

# **Sistema simétrico para el cifrado de imágenes utilizando El Gamal y el número Pi**

**Trabajo Terminal No. 2023-A007**

*Alumnos: \*Pérez Leal Rodolfo<sup>1</sup>*

*Directores: Víctor Manuel Silva García, José Cruz Martínez Perales*

*\*e-mail: rperezl1501@alumno.ipn.mx*

## **Resumen**

Hoy día, la seguridad al momento de transferir información en redes es muy importante, sobre todo al tratarse de imágenes, por lo que se han desarrollado diversos criptosistemas con la intención de mantener oculto el contenido que se transmite. Para conseguir esto, la criptografía emplea un esquema de comunicación segura el cual a su vez emplea criptosistemas simétricos y asimétricos que permiten conseguir este objetivo.

Cada esquema de cifrado que existe tiene ventajas y desventajas cuando se trata de cifrar imágenes, se propone realizar un sistema simétrico basado en ElGamal con el propósito de conservar la velocidad que los sistemas simétricos tradicionales tienen, pero agregando una forma segura de poder propagar las llaves que se requieren al momento del cifrado.

**Palabras Clave** – Cifrado de imágenes, criptosistema ElGamal, correlaciones, entropía, número Pi.

## **1.Introducción.**

Con el uso de teléfonos celulares ha incrementado la cantidad de imágenes digitales que son transmitidas por las redes sociales y aplicaciones de mensajería instantánea, se ha vuelto de mayor importancia mantener confidencial el contenido de las imágenes mientras son enviadas por medios no seguros como Internet [1].

Para mantener la información privada, la criptografía emplea criptosistemas simétricos, también conocidos como criptosistemas de llave privada o criptosistemas asimétricos o de llave pública.

La encriptación por llave publica, permite crear una comunicación sin depender de un canal de comunicación privado, debido a que en este esquema la llave empleada para cifrar los mensajes puede permanecer publica, y se emplea una llave diferente para descifrar, con esto se permite a cualquier persona cifrar un mensaje, pero solo el destinatario puede ver su contenido y comprobar la autenticidad del mensaje mediante el uso de firmas electrónicas [2].

Por otro lado, los criptosistemas simétricos o criptosistemas de llave privada donde las partes involucradas en el intercambio de información acuerdan un algoritmo de cifrado y descifrado mediante una llave privada junto a un esquema de comunicación este tipo de criptosistemas suelen ser más rápidos y seguros, pero no cuentan con firma digital o un método para la distribución de la llave privada [3].

Para que un criptosistema se considere seguro debe de cumplir con cuatro servicios; confidencialidad, autenticación, integridad y no repudio.

Para que un sistema sea confidencial implica que la información que maneje solo puede ser vista por las partes autorizadas, la autenticación se logra al identificar al que envía el mensaje, con la integridad se asegura que solo las partes autorizadas pueden modificar la información transmitida y finalmente el no repudio nos asegura que ni el emisor o el receptor del mensaje pueden negar la transmisión de este mismo [2].

Existen ocasiones en donde se requiere cumplir con estos servicios no solo para textos, sino que también para una imagen digital con la intención de proteger la privacidad de los usuarios, y en ocasiones, las imágenes deben ser comprimidas sin perder información como en el ejército, bancos, astronomía, películas entre otros casos [4].

Usualmente se refiere a una imagen digital a imágenes rasterizadas que tienen un arreglo bidimensional de píxeles de un tamaño definido que puede ser obtenida a partir de cámaras digitales, o documentos escaneados o incluso generadas mediante algún software para creación de imágenes. Una imagen digital también puede ser una imagen vectorial, que resulta de realizar operaciones matemáticas con vectores, que permiten conservar un tamaño consistente sin importar su tamaño [5].

De forma general se puede decir que el cifrado de imágenes se clasifica en dos apartados, de acuerdo a como se realicen las operaciones para cifrado dentro de la imagen, estas pueden ser a nivel de píxeles o a nivel de bit, en la primera categoría las operaciones son aplicadas directamente en los píxeles de la imagen, por otro lado en la segunda categoría cada píxel es dividido en bits y las operaciones son realizadas en bloques de tamaño definido por el algoritmo a ocupar en lugar de cada píxel [6].

El cifrado de imágenes es diferente al cifrado de textos por características de las imágenes digitales como la redundancia de datos, la relación entre píxeles adyacentes y la gran capacidad de información que se maneja en una imagen por lo que muchos algoritmos de encriptación tradicional, como Data Encryption Estándar (DES), Triple Data Encryption Algorithm (TDEA), Advanced Encryption Estándar (AES) y RSA nombrado así por sus creadores Rivest, Shamir y Adleman, cuentan con debilidades al momento de cifrar imágenes [1].

Para solucionar este problema, se han propuesto diversos algoritmos para el cifrado de imágenes, una de estas propuestas son los algoritmos basados en caos, con los cuales se emplean diversos métodos que permiten crear valores impredecibles con los que posteriormente se puede cifrar la imagen [4].

Investigaciones más recientes han propuesto un sistema para el cifrado de imágenes basado en las reglas de operación del ADN junto a Secure Hash Algorithm-512 (SHA-512) que permite generar un valor hash de 512 bits que permiten generar los valores iniciales para un sistema caótico [7].

Uno de los criptosistemas más empleados de llave pública es RSA nombrado así por sus creadores Rivest, Shamir y Adleman. La seguridad de RSA reside en su complejidad computacional para factorizar números grandes, en la actualidad estos números primos deben de ser de un factor de  $10^{300}$ . Hoy en día este problema puede considerarse computacionalmente imposible, debido a que la forma más simple de encontrar los factores (números primos) de un número dado, consiste en ir dividiendo entre todos los números primos inferiores al número dado, lo cual es lento al tratarse de números grandes, no es señal de que en el futuro no pueda resolverse en cuestión de segundos [8].

Otro criptosistema de llave pública ocupado es ElGamal, la seguridad de este sistema está basado en el problema del logaritmo discreto, el cual no puede encontrarse en un tiempo práctico, mientras que su operación inversa (la potenciación) puede realizarse de forma eficiente usando valores como mínimo de  $10^{150}$  para los valores de  $p$  y  $q$  [9].

Otra ventaja que este criptosistema ofrece es la firma de mensajes electrónicos, lo que permite al que recibe el mensaje verificar que este proviene de la persona correcta, aunque no garantiza que esa persona fue la que lo escribió o si era su intención enviar el mensaje, además de que con la firma el receptor puede verificar que el mensaje no fue alterado en la transmisión [9].

Una forma de corroborar la eficiencia de estos algoritmos es mediante la entropía de Shannon Ecuación 1, que es una medición que permite obtener información sobre la incertidumbre de la información, una imagen a color está conformada por tres canales (rojo, verde, azul) con 256 niveles de profundidad, por cada uno, por lo que si se desea que los colores tengan una distribución uniforme se busca un valor de entropía por canal de 8, en trabajos basados en ADN se obtienen valores cercanos a 7.997, y algoritmos donde se emplea el caos tienen valores de 7.999 [4], [7].

$$H(x) = - \sum_{x \in X} P(x) \log_2 P(x)$$

### *Ecuación 1*

Otro método empleado es el coeficiente de correlación entre los píxeles, este método nos indica cuanto se relacionan dos píxeles adyacentes dentro de una imagen, por lo que se buscan valores cercanos a cero indicando que una vez se ha cifrado la imagen no hay forma de ver su contenido, dependiendo del método empleado se obtienen valores entre -0.002 y 0.006 [4], [7].

## **2. Objetivo**

Desarrollar un criptosistema simétrico de doce rondas para el cifrado de imágenes basado en el criptosistema ElGamal y el número Pi que permita realizar permutaciones dinámicas del tamaño de la imagen obteniendo valores de entropía cercanos a un valor de 8.

### **2.1. Objetivos específicos**

- Programar un algoritmo de permutación dinámica para permitir el cifrado de imágenes.
- Programar un algoritmo para generar las llaves que utilice los dígitos del número Pi.
- Programar un algoritmo que permita propagar las llaves a partir de ElGamal
- Programar un criptosistema basado en ElGamal para el cifrado de imágenes.
- El criptosistema debe de ser capaz de cifrar cualquier tipo de imagen bitmap
- La entropía de una imagen cifrada debe ser cercana a ocho.
- La correlación de una imagen cifrada debe ser cercana a cero.

## **3. Justificación**

Como se mencionó previamente, en la actualidad compartir información por medios digitales, donde las imágenes juegan un papel importante dentro de la información que se comparte, y que en ocasiones puede contener información sensible que se desea mantener de forma confidencial y privada a terceros, donde el mayor problema radica en el intercambio de la llave privada.

Como otra solución a este problema, se propone crear un criptosistema simétrico que tiene la misma seguridad que propuestas anteriores, para conseguir esto, se emplearan las bases del criptosistema ElGamal para la generación y propagación de las llaves que se emplearan al momento de cifrado en cada ronda con la ayuda del número Pi.

El numero Pi es un numero transcendental, por lo que los dígitos a la derecha del punto decimal no siguen ningún patrón conocido, además de que no son raíz de la Ecuación 2 [4].

$$a_0 + a_1x + a_2x^2 + \dots + a_nx^n = 0$$

### *Ecuación 2*

Gracias a estas propiedades, un número transcendental es muy importante cuando lo que se requiere es combinar información para que no exista ninguna relación entre los datos cifrados, consiguiendo valores de entropía cercanos a ocho y un nivel de correlación similar a cero.

Para conseguir estos valores durante el cifrado de doce rondas se empleará una caja de sustitución diferente a las existentes en algoritmos como el criptosistema AES, con este cambio, los algoritmos empleados y el tiempo de ejecución serán distintos a los que existen actualmente, la seguridad obtenida será igual o mejor.

Otra ventaja que esta solución presenta esta alternativa frente a un criptosistema simétrico tradicional es la posibilidad de propagar las llaves que se emplearan para cifrar la imagen, a su vez al ser una adaptación de el criptosistema ElGamal, el algoritmo para generar los números primos difiere del tradicional con el propósito de que este algoritmo pueda realizarse de forma paralela y aumentar la rapidez de ejecución, para conseguir esto se buscara una forma en la cual no sea necesario encontrar el inverso multiplicativo de un número y por consiguiente no realizar el algoritmo de Arquímedes extendido.

A su vez una posible ventaja que se obtiene de este criptosistema es que no solo se mantendrá el contenido de las imágenes oculto a las personas que no estén autorizadas, si no que se conservará toda la información al manejarse imágenes bitmap, puesto que no cuentan con un algoritmo de compresión como otros formatos de imagen.

Como consecuencia de esto, no solo se mantiene el contenido de las imágenes oculto a personas no autorizadas durante el intercambio de la información, si no que, además, se consigue un método seguro para el intercambio de la llave privada dentro de un criptosistema simétrico.

#### **4. Productos o Resultados esperados**

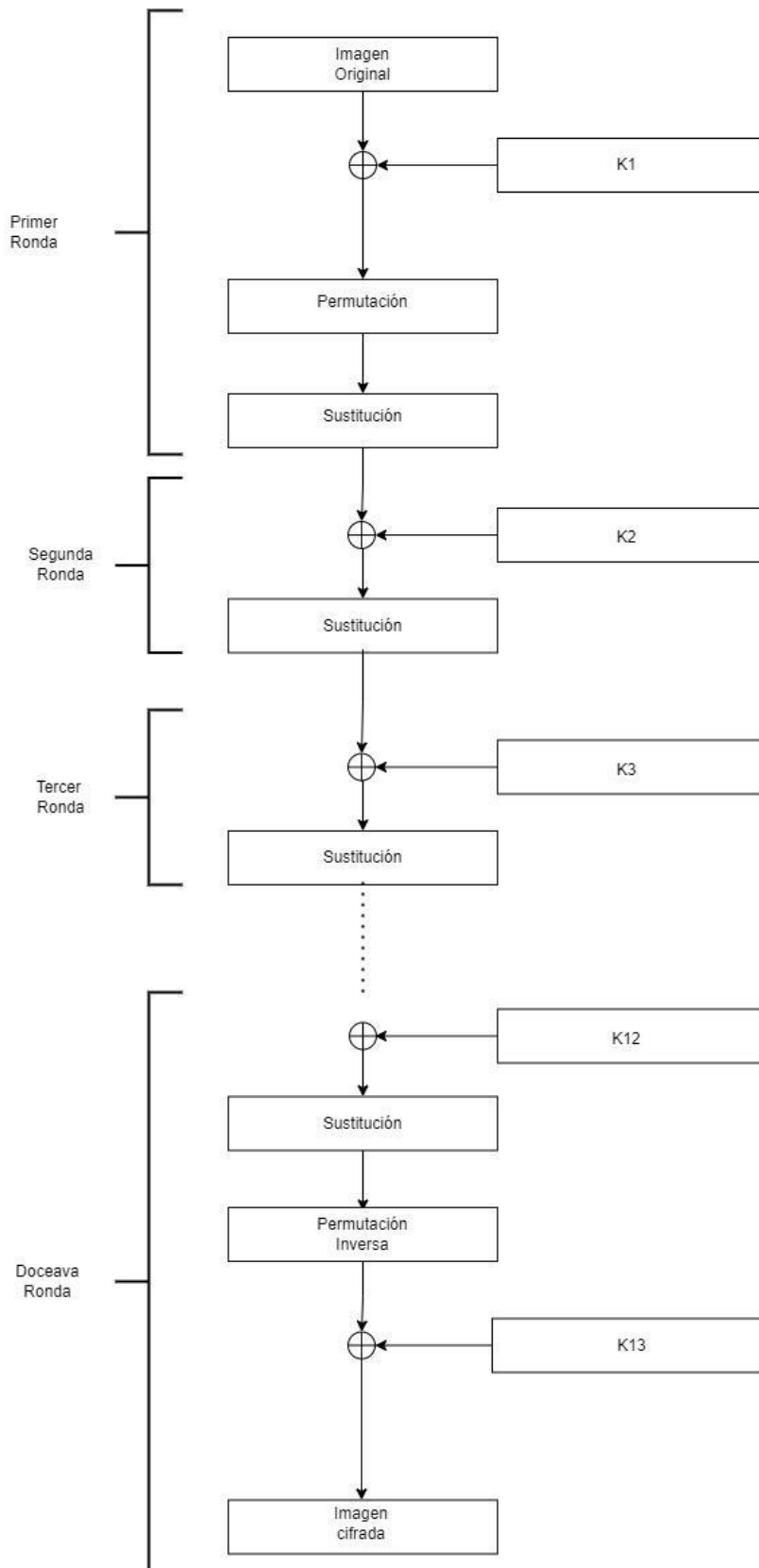
Se realizará un criptosistema simétrico de doce rondas para cifrar imágenes tanto a color como blanco y negro empleando un cifrado de doce rondas como se muestra en la Ilustración 1, en cada ronda se empleará una llave ( $k$ ) que se formará a partir del número Pi y una semilla aleatoria.

Durante este proceso se requieren realizar permutaciones para alterar la imagen original e incrementar el nivel de entropía al momento de cifrado, para conseguir este objetivo se realizará una implementación del Teorema JV, junto a una caja de sustitución diferente a la empleada en el criptosistema AES que se obtiene por medio del caos. Con esto se espera conseguir un nivel de entropía cercano a 8 como en propuestas anteriores donde el contenido original no sea distinguible en la imagen cifrada.

Una parte crucial de un criptosistema es mantener la llave privada oculta a personas ajenas al sistema, para solucionar esto, se implementará un algoritmo para el intercambio de llaves tomando como base el que se emplea en el criptosistema ElGamal.

Se busca entregar los siguientes resultados dentro de una aplicación de escritorio para el cifrado de imágenes.

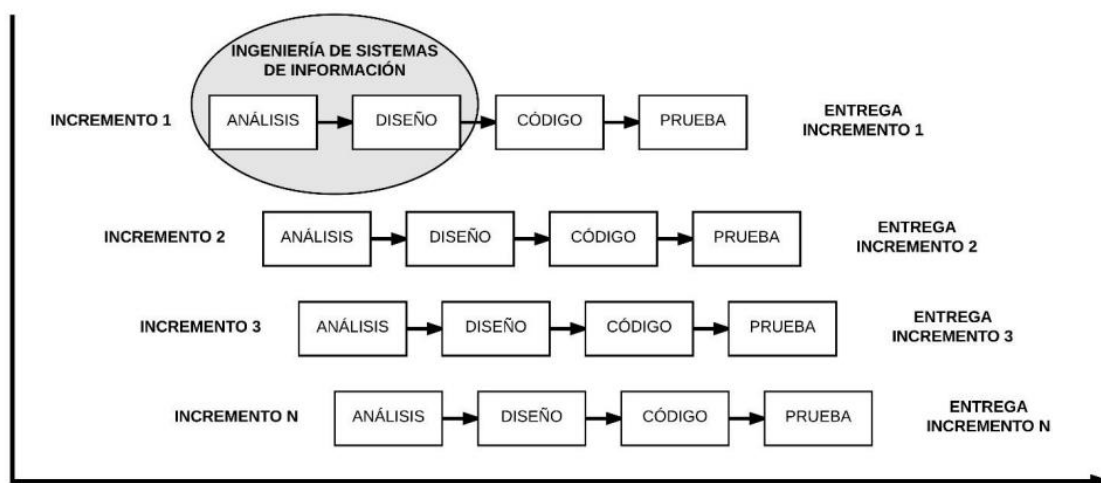
- Algoritmo de permutación dinámica
- Algoritmo para generar llaves
- Algoritmo para la distribución de llaves
- Algoritmo de cifrado
- Aplicación de escritorio para el cifrado de imágenes
- Documentación técnica
- Manual técnico
- Manual de usuario
- Documento de pruebas comprobando la correlación y entropía del sistema.



*Ilustración 1 Bloques de cifrado*

## 5. Metodología

La metodología incremental orientada a objetos combina una forma secuencial e iterativa a través de prototipos funcionales o incrementos. El primer incremento que se obtiene contiene los elementos básicos del proyecto, continuando con los demás incrementos que mejoran la funcionalidad priorizando los requerimientos importantes, esta metodología se representa en la Ilustración 2 [10].



*Ilustración 2. Esquema del modelo incremental (Pressman)*

Siguiendo esta metodología, se planea realizar cuatro entregas, en cada entrega se realizará el análisis de requerimientos, diseño, implementación y pruebas necesarias para su correcto funcionamiento. Los incrementos que se planea tener son: algoritmo de permutación dinámica (entrega 1), algoritmo para generar llaves (entrega 2), algoritmo para la propagación de llaves (entrega 3), y aplicación de escritorio para el cifrado de imágenes que junta los incrementos anteriores para crear el algoritmo de cifrado (entrega 4).

## 6. Cronograma

## 7. Bibliografía

- [1] A. Moatsum, S. Azman, T. Je Sen y R. S. Alkhawaldeh, «A new hybrid digital chaotic system with applications in image,» *Signal Processing*, vol. 160, pp. 45-58, 2019.
- [2] A. M. Qadir y N. Varol, «A Review Paper on Cryptograph,» *International Symposium on Digital Forensics and Security (ISDFS)*, vol. 7, 2019.
- [3] D. Liestyowati, «Public Key Cryptography,» *Journal of Physics: Conference Series*, 2020.
- [4] V. M. SILVA GARCÍA, M. D. GONZÁLEZ RAMÍREZ, R. FLORES CARAPIA, E. VEGA ALVARADO y E. RODRÍGUEZ ESCOBAR, «A Novel Method for Image Encryption Based on Chaos and Transcendental Numbers,» *IEEE Access*, vol. PP, pp. 1-1, 2019.
- [5] R. Gonzalez, *Digital image processing*, New York, NY: Pearson, 2018.
- [6] C. S. X. X. y. X. M. H. Linqing, «On symmetric color image encryption system with permutation-diffusion simultaneous operation,» *Optics and Lasers in Engineering*, vol. 115, pp. 7-20, 2019.
- [7] Z. Shihua, H. Pinyan y K. Nikola , «A Dynamic DNA Color Image Encryption Method Based on SHA-512,» *Entropy*, 2020.
- [8] D. Lerch Hostalot, «Ataque de factorización a RSA».
- [9] A. V. Meier, «The ElGamal Cryptosystem,» 8 Junio 2008.
- [10] R. S. Pressman, *Ingeniería del software un enfoque practico*, Mc Graw Hill.

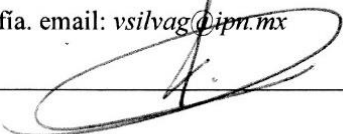
## 8. Alumnos y directores

ESCOM, Especialidad Sistemas, Boleta:  
2016630302, Tel. 5530826974, email  
*rperez11501@alumno.ipn.mx*

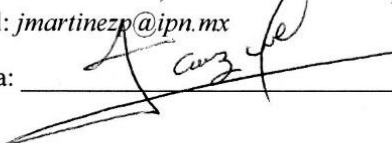
CARÁCTER: Confidencial  
FUNDAMENTO LEGAL: Artículo 11 Fracc. V y Artículos  
108, 113 y 117 de la Ley Federal de Transparencia y Acceso  
a la Información Pública.  
PARTES CONFIDENCIALES: Número de boleta y teléfono.

Firma:  \_\_\_\_\_

Víctor Manuel Silva García. Profesor de  
CIDETEC del IPN, Doctorado en ciencias de la  
computación, miembro del Sistema Nacional de  
Investigadores, Coordinador de la Red de  
Seguridad del CIDETEC, miembro de la Sociedad  
Matemática Mexicana, ORCID  
0000-0008-1312-5294 Área de interés:  
Criptografía. email: *vsilvag@ipn.mx*

Firma:  \_\_\_\_\_

José Cruz Martínez Perales. Profesor de ESCOM  
del IPN. Maestro en Administración de Negocios,  
egresado de UPIICSA en la licenciatura en  
Administración Industrial. Área de interés:  
autómatas celulares, reconocimiento de patrones.  
email: *jmartinezp@ipn.mx*

Firma:  \_\_\_\_\_



CRONOGRAMA: PÉREZ LEAL RODOLFO

Sistema simétrico para el cifrado de imágenes utilizando El Gamal y el número Pi

Actividad	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Enero	Febrero	Marzo	Abril	Mayo	Junio
Investigación acerca del algoritmo de permutación dinámica.											
Análisis y diseño de requerimientos necesarios en el algoritmo de permutación dinámica											
Desarrollo y pruebas del algoritmo de permutación dinámica											
Investigación relacionada al algoritmo para generación de llaves											
Análisis, diseño de requerimientos necesarios en el Algoritmo para generación de llaves											
Desarrollo y pruebas del Algoritmo para generación de llaves											
Evaluación de TT I											
Investigación relacionada al algoritmo para la propagación de llaves											

Análisis y diseño de requerimientos para el algoritmo de propagación de llaves											
Desarrollo y pruebas del algoritmo de propagación de llaves											
Análisis y diseño de requerimientos para el algoritmo de cifrado											
Desarrollo del algoritmo de cifrado juntando los entregables anteriores.											
Pruebas del algoritmo de cifrado											
Elaboración de documentación técnica.											
Evaluación de TT II											