INSTITUTO POLITÉCNICO NACIONAL

Escuela Superior de Cómputo

ESCOM

Trabajo Terminal

"Aplicación de cifrado contra adversarios clasificadores, para el correo electrónico"

2015-A010

Presentan

Arcos Ayala Jonathan
Zepeda Ibarra Allan Ulises

Directores

Dra. Sandra Díaz Santiago
M. en C. Manuel Alejandro Soto Ramos

Mayo 2016

Índice

Índice de Figuras

Índice de Tablas

Capítulo 1

Introducción

Actualmente, una gran cantidad de personas hacen uso del internet y de las nuevas tecnologías para comunicarse. Con ello, también se incrementa la cantidad de información que se transmite y/o almacena. En diversas ocasiones, esta información es susceptible a sufrir distintos tipos de ataques tales como acceso no autorizado, modificación o destrucción de la misma, entre otros. Adicionalmente, cada día aparecen nuevos tipos de ataques a los sistemas de información. Por lo tanto, surge la necesidad de proteger dicha información.

Una de las tecnologías ampliamente usada para comunicarse es el correo electrónico [30]. Los mensajes que envían y reciben los usuarios de correo electrónico pueden ser de diferentes tipos: personales, transaccionales, de notificación o de publicidad. Por lo tanto, cada vez que se escribe y envía un correo electrónico, se está revelando información acerca de las preferencias y/o intereses del usuario. Estos datos, son el insumo más importante, para distintas entidades, entre las cuales están empresas que realizan publicidad en línea, proveedores de internet, instituciones de gobierno, entre otros [10]. El propósito de tener estos datos puede ser realizar publicidad efectiva, vender los datos a empresas de publicidad o averiguar si determinado usuario es una amenaza para el gobierno. Para obtener información acerca de los intereses y/o preferencias del usuario, se hace uso de programas de cómputo denominados *clasificadores*. Los clasificadores son herramientas informáticas que analizan una gran cantidad de información, haciendo uso de técnicas de aprendizaje máquina [15], y posteriormente clasifican un mensaje en determinada categoría o perfil. En este contexto, los clasificadores pueden constituir una amenaza para algunos usuarios del correo electrónico, por tal motivo de ahora en adelante a los programas que clasifican se les denominará *adversarios clasificadores*.

Ante tal escenario, surge la pregunta ¿cómo se puede proteger un usuario contra los adversarios clasificadores? Una posible respuesta es hacer uso de algoritmos de cifrado estándar. Sin embargo, hacer uso de tales algoritmos, implica que los participantes en la comunicación acuerden una clave de cifrado. Desafortunadamente, acordar una clave, no es un proceso sencillo para el usuario común. Otra desventaja de esta primera solución, es que los algoritmos de cifrado estándar ofrecen un alto nivel de seguridad, el cual resulta excesivo cuando se consideran los recursos y el objetivo de un adversario clasificador [12].

1.1. Justificación

La comunicación por medio del correo electrónico es atacada constantemente y por ello se han creado diferentes herramientas para asegurar la transferencia de información entre los usuarios. Pero estas herramientas ofrecen un conjunto de servicios como confidencialidad, no repudio, autenticación, entre otros y es porque están pensadas para hacer frente a adversarios mejor capacitados en la adquisición de información de los usuarios de correo electrónico.
Estas herramientas al enfrentarse a adversarios más capacitados necesitan implementar esquemas y técnicas más sofisticadas para establecer una comunicación segura entre usuarios y el mayor reto que se les presenta es el intercambio de claves, porque si un adversario llega a obtener al menos una clave, el esquema de seguridad se considera roto y la comunicación es vulnerable al ataque del o los adversarios que tengan esa clave robada.
Si tomamos en cuenta que los adversarios clasificadores son programas de cómputo que solo leen el contenido del correo y buscan palabras específicas no necesitan tantos servicios criptográficos para detener los ataques a los correos electrónicos. Sería suficiente con tener un esquema de cifrado que proporcione confidencialidad durante el envío de mensajes.
Pero este esquema no solo tiene que preocuparse por la confidencialidad en el envío de los mensajes, también se enfrenta al problema de intercambio de claves para poder descifrar el mensaje por el usuario que recibe el mensaje.
Por lo tanto en este trabajo terminal se propone utilizar CAPTCHAS para el envío de claves entre los usuarios. Los CAPTCHAS contienen una cadena de caracteres que al ser resueltos por un ser humano es posible calcular la clave con que fue cifrado el mensaje, y como el adversario clasificador es un programa de cómputo, le es muy complicado encontrar la clave para descifrar el mensaje y poderlo clasificar correctamente.

1.2. Objetivos

1.2.1. Objetivos Generales

Desarrollar una herramienta para un cliente de correo electrónico que permita cifrar el contenido de los mensajes para evitar su clasificación, haciendo uso de técnicas criptográficas simétricas y un servidor que verifique el envío y recepción de CAPTCHAS entre usuarios.

1.2.2. Objetivos Específicos

1. Desarrollar una herramienta en un cliente de correo electrónico para el envío y recepción de los correos cifrados y la generación, envío y recepción de CAPTCHAS.

2. Desarrollar un servidor de llaves que reciba, aloje y envíe los CAPTCHAS a los usuarios para descifrar los correos electrónicos.

3. Desarrollar un algoritmo de cifrado y descifrado basado en el envío y recepción de CAPTCHAS.

1.3. PGP (Pretty Good Privacy).

Es un programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.
PGP es un sistema híbrido que combina técnicas de criptografía simétrica y criptografía asimétrica, la velocidad de cifrado del método simétrico y la distribución de la claves del método asimétrico.
Cuando un usuario emplea PGP para cifrar un texto en claro, dicho texto es comprimido. La compresión de los datos ahorra espacio en disco y tiempos de transmisión, después de comprimir el texto, PGP crea una clave de sesión secreta que solo se empleará una vez. Esta clave es un número aleatorio generado a partir de los movimientos del ratón y las teclas que se pulsen. Esta clave de sesión se usa con un algoritmo para cifrar el texto claro, una vez que los datos se encuentran cifrados, la clave de sesión se cifra con la clave pública del receptor y se adjunta al texto cifrado enviándose al receptor.
El descifrado sigue el proceso inverso. El receptor usa su clave privada para recuperar la clave de sesión simétrica, que PGP luego usa para descifrar los datos. [31]

1.4. GPG (GnuPG o GNU Privacy Guard).

GnuPG es una herramienta de seguridad en comunicaciones electrónicas desarrollada por Werner Koch. GnuPG, o también conocida como GPG, implementa el sistema de seguridad OpenPGP. OpenPGP es la implementación libre de PGP y esta bajo la licencia GPL.

GPG, al igual que PGP, utiliza criptografía de clave pública para que los usuarios puedan comunicarse de modo seguro. También cuenta con sistema de cifrado híbrido para mejorar la velocidad en envió de información y la posibilidad de manejar claves de sesión. [18]

Capítulo 2

Adversarios Clasificadores

Los adversarios clasificadores son programas de cómputo que se dedican a observar mensajes que se intercambian entre los usuarios de correo electrónico, con el fin de clasificarlos e identificar a todos los usuarios que cumplan con cierto criterio. Esta clasificación se hace de manera masiva a través de una búsqueda de palabras clave dentro de los mensajes de los usuarios. Por ejemplo, el clasificador puede estar interesado en los mensajes que contienen la palabra clave "Bomba", así que todos los mensajes que contengan esta palabra serán etiquetados en una clasificación en específico, este proceso se lleva a cabo por medio de técnicas de "Reconocimiento de patrones" y "Aprendizaje Máquina" para encontrar y clasificar los mensajes que intercepta [12, 13].
La clasificación de estos mensajes tiene diversos usos, ya que pueden ser clasificados con fines demográficos, con fines comerciales o con fines gubernamentales. Todo esto con el propósito de generar las estadísticas de comportamientos e intereses de los usuarios de correo electrónico.

En este trabajo terminal, se considera que un adversario clasificador solo es capaz de realizar ataques de texto cifrado (ciphertext only attack, en inglés). Como se mencionó en el capítulo anterior, en este ataque el adversario solo cuenta con los textos cifrados que va recopilando de un canal o base de datos. Posteriormente, el adversario utiliza estos textos cifrados para hacer un análisis criptográfico de cómo se comporta la técnica de cifrado y tratar de hallar el texto en claro a partir de los textos cifrados que va recopilando.
Este tipo de ataques es muy común en el internet aunque con muy baja efectividad cuando se implementa en comunicaciones altamente protegidas, y cuando se implementa en canales de comunicación desprotegidos la información obtenida llega a ser muy pobre. En los últimos años se han dado cuenta que si este tipo de adversarios atacan las comunicaciones sin cifrado se obtienen características valiosas sobre los usuarios que utilizan este tipo de canales de comunicación, este tipo de ataques son ejecutados por adversarios clasificadores.

2.0.1. Esquema Golle - Farahat

La única referencia que se tiene sobre un esquema criptográfico contra adversarios clasificadores es el que propusieron Golle y Farahat [13]. En este artículo se habla por primera vez de las características de este tipo de adversarios y se considera la posibilidad de utilizar un esquema de cifrado con un nivel de seguridad menor. Golle y Farahat proponen un protocolo

que hace uso de una función de cifrado, el cual sustituye cada una de las palabras del mensaje por otra de la misma extensión y frecuencia gramatical, esta función esta pensada para textos en idioma inglés. Para cifrar se utiliza una clave que se genera usando los datos de cabecera que acompañan al mensaje los cuales pueden ser dirección del remitente, la dirección del destinatario, la hora a la que se envía el correo electrónico y potencialmente otros campos. Estos datos se introducen en una función hash lenta y el resultado de esta función es la clave K. Estas funciones hash tiene con una complejidad de cálculo moderadamente mas alta que las funciones hash estándar.
Este protocolo resulta inseguro para la criptografía moderna pero es efectivo contra el ataque de clasificadores. Por otro lado este protocolo resuelve dos problemas, le permite a los usuarios calcular la clave de cifrado y descifrado fácilmente ya que los datos del mensaje con que se calcula son públicos, resolviendo así el intercambio de claves. Al usar un cifrado de tipo semántico se permite que el texto se vea como un texto en inglés pero indistinguible para los clasificadores y por lo tanto este clasifica incorrectamente el mensaje cifrado.

2.1. CAPTCHA

Es un programa informático diseñado para diferenciar un ser humano de una computadora, CAPTCHA son las siglas de prueba de Turing completamente automática y pública para diferenciar computadoras de humanos (*Completely Automated Public Turing test to tell Computers and Humans Apart* por sus siglas en inglés). Un CAPTCHA es una prueba que es fácil de pasar por un usuario humano pero difícil de pasar por una máquina. Uno de los CAPTCHAs más comúnes son imágenes distorsionadas de cadenas cortas de caracteres. Para un humano es generalmente muy fácil recuperar la cadena original de la imagen distorsionada, pero es difícil para los algoritmos de reconocimiento de caracteres recuperar la cadena original de la imagen distorsionada.
Un CAPTCHA en un algoritmo aleatorio G, que recibe como parámetro una cadena de caracteres STR y produce como resultado un CAPTCHA $G(x)$

Figura 2.1: CAPTCHA

2.2. Esquema de Secreto Compartido de Shamir

El esquema de secreto compartido fue propuesto por Adi Shamir en 1997 [24]. El objetivo de este método es dividir un secreto K en w partes,que son dadas a w participantes. Para recuperar el secreto es necesario tener al menos u elementos de las w partes siendo $u \leq w$. Y no es posible recuperar el secreto si se tienen menos que u partes.

Para construir el esquema del secreto compartido primero es necesario seleccionar un número primo $p \geq w + 1$ el cual define al conjunto $\mathbb{Z}_p$.

El procedimiento para dividir un secreto K en w partes es el siguiente:

1. Se seleccionan w elementos distintos de cero del conjunto $\mathbb{Z}_p$ denotados como x_i donde $1 \leq i \leq w$.

2. Se seleccionan $u - 1$ elementos aleatorios de $\mathbb{Z}_p$ denotados como $a_1, ..., a_{u-1}$.

3. Se construye el polinomio y_x de la siguiente forma. Sea

$$y(x) = K + \sum_{j=1}^{u-1} a_j x^j \text{ mód } \quad p \tag{2.1}$$

   Por medio de este polinomio se calculan los elementos y_i.

4. La salida es el conjunto $S = \{(x_1, y_1), ..., (x_w, y_w)\}$.

Para recuperar el secreto solo tenemos que resolver un sistema de ecuaciones que es definido por el polinomio característico $a(x) = a_0 + a_1 x + ... + a_{u-1} x^{u-1}$.

Posteriormente se seleccionan u pares de elementos (x_w, y_w) con los que obtendremos nuestro sistema de ecuaciones a resolver. El elemento que nos interesa obtener del sistema de ecuaciones es a_0 ya que este es el valor de nuestro secreto K.

Ejemplo 2.1 *Si se considera el conjunto $\mathbb{Z}_{11}$ y se desea compartir el secreto $K = 8$, entre 5 participantes, de tal manera que solo cuando se reúnan cualesquiera 2 de ellos sea posible recuperar K, es decir $w = 5$ y $u = 2$.*

Se seleccionan los $u - 1$ elementos del conjunto $\mathbb{Z}_{11}$, puesto que $u = 2$ en este caso solo hay que escoger un elemento: $a_1 = 5$.

A continuación se seleccionan w elementos de $\mathbb{Z}_{11}$, por ejemplo $x_1 = 2, x_2 = 7, x_3 = 9, x_4 = 10, x_5 = 3$.

Posteriormente, se calcula el conjunto de elementos y_i por medio de la ecuación

$$y_i = k + \sum_{j=1}^{u-1} a_j x_i^j \text{ mód } \quad p$$

En el caso del ejemplo, la ecuación anterior queda como sigue:

$$y_i = K + a_1 x_i \text{ mód } \quad p$$

Y se obtienen los siguientes valores:

$$\begin{aligned} y_1 &= 8 + 5(2) \text{ mód } 11 = 7, \\ y_2 &= 8 + 5(7) \text{ mód } 11 = 10, \\ y_3 &= 8 + 5(9) \text{ mód } 11 = 9, \\ y_4 &= 8 + 5(10) \text{ mód } 11 = 3, \\ y_5 &= 8 + 5(3) \text{ mód } 11 = 1. \end{aligned}$$

Finalmente, se tienen los pares $S = \{(2,7),(7,10),(9,9),(10,3),(3,1)\}$

Para recuperar la llave K *es necesario seleccionar* $u = 2$ *pares del conjunto* S*, por ejemplo* $A_2(7,10)$*,* $A_4(10,3)$*. Con estos pares se puede crear el siguiente sistema de ecuaciones:*

$$\begin{aligned} a_0 + a_1 x_2 &= y_2 \\ a_0 + a_1 x_4 &= y_4 \end{aligned}$$

Es importante notar, que en tal sistema de ecuaciones, las incógnitas son a_0 *y* a_1*, las cuales son desconocidas para los* w *participantes. Para el esquema de secreto compartido de Shamir, es de particular interés* a_0*, ya que* $a_0 = K$*. Al sustituir los pares* A_2 *y* A_4 *en el sistema de ecuaciones anterior, se tiene:*

$$a_0 + 7a_1 = 10 \tag{2.2}$$
$$a_0 + 10a_1 = 3 \tag{2.3}$$

Para resolver este sistema se puede utilizar cualquiera de los métodos comúnes que se usan en álgebra, solo que respetando el conjunto $\mathbb{Z}_p$*, en este caso se resolverá por el método suma y resta.*
Multiplicamos la ecuación (2.2) por -1 *y obtenemos:*

$$-a_0 - 7a_1 = -10 \tag{2.4}$$

sumamos la ecuación (2.3) con (2.4) dándonos como resultado:

$$3a_1 = 4$$

de donde es posible despejara$_1$

$$a_1 = \frac{4}{3} \tag{2.5}$$

Puesto que 4 es el inverso multiplicativo de 3, la ecuación (2.5) queda de la siguiente forma

$$a_1 = (4)(4) = 16 \text{ mód } 11 = 5$$

Sustituimos a_1 *en la ecuación (2.3)*

$$a_0 + 10(5) = 3$$

Simplificamos y despejamos a_0

$$\begin{aligned} a_0 + (50 \text{ mód } 11) &= 3 \\ a_0 = -3 \text{ mód } 11 &= 8 \end{aligned}$$

Como $a_0 = 8$ *podemos ver que se recuperó a* K *exitosamente ya que* $a_0 = K$*.*

2.2.1. Polinomio de interpolación de Lagrange

Para ejemplificar el método de Lagrange se usará el mismo ejercicio que en el método de Shamir.

Ejemplo 2.2 *Si se considera el conjunto* $\mathbb{Z}_{11}$ *y se desea compartir el secreto* $K = 8$*, entre 5 participantes, de tal manera que solo cuando se reúnan cualesquiera 2 de ellos sea posible recuperar* K*, es decir* $w = 5$ *y* $u = 2$*.*

Se seleccionan los $u - 1$ *elementos del conjunto* $\mathbb{Z}_{11}$*, puesto que* $u = 2$ *en este caso solo hay que escoger un elemento:* $a_1 = 5$*.*

A continuación se seleccionan w *elementos de* $\mathbb{Z}_{11}$*, por ejemplo* $x_1 = 2, x_2 = 7, x_3 = 9, x_4 = 10, x_5 = 3$*.*

Posteriormente, se calcula el conjunto de elementos y_i *por medio de la ecuación*

$$y_i = k + \sum_{j=1}^{u-1} a_j x_i^j \text{ mód } \quad p$$

En el caso del ejemplo, la ecuación anterior queda como sigue:

$$y_i = K + a_1 x_i \text{ mód } \quad p$$

Y se obtienen los siguientes valores:

$$\begin{aligned} y_1 &= 8 + 5(2) \text{ mód } 11 = 7, \\ y_2 &= 8 + 5(7) \text{ mód } 11 = 10, \\ y_3 &= 8 + 5(9) \text{ mód } 11 = 9, \\ y_4 &= 8 + 5(10) \text{ mód } 11 = 3, \\ y_5 &= 8 + 5(3) \text{ mód } 11 = 1. \end{aligned}$$

Finalmente, se tienen los pares $S = \{(2, 7), (7, 10), (9, 9), (10, 3), (3, 1)\}$

Para recuperar la llave K *es necesario seleccionar* $u = 2$ *pares del conjunto* S*, por ejemplo* $A_2(7, 10)$*,* $A_4(10, 3)$*. Con estos pares se puede crear el siguiente sistema de ecuaciones:*

$$\begin{aligned} a_0 + a_1 x_2 &= y_2 \\ a_0 + a_1 x_4 &= y_4 \end{aligned}$$

Es importante notar, que en tal sistema de ecuaciones, las incógnitas son a_0 *y* a_1*, las cuales son desconocidas para los* w *participantes. Para el esquema de secreto compartido de Shamir, es de particular interés* a_0*, ya que* $a_0 = K$*. Al sustituir los pares* A_2 *y* A_4 *en el sistema de ecuaciones anterior, se tiene:*

$$a_0 + 7a_1 = 10 \tag{2.6}$$

$$a_0 + 10a_1 = 3 \tag{2.7}$$

Para resolver este sistema se puede utilizar cualquiera de los métodos comúnes que se usan en álgebra, solo que respetando el conjunto $\mathbb{Z}_p$*, en este caso se resolverá por el polinomio de interpolación de Lagrange.*

$$a_x = \sum_{j=1}^{u} y_i \prod \frac{x - x_j}{x_i - x_j} mod \quad p \tag{2.8}$$

Al sustituir los valor A_2 *y* A_4 *en la ecuación anterior se puede calcular* a_0*. Pero una simplificación es posible, si se toma en cuenta que no es necesario conocer todo el polinomio,*

bastará con sólo deducir el termino a_0. Por lo tanto en la ecuación (2.8) se sustituye $x = 0$ quedando de la siguiente forma.

$$l_i = \prod \frac{-x_j}{x_i - x_j} \tag{2.9}$$

$$a_0 = \sum_{j=1}^{u} y_i \, l_i \, mod \quad p \tag{2.10}$$

Sustituyendo el par A_2 en la ecuación (2.9), se tiene:

$$l_2 = \frac{-x_4}{x_2 - x_4} = \frac{-10}{7 - 10} = \frac{-10}{-3} \, mod \, 11 = \frac{1}{8} \tag{2.11}$$

Se realiza la misma sustitución en la ecuación (2.9) pero con el par A_4 dándonos como resultado:

$$l_4 = \frac{-x_2}{x_4 - x_2} = \frac{-7}{10 - 7} = \frac{-7}{3} \, mod \, 11 = \frac{4}{3} \tag{2.12}$$

Como la ecuación (2.10) es una sumatoria podemos desarrollarla, dándonos como resultado:

$$a_0 = (y_2 \, l_2 + y_4 \, l_4) \, mod \, 11 \tag{2.13}$$

realizamos la sustitución de y_2, l_2, y_4 y l_4.

$$a_0 = (10 \, (\frac{1}{8}) + 3 \, (\frac{4}{3})) \, mod \, 11 \tag{2.14}$$

Puesto que 7 es el inverso multiplicativo de 8 y 4 es el inverso multiplicativo de 3, la ecuación (2.14) queda de la siguiente forma

$$a_0 = ((10) \, (7) + (3) \, (4)) \, mod \, 11 = 8 \tag{2.15}$$

Como $a_0 = 8$ podemos ver que se recuperó a K exitosamente ya que $a_0 = K$.

2.3. Esquema Díaz - Chakraborty

Otro esquema para combatir a los adversarios clasificadores fue propuesto en 2012 por Díaz y Chakraborty [12]. El esquema Díaz-Chakraborty utiliza CAPTCHAs y un algoritmo de clave secreta, para proteger el correo electrónico. Para obtener la clave se genera una cadena al azar, a la se le aplica una función hash, con esta clave se cifra el mensaje. Tanto el mensaje cifrado como el CAPTCHA se envían al receptor. El receptor debe resolver el CAPTCHA, para obtener la cadena, aplicarle la función hash y así obtener la clave de cifrado. Puesto que un adversario clasificador es un programa de cómputo, no podrá resolver un CAPTCHA y por tanto no podrá obtener la clave de cifrado. Este esquema se muestra en la Figura 2.2.

Contemplando que es muy común que el usuario no consiga resolver el CAPTCHA Díaz y Chakraborty propusieron una variante del esquema anterior, el cual se describe a continuación. Se genera una cadena de caracteres aleatoriamente llamada STR la cual se codifica

Protocol $\mathbb{P}(x)$

1. $k \xleftarrow{\$} \mathsf{STR}$;
2. $k' \leftarrow G(k)$;
3. $K \leftarrow H(k)$;
4. $c \leftarrow E_K(x)$;
5. **return** (c, k')

Figura 2.2: Protocol Díaz-Chakraborty.

a un valor entero. El valor entero es dividido en 5 pares (x, k') por medio del algoritmo de Secreto Compartido, cada uno de los elementos k' de los pares generados es decodificado a su correspondiente valor en cadena de caracteres para posteriormente ser convertidos en CAPTCHAS. Para finalizar la cadena STR se introduce en una función Hash para generar la llave K. Con esta llave se cifra el mensaje de correo y se envía junto con los pares de $(x, CAPTCHA)$. Este esquema se puede observar en la Figura 2.3.

Protocol $\mathbb{P}'(x)$

1. $k \xleftarrow{\$} \mathsf{STR}$;
2. $k' \leftarrow \mathsf{ENCD}(k, 0)$;
3. $\{(x_1, k'_1), \ldots, (x_w, k'_w)\} \leftarrow \mathsf{SHARE}^p_{u,w}(k')$;
4. **for** $i = 1$ **to** w;
5. $\quad (k_i, \lambda_i) \leftarrow \mathsf{ENCD}^{-1}(k'_i)$;
6. $\quad c_i \leftarrow G(k_i)$;
7. **end for**
8. $K \leftarrow H(k)$;
9. $C \leftarrow E_K(x)$;
10. **return** $[C, \{(x_1, c_1, \lambda_1), \ldots, (x_w, c_w, \lambda_w)\}]$

Figura 2.3: Variante del protocolo Díaz-Chakraborty

Este nuevo esquema se creó pensando en que el usuario pueda tener más oportunidades de recuperar el mensaje cifrado y esto sucede gracias a el algoritmo de Secreto Compartido, ya que no este podemos tener la misma llave repartida en n CAPTCHAS. A continuación se describe las funciones ENCD y ENCD^{-1}, cuyo propósito es convertir una cadena de caracteres a enteros y viceversa.

2.3.1. Codificación de caracteres a enteros

Se tiene un conjunto de caracteres AL compuesto por $AL = \{A, B, ..., Z\} \cup \{a, b, ..., z\} \cup \{0, 1, ..., 9\} \cup \{+, /\}$ con una cardinalidad $|AL| = 64$.

Para obtener una representación binaria de 64 elementos son necesarios 6 bits por lo que para todos los elementos $\sigma \epsilon AL$ existe una cadena binaria. Una vez establecido esto el procedimiento para realizar la conversión es el siguiente:

1. Tomamos una cadena de caracteres y la separamos caracter por caracter y los intercambiamos por su correspondiente número entero en AL $\alpha_0||\alpha_1||...||\alpha_m$

2. Posteriormente cada uno de los enteros lo convertimos en un binario de 6 bits y se concatenan uno detrás del otro $\Psi \longleftarrow bin_6(\alpha_0)||bin_6(\alpha_1)||...||bin_6(\alpha_m$

3. La cadena binaria Ψ la convertimos a entero $v \longleftarrow toInt(\Psi)$

Ejemplo:
Tenemos la cadena $STR =$ 'ABC' de la cual cambiaremos cada caracter por su correspondiente valor entero en AL quedando de la siguiente manera $\alpha = \{0, 1, 2\}$

Ahora cada uno de los elementos de α lo convertiremos a su correspondiente representacion binaria, $bin_6(0) = 000000, bin_6(1) = 000001, bin_6(2) = 000010$ y concatenamos cada una quedando $\Psi = 000000000001000010$.

La cadena binaria Ψ se convertirá en un entero $v = toInt(\Psi)$ que da como resultado $v = 66$. El entero v que obtenemos es el valor entero.

2.3.2. Decodificación de enteros a caracteres

También es necesario convertir un entero a una cadena de caracteres y para esto se realiza el proceso inverso:

1. El entero v es convertido en un número binario $z = toBin_6(v)$

2. Separamos z en cadenas de 6 bits y cada una de ellas la interpretamos como un entero $toInt(z_0)||toInt(z_1)||...||toInt(z_w)$

3. Cada uno de estos valores se convierte a su correspondiente caracter en AL se concatenan para generar la cadena de caracteres final.

Ejemplo:
El entero $v = 66$ se representa como una cadena de 18 bits $z = 000000000001000010$, la cual se divide en sub cadenas 6 bits quedando $z_0 = 000000, z_1 = 000001, z_2 = 000010$, para cada uno de estos números binarios se procede a convertirlo en un entero $toInt(z_0) = 0, toInt(z_1) = 1, toInt(z_2) = 2$, por último estos son intercambiados por sus correspondientes caracteres en AL y concatenados resultando en $s =$ 'ABC'

Capítulo 3

Tecnologías usadas

Tomando en cuenta la información ya vertida en este documento, a continuación se explicará detalladamente la propuesta de solución.
En la figura 3.1 se tiene el diagrama general del sistema, se puede apreciar la comunicación entre las diferentes entidades que se usaran, que datos se mandan y reciben y por que canales transitan estos datos. A continuación se describe de manera general como es el proceso de envío y recepción de correos electrónicos ideado para este esquema.

1. Envío
    - El remitente escribe el correo electrónico y le da enviar.
    - El correo electrónico pasa por el complemento del cliente de correo.
    - El cliente genera a partir del correo una clave que usaremos para cifrar el mensaje.
    - Se cifra y se empaqueta el mensaje con el protocolo SMTP.
    - Se coloca una bandera en el mensaje.
    - La clave se convierte en CAPTCHA y es enviada al servidor de CAPTCHAS.
    - Se envía el mensaje de correo electrónico al destinatario.
2. Recepción
    - El receptor abre un correo electrónico cifrado con el presente esquema.
    - El cliente lo descarga del servidor por medio del protocolo POP3 o IMAP.
    - Se hace una petición al servidor de CAPTCHAS para recuperar los CAPTCHAS del correo.

- El usuario resuelve el CAPTCHA y se recalcula la clave de descifrado.
- Se descifra el mensaje y se le muestra al usuario.

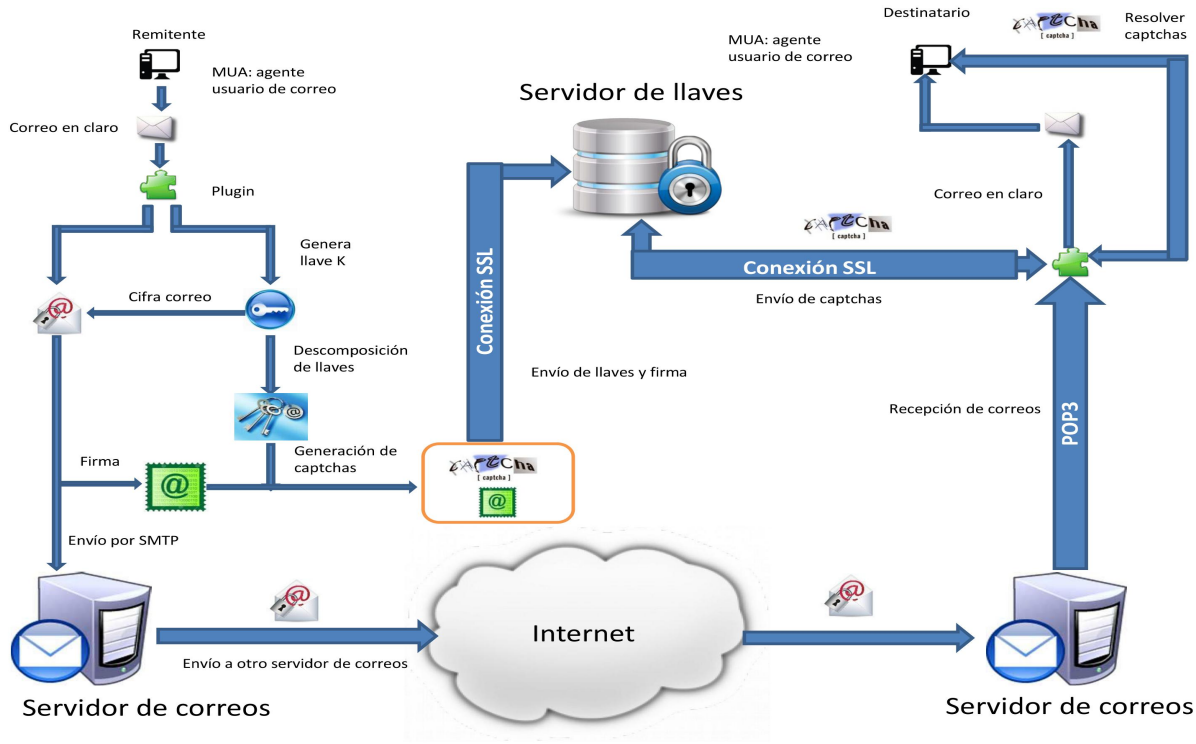

Figura 3.1: Diagrama General del sistema

3.1. Tecnologías

Como ya se ha visto en el esquema anterior se necesita hacer uso de las herramientas adecuadas para poder desarrollar este esquema de cifrado. Las herramientas que se analizaron se describen en las siguientes secciones.

3.1.1. Cliente de correo electrónico

Un cliente de correo electrónico es necesario para el desarrollo de este proyecto ya que en él se instalará un complemento que cifre el mensaje, envíe los CAPTCHAS y descifre los mensajes de correo electrónico. Para ello buscamos un cliente de correo electrónico que cuente con el soporte de los protocolos POP3, SMTP y IMAP; sus licencias son de código libre; soporte la instalación de APIs externas; y tenga soporte en los sistemas operativos ***Windows***, ***IOS*** y ***Linux***. Por lo tanto se investigaron los siguientes clientes de correo electrónico que se encuentra en el mercado:

Cliente de correo electrónico	Sistema Operativo	Protocolos soportados	Código Libre	Agregar funcionalidad	Extra	Gratuita o de paga
eM client	Windows 7, 8 & 10 ; IOS	POP3, SMTP, IMAP, EWS, AirSyn	NO	NO	100 % compatible con gmail y sus APIs	Ambos
Postbox	Windows, IOS	POP3, SMTP, IMAP	NO	SI por medio de APIs	Sincronización con Dropbox, OneDrive, Facebook y Twitter	Ambos
Zimbra	Windows, IOS & Linux	POP3, SMTP, IMAP	SI	SI por medio de APIs	Una plataforma de nivel empresarial y capas se soportar sincronización con múltiples servicios	Ambos
Opera Mail	Windows, IOS & Linux	POP3, SMTP, IMAP	SI	NO	La plataforma para desarrollar en Opera se actualiza cada semana	Gratuito
Thunderbird	Windows, IOS & Linux	POP3, SMTP, IMAP	SI	SI por medio de APIs	Cliente de correo versátil y fácilmente escalable y una comunicad de desarrollo bastante amplia	Gratuito
Nylas N1	Windows, IOS & Linux	POP3, SMTP, IMAP	SI	Si directamente compilando		Gratuito

- El cliente de correo electrónico ***eM client*** tiene una sincronización a 100 % con las cuentas de ***Gmail*** y sus APIs, cuenta con una versión gratuita y una versión de paga; puede hacer migración de mensajes de correo electrónico y contactos de diversos clientes de correo electrónico y tiene una compatibilidad con muchos servidores de correo electrónico. [2]
  Su desventaja es que su código es cerrado y permite agregar funcionalidades.

- El cliente de correo electrónico ***Postbox*** esta soportada en los sistemas operativos ***Windows 7*** o posteriores y ***IOS***, esta aplicación es generada por el servidor de correo electrónico ***Postbox*** por lo tanto cuenta con una sincronización al 100 % con este servidor, también soporta otros servidores de correo como ***Gmail*** y ***Outlook***; este

cliente puede sincronizarse con ***Dropbox***, ***Onedrive*** y redes sociales como ***Facebook***, ***Twitter***, entre otras. Es posible agregar más funcionalidades con la instalación de APIs.
Una desventaja de esta aplicación es que su código es cerrado, pero gracias a que esta basado en código de ***Mozilla*** puedes desarrollar APIs para agregarle tus propias funciones. [4]

- El cliente de correo electrónico ***zimbra*** es la aplicación más completa que se analizó, tiene compatibilidad con el servidor ***zimbra*** pero es capaz de soportar otros servidores de correo electrónico, se encuentra en los 3 sistemas para PC, ***Windows***, ***IOS*** & ***Linux***, da la facilidad de agregarle funcionalidades por medio de la instalación de APIs y gracias a que su código es abierto se pueden programar funciones propias. Este cliente cuenta con la versión gratuita y la versión de paga. Una gran ventaja que tiene es que oferta certificaciones en el desarrollo APIs para este cliente de correo electrónico. [6]
  La única desventaja que se encontró en este cliente de correo es que la plataforma es demasiado grande y el tiempo que se necesita invertir al estudio del código es demasiado y el tiempo de desarrollo de este proyecto es muy corto.

- ***Opera mail*** es un cliente de correo electrónico que salió al mercado recientemente y se puede instalar en los sistemas operativos ***Windows***, ***IOS*** & ***Linux***, es capaz de comunicarse con diversos servidores de correo electrónico y su código es de libre acceso. Su principal desventaja es que las funcionalidades que se quieran agregar no pueden ser adquiridas por medio de la instalación de complementos o APIs. [3]

- Por último tenemos a ***Thunderbird*** que es un cliente de correo electrónico desarrollado por ***Mozilla***, este cliente es de código abierto y la instalación de APIs para agregar funcionalidad es demasiado sencilla; es un cliente de correo que puede ser instalado en los sistemas operativos ***Windows***, ***IOS*** y ***Linux***. [5]

Por lo tanto el cliente de correo electrónico que se usará es ***Thunderbird***, al ser un cliente de correo electrónico casi tan completo como ***zimbra*** pero con la facilidad de desarrollar APIs más rápido.

3.1.2. Lenguajes de programación.

Uno de los objetivos que se tienen en este proyecto es generar un complemento para un cliente de correo electrónico por lo tanto al escoger a ***Thunderbird*** como cliente tenemos que programar con el lenguaje que fue desarrollado para tener la mayor compatibilidad.
Para el desarrollo de este proyecto se utilizará [5]:

- Lenguaje Python
- HTML 5
- CSS3

A pesar de ser una aplicación de escritorio este cliente de correo electrónico está construido con lenguajes web.

3.1.3. Tipos de CAPTCHAS

En el esquema de cifrado es necesario esconder la palabra que genera la clave en un CAPTCHA para ser enviado a otro usuario y descifre el mensaje, pero existen varios tipos de CAPTCHAS que se pueden utilizar [22].
Los CAPTCHAS se pueden clasificar de la siguiente forma:

- CAPTCHAS de texto: Este tipo de CAPTCHAS genera una pregunta sencilla donde la respuesta a la pregunta es la respuesta al CAPTCHA.
- CAPTCHAS de imágenes: Este tipo de CAPTCHAS nos muestran en una imagen una cadena de caracteres distorsionados, esta cadena de caracteres es la repuesta del CAPCHA transformada en una imagen.
- CAPTCHAS de audio: Este tipo de CAPTCHAS se caracterizan por ser un audio con ruidos de fondo, donde nos dirán la respuesta oculta.
- CAPTCHAS de video: Este tipo de CAPTCHAS nos muestran un video de unos cuantos segundos donde una palabra aparece alrededor de la pantalla, esta palabra es la respuesta al CAPTCHA.
- CAPTCHAS de acertijos: Este tipo de CPATCHAS es versatil, ya que se trata de pequeños acertijos que resolver donde la respuesta no es una palabra si no una acción o serie de acciones. Los CAPTCHAS de acertijos pueden ser armar un rompecabezas pequeño, seleccionar la imagen que no corresponde, unir figurar geométricas, etc.

Para poder decidir qué tipo de CAPTCHAS se utilizará se consideró los siguientes puntos:

- Facilidad de creación.
- Peso en bytes del CAPTCHA.
- Forma del despliegue.
- Tipo de respuesta.

Por lo tanto se necesita un tipo de CAPTCHA con poco peso, cuya respuesta sea una cadena de caracteres y su forma de despliegue sea fácil de implementar.
Considerando las necesidades anteriores las opciones son CAPTCHAS de imágenes y CAPTCHAS de texto, pero en este proyecto se utilizarán los CAPTCHAS de imágenes porque en ellos seran almacenadas las palabras claves de cifrado de los diferentes mensajes de correo electrónico y estas son cadenas de caracteres que no se les puede generar una pregunta coherente.

3.1.4. Bases de datos para almacenar los CAPTCHAS.

Para escoger un gestor de base de datos que controle la información de los usuarios registrados en la aplicación propuesta, la información de los mensajes que envían entre usuarios y los CAPTCHAS asociados a los mensajes para ser descifrados se consideraron 3 características principales en un gestor base de datos relacional:

- Rapidez en transferencias de información.
- Número de usuarios conectados que soporta.
- Facilidad de comunicación entre los lenguajes Python, HTML con los gestores de base de datos.

Los 3 gestores que se analizaron fueron SQLite, MySQL y PostGreSQL.
SQLite es un gestor de base de datos sumamente ligero que soporta hasta 2 terabytes de información, esta base de datos es compatible con python y lenguajes de programación web. Este gestor por su misma ligereza es posible implementarla en dispositivos móviles, pero no es recomendable cuando múltiples usuarios están haciendo peticiones al mismo tiempo ya que su rendimiento baja [27].
MySQL es un gestor de base de datos que se caracteriza por su transferencia al hacer consultas de datos almacenados; es uno de los gestores libres más utilizados en aplicaciones web y cuenta con diferentes APIs para hacer la comunicación con los lenguajes Python, PHP, C++, etc. Y soporta peticiones de múltiples usuarios gracias a la implementación de hilos.
PostGreSQL es un gestor de base de datos que puede hacer operaciones complejas como subconsultas, transacciones y rollbacks's. Soporta las peticiones de múltiples usuarios pero en cuanto a la velocidad de transferencia de información, comparado con MySQL, es muy lenta pero lo compensa manteniendo una velocidad casi invariable a pesar de que la base se mantenga con un número grande de registros. [19]
Se eligió el gestor de base de datos MySQL porque el proyecto necesita mayor rapidez en la transferencia de información más que generar filtros muy complejos para la búsqueda de información.

Capítulo 4

Desarrollo de prototipos

4.1. Prototipo 1

Objetivo del prototipo: Conocer el uso, funcionamiento e implementación de herramientas de cifrado, hashing y generación de CAPTCHAS, con el fin de conocer la integración de estos módulos en diferentes lenguajes de programación.
Se implementó un módulo de cifrado de mensajes de texto en lenguaje C++. Tratando de simular el proceso de cifrado del esquema que se esta usando.
La primera parte del proceso es abrir el mensaje para lo cual se estan usando los métodos estándar definidos en las bibliotecas nativas de C++, posteriormente se generará una palabra aleatoria de 5 caracteres usando una función Rand() %100 y transformando el valor de salida a un char.
Al resultado se pasa por una función de hashing, esta función no es nativa de ninguna biblioteca estándar de C++ ni de C, por lo que se tuvo que conseguir una en internet y probar que efectivamente funcionara como se necesita.
Posteriormente este hash se usará como clave para cifrar el mensaje que ya se ha abierto, para esto se necesita una función AES o DES, ninguna de éstas es estándar de alguna biblioteca de C o C++, así que se tendrá que buscar y verificar su funcionamiento.

Conclusión: Podemos ver que en C++ el proceso es simple pero se necesita buscar muy bien las bibliotecas externas que se usarán, ya que no siempre están funcionando correctamente, en algunos casos estas ni siquiera compilan.
Este caso fue particularmente evidente al buscar una biblioteca de C o C++ que pudiera realizar el cifrado con AES o DES, se encontro con bibliotecas que cifraban mal ya que al meter la misma llave no descifraban e incluso bibliotecas que no se lograron compilar.

4.2. Prototipo 2

Se implementó un módulo de cifrado, descifrado y generación de CAPTCHAS en Python, simulando el proceso antes del envío del correo y el que se hace después de la recepción de los correos electrónicos.

Para este se usó el formato estándar del correo electrónico especificado en el RFC 822, también se usaron bibliotecas ya estandarizadas de Python para la implementación de las funciones de hashing, funciones de cifrado y descifrado (AES o DES), funciones aleatorias y la generación de los CAPTCHAS. El codigo fuente de las funciones se encuentra en el Anexo 1.

Conclusión: Se logró generar todo el proceso de envío y parte del proceso de recepción de mensajes. En cuanto al envío se logró leer el mensaje, crear una palabra a partir de funciones random, crear la clave con dicha cadena de caracteres y cifrar el correo exitosamente, además de esto se logró leer el archivo de mensaje de correo electrónico y cifrar únicamente el mensaje que viene en este.
Por su parte el módulo de generación de CAPTCHAS mostró muchos problemas para generarlos, ya que no se logró hacer que el intérprete pudiera encontrar correctamente las funciones de la biblioteca de generación CAPTCHAS por lo que al no poder generar un CAPTCHA la recuperación no se puede realizar como se planteó, para verificar únicamente que las funciones trabajan correctamente se implementó el descifrado del mensaje en el mismo método.

4.3. Prototipo 3

Objetivo Generar una imagen CAPTCHA a partir de una cadena de caracteres ingresada desde una interfaz gráfica. Este prototipo se construyó en 2 partes; la primera parte fue la interfaz gráfica y sus herramientas, y la segunda en las herramientas para generar la imagen a partir de una cadena de caracteres.
Para la interfaz gráfica se utilizaron las siguientes herramientas para desarrollar este prototipo:
Biblioteca ***Qt*** y ***Qt creator***: Utilizamos esta biblioteca para generar la interfaz gráfica con la que ingresa la cadena de caracteres y el IDE ***Qt Creator*** para facilitar la gestión de las clases.
La interfaz gráfica consta de un apartado para ingresar la cadena de caracteres y un botón para convertir la cadena a una imagen de CAPTCHAS.
Para generar CAPTCHAS se utilizaron las siguientes herramientas:
Lenguaje PHP: se utilizó para genera las imágenes CAPTCHAS con la cadena de caracteres proporcionada anteriormente.
En un principio se buscó una biblioteca que generara las imágenes CAPTCHAS en el lenguaje C++, pero las bibliotecas de imagenes encontradas no hacen rotaciones, inclinaciones, cambio de tamaños y colores variables para generar CAPTCHAS, por lo tanto las bilbiotecas encontradas tenían que adaptarse a la funcionalidad del prototipo.
Conclusión. La generación de imágenes CAPTCHAS es rápida y fácil de implementar, pero durante la investigación llegamos a la conclusión que el cliente de correo "Thunderbird" está desarrollado en el lenguaje de programación Python y al no tener una biblioteca nativa en el lenguaje C++ para convertir una cadena de caracteres en CAPTCHAS y se decidió cambiar de lenguaje de programación.

4.4. Prototipo 4

Objetivo del prototipo. Instalar y configurar un servidor de correo electrónico para el envío de mensajes de correo electrónico entre diferentes usuarios.
Instalación y configuración de un servidor de correo electrónico y un servidor DNS.

Para el desarrollo de este prototipo fue necesario instalar el servidor de correo electrónico con el protocolo pop y imap, un cliente de correo electrónico web, un servidor DNS y el servidor HTTP Apache. Estos 3 servicios se levantaron en una computadora con un sistema operativo Xubuntu 15.04; primero se instaló el servidor HTTP [8], posteriormente se pasó a la instalación del servidor DNS y configuración de un dominio [23]; se seguió con la instalación del servidor de correo electrónico y los protocolos pop y imap; y por último se instaló y configuró el cliente de correo web [9].
Para la instalación de servidor HTTP fue necesario seguir los siguientes pasos:

- Se abre una terminal en Ubuntu y se escribe el comando: "sudo apt-get install apache2"
- Se abre como administrador el archivo /etc/apache2/sites-enabled/00-default.conf y se escribe la siguiente configuración:

```
<VirtualHost *:80>
    ServerAdmin nombredelsitio@example.com
    ServerName nombredelsitio
    ServerAlias www.nombredelsitio.com
    DocumentRoot /var/www/nombredelsitio.com/public_html/
    ErrorLog /var/www/nombredelsitio.com/logs/error.log
    CustomLog /var/www/nombredelsitio.com/logs/access.log
     combined
</VirtualHost>
```

- Se levanta el servicio http con el siguiente comando: "sudo service apahce2 start"
- Para verificar la instalación Se abre un explorador y escribirlos en la barra de búsqueda la siguiente dirección: http://localhost/ y nos aparecerá la siguiente pantalla.

Una vez instalado el servidor HTTP se prosigue a instalar el servidor DNS, para levantar este servicio es necesario seguir los siguientes pasos:

- Se selecciona un nombre de dominio, para fines prácticos nuestro dominio privado será "correocifrado.edu".
- Se abre una terminal en Ubuntu y se escribe el siguiente comando: "sudo apt-get install bind9"
- Realizar una copia de respaldo del archivo de configuración original con el comando "cp /etc/bind/named.conf.local
  /etc/bind/named.conf.local.original"
- Se edita el archivo de configuración con: "nano /etc/bind/named.conf.local"

- Se agrega al final del archivo lo siguiente:

```
zone "correocifrado.edu" {
type master;
file "correocifrado.edu.zone";
};

zone "10.168.192.in-addr.arpa" {
type master;
file "db.192.168.10";
};
```

- Se procede a crear los (nuevos) archivos de zona, esos archivos contienen los registros del DNS y en Ubuntu se encuentran en el directorio /var/cache/bind/ "nano /var/cache/bind/db.isti.edu.ni.zone"

- En el archivo Se agrega el siguiente texto:

```
$ORIGIN correocifrado.edu.
$TTL 86400              ; 1 dia
@  IN  SOA ns.correocifrado.edu. info.correocifrado.edu. (
        2014112401      ; serie
        6H              ; refresco (6 horas)
        1H              ; reintentos (1 hora)
        2W              ; expira (2 semanas)
        3H              ; minimo (3 horas)
)

@       IN      NS      ns
@       IN      MX 10   mail
ns      IN      A       192.168.10.10
mail    IN      A       192.168.10.10
www     IN      A       192.168.10.10
```

- De igual manera el archivo de zona de búsqueda inversa:
nano /var/cache/bind/db.192.168.10

- Se agrega la siguiente configuración:

```
$ORIGIN 10.168.192.in-addr.arpa.
$TTL 86400      ; 1 dia
@  IN  SOA ns.correocifrado.edu. info.correocifrado.edu. (
        2014112401      ; serie
        6H              ; refresco (6 horas)
        1H              ; reintentos (1 hora)
        2W              ; expira (2 semanas)
        3H              ; minimo (3 horas)
)
```

```
@       IN      NS      correocifrado.edu.
10      IN      PTR      correocifrado.edu.
10      IN      PTR      mail.correocifrado.edu.
10      IN      PTR      www.correocifrado.edu.
```

- Se procede a re-iniciar el servicio con el comando “service bind9 restart”
- Cambiar el primero de los servidores DNS por la IP del nuestro: “nameserver 192.168.10.10”
- Por último se ejecuta el siguiente comando “nslookup www.correocifrado.edu” y nos dará un resumen de los DNS configurados.

Se prosigue con la instalación del servidor de correo electrónico y los servicios del protocolo pop y imap con la aplicación courier-pop y courier-imap:

- Se abre una terminal y se escribe el siguiente comando: “sudo apt-get install postfix”
- Durante la instalación aparecerá una pantalla de configuración, se da enter para aceptar la configuración.
- En tipo genérico de configuración de correo se selecciona "Sitio de Internet".
- A continuación se indica el nombre de sistema de correo, normalmente la dirección del dominio registrado, en este caso çifradocorreo.net".
- Con esto se verá que postfix termina de instalarse y se procede a editar el archivo “/etc/postfix/main.cf”.
- Se añade al final del fichero main.cf las líneas:

```
  inet_protocols = ipv4
home_mailbox = emails/
```

- Una vez guardado el archivo que se edita se procede a reiniciar el servidor con el comando “sudo /etc/init.d/posrfix restart”

Una vez instalado el servicio de correo electrónico se procede a instalar el courier-pop y el courier-imap.

- Se abre una terminal el Ubuntu y se escribe el siguiente comando “sudo apt-get install courier-pop”.
- Nos mostrará una ventana de configuración de courier-base, se selecciona “NO”.
- Se procede a instalar courier-imap con el siguiente comando “sudo apt-get install courier-imap”.
- Se espera a que finalice la instalación.

Por último es necesario instalar una aplicación webmail para enviar correos entre usuarios del correo electrónico.

- Se abre una terminal en Ubuntu y se escribe el siguiente comando “sudo apt-get install squirrelmail”.
- Tras la instalación de SquirrelMail se configura ejecutando el siguiente comando “sudo squirrelmail-configure”
- Se selecciona la letra D y se da enter.
- En este nuevo menú se teclea la opción courier y se da enter.
- Nos dará un informe de la configuración que se seleccionó y se da enter para continuar.
- Se regresa al primer menú, ahora se teclea el número 2 y se da enter.
- Se selecciona en este nuevo menú la opción 1 y se da enter nuevamente.
- Pedirá nuestro nombre de dominio, en este caso es el dominio que se configuró en el servidor DNS “correocifrado.net”
- Regresará al menú principal y se teclea la letra Q para salir de la configuración.
- Preguntará si queremos guardar los cambios y se teclea la letra Y.
- Por último se ejecuta el siguiente comando para levantar SquirrelMail en Apache “sudo ln -s /usr/share/squirrelmail /var/www/webmail”
- Se reinicia el servicio apache con el comando “sudo service restart apache2”.
- Se podrá entrar a la aplicación escribiendo el explorador “www.correocifrado.edu/webmail”

Para poder enviar correos se necesitan usuarios que desean enviar mensajes entre usuarios, primero se creará un usuario

- Se abre una terminal de Ubuntu y se escribe el siguiente comando “sudo adduser nombreusuario”.
- Se introduce la nueva contraseña de UNIX: introduciremos la contraseña para el usuario, es importante que sea segura (números, letras, mayúsculas y minúsculas) pues con el usuario y la contraseña podremos acceder vía web al servidor de correo electrónico desde cualquier parte del mundo.
- Vuelva a escribir la nueva contraseña de UNIX: se repite la contraseña.
- Full Name: Se introduce el nombre completo, por ejemplo “Alicia Robles Maldonado”.
- Room Number: Número de oficina.
- Work Phone: teléfono del trabajo.
- Home Phone: teléfono particular.
- Other: otros datos del usuario.

- Se responde “S” a la pregunta “¿Es correcta la información?”. Y se tendrá el usuario creado en el sistema operativo, que también servirá como usuario (buzón) para el servidor de mail.
- Ahora se generará el buzón con el siguiente comando “sudo maildirmake /home/nombreusuario/emails”
- Se cambian los permisos de las carpeta emails con el comando “sudo chdown nombreusuario:nombreusuario /home/nombreusuario/emails -R

Para crear otro usuario es necesario repetir los pasos anteriores.

4.5. Prototipo 5

Objetivo: Familiarizarse con el uso de la tecnología y estructura del cliente de correo electrónico Thunderbird.
Se planeó la creación de un completo para el cliente de correo electrónico Thunderbird, para dar paso al desarrollo del complemento es necesaria la documentación de dicho cliente de correo, la cual debe de ser debidamente requisitada a su desarrollador que en este caso es Mozilla. El cliente Thunderbir al ser un cliente de software libre debe de contar con una documentación pública. Al buscar documentación en la página de desarrollo de Mozilla resulta evidente que no está, pero puede ser pedida a Mozilla por medio de la misma página. La documentación fue pedida el 03-03-16 y a la fecha de escritura de este reporte 20-04-16 no se ha obtenido una respuesta por parte de Mozilla.
Conclusión: Por el tiempo de respuesta y la falta de documentación implementar un complemento para thunderbird en el tiempo proporcionado para este trabajo terminal no es viable.

4.6. Prototipo 6

Objetivo: Familiarizarse con el uso de las tecnologías y estructuras de Nylas N1, así como verificar su viabilidad como solución factible para el presente trabajo.
La documentación de este cliente de correo electrónico es fácil de conseguir ya que es pública directamente en su página oficial, además de contar con breves tutoral de como usarse. Se implementó sobre la interfaz incluir imágenes y mostrar información nueva sobre el panel auxiliar, también la obtención directa del cuerpo del mensaje para poder procesarlo, agregar una clase dentro del complemento que permita la comunicación con el servidor de CAPTCHAS.

- Inclusión de texto e imagen en la interfase: El mismo N1 da la posibilidad de generar tu propio complemento de correo ya que el mismo te proporciona un formato estándar y una opción para modificar los textos de sus diferentes áreas, se modifico justo la opción de texto en la barra lateral derecha pero para agregar una imagen y texto al mismo tiempo.
- Obtención del cuerpo del mensaje: Despues de analizar la estructura del complemento se creo uno propio en el cual se mandaron llamar el cuerpo del mensaje y el asunto por medio de métodos que el mismo N1 proporciona.

- Comunicación con el servidor de CAPTCHAS: En complemento creado por nosostros se generó una clase que hace una llamada al servidor de CAPTCHAS que espera una respuesta para poder empaquetar el nuevo cuerpo del mensaje y poder mandarlo por correo. Todas estas clases están implementadas en CoffeScript este lenguaje no es secuencial si no concurrente, como la función de empaquetamiento del cuerpo espera la respuesta del servidor y esta no llega si no hasta después de que ya se ejecutó esta función genera un error.

Conclusión: No es posible hacer una sincronización con los servidores externos que necesitamos, por lo que la implementación no es viable en Nylas N1.

4.7. Prototipo 7

Objetivo: Evaluar la viabilidad y compatibilidad del algoritmo de cifrado así como su integración con Nylas N1.
Se implementaron los algoritmos de cifrado, descifrado, generación de llave y generación de CAPTCHA en el lenguaje JavaScript. considerando que Nylas N1 esta implementado en CoffeScript que es una versión de escritorio de JavaScript.

- Generación de llave: Se genera una cadena de caracteres aleatorio de tamaño 5. Primero se genera un número aleatorio del 0 al 63 y este se manda a otra función que lo mapea a su caracter correspondiente en el conjunto de enteros $AL = \{A-Z\} \cup \{a-z\} \cup \{0-9\} \cup \{+,/\}$

```
  var map;map = [];

map=["A","B","C","D","E","F","G","H","I","J","K","L","M","N"
,"O","P","Q","R","S","T","U","V","W","X","Y","Z","a","b","c"
,"d","e","f","g","h","i","j","k","l","m","n","o","p","q","r"
,"s","t","u","v","w","x","y","z","0","1","2","3","4","5","6"
,"7","8","9","+","/"];
//alert(map.length);

function CtoI(let){
        var a;
        for (var i = 0; i < map.length; i++) {
                if (map[i]==let) {
                        a=i;
                        //alert(a);
                }
        }
        return a;
}

function ItoC(num){
        return map[num];
}
```

de esta cadena generaremos un digesto por medio de una función hash sha256 y recortada a una cadena de caracteres tamaño 16 la cual se usará como llave para la función de cifrado.

- Cifrado: se cifra el texto con una función AES 128bits usando la llave generada anteriormente
- Generación de CAPTCHA: JavaScript no tiene métodos propios de edición de imagen ni bibliotecas de creación de CAPTCHAS, pero se pueden pasar las variables declaradas en JavaScript a PHP y que este lenguaje termine el proceso, solo que es necesaria la creación de un formulario HTML para que esto suceda, en el caso nuestro esto no es factible ya que Nylas N1 no hace uso de estas herramientas.

```
 var semilla="";
for (var i = 0; i < 5; i++) {
        var r = Math.floor((Math.random() * 63) + 1);
        semilla=semilla + ItoC(r);
}

alert(semilla);

var shaObj = new jsSHA("SHA-1", "TEXT");
shaObj.update(semilla);
var hash = shaObj.getHash("HEX");

alert(hash);
var llave;
llave = hash[0];
//llave = llave + hash[1];
for (var i = 1; i < 16; i++) {
        llave=llave + String(hash[i]);
}
alert(String(llave));

usedKey=llave;
myStr="Osama Oransa2012Osama Oransa2011RashaOsama Oransa2012Osa
Oransa2011RashaOsama Oransa2012Osama Oransa2011RashaOsama
Oransa2012Osama Oransa2011Rasha";
alert(myStr);

var key=init(usedKey);
alert(key);
encrypted=encryptLongString(myStr,key);
alert('after encrypt='+encrypted);
decrypted=decryptLongString(encrypted,key);
alert('after decrypt='+decrypted);
finish();
```

Conclusión: El uso de JavaScript para implementar el esquema propuesto en este trabajo no es totalmente posible ya que el mismo lenguaje no nos permite la creación de CAPTCHAS ni la llamada a sistema por lo que limita la capacidad de desarrollo.

4.8. Prototipo 8

Objetivo: Crear una biblioteca en lenguaje Python que contenga el esquema de cifrado por CAPTCHA. El cliente de correo electrónico ***Thunderbird*** tiene una parte implementada en python, pensado para esto se implemento el presente esquema en el lenguaje Python. Para continuar con el desarrollo del presente trabajo se decidió crear una biblioteca en el lenguaje Python.
En esta biblioteca se implementaron en métodos por separado: la creación de la cadena original llamada semilla, la creación de la llave, la creación del CAPTCHA, cifrado y descifrado. En esta biblioteca se esta considerando un esquema en el cual se pueda generar un solo CAPTCHA por mensaje cifrado o "n"número de CAPTCHA's por cada mensaje cifrado, para el esquema multi CAPTCHA se hace uso de el algoritmo de secreto compartido por lo que para este se implementaron los metodos: Codificación, decodificación, repartir el secreto y recuperar el secreto. El código fuente se encuentra en el Anexo 2.

- Crear Semilla: para este método originalmente esta configurado para hacer una palabra de 5 caracteres, pero puede introducir manualmente el numero de caracteres deseados, esto es generando 5 números aleatorios en un rango de 0 a 63 que posteriormente son asignados a su correspondiente caracter en el conjunto de enteros $AL = \{A-Z\} \cup \{a-z\} \cup \{0-9\} \cup \{+, /\}$

- Crear Llave: En este método se manda la semilla y a esta se le genera un digesto con una función SHA256 que posteriormente es recortada a 16 bits.

- Crear CAPTCHA: este método recibe la opción, la semilla, y el asunto. La opción define cual es el funcionamiento de este método, si la opción es 0 el método toma la semilla y crea un CAPTCHA a partir de ella usando la biblioteca CAPTCHA de Python. Por el contrario si la opción es 1 lo que recibe la función en el parametro semilla, es un arreglo de caracteres y uno a uno lo convierte en CAPTCHA. En el caso particular de la generación de CAPTCHAS, se modificó la biblioteca que los crea, ya que esta función arrojaba CAPTCHAS ilegibles.

- Codificar: La función Codificar toma como parámetro, una cadena de caracteres y la transforma en un número entero, primero caracter a caracter se busca su correspondiente número entero en el conjunto de enteros AL posteriormente este se pasa a una representación en 6 bits y por último se convierte a un número entero.

- Decodificar: La función decodificar recibe como parámetro un número entero y el número de partes en las que tiene que partir el número, esto lo hace convirtiendo el número entero a su representación binaria, posteriormente se separa en números binarios de 6 bits y cada uno es convertido en un número entero e intercambiado por su correspondiente caracter del conjunto de enteros AL.

- Generar Partes: Se reciben como parámetro el conjunto de enteros módulo Zp , el número de partes en que se dividirá el secreto w, el número de partes necesarias para

recuperar el secreto t y el secreto k. Se generan aleatoriamente w que son las x e igualmente de manera aleatoria se generan t elementos que son los elementos a, con esto se genera la sumatoria correspondiente para generar los elementos y. La función retorna pares de números que están conformados por x, y.

- Recuperar secreto: por medio del algoritmo de Lagrange se resuelve el sistema de ecuaciones y así recuperando el secreto

- Cifrar: Este método recibe como parámetro el cuerpo del mensaje, el asunto y de manera opcional recibe la opción de cifrado, el número de caracteres de los CAPTCHAS, el número de partes en que se divide el secreto, y el número de pares necesarios para recuperar el secreto. Este método hace las funciones de un main, ya que en este método se invocan todos los demás para poder realizar el funcionamiento del esquema completo. Este método tiene dos funciones, la primera es la opción 0 en la que se crea la semilla, se calcula el conjunto de enteros módulo Zp, con la semilla se crea el CAPTCHA con opción 0, con la semilla se crea la llave y con esta se procede a cifrar el cuerpo del mensaje siempre cuidando que los bloques sean del tamaño de la llave, en este caso el meto retorna el cuerpo cifrado y la ruta en la que están los CAPTCHAS. Este método en opción 1 genera la semilla, despues calcula Zp, mapea a número la semilla por medio de Codificar, con este número se generan los pares del secreto compartido, estos son mapeados a cadena de caracteres y convertidos en CAPTCHAS, se crea la llave y por último se cifra el cuerpo del mensaje con esta, en este caso el método retorna el cuerpo del mensaje cifrado y una lista de pares donde esta el número x y su correspondiente imagen CAPTCHA.

- Descifrar: este método hace le proceso inverso que el método cifrar, este recibe como parámetro el cuerpo cifrado, una cadena con el CAPTCHA o una lista de pares, $x, CAPTCHA$. Con la opción 0 recibe una cadena de caracteres en la opción CAPTCHA con este se genera la llave y se descifra el cuerpo obteniendo el mensaje original. En caso de tener la opción 1 se recibe en el parámetro CAPTCHA una lista que contiene los pares $x, CAPTCHA$ de este se obtiene el tamaño del CAPTCHA y se calcula el conjunto de enteros módulo Zp, con esto se toman los CAPTCHAS y se mapean a su representación numérica por medio de Codificar, los pares de números se ingresan al método que calcula el secreto compartido, lo arrojado por este método se mapea a su representación en cadena de caracteres y se genera la llave con esto se descifra el cuerpo del mensaje y se obtiene el mensaje original. Este metodo retorna el cuerpo del mensaje original.

Conclusión: La funcionalidad de la biblioteca ya implementada, corresponde al esquema propuesto en "On Securing Communication from Profilers", al tener todas las funciones separadas lo hace tener una funcionalidad modular. Esta implementación se usará para integrarla al siguiente prototipo.

4.9. Prototipo 9

Objetivo: Dar de alta un servidor en el lenguaje PHP donde se alojen, busquen y se realice el intercambio de CAPTCHAS entre los usuarios que utilicen los protocolos P y P' del esquema Díaz – Chakraborty.

En éste prototipo se tienen implementados por separado 3 archivos PHP que se encargan, cada uno, de dan de alta a los usuarios que desean utilizan el esquema "On Securing Communication from Profilers"; subir al servidor los CAPTCHAS que contiene la clave de descifrado de los mensajes redactados por los usuarios previamente registrados; y realizan la descarga de los mismos al momento de que el usuario destino desee recuperar el mensaje, esto con el fin de poder hacer el intercambio y resguardo de las claves para el descifrado de los mensajes de correo electrónico entre usuarios registrados. Tambien se cuenta con una base de datos que nos guarda la relación entre los mensajes enviados y los CAPTCHAS que contienen la clave para ser descifrados. El código fuente de encuentra en el anexo 3

- Alta de usuarios: El servidor cuenta con un archivo PHP donde recibe las peticiones de los nuevos usuarios que quieran hacer uso de los protocolos P y P' bajo el esquema propuesto en este documento, este archivo PHP recibe un formulario HTML llenado previamente con el correo electrónico del usuario, nombre de usuario que lo identificara en el servidor y una contraseña. El nombre de usuarios y la contraseña son utilizados para autenticar a los usuarios y se lleve un control de los CAPTCHAS que se tienen listos para ser intercambiados.
  La respuesta entregada por este archivo PHP es una respuesta HTML, la cual contiene la respuesta con códigos para saber si se realizo correctamente la operación.

- Cargar CAPTCHAS: Este servidor cuenta con un archivo PHP que recibe las peticiones de los usuarios ya registrados que quieren subir los CAPTCHAS generados por los protocolos P y P'. La carga de los CAPTCHAS se hace mediante un formulario HTML llenado previamente y archivo PHP se encarga de darnos un código para saber si la carga de los CAPTCHAS fue realizada satisfactoriamente.

- Descargar CAPTCHAS: Por último, el servidor cuenta con un archivo PHP que recibe por medio de un formulario HTML el correo destino, el correo origen y la firma que identifica al mensaje de correo electrónico que se desea descifrar. Este archivo nos devuelve una URL para descargar los CAPTCHAS deseados ó un mensaje de error en caso de pedir los CAPTCHAS de un mensaje inexistente en la base de datos.

Conclusión: La funcionalidad de este servidor es simple ya que se limitan a la distribución y resguardo de los CAPTCHAS generados por los usuarios registrados que utilizan los protocolos P y P' del prototipo anterior. Su implementación corresponde al esquema propuesto en "On Securing Communication from Profilers" y se integra en el prototipo siguiente para completar dicho esquema.

4.10. Prototipo 10

Objetivo: Crear un cliente de correo electrónico de escritorio que utilice el esquema descrito en este documento.

El cliente de correo electrónico se programó utilizando la biblioteca grafica GTK3+, el entorno gráfico de GNOME 3 y el lenguaje de programación Python. Para poder inicial el desarrollo de este prototipo es necesario instalar previamente la biblioteca gráfica GTK3+ y el entorno gráfico GNOME 3, ver anexo 4.

Se inicio el desarrollo de este prototipo generando una interfaz gráfica que ayude a establecer las configuraciones básicas para conectarse con los servidores de correo electrónico por los protocolos POP3 y SMTP. Esta interfaz también establece la configuración necesaria para conectarse con el servidor de CAPTCHAS y para escoger el protocolo de cifrado de mensajes que se utilizará.

- Configuración básica POP3: El cliente de correo electrónico establece una conexión POP3 con un servidor de correo electrónico para poder descargar los mensajes de un usuario, para poder hacerlo se necesita nombre de host, puerto de comunicación, nombre de usuario, contraseña del usuario y si se utilizara una conexión segura. Todos estos datos son proporcionados por el servidor de correo electrónico con el que se desea comunicar.

- Configuración básica SMTP: El envío de mensajes de correo electrónico se realiza estableciendo una comunicación con nuestro servidor de correo electrónico, para ello se necesita nombre de host, puerto de comunicación, nombre de usuario y contraseña del usuario. Al igual que en la configuración POP3 estos datos son proporcionados por el servidor de correo electrónico con el que se desea comunicar.

- Configuración con el servidor de CAPTCHAS: El envío de la imágenes CAPTCHAS generadas después del cifrado de los mensajes necesitan ser resguardadas en el servidor de CAPTCHAS, prototipo 9, para ello es necesario enviar al servidor su dirección de correo electrónico, un nombre de usuario y una contraseña. El servidor valida si el usuario ya esta registrado, en caso contrario el servidor realiza el registro del usuario con los datos proporcionados.

Estas 3 configuraciones se establecen llenando los campos de la interfaz, ver figura n, la cual llamaremos ventana de configuración. Esta ventana genera un archivo JSON donde se guardan estos datos para poder ser utilizado mas adelante para el envío y recepción de mensajes de correo electrónico, así como la subida y descarga de las imágenes CAPTCHA y la selección entre los protocolos P y P' para cifrar los mensajes de correo electrónico.

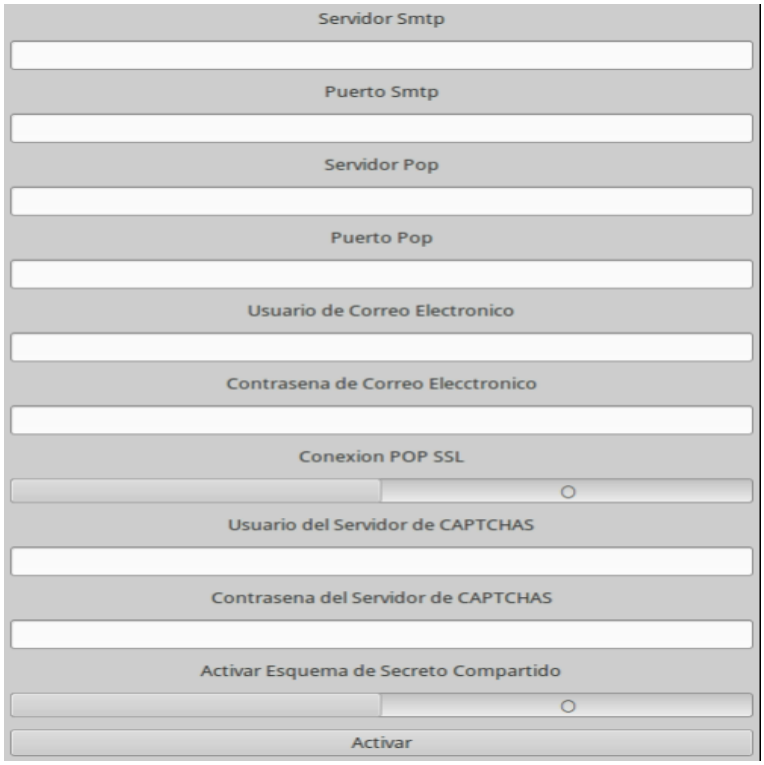

Figura 4.1: Ventana de Configuración

Posteriormente se genero una interfaz gráfica principal para visualizar los mensajes de correos electrónicos y una segunda interfaz para la redacción de los mismos.

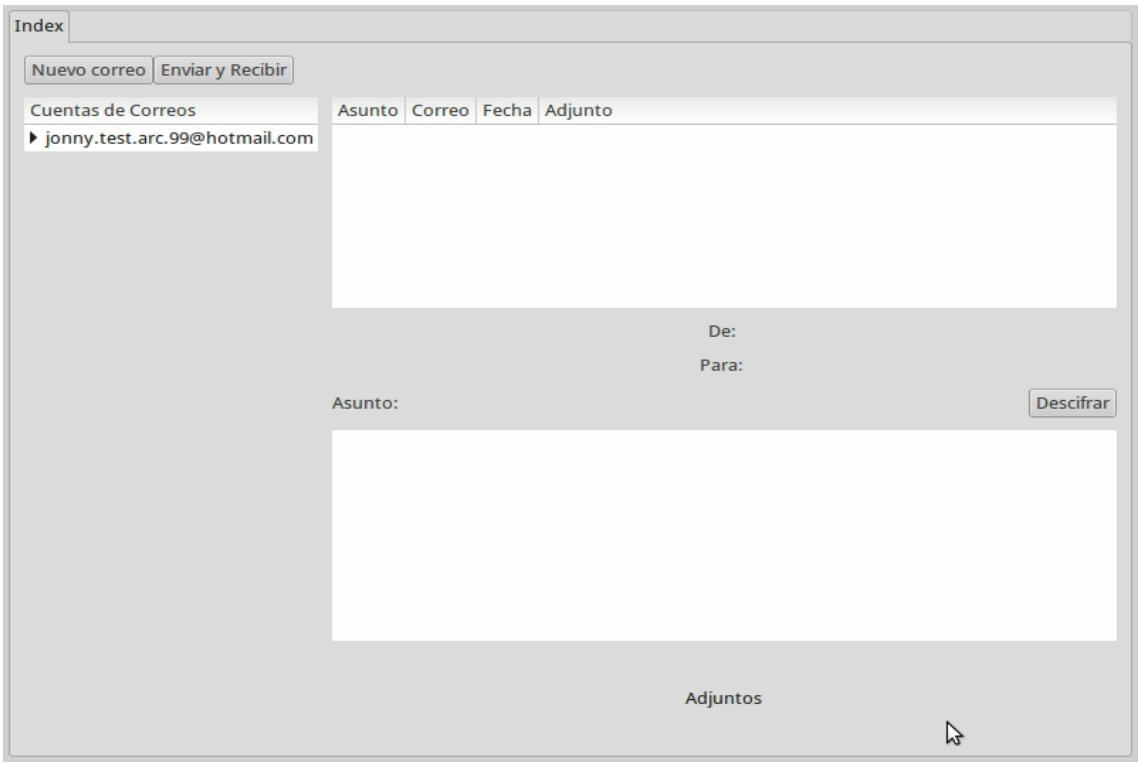

Figura 4.2: Ventana Principal

La primera interfaz, también llamada ventana principal, esta dividida en 3 parte una barra lateral, un listado y un visualizador de mensajes de correo electrónico. En la barra lateral encontramos las carpetas donde se almacenan los correo electrónicos, en el listado encontramos los mensajes de correos electrónicos que se han almacenado en la carpeta seleccionada de la barra lateral y por ultimo tenemos el visualizador de mensajes, el cual despliega la dirección de correo del usuario que mando ese mensaje, los destinatarios a donde fue dirigido el mensaje y por ultimo el cuerpo del mensaje, ver Figura 4.2.

La segunda interfaz, también llamada ventana de envío de mensajes, tiene un diseño simple para redactar los mensajes de correo electrónico, esta interfaz cuenta con 3 espacios, el primero es para escribir la dirección de correo donde se enviará el mensaje; el segundo espacio es para escribir el asunto que se adjunta al mensaje; y por último espacio es para la redacción del mismo, ver Figura 4.3.

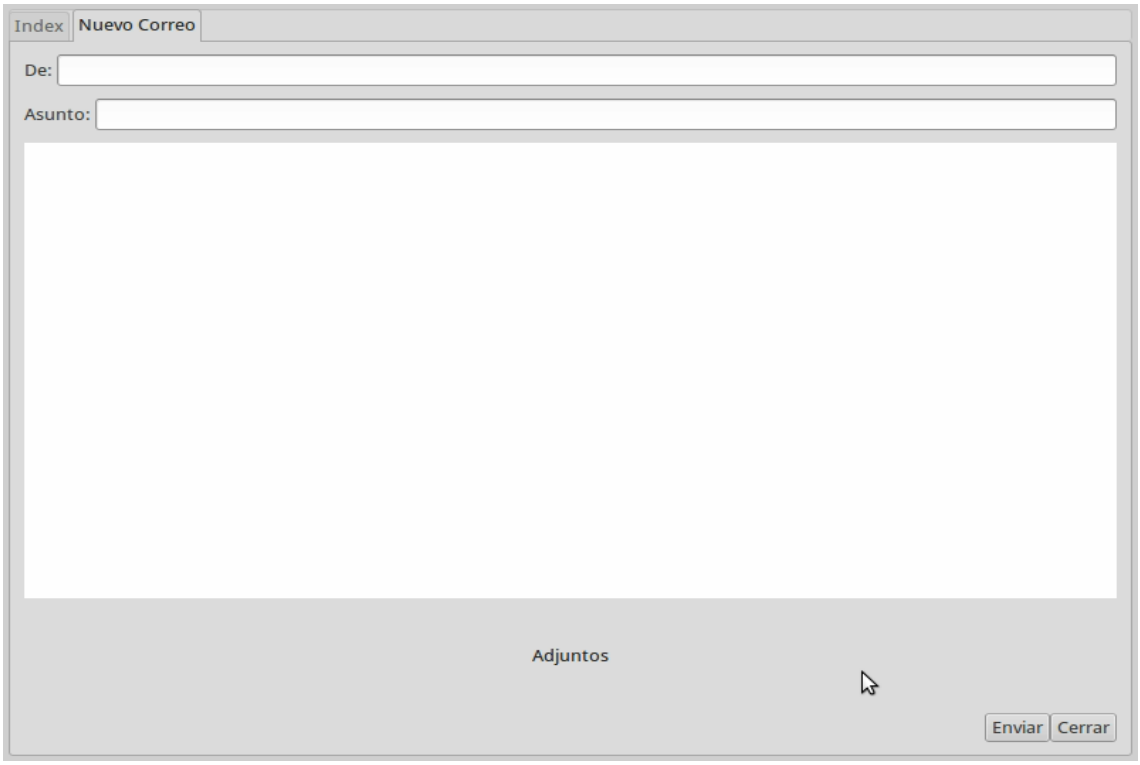

Figura 4.3: Ventana de Nuevo Correo

Una vez que se tienen las interfaces listas se procede a darles funcionalidad, para ello se llevaron a cabo las siguientes actividades.

- Cifrado de mensajes de correo electrónico por el protocolo P y P': Esta actividad se inicia al redactar un correo electrónico en la ventana de envío de mensaje y pulsar el botón enviar. Lo primero que hace es toma la fecha actual de la computadora y la concatena con las dirección de correo destino y origen, a esta cadena generada se le obtiene un digesto MD5, el cual sera utilizado como firma para el mensaje de correo. Posteriormente se toma el mensaje redactado por el usuario y es enviado a la biblioteca de cifrado, prototipo 8, especificando el protocolo a usar. Esta biblioteca nos regresa el mensaje cifrado junto con la ruta de la imágenes CAPTCHAS que descifran el

mensaje. Después se toma este mensaje cifrado y es concatenado con la firma generada anteriormente y con una cabecera que nos indicara si el mensaje esta cifrado o no al momento de visualizarlo. A continuación toma las direcciones de correo, origen y destino, el asunto redactado y el mensaje cifrado para generar un mensaje de correo electrónico y guardalo en la carpeta de salida, éste mensaje será enviado posteriormente por el protocolo SMTP al servidor de correos. Por último esta actividad activa el envío de imágenes CAPTCHAS al servidor de CAPTCHAS.

- Envío de imágenes CAPTCHAS al servidor de CAPTCHAS: Esta actividad se inicia al momento de pulsar el botón "Enviar y Recibir" de la ventana principal o al termino del cifrado de mensajes de correo electrónico. Esta actividad inicia tomando un listado de los mensajes de correo que se tienen pendientes de envío en la carpeta de salida y buscando los CAPTCHAS correspondientes a cada mensaje. Cada uno de estos CAPTCHAS son enviados al servidor junto con las direcciones de correo origen y destino, la firma del mensaje de correo y los datos de configuración del archivo JSON por medio de una petición HTTP. Por último, por cada CAPTCHA enviado exitosamente se envía su correspondiente mensaje al servidor de correo por el protocolo SMTP.

- Envío de mensajes por el protocolo SMTP: Esta actividad se inicia al momento de pulsar el botón "Enviar y Recibir" de la ventana principal o al termino de un envío exitoso de un CAPTCHA. Para hacer el envío de un mensaje de correo electrónico se necesitan los datos de configuración que se tienen el el archivo JSON junto con el mensaje que se desea enviar. En caso de error el mensaje se almacena en la carpeta de salida.

- Descargar mensajes por POP3: Esta actividad se inicia al momento de pulsar el botón "Enviar y Recibir" de la ventana principal. Para iniciar la descarga de los mensajes de correo electrónico se toman los datos básicos del archivo JSON para establecer comunicación con el servidor. Una vez establecida la conexión el servidor de correo electrónico nos dará uno a uno los mensajes y el cliente de correo electrónico guardará cada mensaje en un archivo txt en la carpeta de entrada.

- Descarga de imágenes CAPTCHAS del servidor de CAPTCHAS: Esta actividad se inicia al momento de pulsar el botón "Descifrar" de la ventana principal. Para saber si el mensaje esta cifrado se busca en el cuerpo del mensaje la cabecera de cifrado de donde obtenemos la firma del mensaje. Con la firma del mensaje se buscan las imágenes de descifrado en la carpeta CAPTCHA, esta carpeta se crea con la instalación del prototipo, en caso de no encontrar las imágenes en la carpeta el cliente de correo hacer una petición HTTP al servidor de CAPTCHAS adjuntando la firma del mensaje, las direcciones de origen y la dirección destino. El servidor contesta enviando la dirección URL de la imágenes de donde el cliente descarga las imágenes y las guarda en la carpeta CAPTCHA. Después de guardarlas, el cliente despliega la o las imágenes CAPTCHA en una ventana para que el usuario lo resuelva, esta ventana la llamaremos ventana de Descifrado. El despliegue de una o mas imágenes dependerá del protocolo que se haya utilizado para cifrar.

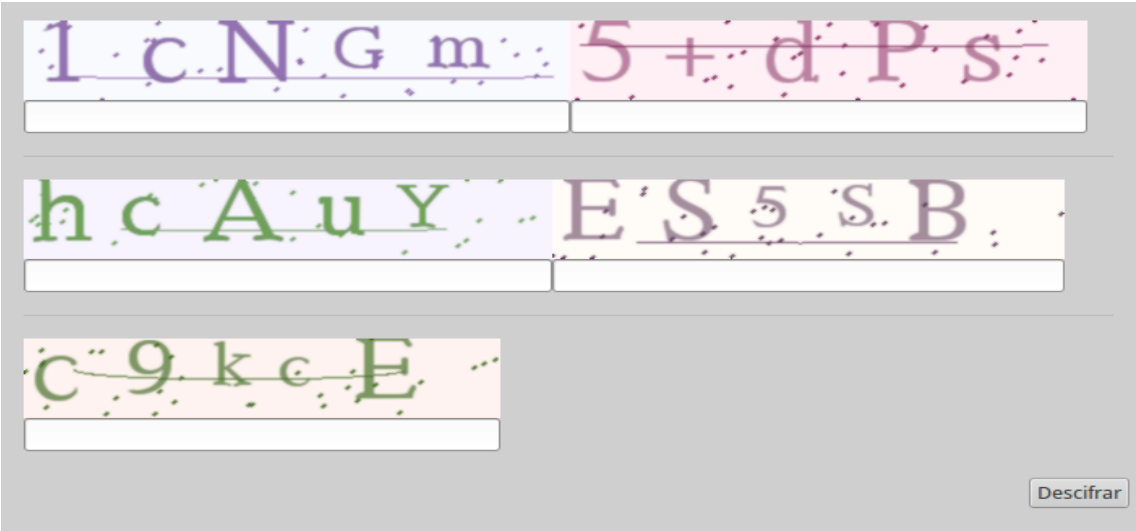

Figura 4.4: Ventana Multi-CAPTCHAS

- Descifrado de mensajes de correo electrónico por el protocolo P y P': Esta actividad se inicia al momento de pulsar el botón "Descifrar" de la ventana de Descifrado. Una vez que el usuario resuelve los CAPTCHAS se toman las respuestas junto con el cuerpo del mensaje cifrado sin la cabecera de cifrado y se envían a la biblioteca de cifrado, prototipo 8, la cual nos regresa el texto descifrado. En caso de que los CAPTCHAS sean ingresados incorrectamente el texto regresado por la biblioteca sera ilegible y el cliente de correos lo detectara.

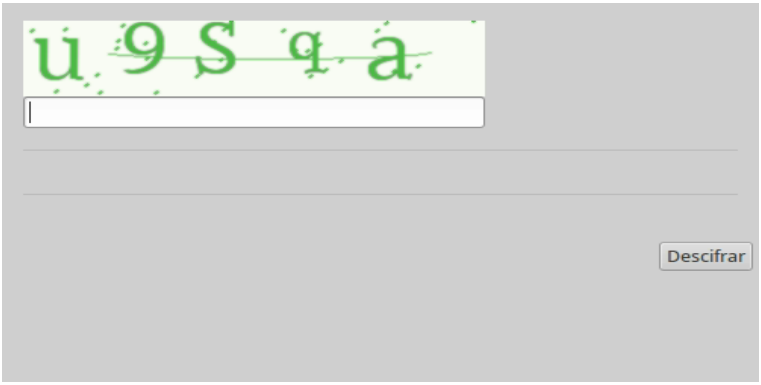

Figura 4.5: Ventana CAPTCHAS

Conclusión: El cliente de correo electrónico que se describió en este prototipo es completamente funcional y en conjunto con los prototipos 8 y 9 cumplen con el funcionamiento del esquema propuesto en este documento para implementar los protocolos P y P' del esquema Díaz -Chakraborty. Para ver el codigo completo del prototipo 10 ver el anexo 5.

Capítulo 5

Pruebas

En este capitulo se muestran los resultados de las pruebas realizadas sobre el prototipo 10. Las pruebas realizadas fueron de tiempo de respuesta y de trafico de información en la red.

5.1. Prueba de rendimiento, Cifrado y Descifrado de un solo CAPTCHA

En la figura 5.1 se muestra la relación de metodos que permiten el cifrado del mensaje y la generación de un solo CAPTCHA. El tiempo total que tarda en hacer todo el proceso es de 0.17s donde las funciones que tardan mas en realizar sus tareas son Ek_din.crearCAPTCHA que se encarga de crear el CAPTCHA y la función Ek_din.primoSig que calcula el numero primo mas cercano dependiendo del tamaño del CAPTCHA a realizar.

En la figura 5.2 se muestra la relación de metodos que permiten el descifrado del mensaje, este proceso es muy sencillo para un solo CAPTCHA ya que lo que introduce en usuario es lo que se canvierte en la clave de descifrado. El tiempo que tarda este proceso es de 0.004s.

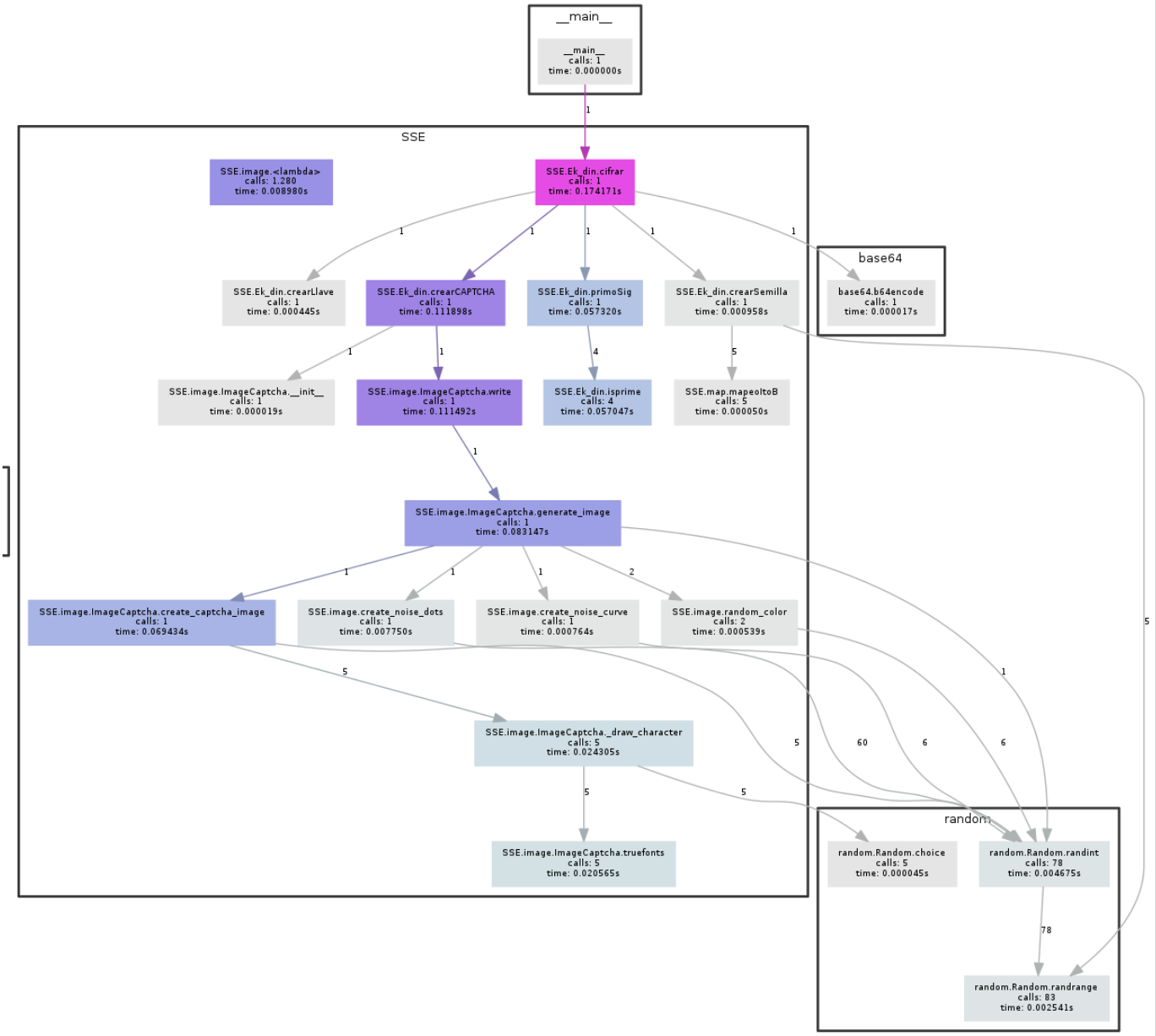

Figura 5.1: Rendimiento del esquema para un solo CAPTCHA

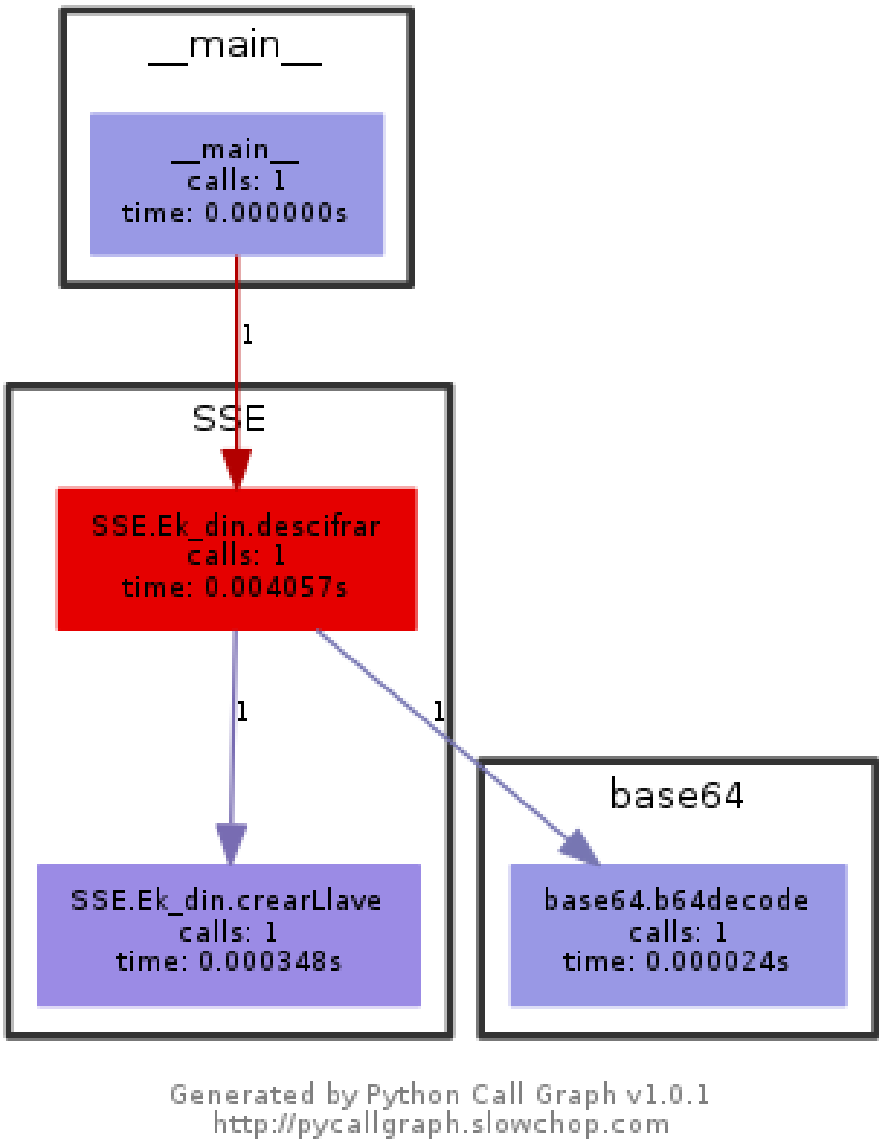

Figura 5.2: Rendimiento del esquema para un solo CAPTCHA

5.2. Prueba de rendimiento, Cifrado y Descifrado de multiples CAPTCHA's

En la figura 5.3 se encuentra la relación de funciones que generan múltiples CAPTCHAS y cifran el mensaje, en este caso la llamada a funciones es mayor que para un solo CAPTCHA, se puede ver que al igual que en el esquema de un solo CAPTCHA las funciones que mas tardan son las de Ek_din.crearCAPTCHA y la función Ek_din.primoSig dandonos un tiempo total para todo el proceso de 0.47s.

En la figura 5.4 se encuentra la relación de funciones que resuelve el algoritmo de secreto compartido y descifra el mensaje, este es mas elaborado que el descifrado para un solo

CAPTCHA en este la función que mas tarda es Ek_din.primoSig por el tamaño de numero que esta manejando, el tiempo total de termino de la tarea es 0.062s.

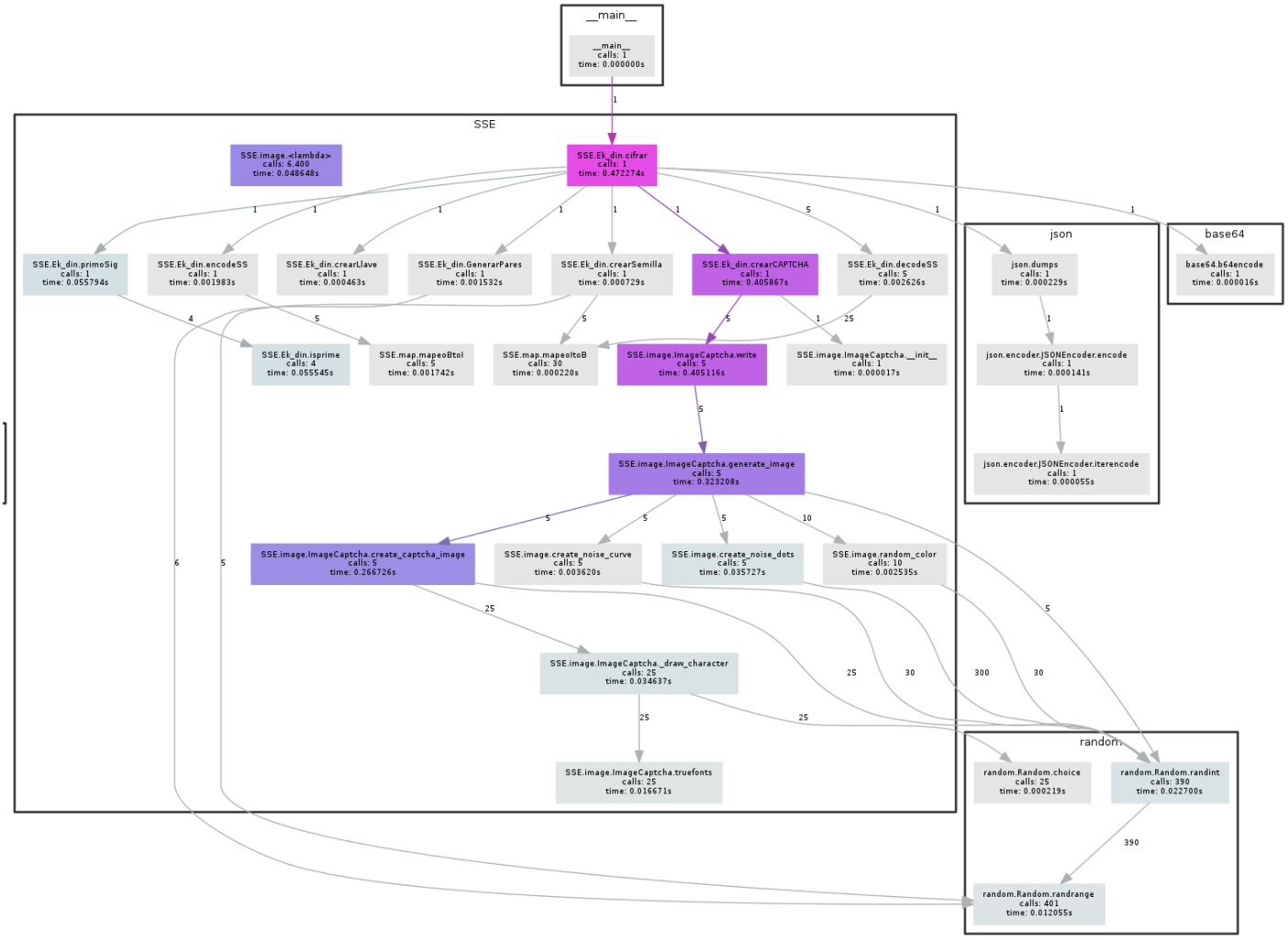

Figura 5.3: Rendimiento del esquema multiCAPTCHA

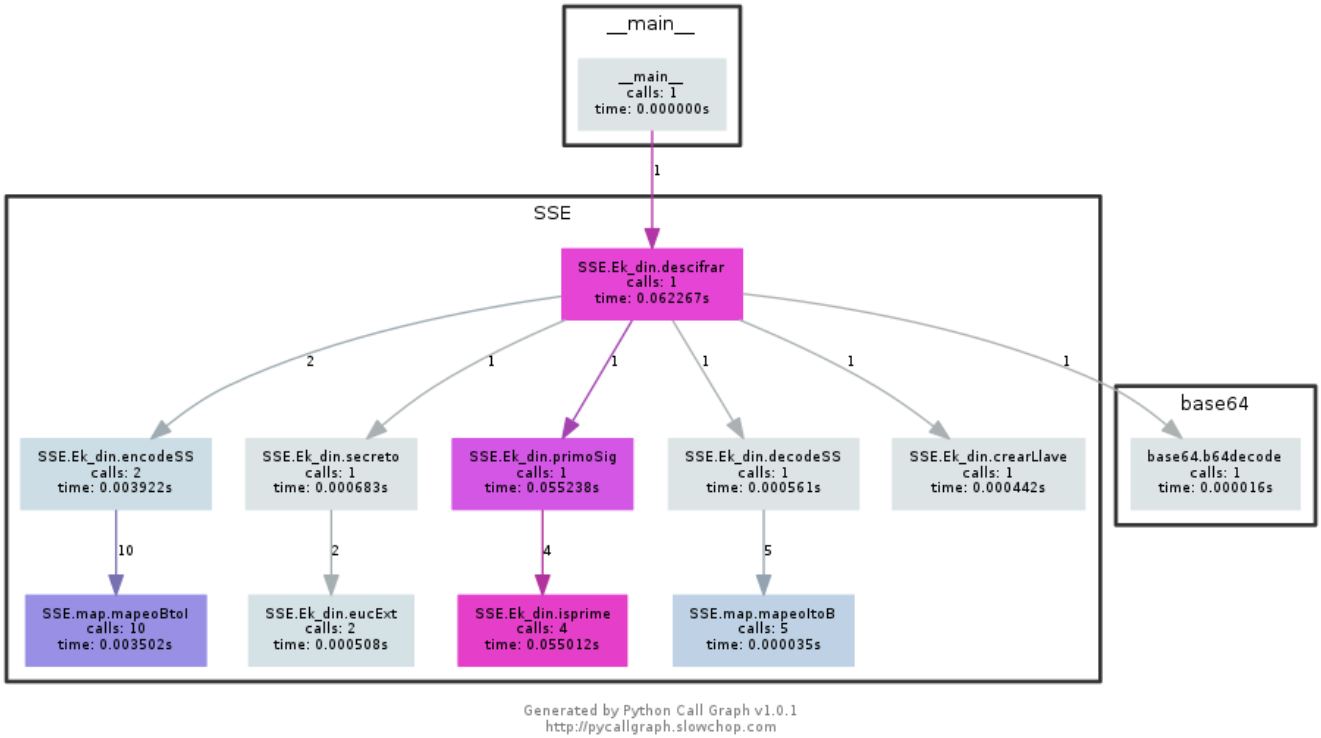

Figura 5.4: Rendimiento del esquema multiCAPTCHA

Capítulo 6

Conclusiones y Trabajo a Futuro

6.1. Conclusiones

En el desarrollo de este trabajo terminal se encontraron varios problemas al desarrollar complementos para clientes de correo electrónico comerciales los cuales describiremos a continuación.

El primer problema encontrado fue la gran cantidad de tiempo que se invierte en la investigación, desarrollo, revisión y correcciones de los complementos que se implementan para los clientes de correo estándar, ya que si se desea publicar un complemento con la empresa que desarrollo el cliente, éstos son sometido a una evaluación para verificar que no altere el funcionamiento de otros módulos de su cliente.

Otro problema a tomar en cuenta es la fase de desarrollo en la que se encuentra el cliente de correo que se desea ocupar, ya que si se encuentra en una etapa muy temprana de desarrollo se encontrara poca documentación; las funciones disponibles serán limitadas; y muy probablemente cambien la compatibilidad entre módulos de una versión a otra.

La solución que se implemento fue desarrollar un cliente de correo electrónico que tuviera las funciones básicas de envío y recepción de mensajes de correo electrónico por los protocolos POP3 y SMTP, junto con la implementación de los protocolos P y P' del esquema Díaz – Chakraborty para el cifrado y descifrado de los mensajes de correo electrónico por medio de CAPTCHAS. Se observó que el intercambio de clave y la implementación de los protocolos P y P' del esquema Díaz - Chakraborty se llevó con éxito. También se concluye que estos esquemas pueden implementarse en los modelos actuales de comunicación de correo electrónico de una manera trasparente al usuario al momento del envío y recepción de los correos electrónicos. Cabe destacar que es la primera implementación funcional que se tiene del esquema de secreto compartido de Adi Shamir para el correo electrónico e inhibiendo los ataques de los agentes clasificadores.

Por último se encontró que las comunicaciones que se establecen actualmente entre los servidores de correo electrónico y los usuarios son canales seguros. Lo cual fue confirmado por las pruebas realizadas a la aplicación, por lo tanto se concluye que el ataque de los adversarios clasificadores se hace en los servidores de correo electrónico donde son almacenados los mensajes en claro y se tiene acceso a un gran número de mensajes para su clasificación.

6.2. Trabajo a futuro.

Las líneas de trabajo que sugieren los autores de este trabajo terminal son las siguientes.

- La implementación del esquema Díaz – Chakraborty y el esquema de intercambio de claves en un cliente de correo electrónico de escritorio comercial o en otros clientes de correo como los clientes web o móviles.
- En el esquema de intercambio de claves en este trabajo terminal se utilizó un servidor que aloja y distribuye los CAPTCHAS entre los usuarios, por lo tanto se sugiere trabajar en la gestión de los CAPTCHAS para mejorar el intercambio de claves entre los usuarios.
- El cifrado del contenido de los mensaje de correo electrónico no es detectado por los protocolos de SMTP y POP3, pero en algunos países el uso de algoritmos criptográficos esta prohibido. Para evitar una sanción por parte de estos países y que a su vez los adversarios clasificadores no puedan clasificar los mensajes se sugiere implementar un cifrado no estandar como los son AES y DES.
- Por último se sugiere una implementación de una biblioteca de creación de CAPTCHA's en el lenguaje PYTHON para mejorar las imágenes generadas.

Referencias

[1] Cifrado simetrico. Guía de Gnu Privacy Guard, 2015. https://www.gnupg.org/gph/es/manual/c190.html#AEN201.

[2] em client. eM Client web page, 2015. http://www.emclient.com/.

[3] Opera mail. Opera Mail web pages, 2015. http://www.opera.com/es-419/computer/mail.

[4] Post box. Post Box web page, 2015. https://www.postbox-inc.com/.

[5] Thunderbird. Thunderbird web pages, 2015. https://www.mozilla.org/es-ES/thunderbird/.

[6] Zimbra. Zimbra web pages, 2015. https://www.zimbra.com/.

[7] R. Allenby. *Rings, fields, and groups: an introduction to abstract algebra*. E. Arnold, 1983.

[8] Alonsojpd. Montar un servidor de correo electrónico mail en linux ubuntu. AJPDsoft, 2015. http://www.ajpdsoft.com/modules.php?name=News&file=article&sid=506.

[9] T. Brehm. The perfect server - ubuntu 15.10 (wily werewolf) with apache, php, mysql, pureftpd, bind, postfix, dovecot and ispconfig 3. How to Forge, 2015. https://www.howtoforge.com/tutorial/ubuntu-perfect-server-with-apache-php-myqsl-pureftpd-bind-postfix-doveot-and-ispc

[10] M. Brodsky. Reflexiones jurídicas sobre el e-marketing en chile. Interactive Advertising Bureau, 2015. http://www.iab.cl/reflexiones-juridicas-sobre-el-e-marketing-en-chile/.

[11] D. Chakraborty and F. Rodríguez-Henríquez. Block cipher modes of operation from a hardware implementation perspective. In Ç. K. Koç, editor, *Cryptographic Engineering*, pages 321–363. Springer, 2009.

[12] S. Diaz-Santiago and D. Chakraborty. On securing communication from profilers. In P. Samarati, W. Lou, and J. Zhou, editors, *SECRYPT 2012 - Proceedings of the International Conference on Security and Cryptography, Rome, Italy, 24-27 July, 2012, SECRYPT is part of ICETE - The International Joint Conference on e-Business and Telecommunications*, pages 154–162. SciTePress, 2012.

[13] P. Golle and A. Farahat. Defending email communication against profiling attacks. In *Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society, WPES 2004, Washington, DC, USA, October 28, 2004*, pages 39–40, 2004.

[14] A. Gulbrandsen and N. Freed. Internet Message Access Protocol (IMAP) - MOVE Extension. RFC 6851, 2015.

[15] D. Jurafsky and J. H. Martin. *Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition*. Prentice Hall PTR, Upper Saddle River, NJ, USA, 1st edition, 2000.

[16] D. J. C. Klensin. Simple Mail Transfer Protocol. RFC 5321, 2015.

[17] J. Klensin. Simple Mail Transfer Protocol. RFC 2821 (Proposed Standard), April 2001. Obsoleted by RFC 5321, updated by RFC 5336.

[18] W. Koch. The gnu privacy guard. GnuPG web page, 2016. `https://www.gnupg.org/index.html`.

[19] D. P. Martínez. Postgresql vs. mysql. geekWare, 2015. `https://danielpecos.com/documents/postgresql-vs-mysql/`.

[20] J. Myers and M. Rose. Post Office Protocol - Version 3. RFC 1939 (Standard), 1996. Updated by RFCs 1957, 2449.

[21] J. Peralta. Anillos y cuerpos. Campus Virtual Univesidad de Almería, 2016. `http://www.ual.es/personal/jperalta/anilloscuerpos.pdf`.

[22] N. Roshanbin and J. Miller. A survey and analysis of current captcha approaches. *J. Web Eng.*, 12(1-2):1–40, 2013.

[23] sawiyati. How to install apache, php and mariadb on ubuntu 15.04. Server Mom, 2015. `http://www.servermom.org/install-apache-php-mariadb-ubuntu-15-04/2208/`.

[24] A. Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.

[25] W. Stallings. *Cryptography and Network Security: Principles and Practice*. Pearson Education, 5a edition, 2002.

[26] D. R. Stinson. *Cryptography Theory and Practice*. Chapman & Hall/CRC, 3a edition, 2006.

[27] O. Tezer. Sqlite vs mysql vs postgresql: A comparison of relational database management systems. Digital Ocean, 2014. `https://www.digitalocean.com/community/tutorials/sqlite-vs-mysql-vs-postgresql-a-comparison-of-relational-database-management-syst`

[28] M. R. S. Villanueva. Aritmética del reloj. Departamento de Matemáticas de la Universidad de Puerto Rico en Aguadilla, 2016. `http://math.uprag.edu/milena/4.5%20ARITMETICA%20DEL%20RELOJ.pdf`.

[29] Wikipedia. Ciphertext-only attack — Wikipedia, the free encyclopedia, 2015. https://en.wikipedia.org/wiki/Ciphertext-only_attack.

[30] Wikipedia. Email — Wikipedia, the free encyclopedia, 2015. http://en.wikipedia.org/wiki/Email.

[31] Wikipedia. Pretty good privacy — Wikipedia, the free encyclopedia, 2015. https://es.wikipedia.org/wiki/Pretty_Good_Privacy.

[32] L. G. G. y Dr. Sergio Rajsbaum. Critofrafía. Temas selectos de la web, 2015. http://www.matem.unam.mx/rajsbaum/cursos/web/presentacion_seguridad_1.pdf.

[33] E. A. M. y M.C. Ma. Jaquelina López Barrientos. Fundamentos de critofrafía. Universidad Nacional Autonoma de México Facultad de Ingenieria, 2015. http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/.