjetas inteligentes, sistemas embebidos.

Recomendaciones.

1. Se recomienda como futuros proyectos de investigación, la implementación de criptosistemas con curvas elípticas, utilizando claves con tamaño reducido; estos criptosistemas deberán ser curvas criptográficamente buenas y, además que se correlacione con curvas estandarizadas.

2. Para futuros proyectos de investigación, se recomienda la implementación de criptosistemas con curvas elípticas en firmas digitales, Comercio Electrónico basado en Internet, tarjetas inteligentes, redes Wireless y bitcoins.

3. De igual forma, se recomienda a futuro, proponer un estudio teórico acerca de sistemas de criptoanálisis para sistemas criptográficos basados en curvas elípticas; esto trasladara a realizar investigaciones que formulen otros esquemas de criptografía, que de igual forma briden seguridad y, además la ventaja de utilización de claves cortas.

Bibliografía.

Ángel, J. (2012). *De Turing y la Criptografía*. Obtenido de http://www.uam.mx/difusion/casadeltiempo/56_v_jun_2012/casa_del_tiempo_eIV_num_56_27_30.pdf

Brotons, F. (2016). Obtenido de http://hdl.handle.net/10045/54171

Carrasco, A. (2015). *Contribuciones a las comunicaciones ópticas en espacio libre: utilización de telescopios Cherenkov como receptores y corrección de Beam Wander en comunicaciones cuánticas*. Obtenido de Universidad Carlos III de Madrid: http://hdl.handle.net/10016/21650

Cesaratto, E., & Fuentes, C. (2015). *Revista de Educación Matemática.* Obtenido de Revista de Educación Matemática: https://revistas.unc.edu.ar/index.php/REM/article/view/12388/12704

CISCO. (2017). *CISCO*. Obtenido de CISCO: https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/1456403/Cisco_2017_Midyear_Cybersecurity_Report.pdf?elqTrackId=f6ccd8439e9945639096a9846044695a&elqaid=5897&elqat=2

Cordova, D., & Méndez-Garabetti, M. (2017). Criptografía Post Cúantica. Mendoza, Argentina.

Costas, J. (2011). *Seguridad Informática.* Ra-ma (España).

Departamento de Análisis Matemático, Facultad de Matemáticas de la universidad Complutense de Madrid. (s.f.). Lema Bezout, Teorema de Factorización Única .

Fernández, S. (2011). *La Criptografía Clásica.* Obtenido de http://www.interaktiv.cl/blog/wp-content/uploads/2011/08/9_Criptografia_clasica.pdf

FirmaDigitalUAP. (24 de 06 de 2010). Obtenido de FirmaDigitalUAP: http://firmadigitaluap.blogspot.com/2010/06/firma-digital.html

Garcia Belmont , R. (abril de 2016). Obtenido de http://tesis.ipn.mx/handle/123456789/20224

García, M. (2013). *Design and implementation of a high-speed free-space quantum key distribution system for urban scenarios*. Obtenido de Repositorio Dspace: http://hdl.handle.net/10486/14118

Garcia, R. (2016). *Firma digital basada en funciones HASH y un algoritmo criptográfico híbrido*. Obtenido de Repositorio Dspace: http://tesis.ipn.mx/handle/123456789/20224

GNUPG. (s.f.). Obtenido de GNUPG: https://www.gnupg.org/gph/es/manual/x232.html

Hernández , G. (febrero de 2010). Paralelización de la multiplicación escaalr en curvas elípticas en una arquitectura multinucleo de Intel . México , México .

Hernández, F. (2015). *Autenticación biométrica de usuarios a través del iris mediante la ocultación de claves y funciones resumen que preservan la similitud*. Obtenido de Archivo digital UPM: http://oa.upm.es/39099/

Ivorra, C. (s.f.). *Teoría de Cuerpos de Clases.*

Javier Campos Blog . (22 de 07 de 2011). Obtenido de Javier Campos Blog : http://www.javiercampos.es/blog/2011/07/22/el-algoritmo-de-diffie-hellman/

Joseph , P. (2015). Cognitive Analytics and Comparison of Symmetric and Asymmetric Cryptography Algorithms. *Researchgate*.

Lucena, M. (2010). *Criptografía y Seguridad en Computadores. Versión 4-0.8.1*. Obtenido de http://www.grc.upv.es/biblioteca/cripto.pdf

Lumbiarres-López, R., López Garcia, M., & Cantó-Navarro, E. (s.f.). Ataques por canal lateral sobre el algoritmo de encriptación AES implementado en MicroBlaze.

Martínez Rodríguez, H., & Borges Trenard, M. (s.f.). *Curvas Elípticas en la Criptografía.* Académica Española.

Méndez Naranjo , P. M. (2015). Nuevo Algoritmo Criptografico con la incorporación de la Esteganografía en Imágenes. Riobamba.

Miret Biosca, J. (s.f.). Criptografía con curvas elípticas.

Miret, J., & Valera, J. (2015). *CriptoRed.UPM*. Obtenido de CriptoRed.UPM: http://www.criptored.upm.es/crypt4you/temas/ECC/leccion1/leccion1.html

Navarro, P. (2013). Intercambio de claves sobre anillos no conmutativos. *Intercambio de claves sobre anillos no conmutativos*. Alicante.

NIST. (2013). *FIPS 186-4.*

Pacheco, F. (2014). *Criptografía desde los sistemas clásicos hasta el futuro de la privacidad.* Buenos Aires : Fox Andina S.A.

Paguay. (junio de 2015). *Repositorio Institucional de la Escuela Superior Politécnica de Chimborazo.* Obtenido de Repositorio Institucional de la Escuela Superior Politécnica de Chimborazo: http://dspace.espoch.edu.ec/handle/123456789/4431#sthash.w9g0rANU.dpuf

Ramió, J. (2006). *Seguridad Informática y Criptografía.* Obtenido de http://www.criptored.upm.es/guiateoria/gt_m001a.htm

Roe Buendia , J. F. (2013). *Seguridad Informatica.* Madrid: McGraw Hill.

Sánchez Acosta , E. (s.f.). Criptoanálisis más utilizados en la actualidad.

Sánchez, G., & González, C. (2016).

SSL247. (s.f.). Obtenido de SSL247: https://www.ssl247.es/certificats-ssl/rsa-dsa-ecc

Tabara, J. (2014). *Criptografía Clásica*. Obtenido de https://joseluistabaracarbajo.gitbooks.io/criptografia-clasica/content/Cripto03.html

Tena, J. (2014). 25 Años de Criptografía de Curvas Elíticas. *RECSI* .

Ubiquitour. (08 de 09 de 2015). *Ubiquitour*. Obtenido de Ubiquitour: http://www.ubiquitour.com/aWNXMbBZ/

UIT-T-X.805. (s.f.).

Zapata, R. (2014). Obtenido de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0551_ZapataValdezRH.pdf

Glosario de Términos.

3DES: *Triple DES.* Triple Data Encryption Standard, Triple Estándar de Encriptación de Datos.

a.C: Antes de Cristo.

AES: Advanced Encryption Standard.

ANSI: *American National Standards Institute,* Instituto Nacional Estadounidense de Estándares.

ATM: Asynchronous Transfer Mode, Modo de Transferencia Asíncrona.

CISCO: Cisco Systems. Sistemas CISCO.

CRLF: CR (retorno de carro) y LF (salto de línea).

DES: Data Encryption Standard, Estándar de Encriptación de Datos.

D-H: Diffie-Hellman.

DL: Discrete Logarithm*, Logaritmo Discreto.*

DSA: *Digital Signature Algorithm*, Algoritmo de Firma Digital.

DNSSEC: Domain Name System Security Extensions, Extensiones de Seguridad para el Sistema de Nombres de Dominio.

ETCD (DTE): Data Circuit-terminating Equipment, Equipo Terminal del Circuito de Datos.

FIPS: Federal Information Processing Standards, Estándares Federales de Procesamiento de la Información.

IBM: *International Business Machines,* Equipos de Negocios Internacionales.

IDEA: International Data Encryption Algorithm, algoritmo internacional de cifrado de datos.

IEEE: Institute of Electrical and Electronics Engineers, Instituto de Ingeniería Eléctrica y Electrónica.

IETF: Internet Engineering Task Force, Grupo de Trabajo de Ingeniería de Internet.

IF: Integer Factorization, Factorización de Enteros.

IP: Internet Protocol, Protocolo de Internet.

IPsec: Internet Protocol security. Protocolo de Internet Seguro.

IPv4: Internet Protocol version 4, Protocolo de Internet versión 4.

IPv6: Internet Protocol version 6, Protocolo de Internet versión 6.

ISO: International Organization for Standardization, Organización Internacional de Normalización.

MD5: Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5.

MOV: *Menezes-Okamoto-Vanstone.*

NIST: *National Institute of Standards and Technology,* Instituto Nacional de Estándares y Tecnología.

NSA: *National Security Agency*, Agencia de Seguridad Nacional.

OSI: Open System Interconnection, Interconexión de sistemas abiertos.

PLD: Problema del Logaritmo Discreto.

RSA: *Rivest, Shamir y Adleman.*

S/MIME: Secure / Multipurpose Internet Mail Extensions, Extensiones de Correo de Internet de Propósitos Múltiples / Seguro.

SEC: Securities and Exchange Commission, Comisión de Bolsa y Valores.

SHA: *Secure Hash Algorithm*, Algoritmo de Hash Seguro.

SSH: Secure SHell, Intérprete de Órdenes Seguro.

SSL: *Secure Sockets Layer.*

TCP-IP: Transmission Control Protocol/Internet Protocol, Protocolo de Control de Transmisión/Protocolo de Internet.

TLS: *Transport Layer Security*, Seguridad de la Capa de Transporte.

TPDU: Transaction Protocol Data Unit, Unidad de Datos de Protocolo.

WAP WTLS: Wireless Transport Layer Security, Seguridad para la Capa de Transporte en Comunicaciones Inalámbricas.

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Proaño Andrade Juan Carlos**, con C.C: # **1714113030** autor/a del trabajo de titulación: **Técnicas de criptografía en las comunicaciones modernas. Empleo del método de curvas elípticas** previo a la obtención del título de **Magíster en Telecomunicaciones** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 26 de octubre del año 2018

f. _____

Nombre: **Proaño Andrade Juan Carlos**

C.C: **1714113030**

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Técnicas de criptografía en las comunicaciones modernas. Empleo del método de curvas elípticas		
AUTOR(ES)	Proaño Andrade Juan Carlos		
REVISOR(ES)/TUTOR	MSc. Edwin Palacios Meléndez; MSc. Luis Córdova Rivadeneira / MSc. Manuel Romero Paz		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Sistema de Posgrado		
PROGRAMA:	Maestría en Telecomunicaciones		
TITULO OBTENIDO:	Magister en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	Guayaquil, 26 de octubre del año 2018	**No. DE PÁGINAS:**	**79**
ÁREAS TEMÁTICAS:	Criptografía, Criptosistema, Criptoanálisis, Estenografía, Estegoanálisis, Seguridad		
PALABRAS CLAVES/ KEYWORDS:	Criptografía, Seguridad, Simetrico, Asimétrico, Curvas Elípticas		

RESUMEN/ABSTRACT: El presente proyecto de titulación está orientado a realizar una simulación de un algoritmo criptográfico asimétrico de clave corte utilizando el método de curvas elípticas; este trabajo de investigación, está estructurado de tres capítulos. En el capítulo uno, se efectúa la descripción del presente trabajo de titulación, tales como: la justificación, antecedentes, definición del problema, objetivo general, objetivos específicos, hipótesis y, la metodología a seguir. En el capítulo dos, se desarrolla la fundamentación teórica de la Criptografía, la cual explica los orígenes de la Criptografía y, sus principales definiciones empleadas; luego se describe la Criptografía Simétrica y, el desarrollo de la Criptografía Asimétrica; se ha tratado, en cada tipo de Criptografía especificar lo más relevante de los algoritmos más empleados, lo cual no deja ser temas menos importantes de destacar. Se hace una breve referencia, al Criptoanálisis, tanto, para Sistemas Simétricos como para Asimétricos y, finalmente se hace una breve descripción en cuanto al Cifrado y, Criptoanálisis cuántico. En el capítulo tres, se realiza toda la parte teórica relacionada con la Criptografía con Curvas Elípticas; con estas bases, se hace una propuesta de modelamiento de un algoritmo asimétrico por medio de una herramienta de código abierto, finalmente, se muestran las conclusiones y, recomendaciones.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-987915485	**E-mail:** juankarlos2006@gmail.com
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE):	**Nombre:** Romero Paz Manuel de Jesús	
	Teléfono: +593-994606932	
	E-mail: manuel.romero@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	