Instituto Politécnico Nacional

Centro de Innovación y Desarrollo Tecnológico en Cómputo

Protocolo Diffie Hellman utilizando los criptosistemas ElGamal y AES

Tesis

Que para obtener el grado de

Maestría en Tecnología de Cómputo

Presenta:

Edgar Misael Islas Mendoza

Directores:

Dr. Víctor Manuel Silva García

Dra. Hind Taud

2013

SIP-14-BIS

INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

ACTA DE REVISIÓN DE TESIS

En la Ciudad de México, D.F. siendo las 17:00 horas del día 30 del mes de mayo del 2013 se reunieron los miembros de la Comisión Revisora de la Tesis, designada por el Colegio de Profesores de Estudios de Posgrado e Investigación del CIDETEC para examinar la tesis titulada:

"PROTOCOLO DIFFIE HELLMAN UTILIZANDO LOS CRIPTOSISTEMAS ELGAMAL Y AES"

Presentada por el alumno:

ISLAS	MENDOZA	EDGAR MISAEL
Apellido paterno	Apellido materno	Nombre(s)

Con registro:

B	1	1	0	9	4	2

aspirante de:

Maestría en Tecnología de Cómputo

Después de intercambiar opiniones los miembros de la Comisión manifestaron ***APROBAR LA TESIS***, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISIÓN REVISORA

Directores de tesis

DR. VÍCTOR MANUEL SILVA GARCÍA
Primer Vocal

DRA. HIND TAUD
Segundo Vocal

DR. ROLANDO FLORES CARAPIA
Presidente

M. EN C. EDUARDO RODRÍGUEZ ESCOBAR
Secretario

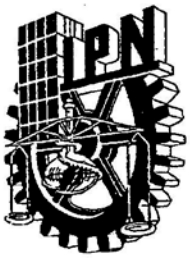
DR. CARLOS BENTERÍA MÁRQUEZ
Tercer Vocal

M. EN C. JUAN CARLOS GONZÁLEZ ROBLES
Suplente

PRESIDENTE DEL COLEGIO DE PROFESORES

DR. OSCAR CAMACHO NIETO

S. E. P.
INSTITUTO POLITECNICO NACIONAL
CENTRO DE INNOVACION Y DESARROLLO TECNOLOGICO EN COMPUTO



INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

CARTA CESIÓN DE DERECHOS

En la Ciudad de México el día 11 del mes de junio del año 2013, el que suscribe Edgar Misael Islas Mendoza alumno del Programa de Maestría en Tecnología de Cómputo con número de registro B110942, adscrito al Centro de Innovación y Desarrollo Tecnológico en Cómputo, manifiesta que es autor intelectual del presente trabajo de Tesis bajo la dirección del Dr. Víctor Manuel Silva García y la Dra. Hind Taud y cede los derechos del trabajo intitulado **Protocolo Diffie - Hellman utilizando los criptosistemas Elgamal y AES**, al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso del autor y/o director del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección emim.88@hotmail.com. Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

Edgar Misael Islas Mendoza

Resumen

En el presente trabajo se diseña un esquema de comunicación de mensajería segura a través de redes de área local (LAN).

Este esquema implementa un criptosistema híbrido el cual se encuentra constituido por AES-256 en su parte simétrica y es utilizado para el cifrado de los mensajes; en la parte asimétrica, se utiliza a ElGamal para el cifrado de las claves donde el primo consta de 400 dígitos y el primitivo alfa de 200 dígitos. Asimismo se aplica el protocolo Diffie - Hellman para la distribución segura de las claves.

Esta implementación está dirigida a los miembros de alta gerencia o grupos de confianza de algún corporativo donde el número de usuarios es reducido, esto es, menor a 15 participantes. Sin embargo, el sistema soporta más usuarios pero éste empezaría a retardar el tiempo de respuesta del sistema por la distribución de las claves entre los usuarios; ya que dicha distribución de claves requiere un número de rondas igual al número de usuarios menos uno.

Abstract

In the present work, a secure messenger communication scheme is designed through local area networks (LAN).

This scheme implements an hybrid cryptosystem, which is constituted for AES-256 in its symmetrical part and is used for the messages encryption; in the asymmetric part ElGamal is used for the keys encryption where the prime number consists of 400 digits y the alfa primitive of 200 digits. Also the protocol Diffie- Hellman is applied for the secure keys distribution.

This implementation is directed to the senior management members or confidence personnel of some corporation where the users number is reduced, this means, less than 15 participants. However, the system supports more users, but this would start to delay the reply time system because of the keys distribution among the users; since this keys distribution requires a number of rounds equal to the users number less one.

Agradecimientos

A mi madre:

Por su tenacidad e ilusión de verme desarrollar profesionalmente y porque seguimos recogiendo los frutos de una herencia invaluable como lo es el estudio.

A mi hermano:

No quiero ser su ejemplo, pero si quisiera que siguiera este camino...

A mi novia:

Por todo su apoyo y porque compartimos adversidades y malos ratos pero también dicha, felicidad y mucho amor.

A mis directores de tesis:

Dr. Víctor Manuel Silva García y Dra. Hind Taud, por todo lo que aportaron para la realización de este trabajo con su conocimiento y enseñanza, agradeciendo también su valioso tiempo y paciencia que siempre tuvieron para conmigo.

Al comité revisor:

Dr. Rolando Flores Carapia, Dr. Carlos Rentería Márquez, M. en C. Eduardo Rodríguez Escobar y M. en C. Juan Carlos González Robles, cuyo conocimiento y aportaciones contribuyeron a consolidar este trabajo.

A mis amigos:

Porque sé que puedo contar con ustedes y que no los nombro porque saben perfectamente quiénes son...

Glosario

Autenticación: La autenticación garantiza que la identidad del creador del mensaje es legítima; es decir, con esta función el destinatario de un mensaje podrá estar seguro que su creador es la persona que figura como remitente de dicho mensaje.

Autoría: Condición de autor o persona que generó el mensaje.

Clase: Una clase es una construcción que se utiliza como un modelo o plantilla para crear objetos de ese mismo tipo.

Compatibilidad: Es la capacidad que tienen dos sistemas de trabajar uno con otro simultáneamente.

Confidencialidad: La confidencialidad garantiza que cada mensaje transmitido o almacenado en un sistema informático solo podrá ser leído por su legítimo destinatario.

Criptograma: También conocido como texto cifrado. Es el texto que ha sido transformado mediante alguna técnica criptográfica. Este texto resulta ilegible a no ser que se conozca la llave para volver a recuperar el "texto plano" original.

Criptosistema asimétrico: También conocido como criptosistema de clave pública. Utilizan dos claves diferentes, de las cuales una conocida como la clave pública es la que se emplea para el cifrado de la información y la otra conocida como clave privada y esta se emplea para realizar el descifrado de dicha información.

Criptosistema híbrido: Sistema criptográfico basado tanto en criptografía asimétrica como simétrica.

Criptosistema simétrico: También conocido como criptosistema de clave secreta. Utilizan la misma clave tanto para cifrar como descifrar la información.

Desencriptar o descifrar: Es el proceso que recupera el texto plano de un criptograma.

Dirección IP: Serie de números asociados a un dispositivo (generalmente una computadora), con la cual es posible identificarlo dentro de una red configurada específicamente para utilizar este tipo de direcciones.

Encriptar o cifrar: Es el proceso que transforma un texto plano en un criptograma.

Firma digital: Es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente determinar la entidad que lo originó.

GUI: "*Graphical User Interface*" interfaz grafica de usuario, es un programa informático que actúa de interfaz de usuario, utilizando un conjunto de imágenes y objetos gráficos para representar la información y acciones disponibles en la interfaz. Su principal uso, consiste en proporcionar un entorno visual sencillo para permitir la comunicación con el sistema operativo de una máquina o computador.

GPG: Herramienta de cifrado y firmas digitales, el cual es software libre licenciado bajo GPL.

GPL: *"GNU General Public License"*, es la licencia más ampliamente usada en el mundo del software y garantiza a los usuarios finales la libertad de usar, estudiar, compartir y modificar el software.

Hacker: Persona muy aficionada y hábil en informática que entra ilegalmente en sistemas y redes ajenas.

IDE: "I*ntegrated Development Environment*", en español Entorno de Desarrollo Integrado. Es un programa compuesto por un conjunto de herramientas de programación, el cual puede dedicarse únicamente a un solo lenguaje de programación o bien puede utilizarse para varios.

Integridad: La integridad se encarga de garantizar que un mensaje no ha sido modificado desde su creación o durante su transmisión a través de una red informática. De este modo es posible detectar si se ha añadido o eliminado algún dato en un mensaje almacenado, procesado o transmitido por un sistema o red informática.

Java: Lenguaje de programación orientado a objetos, el cual fue desarrollado por James Gosling y sus compañeros de Sun Microsystems al principio de la década de los 90´s.

LAN: *"Local Area Network"*, es la interconexión de varias computadoras y periféricos con la finalidad de comunicarse entre sí y compartir recursos.

Nick: Abreviatura utilizada en Internet, del inglés "*nickname*" ó en español "alias", el cual es nombre de fantasía o verídico que puede utilizar una persona.

No repudio: El no repudio consiste en implementar un mecanismo probatorio que permita demostrar la autoría y envió de un determinado mensaje, de tal modo que el

usuario que lo ha creado y enviado a través del sistema no pueda negar esta circunstancia; situación que también se aplica al destinatario.

PGP: *"Pretty Good Privacy"*, es un programa desarrollado en 1991 por Phil Zimmermann basado en criptografía de clave pública y firmas digitales.

Sistema Operativo: Conjunto de programas que gestiona los recursos de hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los restantes

Socket: Es el mecanismo por el cual dos programas pueden intercambiar cualquier flujo de datos, generalmente de manera fiable y ordenada.

Texto plano: También conocido como texto claro. Es el texto que queremos proteger mediante el uso de técnicas criptográficas.

Índice

Índice de figuras

Índice de tablas

Capítulo I: Introducción

Este trabajo implementa un criptosistema híbrido, el cual tiene como objeto el intercambio seguro de claves bajo el protocolo Diffie - Hellman, cifrando la clave pública con el criptosistema asimétrico ElGamal con la finalidad de compartir una sola clave para el cifrado de los mensajes mediante el criptosistema simétrico AES-256.

En los siguientes apartados de este capítulo, entre otros rubros se describirán los métodos de cifrado o encriptación, tales como:

- Criptografía simétrica.
- Criptografía asimétrica.
- Criptografía híbrida

Iniciando con un panorama general sobre lo que es la criptografía, tipos de criptografía y asimismo una breve descripción de los tipos de descripción.

I.1. Que es la criptografía

La criptografía proviene del griego "krypto", (oculto) y "graphos", (escribir), literalmente "escritura oculta"[1] y es parte de la criptología, la cual utiliza algoritmos que alteran las representaciones lingüísticas de los mensajes mediante el cifrado, con la finalidad de proteger información para evitar que sea accesible por observadores no autorizados, proteger datos, pero también poseen características tales como:

- Autenticación
- Confidencialidad
- Integridad
- No repudio

El mensaje que queremos enviar es llamado "texto plano" o "texto claro" y el mensaje cifrado se le denomina "criptograma" o "texto cifrado". Es decir, el proceso de convertir un texto plano a un texto cifrado se le denomina cifrado y el proceso inverso es llamado descifrado[2][3].

I.2. Tipos de criptosistemas
I.2.1. Criptosistema Simétrico

La criptografía simétrica o también conocida como sistemas criptográficos (criptosistemas) de clave secreta, utilizan una única clave secreta para cifrar y descifrar datos. Las claves simétricas pueden ser útiles en aplicaciones como el cifrado de archivos en el disco duro, cuando la misma persona es la que cifra y descifra los datos[4].

Debido a esto la clave secreta se debe de intercambiar por medio de un canal seguro. La siguiente figura muestra un esquema de comunicación por un sistema criptográfico simétrico.

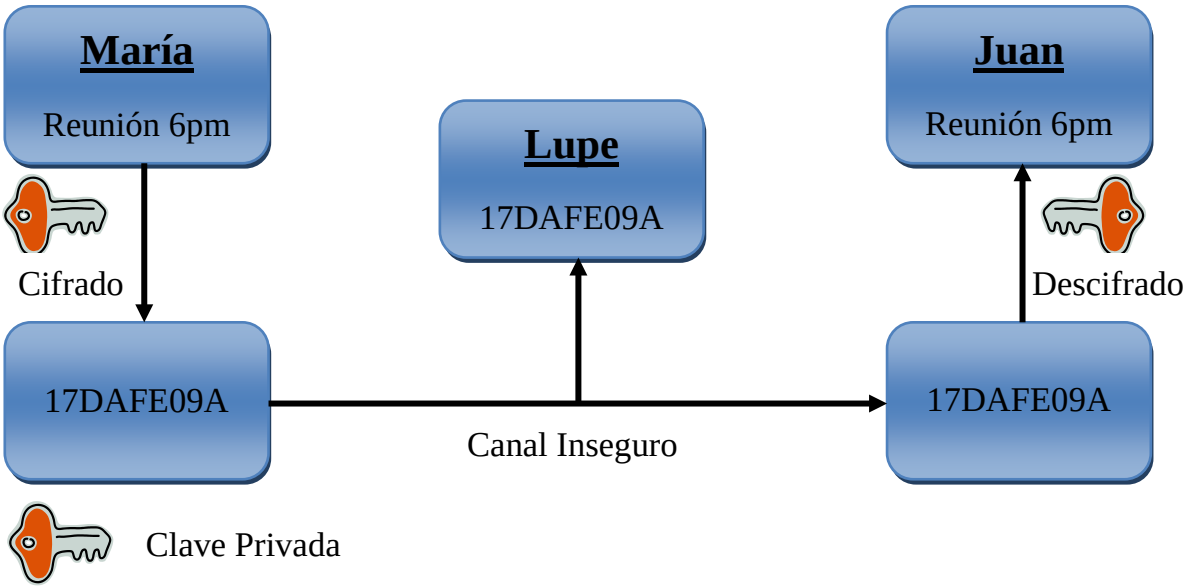


Figura 1.- Esquema de sistema criptográfico simétrico.

Los algoritmos de cifrado simétrico de las normas son:

- DES, publicado por FIPS (Federal Information Processing Standards Publications) en los Estados Unidos en 1976[5].
- 3DES, desarrollado por IBM en 1998.
- AES, publicado por FIPS el 26 de noviembre de 2001[6].

I.2.2. Criptografía Asimétrica

La criptografía asimétrica o también conocida como sistemas criptográficos de clave pública utilizan dos claves diferentes para comunicarse. De las cuales una se le conoce como clave pública y se emplea para el cifrado de la información; mientras que la otra es conocida como clave privada y esta es utilizada para realizar el descifrado de dicha información[4].

La siguiente figura muestra un esquema de comunicación por un criptosistema asimétrica.

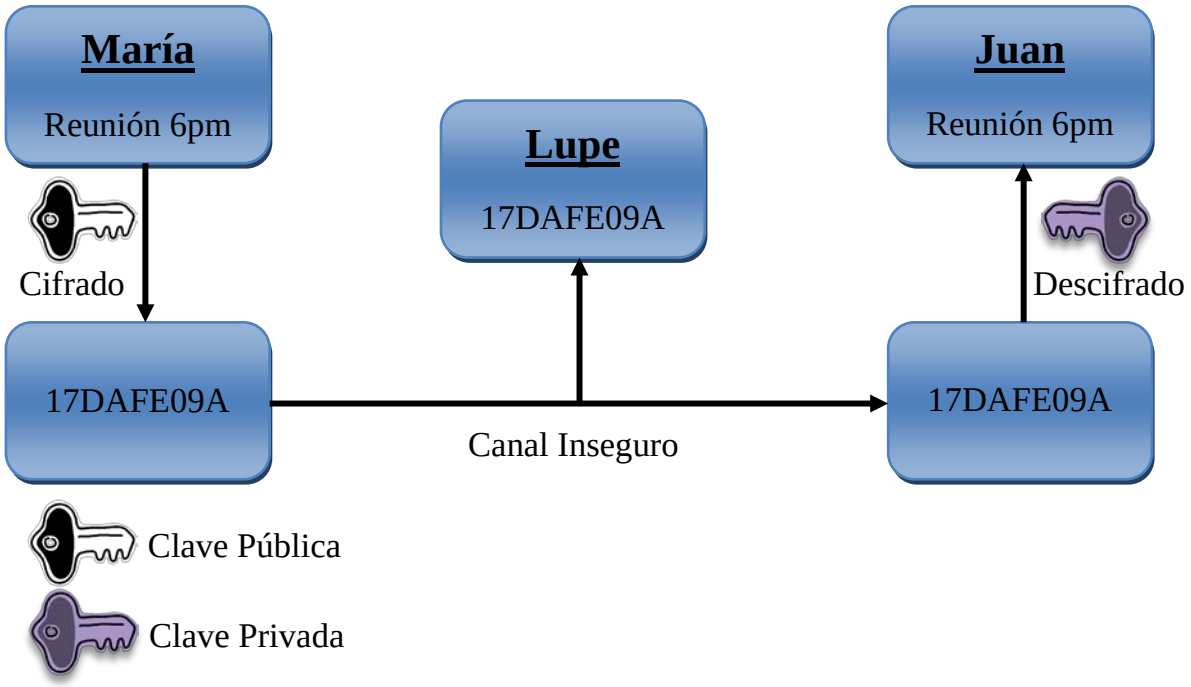


Figura 2.- Esquema de sistema criptográfico asimétrico.

Los algoritmos de cifrado asimétrico más conocidos son:

- RSA, desarrollado en 1977 en el MIT (Massachusetts Institute of Technology)[7].
- ElGamal, desarrollado en 1985[8].
- ECC, propuesto en 1985 por Víctor S. Miller[9].

I.2.3. Criptografía Híbrida

Este tipo de criptografía está basada tanto en criptografía asimétrica como simétrica[4], donde en la idea principal es juntar las fortalezas tanto de la criptografía simétrica como de la asimétrica. La criptografía asimétrica tiende a ser muy lenta en su cifrado; sin embargo, resulta ser mucho más segura en comparación que la criptografía simétrica. Por otro lado, la criptografía simétrica es muy rápida en su cifrado pero su debilidad recae en el momento de compartir la clave de cifrado, ya que con la misma clave se cifra y descifra la información.

En un sistema híbrido, un cifrado asimétrico se utiliza para el intercambio de una clave privada (también llamado una clave de sesión o la clave secreta). La clave secreta se utiliza con un algoritmo de cifrado simétrico para el cifrado y descifrado de la información[4], tal como se muestra en la siguiente figura:

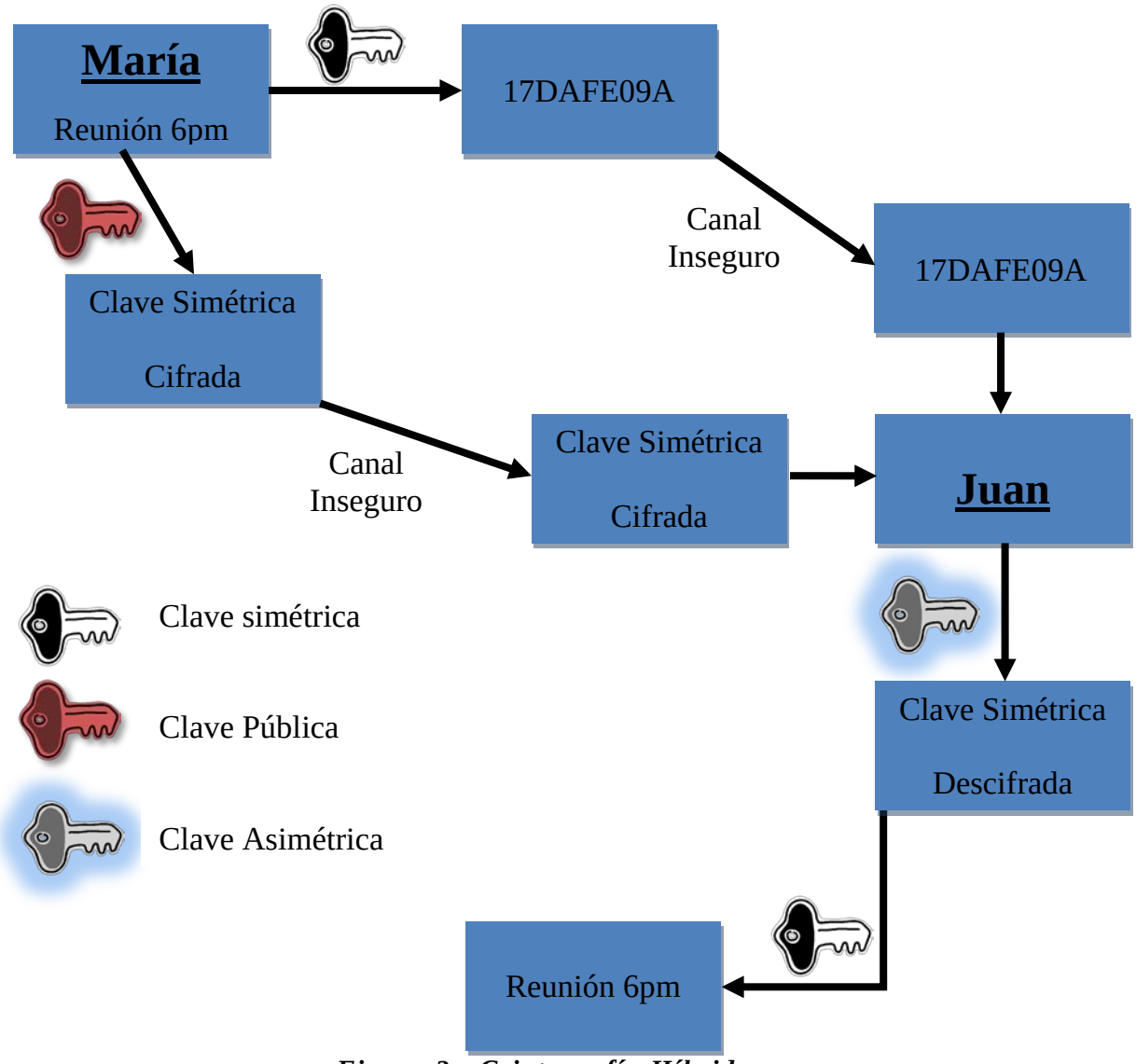


Figura 3.- Criptografía Híbrida.

I.2.4. Esteganografía

Aunque esta tesis no trata sobre esteganografía, cabe mencionar que esta es la otra rama de la criptología, la cual consiste en ocultar la información a simple vista, siendo contenida en otro tipo de información denominada portador[10].

Por ejemplo, en un archivo gráfico utilizar el bit menos significativo del color de todos puntos de la imagen para transmitir una información. Alguien que vea la imagen no se dará cuenta de nada, ya que el cambio que se produce en la imagen no es significativo, como el ejemplo que se presenta en la siguiente figura:

Figura 4.- Esteganografía.

I.3. Que es el criptoanálisis

El objeto del criptoanálisis es la búsqueda de las claves de un sistema criptográfico, a partir del conocimiento de textos cifrados, textos planos antiguos y el conocimiento de los algoritmos y/o estándares de encriptación que componen al sistema.

Cuando un método de criptoanálisis permite descifrar un mensaje cifrado mediante el uso de algún criptosistema, se dice que el algoritmo de cifrado ha sido decodificado[11].

En los siguientes puntos de este apartado se explican las diferentes formas de atacar un sistema criptográfico.

I.4. Tipos de criptoanálisis

I.4.1. Ataque de fuerza bruta

Este tipo de ataque consiste en probar todas las llaves posibles con la finalidad de obtener el texto plano.

Si el conjunto de llaves posibles es muy elevado, este tipo de ataque resulta ser inútil.

En otras bibliografías a este tipo de ataques no se les suele considerar como un tipo de criptoanálisis, esto debido a que no busca puntos débiles en el sistema criptográfico y únicamente utiliza todas las llaves posibles.

I.4.2. Ataque de texto plano escogido

Este ataque radica en la selección de varios textos planos y obtener sus criptogramas asociados. Para poder realizar este tipo de ataque se debe tener acceso al sistema criptográfico, pero no a la clave de cifrado[11].

I.4.3. Ataque a partir de texto plano

Para este tipo de criptoanálisis el atacante tiene acceso a textos planos con sus respectivos criptogramas o textos cifrados[11].

En el capítulo II se presenta el estado del arte, el cual brinda una reseña de lo que se ha hecho hasta hoy en día sobre implementaciones de criptosistemas híbridos, similares con lo que se presenta en este trabajo, así como el problema que aborda y el esquema que se implementa como solución a este.

Capítulo II: Estado del Arte

Para el desarrollo de este apartado se tomaron cuatro trabajos relacionados a los temas que se manejan en esta tesis. Uno de ellos trata sobre el algoritmo de cifrado asimétrico ElGamal, dos sobre el algoritmo de cifrado simétrico AES y uno acerca del protocolo para intercambio de claves "Diffie - Hellman". Dichos trabajos sirvieron para abrir un panorama de lo que se ha realizado con estos algoritmos.

El trabajo titulado: "Análisis del cifrado ElGamal de un módulo con curvas elípticas propuesto para el GnuPG"[12] hace cuatro propuestas para incrementar el nivel de seguridad de un software de cifrado de licencia libre. Estas propuestas consisten en la incorporación de un criptosistema híbrido, el cual utiliza a ElGamal y la Curva Elíptica como base para sus diferentes propuestas.

Las propuestas que este trabajo plantea y analiza son las siguientes:

1. El cifrado de ElGamal como único algoritmo de cifrado.
2. El cifrado por curva elíptica y el cifrado ElGamal.
3. El cifrado por curva elíptica, Diffie Hellman y ElGamal.
4. El cifrado por curva elíptica, Diffie Hellman y AES-256.

El trabajo concluye que la implementación del algoritmo híbrido donde emplea AES tiene una gran ventaja, ya que es el que posee más fortaleza actualmente.

El trabajo titulado: "White-Box Cryptography and an AES Implementation"[13] realiza una demostración donde implementa el algoritmo de cifrado simétrico AES ocultando la clave de cifrado mediante una combinación de cifrado de las tablas con biyecciones al azar con el cual logra composiciones en lugar de pasos individuales en el proceso de cifrado, logrando así una implementación más segura.

En el trabajo titulado como: "A Modified AES Based Algorithm for Image Encryption"[14] analiza e implementa el algoritmo de cifrado AES y le añade un generador de flujo de claves (A5/1), con esto logra una mejora en el rendimiento del cifrado; sin embargo, esta implementación se realiza de forma experimental.

Por último, el trabajo titulado: "Diffie-Hellman Key Exchange Protocol, Its Generalization and Nilpotent Groups"[15] es una tesis que se divide en dos capítulos. El primer capítulo se centra en un análisis del estado actual de la seguridad para el protocolo Diffie Hellman. El segundo capítulo hace un análisis sobre dos protocolos de intercambio de claves similares a Diffie Hellman, los cuales emplean automorfismos para generar el intercambio de las claves.

Con el estudio de estos trabajos se obtuvo una visión de lo que se ha realizado con los algoritmos de cifrado ElGamal, AES y el protocolo Diffie Hellman, los cuales se pretenden implementar en esta tesis con el enfoque de una comunicación segura a través de redes locales, a diferencia de los trabajos vistos en este apartado, los cuales se enfocan en propuestas de mejora de herramientas ya desarrolladas y otros en modificaciones en cada algoritmo.

II.1. Planteamiento del problema

La tecnología en redes de comunicación de área local se ha ido incrementando con el paso de los años y es por ello que ha crecido la necesidad de tener esquemas de seguridad que protejan la información que se transmite a través de estas redes y más aún en un contexto de negocios, ya que estas proporcionan un intercambio rápido y oportuno de información.

Sin embargo, las redes se encuentran obstaculizadas por la inseguridad de ser accedidas sin autorización, la señal puede ser interceptada y los mensajes ser alterados, si la señal resulta hackeada. Debido a esto no se puede tener una comunicación segura. Donde la implementación de una solución basada en criptografía simétrica resultaría vulnerable porque su debilidad recae en el intercambio de la clave secreta y una implementación basada en criptografía asimétrica resultaría muy lento el tiempo de cifrado, lo cual no resulta cómodo para el usuario.

II.2. Propuesta de solución

Se propone desarrollar una aplicación basada por un criptosistema híbrido conformado por ElGamal y AES para la transmisión de mensajes de texto a través de redes locales, incluyendo el protocolo Diffie Hellman para una distribución segura de claves.

II.3. Objetivos

II.3.1. Objetivo general

Implementar una herramienta que permita una comunicación segura para la transmisión de mensajes de texto a través de redes de área local mediante un esquema de criptografía híbrida, asimismo que proporcione un intercambio seguro de la claves.

II.3.2. Objetivos particulares

1. Implementar el criptosistema asimétrico ElGamal para el cifrado de las claves

2. Implementar el criptosistema simétrico AES para el cifrado de los mensajes de texto

3. Implementar el protocolo Diffie-Hellman para distribuir las claves

4. Integrar los criptosistema en una solución

II.4. Justificación

Las redes de área local poseen grandes ventajas como el permitir la comunicación entre diversas áreas de una empresa u organización. Sin embargo; las redes locales tienen el problema de la inseguridad debido a que si son accedidas sin autorización, los mensajes pueden ser interceptados y/o alterados por hackers. Debido a esto, en la comunicación entre dos o más personas es necesario que un mensaje se cifre para obtener un intercambio seguro de información.

Por otra parte, se propone este esquema basado en criptografía híbrida ya que con éste se pretende juntar las fortalezas de la criptografía simétrica así como de la asimétrica, cifrando los mensajes rápidamente mediante el criptosistema simétrico AES-256 y cifrando la clave de cifrado del criptosistema simétrico mediante el criptosistema asimétrico ElGamal y distribuyendo las claves de forma segura, empleando el protocolo Diffie - Hellman.

En el capítulo III se adentrará a los temas relativos de los sistemas criptográficos que componen el esquema de comunicación segura que plantea esta tesis.

Capítulo III: Criptosistemas Implementados

Para iniciar con este capítulo, comenzaremos describiendo algunos fundamentos teóricos a considerar para los punto III.1.1 y III.2.1 de este capítulo:

- Primo 'p':

Un número grande y primo, al cual se le denominará como 'p'[16].

- Raíz primitiva:

Se dice que 'α' es raíz primitiva de 'p' si las potencias de 'α' generan todos los enteros desde 1 hasta 'p'-1[16]:

$\alpha \bmod p$
$\alpha^2 \bmod p$
...
$\alpha^{p-1} \bmod p$

} Son diferentes y consisten en los enteros desde 1 hasta 'p'-1 con alguna permutación.

- Clave privada:

Se elige un primo como clave privada, tal que: a < p.[16]

III.1. Protocolo de Intercambio de Llaves Diffie Hellman

El protocolo criptográfico Diffie - Hellman fue desarrollado por Whitfiled Diffie y Martín Hellman en el año de 1976[17], el cual se emplea para intercambiar claves entre los diferentes participantes que intervienen en la comunicación de un grupo, esto a través de un canal inseguro. Particularmente se utiliza con la finalidad de posteriormente poder establecer una clave en común, la cual será empleada como clave para el cifrado durante un periodo de tiempo (Sesión).

III.1.1. Descripción

Este protocolo de intercambio de claves Diffie Hellman utiliza la función de exponenciación modular a través de canales inseguros. En este protocolo se tienen claves públicas, las cuales pueden llegar a ser conocidas por todos; y claves privadas, donde estas solamente son conocidas por el propietario. Con las claves

públicas y las claves privadas se utilizan para generar una clave secreta en común para ser empleada como clave privada de un criptosistema simétrico[17].

Para comunicar a dos personas 'A' y 'B' mediante este protocolo, se realiza el siguiente algoritmo[18],[19]:

a. 'A' y 'B' eligen un primo p con más de 300 dígitos y una raíz primitiva 'α', los cuales son públicos
b. 'A' y 'B' eligen valores aleatorios privados 'a' y 'b' tales que: $1 < a,b < p-1$
c. 'A' envía a 'B', $\beta_A = \alpha^a \bmod p$
d. 'B' envía a 'A', $\beta_B = \alpha^b \bmod p$
e. Se calcula la clave secreta de cifrado K
   - 'A' la calcula: $K= (\beta_B)^a \bmod p = \alpha^{ab} \bmod p$
   - 'B' la calcula: $K= (\beta_A)^b \bmod p = \alpha^{ab} \bmod p$

III.1.2. Análisis

En este esquema las claves públicas son (p, α, β_A y β_B). Si se intentara obtener la clave secreta conociendo las claves públicas, se tendría que calcular 'a' y 'b' para generar la clave secreta 'K' y para ello se tendrían que resolver las siguientes ecuaciones:

$$\left.\begin{array}{l} a = \log_\alpha \beta_A \bmod P \\ b = \log_\alpha \beta_B \bmod P \end{array}\right\} \text{ 'a' y 'b' como variables.}$$

Para resolver las ecuaciones mencionadas anteriormente se tendría que resolver un problema de complejidad computacional exponencial, y dado que p posee 300 o más dígitos, resulta ser computacionalmente imposible[20].

III.2. ElGamal

Este algoritmo fue propuesto por Taher Elgamal en 1984[8], el cual consiste en un esquema criptográfico asimétrico, el cual se emplea para la generación de claves, así como para cifrar y descifrar. Dicho esquema se encuentra basado en la idea propuesta por Diffie - Hellman, que también emplea el problema del algoritmo discreto[21].

A pesar del tiempo que lleva desde la fecha de su publicación, actualmente se emplea en muchos sistemas criptográficos, tales como GNU Privacy Guard y en las últimas versiones de PGP, entre otros más[16],[22]; esto debido a que este algoritmo no se encuentra patentado con lo cual lo hace de uso libre.

III.2.1. Descripción

A continuación se describe el algoritmo propuesto por Taher Elgamal para el cifrado, el cual en esta tesis se utilizará para el cifrado de las claves:

a. Se selecciona un número primo 'p' que cumpla con que 'p'-1 cuente con un factor primo grande
b. Se eligen dos números aleatorios, 'α' que será la raíz primitiva, la cual se describió anteriormente y 'a' que será la clave privada; tal que $1<a<p-1$
c. Se calcula el valor de $\beta=\alpha^a \bmod p$

Una vez calculada 'β', esta se utilizará como llave pública para una sesión de comunicación.

III.2.2. Análisis

La generación de las claves, cifrado y descifrado requieren de la exponenciación modular, el cual está basado en la dificultad de encontrar el logaritmo discreto.

El exponente a elegido para la generación de claves se debe elegir nuevo y de forma aleatoria en periodos cortos, con ello se evitará ataques de tipo estadísticos.

En la siguiente figura se presenta un intercambio de claves basado en el protocolo Diffie - Hellman y el cifrado mediante ElGamal de dichas claves para una comunicación entre dos sujetos 'A' y 'B':

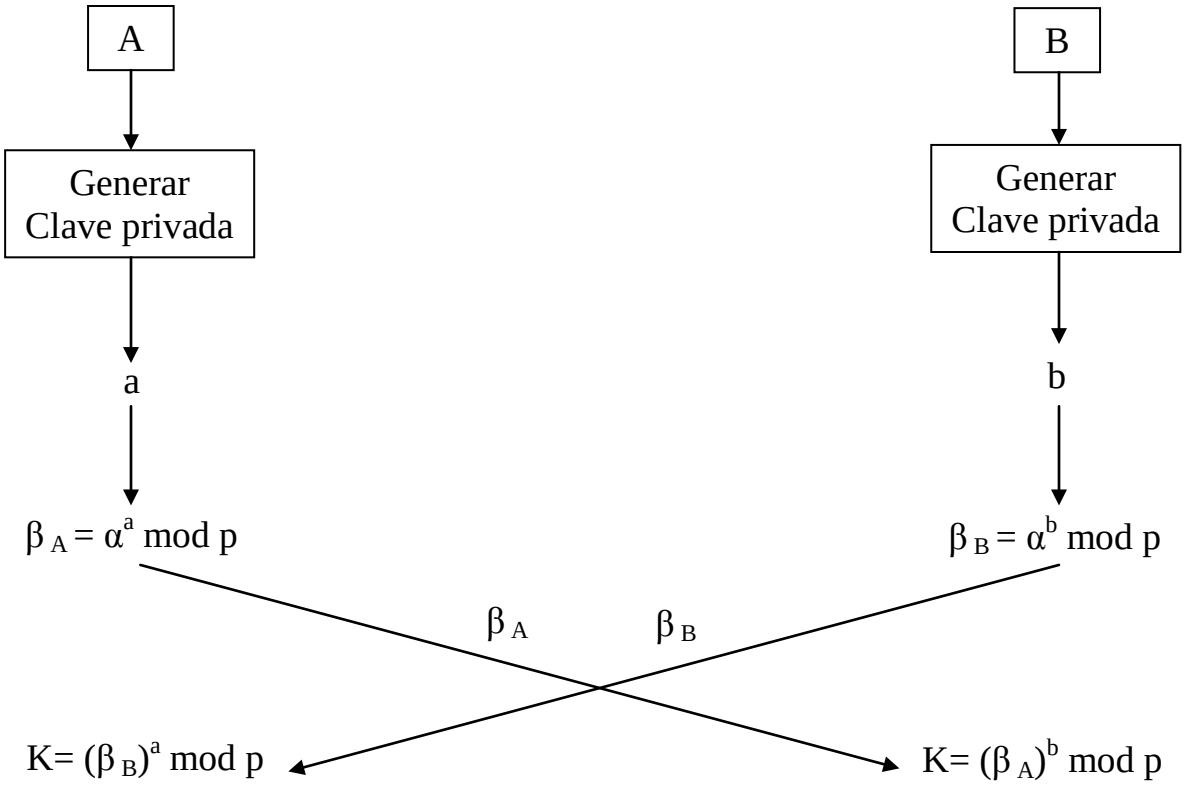


Figura 5.- Ejemplo de intercambio de claves entre dos personas

III.3. AES (Advanced Encryption Standard)

Este esquema de cifrado por bloques también es conocido por el nombre de "*Rijndael*" esto como acrónimo de sus dos desarrolladores de origen belga, los criptólogos Joan Daemen y Vincent Rijmen y el cual fue enviado bajo este nombre al proceso de selección AES[23]. Este esquema de cifrado simétrico resultó ganador y posteriormente anunciado por el Instituto Nacional de Estándares y Tecnología (NIST) como estándar de cifrado (FIPS PUB 197) en 2001[6]. Actualmente este estándar de cifrado se mantiene vigente.

III.3.2. Descripción

El esquema de cifrado AES tiene una longitud de 128 bits en su bloque de cifrado y la longitud de la clave puede ser de 128, 192 ó 256 bits y para cada uno de éstas, AES asigna 10, 12 y 14 iteraciones de cifrado respectivamente[24].

Al igual que otros algoritmos de cifrado en bloque, AES presenta una fase de planificación de claves, la cual implica las siguientes operaciones:

Preparación: La clave original se acomoda en una matriz en forma de columnas, numerándose cada columna como $w0$,$w1$,$w2$,$w3$; la siguiente columna wi, será calculada según la última columna obtenida[6],[25].

Rotación de byte (ROTBYTE): En esta etapa se realiza un desplazamiento circular hacia arriba de la última columna de la matriz de clave anterior[6],[25].

Sustitución de bytes (SUBBYTE): En esta función se procede a realizar una sustitución no lineal que se aplica a cada byte de la columna desplazada, generando un nuevo byte. Esta sustitución se lleva a cabo utilizando la tabla S de la norma[6],[25].

RCON. La columna sustituida del paso anterior se opera mediante la operación xor con una nueva columna denominada Rcon, la cual ya está definida en la norma[6],[25].

El proceso de cifrado AES se presenta en la siguiente figura:

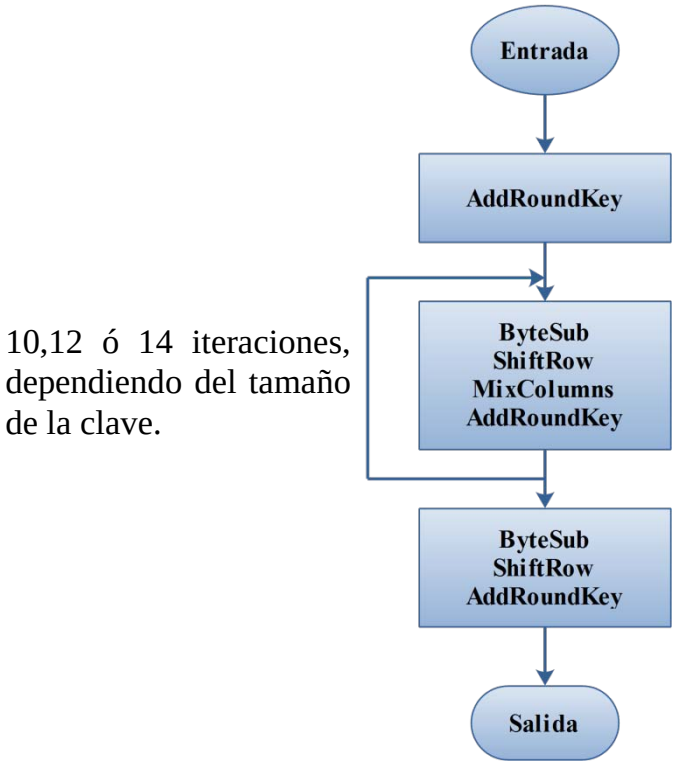


Figura 6.- Proceso de cifrado AES[26]

Como se puede apreciar en la figura 6, existen cuatro transformaciones básicas; dichas transformaciones se describen a continuación:

SubBytes: Esta transformación realiza la sustitución no lineal, que se aplica a cada byte de la matriz de inicio de ronda de forma independiente, generando así un nuevo byte; a cada elemento de la matriz de inicio se le sustituye por otro byte. Esta sustitución se lleva a cabo utilizando la tabla S de la norma[6],[25].

ShiftRows: En la segunda matriz se realiza desplazamiento circular a la izquierda de cada una de las filas que conforman la matriz SubBytes; es decir, un corrimiento izquierdo de los bytes de cada fila de la matriz resultante de la transformación anterior.

Cada fila se desplaza un número de posiciones diferentes; este número de vueltas o rotaciones dependerá del renglón en turno: el renglón cero tiene cero corrimientos, el renglón uno tiene uno, el renglón dos tiene dos, y así sucesivamente[6],[25].

MixColumns: Esta etapa manipula los bytes de una misma columna de la matriz ShiftRows y los multiplica por una matriz fija, que representa al polinomio:

$$c(x)=3x^3+x^2+x+2$$

Dicho polinomio está definido en la norma[6],[25].

AddRoundKey: La última matriz obtenida se combina con la clave planeada para la ronda uno por medio de la operación lógica *XOR*. Aquí finaliza la ronda de cifrado[6],[25].

En la siguiente figura se presenta la operación contraria; es decir, el proceso para el descifrado AES:

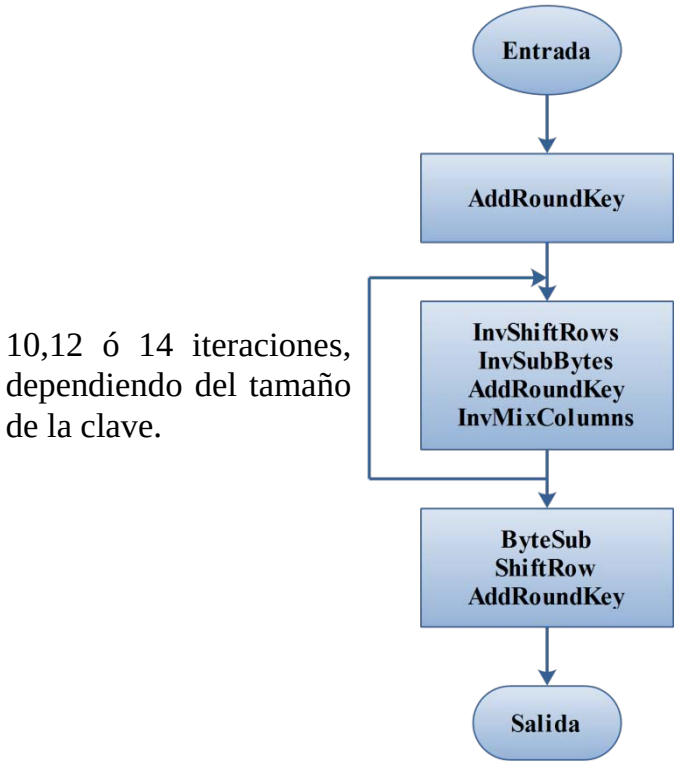


Figura 7.- Proceso para descifrado AES[27]

Como se puede apreciar en la figura 7, existen cuatro transformaciones básicas para el descifrado con AES, las cuales se describen a continuación:

AddRoundKey: Al ser una operación *XOR*, ella misma es su inversa[6],[25].

InvMixMolumns: Esta transformación opera de la misma forma que su contraparte en el cifrado, tomando los bytes y los multiplica por una matriz fija. Esta matriz se obtiene a partir del polinomio

$$d(x)=0Bx3+0Dx2+09x+0E$$

Dicho polinomio está definido en la norma[6],[25].

InvShiftRows: Representa el corrimiento inverso a su contraparte en el cifrado: un corrimiento circular a la derecha dependiendo del renglón que se trabaje. De esta manera, el renglón cero se desplaza cero bytes, el renglón uno un byte, el segundo renglón dos bytes y así sucesivamente[6],[25].

InvSubBytes: La inversa de esta fase corresponde a la sustitución de bytes de manera inversa, utilizando la tabla S inversa de la norma. Debido a que esta es la fase no lineal del algoritmo, se requiere una inversa no lineal[6],[25].

III.3.6. Análisis

Este criptosistema simétrico se mantiene vigente, esto debido que hasta la fecha no se ha encontrado un ataque exitoso en contra de AES[24].

Sin embargo, en el año 2002 un ataque fue publicado por los investigadores Nicolas Courtois y Josef Pieprzyk. Este ataque se basa, en primero analizar el funcionamiento interno de un sistema de cifrado y la obtención de un sistema de ecuaciones cuadráticas. Estos sistemas de ecuaciones suelen ser muy grandes, por ejemplo, 8,000 ecuaciones con 1,600 variables para el AES de 128 bits. Dada la complejidad de este ataque, no afecta la seguridad del AES hasta hoy en día[28].

Capítulo IV: Construcción de la solución integrando Diffie Hellman, ElGamal y AES

IV.1. Construcción

En este capítulo se presenta el análisis, diseño e implementación del esquema de comunicación segura basado en un criptosistema híbrido. Donde dicho criptosistema se encuentra conformado por AES-256 para el cifrado de texto, ElGamal para el cifrado de las claves y Diffie - Hellman para la distribución segura de dichas claves.

La construcción de la solución basada en el esquema de comunicación segura descrito anteriormente debe contemplar buenos tiempos de procesamiento, compatibilidad de la aplicación implementada entre diversas plataformas y una interfaz grafica de usuario (GUI) amigable con la finalidad de proporcionar al usuario una fácil interacción con el criptosistema.

IV.1.1. Análisis

A continuación se especifican los requerimientos para que se realice el sistema que implementa el esquema de comunicación segura basado en el criptosistema híbrido que se detallo anteriormente. Para esto es necesario que el sistema cumpla con las siguientes funciones:

- El sistema deberá cumplir con el modelo cliente - servidor[29], donde las características de cada proceso serán las siguientes:

  El proceso cliente realizará las siguientes funciones:

  - ✓ Administrar la interfaz de usuario
  - ✓ Interactuar con el usuario
  - ✓ Procesar las rondas de intercambio de claves mediante el protocolo Diffie - Hellman y enviarlas al servidor cifradas con ElGamal
  - ✓ Generar la clave secreta para el AES-256 para el cifrado y descifrado de los mensajes
  - ✓ Enviar los mensajes cifrados al servidor
  - ✓ Recibir y descifrar los mensajes del servidor
  - ✓ Contar con envío de mensajes generales (para todos los clientes) y privados (para un cliente en particular)

  Además el cliente deberá solicitar dos parámetros al inicio de cada sesión, en primer lugar solicitará la llave maestra para poder acceder a la conversación del grupo, la cual denominaremos como "Llave maestra de sesión". Y en

segundo lugar se solicitará al usuario que introduzca la dirección IP del servidor.

Por otra parte, una vez iniciada la sesión se podrá tener acceso a las claves generadas para la conversación actual únicamente con una segunda llave maestra, la cual denominaremos como "Llave maestra delta".

Para brindarle mayor seguridad a la conversación se generara una nueva serie de rondas si un nuevo usuario se incorpora a la conversación del grupo o si algún usuario se retira de dicha conversación.

Y el proceso servidor realizará las siguientes funciones:

- ✓ Recibir los mensajes de los clientes
- ✓ Verificar el tipo de mensaje que se recibe ya sea general o privado
- ✓ Trasmitir los mensajes a los clientes

Este proceso podrá ser ejecutado por algún miembro del grupo al momento de iniciar la sesión de conversación previamente acordada por el grupo a reunirse

- El sistema a implementarse se desarrollará en un lenguaje de programación que brinde los menores tiempos en operaciones con números grandes, dicho lenguaje es java; esto debido a que cuenta con la clase *biginteger*[4],[30] para el manejo de números grandes, además de que posee bondades en la utilización de sockets[31], los cuales son vitales para el desarrollo de ésta implementación.

IV.1.2. Diseño

Como se mencionó anteriormente, para el cifrado de los mensajes se utilizará AES-256, la clave simétrica de éste será obtenida a partir de la β final que se genere después de haber concluido las rondas de intercambio de claves entre los usuarios participantes en la comunicación, mediante el protocolo Diffie - Hellman.

Previamente estas claves serán cifradas con ElGamal para después ser intercambiadas bajo el protocolo mencionado anteriormente.

El número de rondas requeridas para el intercambio total de las claves entre los usuario es igual al número de usuarios participantes menos uno.

El método para obtener la clave simétrica de AES-256, será tomar los primeros 256 bits de la β final. Dicha β final será calculada por cada usuario una vez que se hayan

concluido las rondas y ésta será la misma para cada usuario. Por lo que cada usuario contará con la misma clave simétrica.

Para el cifrado de las claves mediante ElGamal se tiene lo siguiente:

El proceso cliente calculará para cada usuario participante su clave privada con alrededor de diez dígitos, la cual será única y exclusiva de cada usuario.

Por otra parte, todos los usuarios compartirán las claves públicas (p y el primitivo), los cuales serán de 400 y 200 dígitos respectivamente con la finalidad de brindar mayor fortaleza al criptosistema.

Para la generación de las claves públicas y la claves privadas se utilizará la clase *Biginteger*; que además de permitir el uso de números grandes, también proporciona el uso de operaciones con la aritmética modular (lo cual resulta muy útil para la implementación de ElGamal), la generación de primos, manipulación de bits, entre otras operaciones muy útiles[13],[30].

A continuación se detalla el funcionamiento planteado en el análisis tanto del proceso cliente como del proceso servidor para el cifrado de los mensajes bajo el esquema de comunicación segura propuesto en esta tesis.

Proceso Cliente:

De acuerdo a las funciones del proceso cliente que se describieron en el análisis (punto IV.1.1); este proceso llevará a cabo el esquema de comunicación segura que se plantea en esta tesis.

La figura que se presenta en la siguiente página, muestra el procesamiento interno que realizará el proceso cliente:

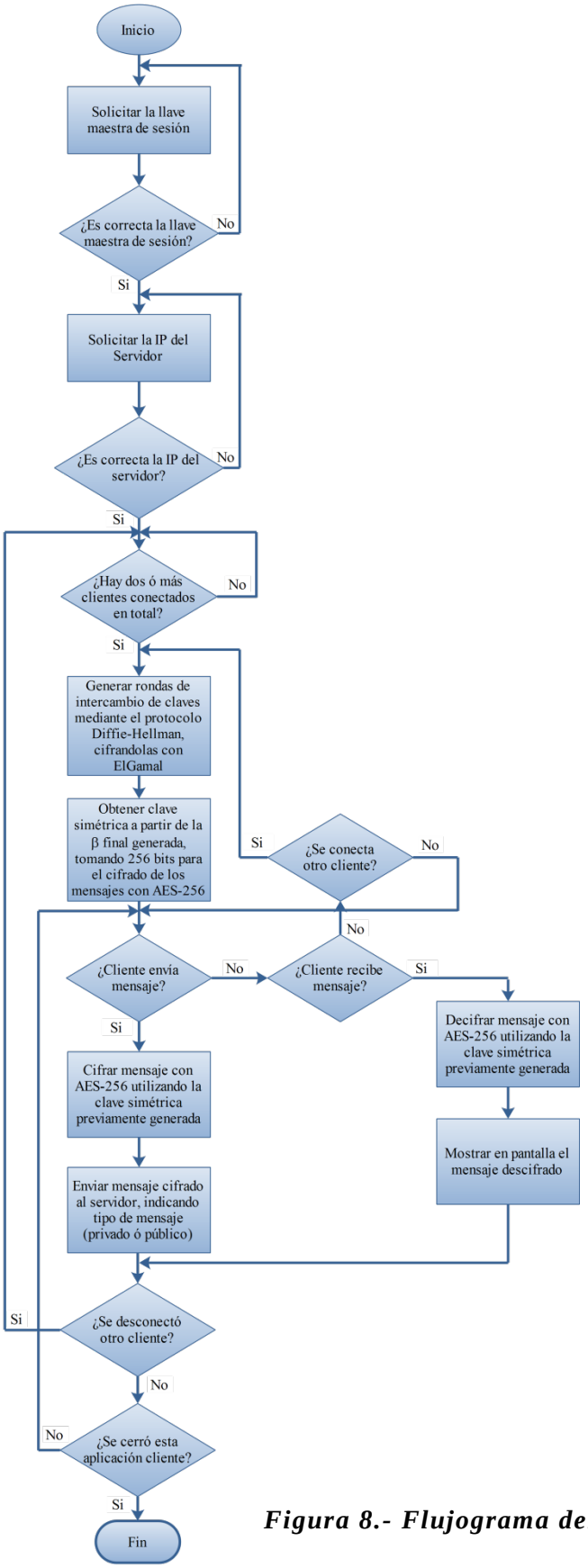


Figura 8.- Flujograma del proceso cliente.

Proceso Servidor:

De acuerdo a las funciones del proceso servidor que se describieron en el análisis (punto IV.1.1); este proceso llevará únicamente la comunicación entre los usuarios participantes; es decir, solo transmitirá y recibirá los mensajes cifrados por parte de los procesos cliente.

La figura que se presenta a continuación, muestra el procesamiento interno que realizará el proceso servidor:

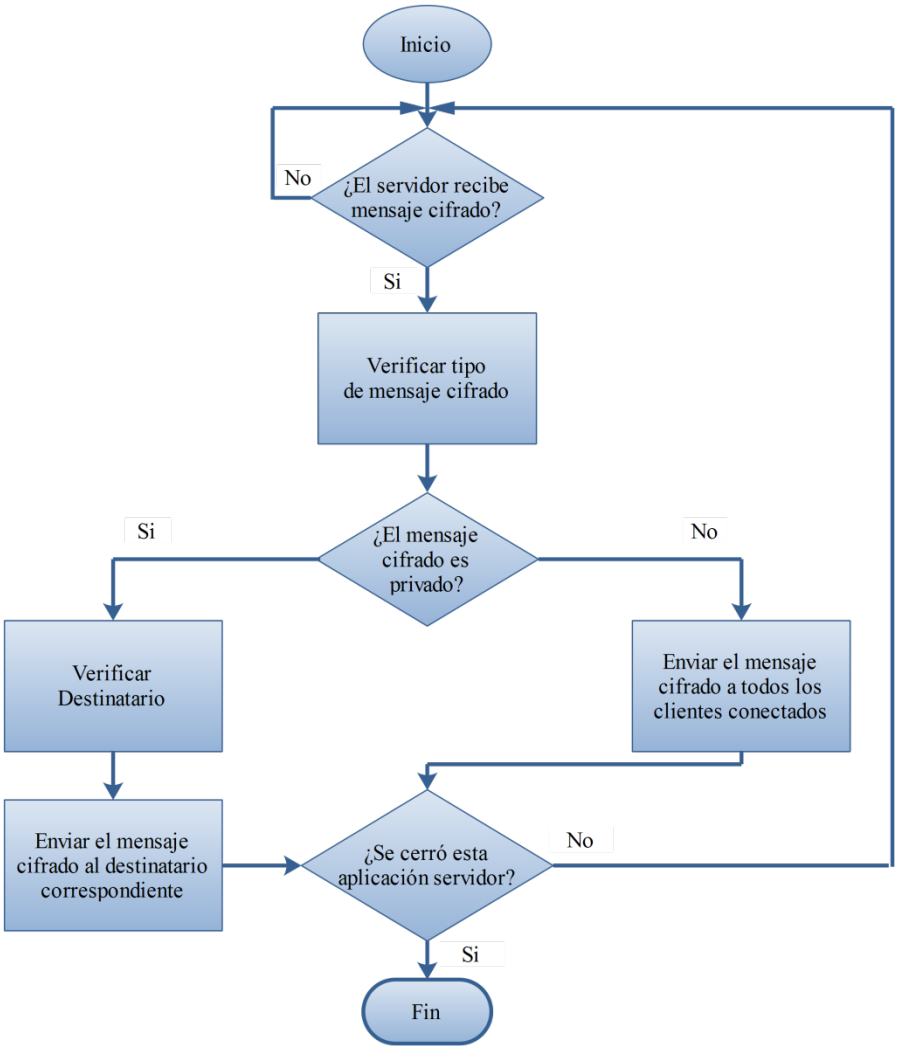


Figura 9.- Flujograma del proceso servidor.

IV.2. Implementación

Como se mencionó en el apartado de construcción (punto IV.1) el sistema deberá contar con una interfaz gráfica de usuario (GUI), con la finalidad de permitir el flujo de información entre el usuario y el sistema; es decir, el conjunto de imágenes y objetos gráficos para representar la información y acciones disponibles en la interfaz.

Para este sistema se empleo una interfaz gráfica tanto para el proceso cliente como para el proceso servidor, los cuales fueron desarrollados en NetBeans IDE 7.2.1.

El proceso de desarrollo del trabajo contempla la implementación e integración de dos criptosistemas. Utilizando AES-256 para el cifrado de los mensajes y ElGamal para el cifrado de las claves, las cuales se intercambiarán entre los participantes de la conversación mediante el protocolo Diffie - Hellman y de esta manera cada participante generará una clave en común para la conversación, dicha clave será utilizada como la clave simétrica para el cifrado de los mensajes con AES-256.

De inicio se tuvo que entender el algoritmo de cifrado de cada criptosistema, basándose en el estudio de la norma oficial de cada uno. Una vez comprendidos estos algoritmos se procedió a su implementación individual. Cabe mencionar que la implementación de AES-256 se realizó para el cifrado de cadenas de texto.

Una vez obtenidos estos algoritmos, el siguiente paso fue integrarlos en una solución que pudiera comunicarse dentro de redes de área local (LAN), para esto se utilizaron sockets los cuales están basados en los protocolos TCP/IP.

En especifico para este trabajo se emplearon los puertos 8081 y el 8082 para la comunicación entre los procesos cliente y el proceso servidor.

La interfaz final planteada para este esquema de comunicación segura se describe a continuación:

Interfaz del proceso servidor:

En primera instancia se debe iniciar el servidor para que los clientes o participantes que se integren a la conversación se conecten a él.

En la siguiente figura se muestra la interfaz del servidor.

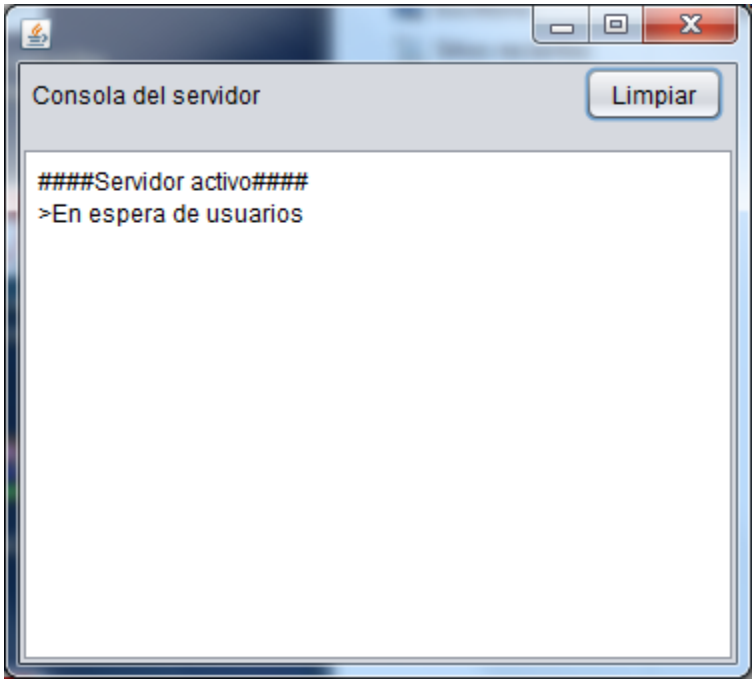


Figura 10.- Interfaz del Servidor.

Interfaz del proceso cliente:

Al iniciar la interfaz del cliente, éste solicitara que se introduzca la IP en la que se encuentra activo el servidor como se muestra en la figura 11.

Figura 11.- Interfaz del Cliente (IP Servidor).

Como se muestra en la figura 11, la IP del servidor introducida pertenece al CIDETEC-IPN, esto debido a que el ejemplo que se está presentando se realizó en la red del centro.

En caso de que la IP introducida no fuera correcta, se mostrara un mensaje de "Servidor no encontrado" y volverá a solicitarla nuevamente.

Una vez validada la IP del servidor, el sistema solicitará que se introduzca la clave maestra de sesión, como se muestra en la siguiente figura.

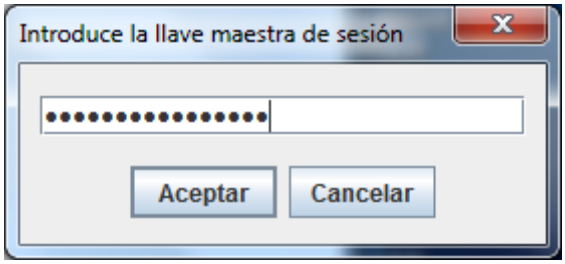


Figura 12.- Interfaz del Cliente (Llave maestra de sesión).

Para este caso la llave maestra de sesión es "*cidetec-ipn-2013*", siendo una clave de 128 bits con un alto grado de fortaleza. Se tienen tres oportunidades para introducir correctamente la llave maestra de sesión; en caso de rebasar el límite de oportunidades, el sistema se cerrara automáticamente como protocolo de seguridad.

Si la llave maestra de sesión se introduce correctamente se mostrara una ventana que solicitará el nick con el que el participante se identificara dentro de la conversación del grupo, como se muestra en la figura 13.

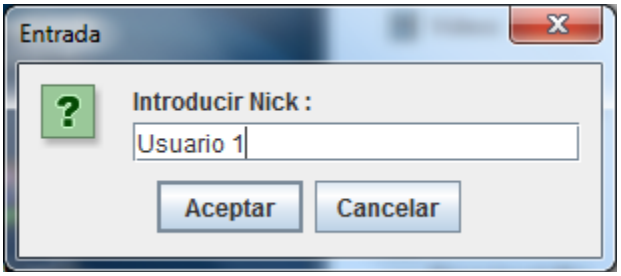


Figura 13.- Interfaz del Cliente (Entrada del Nick).

Después de haber introducido el nick, el sistema mostrara la ventana principal, en la cual se mantendrá la comunicación con los demás usuarios. Esta ventana contara con una barra de menú el cual tiene dos opciones, la primera denominada como archivo y en ésta se tiene la opción de "cerrar la sesión"; es decir, abandonar la conversación. La segunda opción denominada como herramientas tiene la opción "ver llaves", para tener acceso a ésta se debe contar con la "Llave maestra delta", la cual al ser introducida correctamente mostrará los siguientes valores:

- El valor de la Beta final ó total generada.
- El valor del primo utilizado por ElGamal.
- El valor del primitivo utilizado por ElGamal.
- La llave simétrica empleada para el cifrado con AES-256.

Cabe resaltar que estas claves se generaran nuevamente a partir de una nueva serie de rondas cuando algún usuario se incorpore o se retire de la conversación.

Por otro lado, se muestran dos cuadros, el primero llamado como "conversación de grupo", en el cual aquí se comparte el mensaje que se envié a todos los participantes de la conversación. El segundo llamado como "conversación privada", en esta opción se comparten mensajes únicamente con otro usuario y de esta manera tener una conversación privada con un solo participante y para ello se generará una ventana exclusiva para dicha conversación.

En la siguiente figura se muestra la ventana principal del cliente:

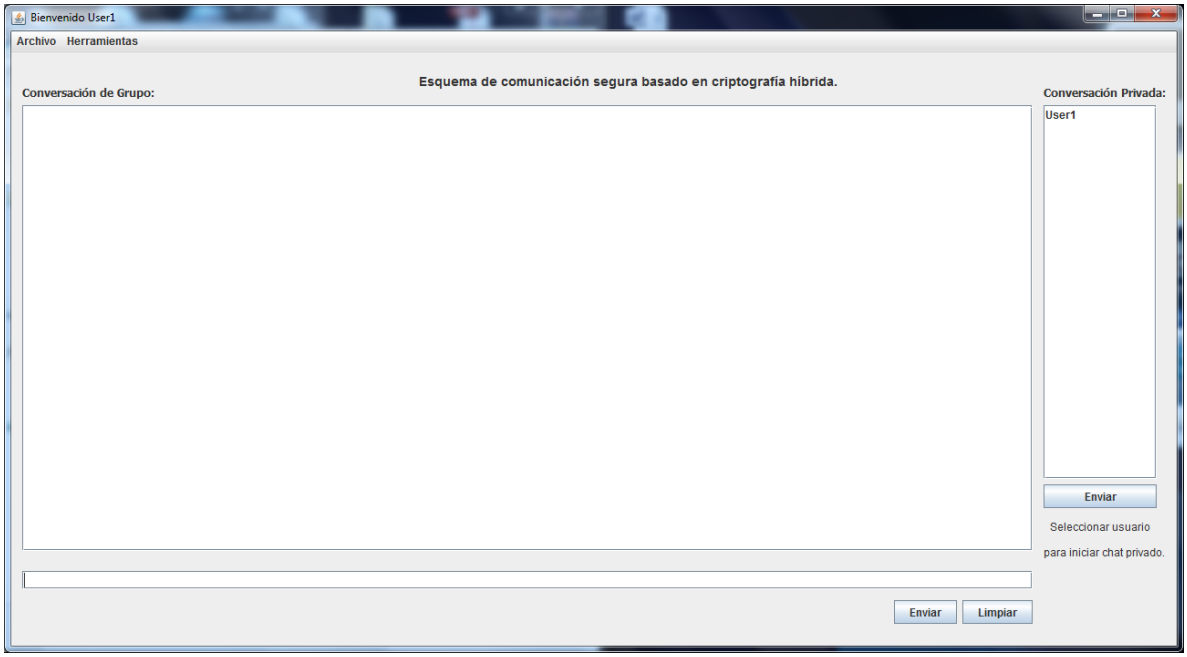


Figura 14.- Interfaz principal del Cliente.

Capítulo V: Pruebas y discusión de resultados

V.1. Pruebas

Para la etapa de pruebas se procedió a revisar y verificar el correcto funcionamiento del software, principalmente se verificó que cumpliera con buenos tiempos en el cifrado e intercambio de las claves, ya que el criptosistema asimétrico y el empleo de operaciones con números grandes es un factor relevante para que el software pueda trabajar con lentitud.

A continuación se presentan las pruebas realizadas al software, las cuales consistieron en incrementar el número de participantes en la conversación (3,5,10 y 15 participantes), donde se envía el mismo mensaje para todos los casos y se verificará el tiempo de respuesta en cada uno.

La cadena que se utilizó en todos los casos de las pruebas realizadas, consta de 150 caracteres.

Caso con 3 participantes:

Para el caso con 3 participantes en la conversación, el tiempo total que se obtuvo al finalizar las rondas de intercambio de claves fue 0.47 segundos.

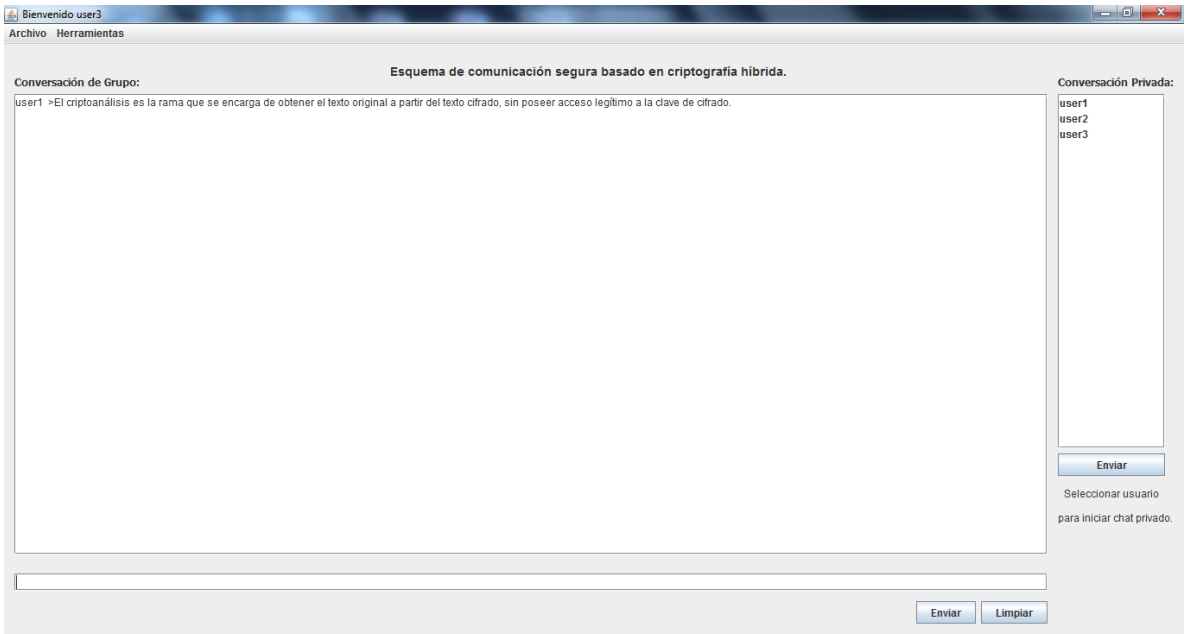


Figura 15.- Prueba de la implementación con tres participantes.

Caso con 5 participantes:

Para el caso con 5 participantes en la conversación, el tiempo total que se obtuvo al finalizar las rondas de intercambio de claves fue 1 segundo.

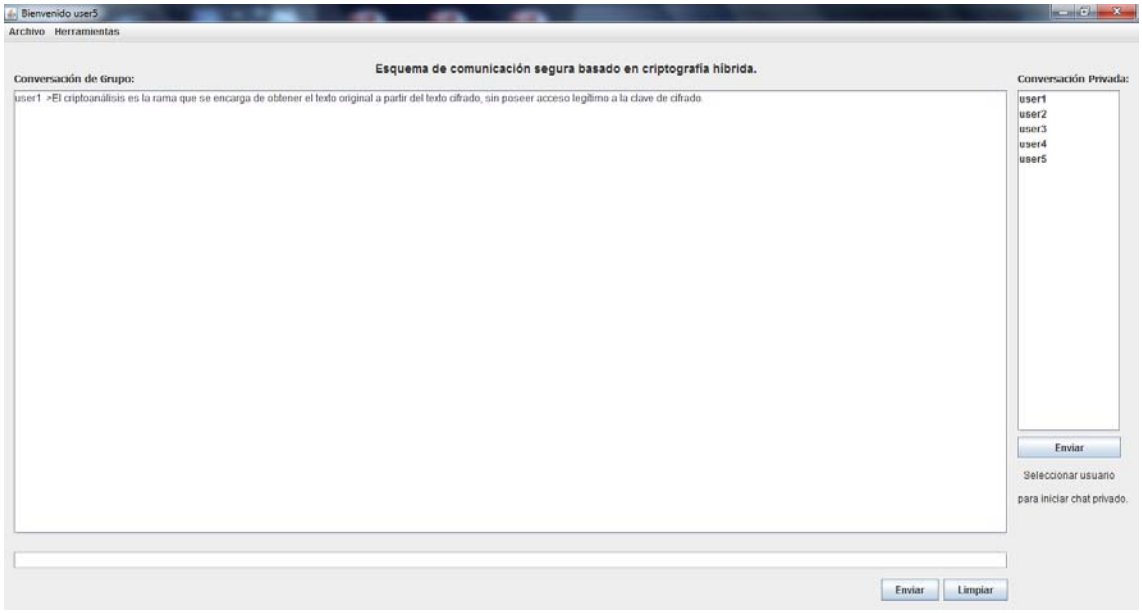


Figura 16.- Prueba de la implementación con cinco participantes.

Caso con 10 participantes:

Para el caso con 10 participantes en la conversación, el tiempo total que se obtuvo al finalizar las rondas de intercambio de claves fue 3.5 segundos.

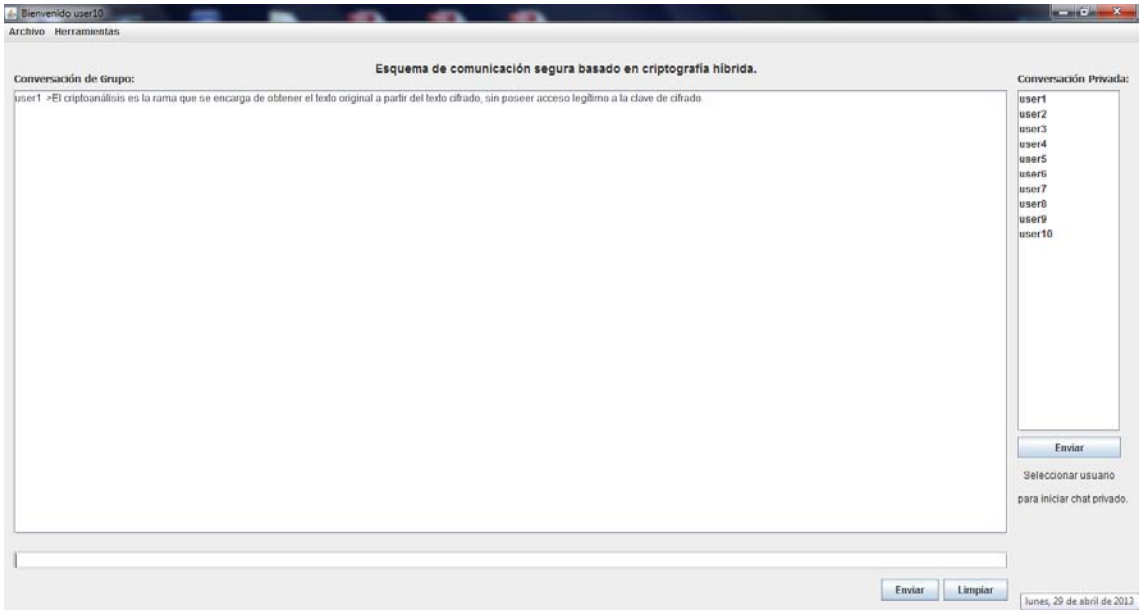


Figura 17.- Prueba de la implementación con diez participantes.

Caso con 15 participantes:

Para el caso con 15 participantes en la conversación, el tiempo total que se obtuvo al finalizar las rondas de intercambio de claves fue 5 segundos.

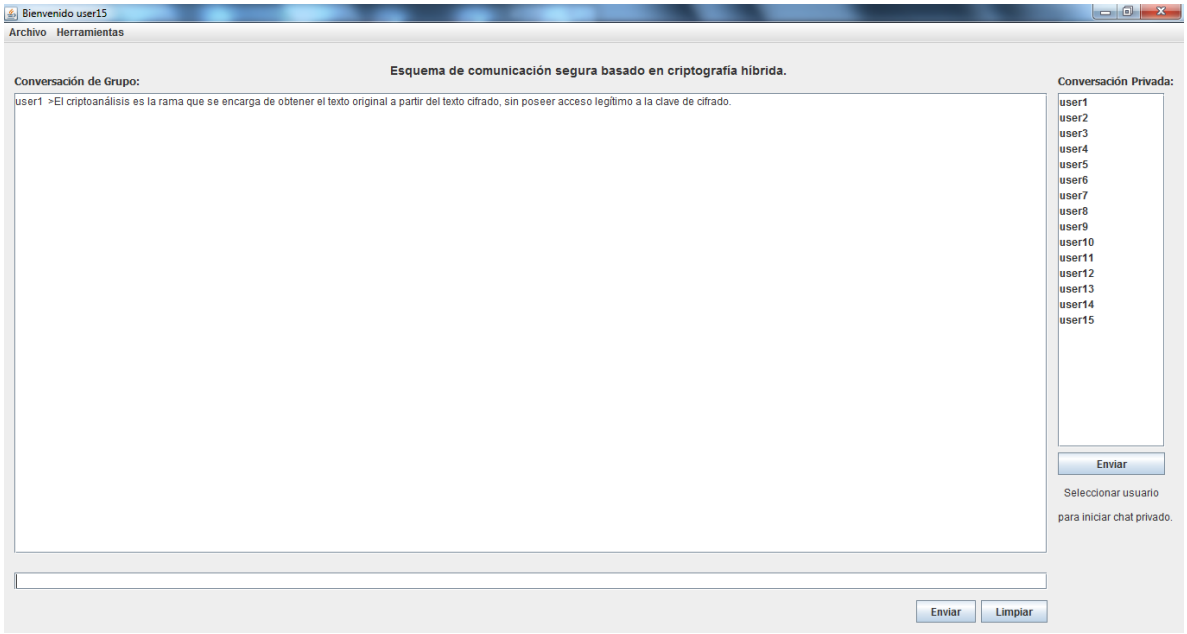


Figura 18.- Prueba de la implementación con quince participantes.

V.2. Discusión de resultados

Dentro de este apartado se presentan los resultados que se obtuvieron a partir de las pruebas realizadas en el capítulo anterior al software obtenido de la implementación del esquema de seguridad que propone esta tesis.

Las pruebas realizadas consistieron en medir el tiempo que se tarda en realizar el cifrado y el intercambio de claves entre el número de participantes que se encuentran en la conversación. Ya que las operaciones matemáticas que se realizan para el cifrado de las claves para su intercambio posterior utilizan números muy grandes y esto se incrementa, si el número de participantes crece; además de que se eleva el número de rondas para el intercambio de las claves.

En la siguiente tabla se presenta un concentrado de los resultados obtenidos:

Tabla 1.- Resultados obtenidos en las pruebas de tiempo en las rondas de intercambio de claves.

Número de participantes	Tiempo de respuesta
3	0.47 segundos
5	1.0 segundos
10	3.5 segundos
15	5.0 segundos

El tiempo obtenido en la primer prueba (con tres participantes) fue de 0.47 segundos; es decir, imperceptible para el usuario, resultando un excelente tiempo para este caso.

En la segunda prueba (con cinco participantes) donde el tiempo obtenido fue de 1 segundo, resultando un buen tiempo.

Para el caso de la tercer prueba (con diez participantes), el tiempo obtenido fue de 3.5 segundos, lo cual es un tiempo considerable de espera por parte del usuario; a diferencia de ésta, con la cuarta prueba (con quince participantes) se obtuvo un tiempo de 5 segundos y con este tiempo puede resultar incomodo para el usuario.

En la siguiente figura se muestra gráficamente el tiempo que tarda el software en concluir las rondas de intercambio de claves en base al número de participantes en la conversación, tomando los resultados a las pruebas realizadas

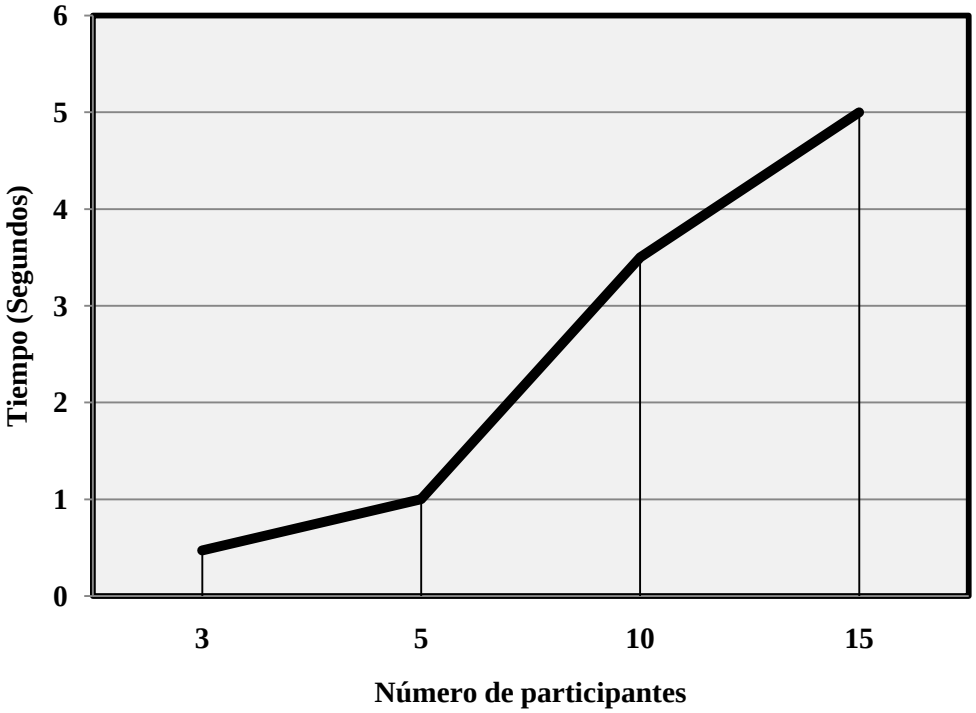


Figura 19.- Comportamiento gráfico de las pruebas realizadas.

Los tiempos obtenidos en las pruebas, cumplieron con las expectativas de este esquema, ya que está enfocado a miembros de alta gerencia o grupos de confianza de algún corporativo donde el número de usuarios es reducido.

Cabe resaltar que para todos los casos, el tiempo de envío/recepción de los mensajes a todos los participantes es instantáneo; es decir, que el proceso donde se demora el sistema es en las rondas de intercambio de claves, donde el tiempo varía dependiendo del número de participantes.

Capítulo VI: Conclusiones y trabajos a futuro

VI.1. Conclusiones

El estudio y análisis del AES-256, ElGamal y el protocolo Diffie - Hellman, así como la comunicación mediante sockets permitieron la implementación del esquema de comunicación segura a través de redes de área local, basado en criptografía híbrida, logrando el cumplimiento satisfactorio de los objetivos planteados en el capítulo II.3, siendo que:

1. Se implementó el criptosistema asimétrico ElGamal para el cifrado de las claves
2. Se implementó el criptosistema simétrico AES para el cifrado de los mensajes de texto
3. Se implementó el protocolo Diffie - Hellman para distribuir las claves
4. Se Integraron los criptosistema en una solución

Cabe mencionar que el desarrollo de dicho esquema se realizó con las herramientas mencionadas anteriormente, y éste se implementó de manera correcta utilizando el lenguaje de programación java.

Las pruebas realizadas al software obtenido en la implementación, corrobora que realiza adecuadamente su proceso, puesto que se aplicaron pruebas con cantidades distintas de usuarios conectados a la misma conversación y los tiempos obtenidos cumplieron con las expectativas planteadas.

Por lo anterior se concluye que el diseño e implementación de este esquema de comunicación segura a través de redes de área local, es totalmente funcional para miembros de alta gerencia o grupos de confianza de algún corporativo donde el número de usuarios es reducido. Inicialmente se esperaba que el número de usuarios máximo recomendable fuera de quince participantes; pero en base a las pruebas realizadas en el capítulo V, se recomienda que el número de usuarios participantes en la conversación no debe rebasar de diez para que el sistema brinde buenos tiempos de respuesta al usuario.

VI.2. Trabajos a Futuro

Con los resultados obtenidos en el desarrollo de esta tesis, se enlista a continuación los trabajos a futuro:

a. Incorporar a este trabajo el cifrado de imágenes mediante el criptosistema AES-256 con la finalidad de utilizar la misma clave simétrica tanto para el cifrado de los mensajes como el de las imágenes.

b. Adaptar el software desarrollado para dispositivos móviles con el objeto de que los miembros del grupo puedan conectarse a través de sus tabletas, teléfonos inteligentes, etc.

c. Aplicar la misma técnica utilizando el estándar de cifrado 3-DES como criptosistema simétrico en lugar del estándar AES-256, ya que actualmente este estándar de cifrado es empleado en varias empresas, tales como algunos bancos.

Referencias

[1] J. J. A. Ángel, "Criptografía para principiantes", CINVESTAV - IPN, México, Reporte, 2000.

[2] M. M. Pons, "Criptología", Departamento de telecomunicaciones - Escuela Universitaria Politécnica de Mataró, España. Reporte, Enero 2000.

[3] N. Koblitz, "A course in number theory and cryptography", *Graduate texts in mathematics*, 2nd ed. University of Washington, EE.UU.: Springer - Verlag, 1994, pp. 54-57.

[4] J. B. Knudsen, *Java Cryptography*, 1st ed. Sebastopol, California: O´Reilly, 1998, pp. 14-16,180.

[5] Data Encryption Standard, FIPS PUB 46-3, October 1999.

[6] Advanced Encryption Standard, FIPS PUB 197, November 2001.

[7] R. L. Rivest, A. Shamir, and L. Adleman "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, vol. 21, 1978, pp. 120-126.

[8] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Transactions on Information Theory*, vol. IT-31, 1985, pp. 469-472.

[9] V. S. Miller, "Use of Elliptic curves in Cryptography", *in Advances in cryptology - CRYPTO 85*, 1986, pp. 417.

[10] C. A. Angulo, S. M. Ocampo, y L. H. Blando, "Una mirada a la esteganografía", Universidad Tecnológica de Pereira, Colombia, Reporte, 2007.

[11] E. S. Acosta, "Criptografía y teoría de códigos", Universidad Francisco Vitoria, España, Reporte final, 2012.

[12] S. B. i Torné y R. C. Moreno, “Análisis del cifrado ElGamal de un módulo con curvas elípticas propuesto para el GnuPG”, Escuela Politécnica Superior, España, Reporte científico, 2007.

[13] S. Chow, P. A. Eisen, and H. Johnson, “White-Box Cryptography and an AES Implementation”, Cloakware Corporation, Ottawa, Canadá, Scientific report, 2003.

[14] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, “A Modified AES Based Algorithm for Image Encryption”, *International Journal of Computer Science & Engineering*, vol. 1, Marzo 2007.

[15] A. Mahalanobis, “Diffie-Hellman Key Exchange Protocol, Its Generalization and Nilpotent Groups”, Universidad de Atlantic Florida, Report, Agosto 2005.

[16] A. Arteaga, "ElGamal", Facultad de Ingeniería - Universidad Nacional Autónoma de México, México, Reporte técnico, 2012.

[17] D. Whitfield and E. M. Hellman, "New directions in cryptography", *IEEE Transactions on information theory*, vol. IT-22, November 1976.

[18] G. Wald, "Algoritmo Diffie - Hellman", Facultad de Ingeniería - Universidad de Buenos Aires, Argentina, Reporte técnico, Noviembre 2012.

[19] J. G. de Jalón de la Fuente, “Intercambio de claves de Diffie Hellman”, España, Reporte, 2009.

[20] F. Delgado y A. Núñez, “El Problema del Logaritmo discreto. Criptosistema de ElGamal”, Universidad de Valladolid, Reporte, España, 2010.

[21] J. J. A. Ángel, "Criptografía y curvas elipticas", Tesis de maestría, Universidad Autónoma Metropolitana, México, 1998.

[22] E. Arias, “Criptografía”, Universidad de Castilla, España, Reporte, 2010.

[23] J. M. Eguílaz, “Algoritmo AES (Advanced Encryption Standard)”, Universidad Politécnica de Cataluña, Barcelona, España, Reporte técnico, 2009.

[24] D. R. Stinson, *Cryptography: Theory and Practice*, 3rd ed. Boca Raton: Chapman & Hall/CRC, 2006, pp. 102-108.

[25] A. Arteaga, "Rijndael - AES", Facultad de Ingeniería - Universidad Nacional Autónoma de México, México, Reporte técnico, 2012.

[26] J. J. A. Ángel, "AES - Advanced Encryption Standard", CINVESTAV - IPN, México, Reporte técnico, 2005.

[27] J. M. Eguílaz, "Apuntes sobre Advanced Encryption Standard", Universidad Politécnica de Cataluña, Barcelona, España, Reporte técnico, 2012.

[28] N. Courtois and J. Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations", *in Advances in Cryptology - ASIACRYPT*, vol. 2501, pp. 267-287. 2002.

[29] E. Hernández y L. Martínez, "Cliente - Servidor", Club de Investigación Tecnológica, San José, Costa Rica, Reporte técnico, Diciembre 1997.

[30] Oracle (2013, abril), Class BigInteger. [En Línea]. Disponible en: http://docs.oracle.com/javase/7/docs/api/java/math /BigInteger.html.

[31] P. M. Barco, "Sockets en Java", Universidad de Alicante, España, Reporte técnico, 2009.