INSTITUTO POLITÉCNICO NACIONAL

Escuela Superior de Cómputo

ESCOM

Trabajo Terminal

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

2015-A010

Presentan

Arcos Ayala Jonathan
Zepeda Ibarra Allan Ulises

Directores

Dr. Días Santiago Sandra
M. en C. Soto Ramos Manuel Alejandro

Noviembre 2015

Índice

Índice de Figuras

Índice de Tablas

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 [1]. 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 [2]. 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 maquina [3], 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 considera los recursos y el objetivo de un adversario clasificador [4].

Objetivos

Objetivos Generales

Desarrollar una herramienta para un cliente de correo electrónico que permita cifrar el contenido de los correos para evitar su clasificación, basándonos en técnicas criptográficas, asegurando el envío y recepción de los CAPTCHAs a través de un repositorio, basándonos en un esquema de cifrado por identidad.

Objetivos Específicos

1. Desarrollar una herramienta en un cliente de correo el ectrónico 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.

Chapter 1

Justificacion

Lo que se pretende en este trabajo terminal, es ofrecer al usuario una solución alternativa para proteger al correo electrónico, contra los clasificadores. Dicha solución se considera más fácil de usar y además ofrece un nivel de seguridad adecuado, teniendo en cuenta las características de los clasificadores. La solución que se propone, hará uso de CAPTCHAs y de un algoritmo criptográfico. Los CAPTCHAs son programas de cómputo, cuyo propósito es distinguir si están interactuando con una máquina o con un ser humano. Este algoritmo criptográfico tiene una gran ventaja al momento de la generación de llaves, ya que sus llaves son simétricas a diferencia de muchos algoritmos estándares que utilizan una generación de un par de llaves asimétricas, estos algoritmos criptográficos asimétricos nos llevan a necesitar una comunicación previa entre el emisor y el receptor del mensaje enviado. Mientras que al usar el esquema aquí propuesto solo es necesario que el emisor genere una llave, la transforme y envíe los CAPTCHAs, y que el receptor resuelva los CAPTCHAs, recupere la llave y posteriormente el mensaje de correo electrónico. El envío de los correos se propone hacerlo enviando el correo electrónico con el contenido cifrado a un servidor de correo electrónico donde se alojará hasta que el cliente de correos electrónico instalado en el equipo de cómputo del receptor lo descargue por medio del protocolo POP3, al mismo tiempo se enviarán los CAPTCHAs que permiten recuperar la llave de cifrado a un tercer agente llamado servidor de llaves, el cuál verificara que la petición hecha por el receptor es válida y que el receptor es un usuario valido. El protocolo SSL se usará para garantizar el envío de los CAPTCHAs por parte del emisor, la correcta recepción por parte el servidor de llaves y la recuperación por parte del receptor para la correcta recuperación de la llave de cifrado y posterior descifrado de los correos electrónicos. El servidor de llaves es fundamental para el funcionamiento de este sistema, ya que esto le da un nivel de seguridad un poco más elevado que si lo enviáramos todo en un sólo paquete.

Chapter 2

Estado del Arte

La única referencia que tenemos sobre un esquema criptográfico contra adversarios clasificadores es el que encontramos en el artículo "Defending Email Communication Against Profiling [5]" de Philippe Golle y Ayman Farahat, ambos miembros del "Palo Alto Research Center".
En su artículo aborda el tema del ataque de los adversarios clasificadores proponiendo un esquema de cifrado simple de llave simétrica en el cual la llave que se usa para cifrar está dada por la cabecera del correo electrónico (que consiste en la dirección del remitente, la dirección del destinatario, la hora a la que se envía el correo electrónico y potencialmente otros campos).
Esto le permite al destinatario calcular la llave fácilmente ya que estos datos son públicos, este esquema es inseguro contra un adversario normal, pero es seguro contra adversarios clasificadores, ya que los clasificadores al procesar la información por volumen si quisieran descifrar el contenido del correo tardarían en descifrar todos por la gran cantidad de correos que procesan en cada lote.
Tomando en cuenta que esta es la única referencia sobre el tema que estamos abordando, podemos decir que trabajamos en el mismo sentido ya que esta propuesta de solución está basada en el artículo "On Securing Communication from Profilers" en el que se propone algo similar en cuanto al cifrado, nos lleva a tomar muy en cuenta el poder del algoritmo de cifrado que usaremos en nuestra propuesta de solución.

Chapter 3

Marco Teórico

En el siguiente capítulos hablaremos sobre el correo electrónico y algunos de los intermediarios que hacen posible que este servicio sea usado en toda la red de internet, también hablaremos de las amenazas que a las que se tiene que enfrentar este servicio para hacer llegar información de un usuario a otro de una manera segura y cuales han sido las respuestas de los proveedores de servicio de correo electrónico para proporcionar dicha seguridad a los usuarios.

3.1 Correo electrónico

El correo electrónico es el servicio de internet por el cual se pueden enviar mensajes entre 2 usuarios que cuenten con este servicio. El correo electrónico o "e-mail" por sus siglas en inglés, basa su funcionamiento en las oficinas postales. Tomando esa analogía podemos decir que los usuarios tienen cartas (mensajes de correo electrónico) que desean enviar a otros usuarios; estas cartas son enviadas a las oficinas postales (servidores de correo electrónico) donde se almacenan con otras cartas que van dirigidas a otros usuarios en diferentes ciudades; estas oficinas postales envían las cartas a otras oficinas postales si es necesario; y por último cada oficina postal se encargan dejan en un buzón asignado a un usuario (buzón de correos electrónicos) las cartas que otros usuarios le han enviado.

3.2 Mensaje de correo electrónico

Los mensajes de correo electrónico al igual que las cartas tienen la dirección del receptor, la dirección del emisor y el cuerpo del mensaje, pero a diferencia de las cartas los correos electrónicos son enviados por internet y necesitan sus propios formatos. Para poder enviar un mensaje de correo electrónico es necesario tener los elementos como mínimo.
Dirección del remitente: Esta dirección se compone por dos elementos importantes, el primero es el nombre de usuario seguido de un carácter "@", el segundo elemento es el dominio donde está alojado el servicio de correo electrónico.
Direcciones de los receptores: En un correo electrónico debe haber al menos una dirección de receptor para ser enviado, esta dirección de receptor tiene la misma estructura que la dirección del remitente.
Contenido del mensaje: Es el texto que se desea transmitir entre el remitente y el receptor. El mensaje de correo electrónico cuenta con más elementos pero estos son opcionales y se pueden consultar en el RFC 2821 extensión MIME.

3.3 Dominio de internet

Es un nombre que identifica a los diferentes dispositivos interconectados en una red sin la necesidad de aprenderse un número de red. Estos dispositivos pueden proporcionar diferentes servicios como el servicio de correo electrónico.

3.4 Buzón de correo electrónico

Un buzón de correo electrónico es un espacio virtual proporcionado por el servicio de correo electrónico que sirve para almacenar los mensajes enviados y recibidos.

3.5 Usuario de correo electrónico

Se le conoce como usuario de correo electrónico a la persona que se registra en un dominio para obtener los servicios de mensajería proporcionados por un servidor de correo electrónico.

3.6 Cliente de correo electrónico

El cliente de correo electrónico es una interfaz por la cual el usuario de correo electrónico puede administrar sus mensajes enviados y recibidos.
El cliente de correo electrónico puede ser de diferentes tipos como son:

3.6.1 Cliente de correo electrónico para la pc

Estos clientes de correo electrónico son instalados en una computadora y es configurado para sincronizarse con un servidor de correo electrónico cada cierto tiempo o cuando el usuario se lo indique. Una de las principales características de éste cliente de correos es la capacidad de descargar los mensajes del servidor a la computadora para ser leídos sin la necesidad de tener una conexión de internet y en cuanto tiene conexión con el servidor otra vez descarga los nuevos mensajes y envía los que se tienen pendientes en la computadora.

3.6.2 Cliente de correo electrónico web

Los clientes web necesitan un explorador de internet y una conexión permanente a la red para que funcione, estos clientes normalmente son proporci onados por el mismo servidor de correo electrónico y nunca descarga los correo en los ordenadores donde son utilizados.

3.6.3 Cliente de correo electrónico para móviles

Un cliente de correo móvil se caracteriza por ser aplicaciones instaladas en los dispositivos móviles, se sincronizan con el servidor continuamente pero no descargan ningún mensaje de correo pero podemos tener cargados los últimos mensajes temporalmente.

3.7 Servidor de Correo electrónico

Un servidor de correo electrónico es un programa que se encarga de enviar y recibir los mensajes de correo electrónicos de sus usuarios registrados, este servidor puede recibir mensajes de usuarios de otros servidores de correos que sean dirigidos a sus usuarios registrados.
Este servidor tiene que seguir algunos estándares que existen en internet para él envió de mensajes de correo electrónico (protocolo smtp) y recepción de mensajes de correo electrónico (protocolo pop3 o imap).

3.8 Protocolo SMTP

El protocolo SMTP significa "protocolo para transferencia simple de correo" o "Simple Mail Transfer Protocol" por sus siglas en inglés, el cual se encarga de enviar los mensajes de correo electrónicos entre dispositivos que se encuentran interconectados en la red o en internet. Este protocolo solo se utiliza para mandar los mensajes entre servidores o entre el usuario emisor y su servidor de correo electrónico. Podemos revisar el protocolo completo en el RFC5321 [6].

3.9 Protocolo POP3

Este protocolo se encarga de descargar los mensajes del servidor a un cliente de correo electrónico que el usuario haya configurado previamente. Una de las características es que solo se sincroniza para la descarga de los mensajes de correo y no deja una copia de seguridad en el servidor de correo electrónico. Podemos consultar el funcionamiento detallado en el RFC1939 [7].

3.10 Protocolo IMAP

Este protocolo, al igual que el protocolo POP3, se encarga de la descarga de los mensajes del servidor a un cliente de correo electrónico con la diferencia de que la sincronización entre el servidor de correos electrónico y el cliente de correos es continua, manteniendo una copia de seguridad en el servidor. Con este protocolo es posible tener varios clientes de correo configurados con la misma cuenta y los cambios que se realicen en cualquiera de los clientes de correo se verán reflejados en el servidor y en los diferentes clientes sincronizados. Este protocolo puede ser consultado en el RFC 6851 [8].

Como hemos podido ver en el presente documento, el servicio de correo electrónico es un canal de comunicación que se ayuda de varios elementos para completar la comunicación entre dos usuarios de correo electrónico, no importando que estos estén registrados en 2 servidores de correo diferentes. Pero para poder entender por completo el comportamiento de este servicio tenemos que definir ciertas características de este servicio.
Este servicio establece una comunicación no orientada a conexión, lo que significa que el receptor no necesita estar conectado al servicio de correo electrónico para recibir el mensaje en su buzón de correo electrónico.
Los mensajes enviados por medio del correo electrónico transitan por el internet como archivos en texto plano, esto quiere decir que cualquiera que tenga una copia del mensaje puede abrir

el correo electrónico y leer el mensaje siguiendo la estructura del protocolo SMTP.
Además de mandar mensajes tiene la facultad de enviar archivos multimedia en el mismo mensaje de correo electrónico, esta característica ha sido explotada bastante por empresas privadas y de gobierno para tener comunicados a sus empleados, departamentos, proveedores, socios, etc.
El correo permite enviar el mismo mensaje a más de un usuario sin la necesidad de hacer un mensaje para cada usuario, esto lo han utilizado muchas empresas de publicidad para hacer marketing a gran escala y a muy bajo costo, a este servicio se le llama SPAM.
Este medio de comunicación es bastante rápido ya que se estima que un mensaje de correo electrónico tiene que llegar a su destino a más tardar en 5 minutos, no importando la ubicación geográfica del servidor de correo electrónico.
Las características mencionadas nos dan a notar que el correo electrónico tiene una baja seguridad al momento de enviar los mensajes, ya que la información que mandamos en sumamente fácil de leer por cualquiera que pueda tener una copia del mensaje de correo electrónico.
Si tomamos en cuenta que un mensaje de correo electrónico tiene que saltar por varios servidores de correo antes de llegar a su destino, es fácil suponer que se pueden interceptar una copia de los mensajes en el envío de servidor a servidor.
Por estos motivos los servidores de correo electrónico han implementado diversos candados de seguridad para blindar la transferencia de mensajes entre servidores. Una de las maneras que han encontrado para proporcionar dicha seguridad ha sido a través de la implementación de técnicas criptográficas.
La criptografía moderna se basa en dos corrientes metodológicas que son la criptografía simétrica y la criptografía asimétrica. Estas dos técnicas tienen como propósito ocultar el contenido de un mensaje con el fin de que solo sea leído por aquellos que estén autorizados, a esto se le llama cifrado.

3.11 Cifrado

Es el procedimiento por el cual la información es transformada, esta transformación se realiza por medio de un algoritmo de cifrado junto con una clave para obtener un texto ilegible, el cual es llamado texto cifrado. Para poder obtener el texto original es necesario transformar el texto cifrado por medio de un algoritmo inverso al algoritmo de cifrado y la llave con que fue cifrado, esto es llamado algoritmo de descifrado.
Como ya fue mencionado la criptografía simétrica y asimétrica llevan a cabo la misma tarea pero a través de diferentes esquemas. Esto les proporciona diferentes características, tanto en seguridad como en implementación.

3.12 Cifrado Simétrico

El Cifrado Simétrico es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes.
La clave al ser usada tanto en el cifrado como en el descifrado se convierte en la parte más vulnerable del método, esta vulnerabilidad es contrarrestada con el tamaño de la clave. El tamaño de la clave es medido por medio del número de bits que la conforma, porque al tener una clave con más bits tendremos un campo de posibles claves más amplio. Por ejemplo, una clave de 56 bits tiene 256 combinaciones que a su vez son 72.057.594.037.927.936 claves

posibles, este espacio de claves tan amplio dificulta al atacante el obtener fácilmente la clave. Otra de las condiciones que se deben de cumplir para este esquema de cifrado se lleve a cabo es el intercambio de claves entre los participantes de la comunicación. Este intercambio de claves tiene que darse antes del envío de los mensajes.

3.13 Cifrado Asimétrica

Este método criptográfico propone la generación de dos claves, de las cuales una es privada y está al resguardo del propietario del par de claves; la otra clave es pública y puede ser vista por cualquier usuario que quiera enviarle un mensaje al propietario.
Estas claves son mucho más grandes que las claves de cifrado simétrico y siempre se generan por pares, haciéndolas claves dependientes una de la otra, esto con el fin de que solo exista una clave privada que descifre lo que cifra su clave pública y viceversa. Este método de cifrado también cambia el esquema de envío de mensajes entre usuario ya que antes de empezar la comunicación los interlocutores tienen que buscar las claves públicas y una vez que tienen las claves públicas los mensajes son cifrados de la siguiente manera:

1. El interlocutor 1 toma su mensaje y es cifrado con la clave pública del interlocutor 2 obteniendo un texto cifrado.

2. Se envía el texto cifrado al interlocutor 2.

3. El interlocutor 2 toma el texto cifrado y lo descifra usando su clave privada para obtener el mensaje del interlocutor 1.

Este método de cifrado propone dar solución a 2 problemas, el primer problema es que para hacer el intercambio de llaves en un cifrado simétrico es muy difícil ya que al pasar la clave por un canal inseguro y se intercepta esta clave la comunicación quedaría expuesta a un ataque. Este problema es resuelto con la clave pública ya que esta llave puede ser vista por cualquier persona y tiene la cualidad de que si se quiere obtener la clave privada a partir de la pública sus cálculos son demasiado difíciles de resolver.
El segundo problema es el manejo de claves para establecer comunicaciones seguras con más de un usuario. Tomando el modelo de cifrado simétrico necesitaríamos tener una clave diferente para cada conexión segura que se desea establecer, mientras que en el cifrado asimétrico se necesita tener un par de claves, pública y privada, por cada usuario y esas claves son suficientes para hacer las conexiones seguras que se requieran.
El beneficio que se tiene al utilizar claves públicas se ve al momento de establecer comunicaciones seguras, por ejemplo si tuviéramos 6 usuarios en una red con un esquema de cifrado asimétrico solo se necesitaría publicar las claves públicas de los usuarios en un lugar común para los 6, y cada vez que se quiera establecer una comunicación segura con algún usuario solo tienen que buscar su clave pública y cifrar el mensaje sin la necesidad de ponerse de acuerdo con cada uno de los usuarios de la red para establecer una clave para cada comunicación que se desea establecer como en el cifrado simétrico.

A pesar de la implementación de estas técnicas criptográficas los ataques a las comunicaciones siguen existiendo y estos ataques se han clasificado dependiendo de cuanta información tenga disponible el adversario para poder romper el cifrado y obtener la información deseada.

Nosotros nos enfocaremos a un tipo de ataque llamado “ataque de texto cifrado” o COA que hace referencia a su nombre en inglés “ Ciphertext-only attack” [9]. Este ataque solo cuenta con los textos cifrados que va recopilando de un canal o base de datos, estos textos cifrados los utiliza para hacer un análisis criptográfico de cómo se comportan la técnica de cifrado y trata de resolver el cifrado de los textos cifrados que ya tiene y los nuevos textos 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 pones a este tipo de agentes a atacar comunicaciones sin cifrado obtienes características valiosas sobre los usuarios que utilizan este tipo de canales de comunicación, este tipo de ataques son ejecutados por programas llamados agentes clasificadores.

3.14 Agentes Clasificadores

Los agentes clasificadores son programas que se dedican a observar los 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 y la realiza haciendo una búsqueda de palabras claves 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 Maquina” para encontrar y clasificar los mensajes que intercepta. [5] [4]
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.

Chapter 4

Análisis y Diseño

Tomando en cuenta la información ya vertida en este documento, explicaremos a profundidad la propuesta de solución que hemos ideado.
En la figura 4.1 tenemos el diagrama general del sistema, se puede apreciar la comunicación entre las diferentes entidades que usaremos, que datos mandan y reciben y por que canales transitan estos datos. A continuación describiremos 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(plugin).
    - El cliente genera a partir del correo una clave que usaremos para cifrar el mensaje.
    - Se cifra el mensaje y se empaqueta el mensaje, antes de enviarse se crea una firma de este.
    - La clave se convierte en CAPTCHA, se firma 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.

- Se resuelven y se recalcula la clave de descifrado.

- Se descifra el mensaje y se le muestra al usuario.

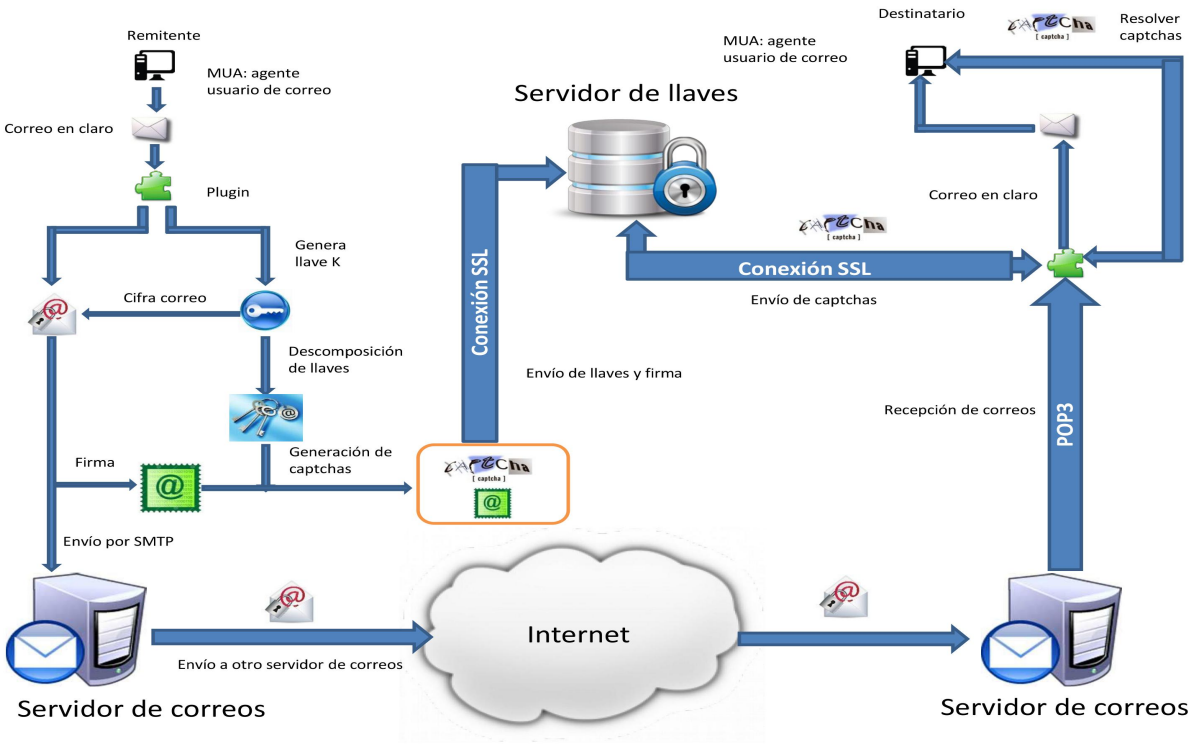

Figure 4.1: Diagrama General del sistema

4.1 Diagramas de caso de uso

Para el desarrollo de esta propuesta se muestran los siguientes diagramas, estos muestran el diseño que nos da una idea mas clara de como quedara el sistema.

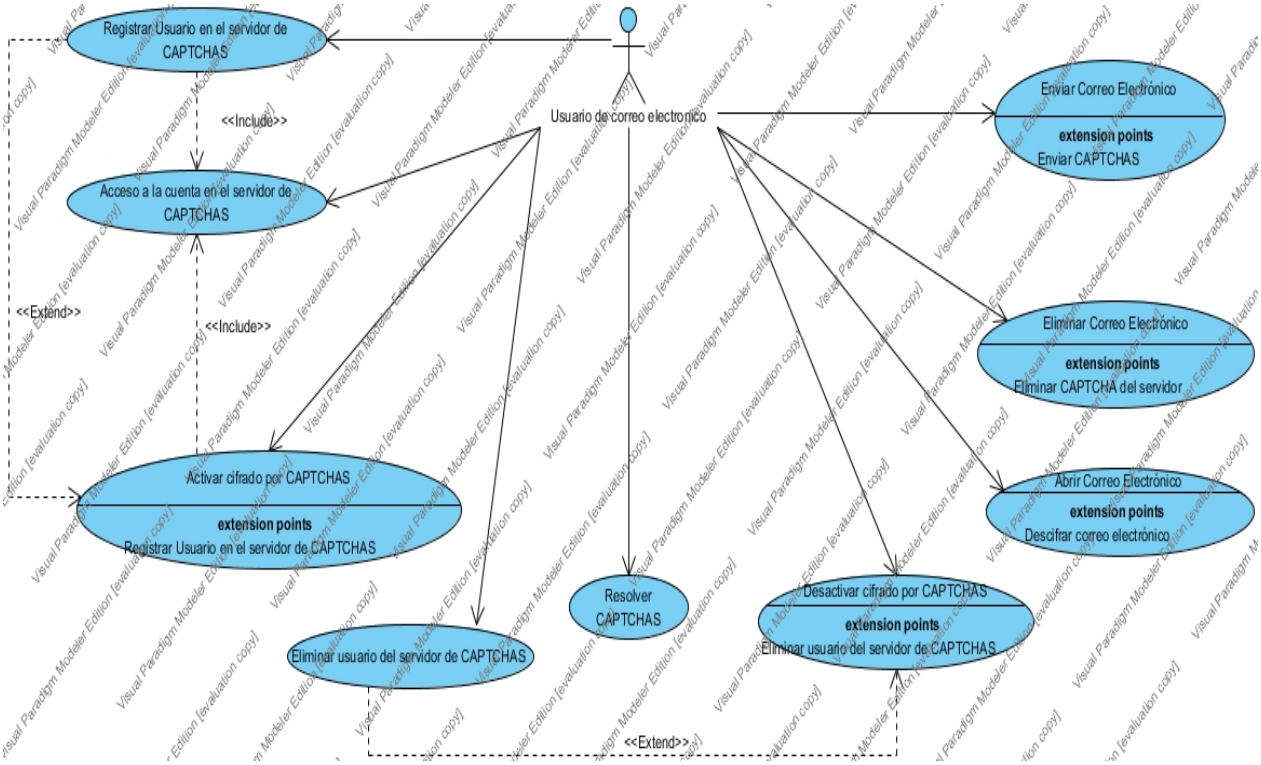

Figure 4.2: Diagrama General de caso de uso

4.1.1 Diagrama de caos de uso CU2 Registrar usuario en el servidor de CAPTCHAS

Caso de Uso	CU2 Registrar Usuario en el servidor de CAPTCHAS		
Actor	Actor1. Usuario de Corro Electrónico		
Descripción	Describe los pasos necesarios para registrar un nuevo usuario en el servidor de CAPTCHAS.		
Pre-condiciones	Tener una cuenta de correo electrónico.		
Post-condiciones	Activación del módulo de cifrado por CAPTCHAS.		
Puntos de inclusión	Acceso a la cuenta en el servidor de CAPTCHAS.		
Puntos de extensión			
Flujo principal		Actor/Sistema	Acción a realizar
	1	Actor	El usuario selecciona la opción registrarse en el servidor de CAPTCHAS

	2	Sistema	El cliente de correo despliega un formulario con la información necesaria para dar de alta en el servidor de CAPTCHAS.
	3	Actor	Completa el formulario y oprime el botón de registrar.
	4	Sistema	El sistema valida los datos proporcionados por el usuario.
	5	Sistema	Se conecta con el servidor y valida si el usuario ya está registrado. <FA01 - Usuario ya registrado> <FA02 - Falla en la conexión con el servidor>
	6	Sistema	Manda la información del usuario y lo da de alta.
	7	Sistema	Despliega el siguiente mensaje "El usuario se ha dado de alta correctamente"
			Fin del flujo principal.
	FA01 - Usuario ya registrado.		
Flujo alternativo		Actor/Sistema	Acción a realizar
	1	Sistema	Despliega el siguiente mensaje "El usuario ya está registrado favor de proporcionar otra cuenta de correo electrónico"
	2		El flujo continúa en el paso 3 del flujo principal.
			Fin del flujo alternativo
	FA02 - Falla en la conexión con el servidor.		
Flujo alternativo		Actor/Sistema	Acción a realizar
	1	Sistema	Despliega el siguiente mensaje " La conexión con la red es nula o limitada, favor de realizar esta operación más tarde"
	2		El flujo continúa en el paso 1 del flujo principal.
			Fin del flujo alternativo

Tabla 4.1: Descripcion CU2.

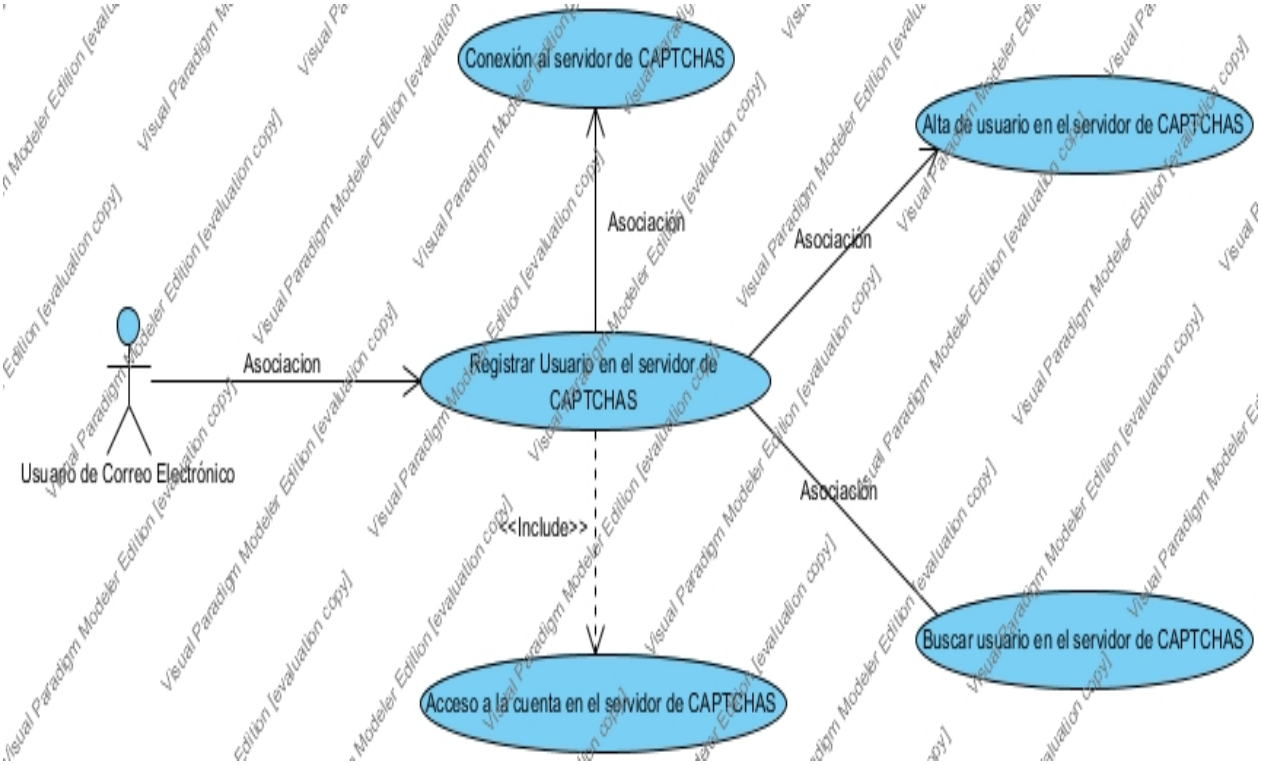

Figure 4.3: Diagrama de caos de uso CU2 Registrar usuario en el servidor de CAPTCHAS

4.1.2 Diagrama de casos de uso CU3 Acceso a la cuenta en el servidor de CAPTCHAS

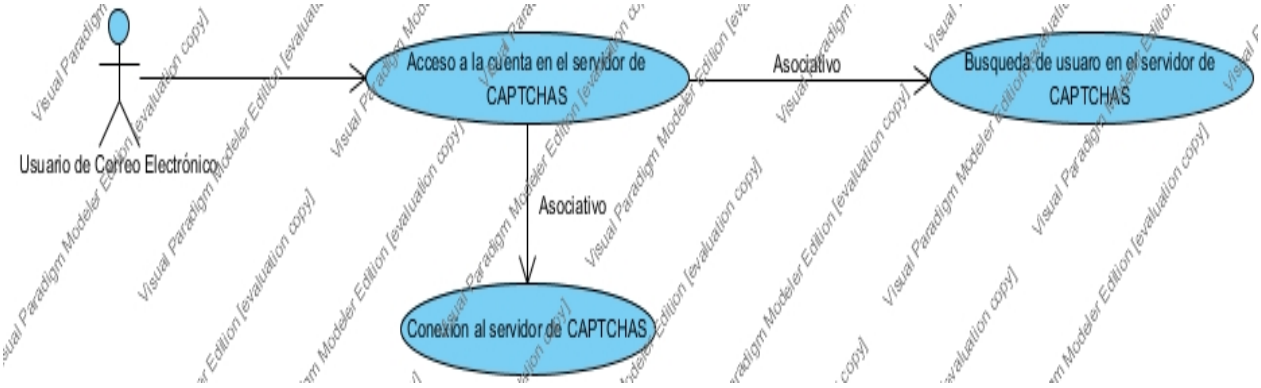

Figure 4.4: Diagrama de casos de uso CU3 Acceso a la cuenta en el servidor de CAPTCHAS

4.1.3 Diagrama de casos de uso CU4 Abrir Correo Electrónico.

Caso de Uso	CU4 Abrir correo electrónico		
Actor	Actor 1. Usuario de correo electrónico		
Descripción	Describe los pasos necesarios para abrir un mensaje de correo electrónico.		
Pre-condiciones	1. Iniciar sesión con su servidor de correo electrónico. 2. Descargar el correo electrónico que se desea abrir.		
Post-condiciones	Despliegue del mensaje de correo electrónico descifrado.		
Puntos de inclusión	Desempaquetar correo electrónico		
Puntos de extensión	Descifrar correo electrónico		
Flujo principal		Actor/Sistema	Acción a realizar
	1	Actor	El caso de uso comienza cuando el usuario selecciona el correo que desea abrir.
	2	Sistema	El sistema manda a llamar a la función de desempaquetar correo electrónico.
	3	Sistema	Valida si el mensaje viene timbrado. <FA01 - El mensaje no viene timbrado>
	4	Sistema	Invoca al caso de uso <CU Descifrar correo electrónico>
	5	Sistema	Recibe el mensaje de correo electrónico descifrado
	6	Sistema	Despliega el contenido completo del mensaje al usuario
			Fin del flujo principal.
	FA01 - El mensaje no viene timbrado.		
Flujo alternativo		Actor/Sistema	Acción a realizar
	1	Sistema	El flujo continúa en el paso 6 del flujo principal.
			Fin del flujo alternativo

Tabla 4.2: Descripcion CU4.

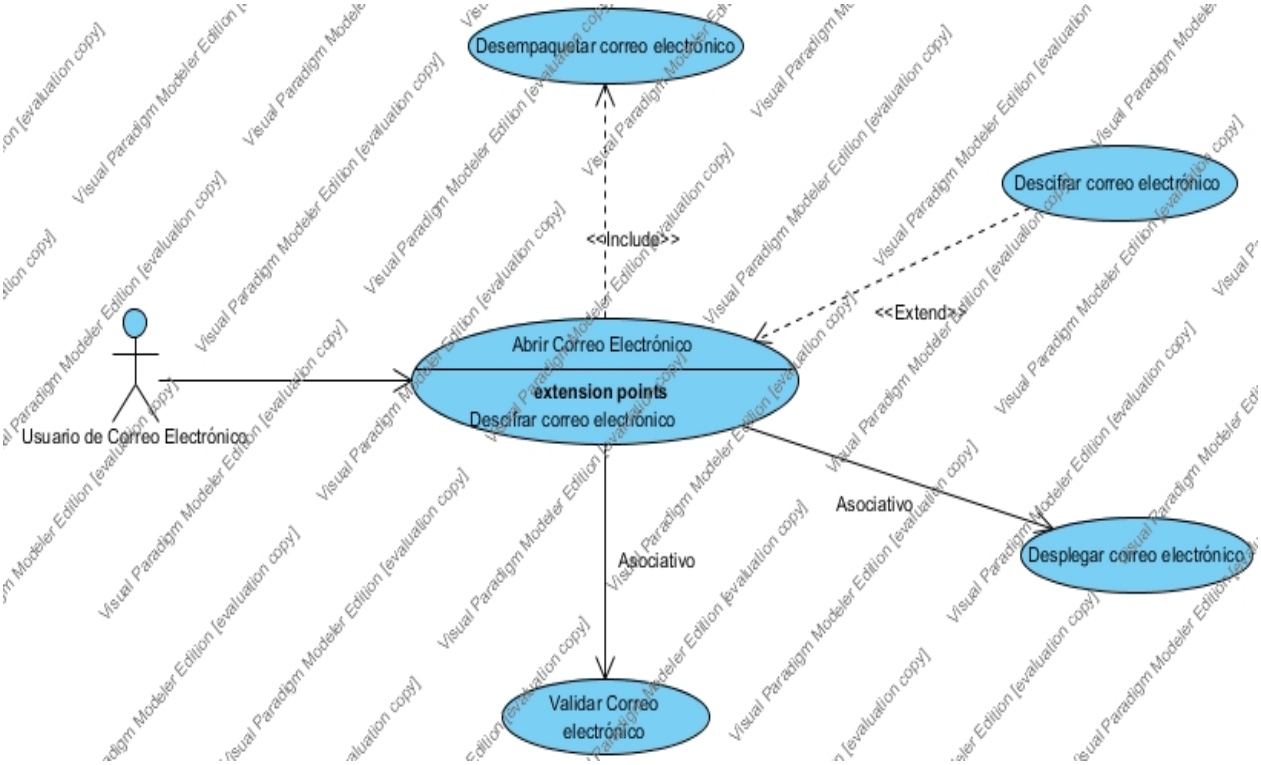

Figure 4.5: Diagrama de casos de uso CU4 Abrir Correo Electrónico.

4.1.4 Diagrama casos de uso CU5 Activar cifrado por CAPTCHAS.

Caso de Uso	CU5 Activar cifrado por CAPTCHAS		
Actor	Actor 1. Usuario de correo electrónico		
Descripción	Describe los pasos necesarios para activar el módulo de cifrado CAPTCHAS en el cliente de correo electrónico.		
Pre-condiciones	1. Instalar el módulo de cifrado por CAPTCHAS		
Post-condiciones	Activación del cifrado y descifrado por CAPTCHAS.		
Puntos de inclusión			
Puntos de extensión	Registrar usuario del servidor de CAPTCHAS		
Flujo principal		Actor/Sistema	Acción a realizar
	1	Actor	El caso de uso inicia cuando el actor seleccionar la opción "Activar cifrado por CAPTCHAS"
	2	Sistema	El sistema verifica si la dirección de correo del usuario está registrada en el servidor de CAPTCHAS<FA01 -Usuario no registrado en el servidor>

	3	Sistema	Despliega una ventana con el mensaje "Activación del módulo de cifrado por CAPTCHAS"
			Fin del flujo principal.
	FA01 -Usuario no registrado en el servidor.		
Flujo alternativo		Actor/Sistema	Acción a realizar
	1	Sistema	El sistema despliega una ventana con las opciones de "Registrarse" y "Cancelar". <FA02 Cancelar activación>
	2	Actor	Oprime el botón de "Registrarse"
	3	Sistema	El sistema invoca al caso de uso <CU Registrar usuario en el servidor de CAPTCHAS>
	4	Sistema	El sistema obtiene una respuesta satisfactoria del registro
	5		El flujo continúa en el paso 2 del flujo principal.
			Fin del flujo alternativo
	FA02 - Cancelar activación.		
Flujo alternativo		Actor/Sistema	Acción a realizar
	1	Actor	El Actor selecciona "Cancelar"
	2	Sistema	Cierra la ventana de selección
	3		El flujo continúa en el paso 1 del flujo principal.
			Fin del flujo alternativo

Tabla 4.3: Descripcion CU5.

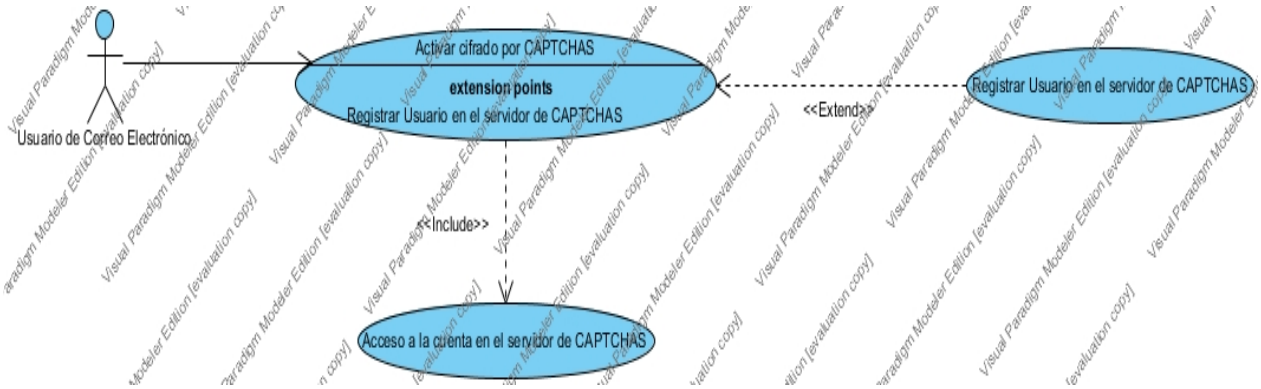

Figure 4.6: Diagrama casos de uso CU5 Activar cifrado por CAPTCHAS.

4.1.5 Diagrama de casos de uso CU6 Descifrar correo electrónico.

Caso de Uso	CU6 Descifrar correo electrónico.		
Actor	Actor 1. Usuario de correo electrónico		
Descripción	Describe los pasos necesarios para desactivar el módulo de cifrado CAPTCHAS en el cliente de correo electrónico		
Pre-condiciones	1. Activar cifrado por CAPTCHAS. 2. Registrar usuario en el servidor de CAPTCHAS		
Post-condiciones	Desactivación del cifrado y descifrado por CAPTCHAS.		
Puntos de inclusión			
Puntos de extensión	Eliminar usuario del servidor de CAPTCHAS		
Flujo principal		Actor/Sistema	Acción a realizar
	1	Actor	El caso de uso inicia cuando el actor seleccionar la opción "Desactivar cifrado por CAPTCHAS"
	2	Sistema	El sistema despliega la venta con las opciones de "Desactivar cifrado" y "Eliminar usuario" <FA01 - Eliminar usuario>
	3	Actor	Selecciona la Desactivación del cifrado por CAPTCHAS
	4	Sistema	El sistema desactiva el módulo de cifrado por CAPTCHA
			Fin del flujo principal.
	FA01 - Eliminar usuario.		
Flujo alternativo		Actor/Sistema	Acción a realizar
	1	Actor	El Actor selecciona "Eliminar usuario"

	2	Sistema	El sistema despliega una ventana con las opciones de "Aceptar" y "Cancelar" para confirmar la eliminación del usuario. <FA02 - Cancelar acción eliminar usuario>
	3	Actor	Oprime el botón de "Aceptar"
	4	Sistema	Establece la conexión con el servidor de CAPTCHAS <FA03 - Fallo en la conexión con el servidor>
	5	Sistema	Busca y elimina al usuario de la base de datos desplegando la confirmación del servidor.
	6	Actor	Oprime el botón de "Aceptar"
	7	Sistema	Desactiva el módulo de cifrado por CAPTCHA
			Fin del flujo alternativo
	FA02 - Cancelar acción eliminar usuario.		
Flujo alternativo		Actor/Sistema	Acción a realizar
	1	Actor	El Actor selecciona "Cancelar"
	2	Sistema	Cierra la ventana de confirmación
			Fin del flujo alternativo
	FA03 - Fallo en la conexión con el servidor.		
Flujo alternativo		Actor/Sistema	Acción a realizar
	1	Sistema	Despliega una ventana de alerta con el mensaje "No sé a podido establecer la conexión con el servidor, es probable que no se tenga conexión a internet. Favor de intentarlo más tarde"
	2	Actor	Cierra la ventana de alerta
	3		El flujo continua en el paso 1 del flujo principal
			Fin del flujo alternativo

Tabla 4.4: Descripcion CU6.

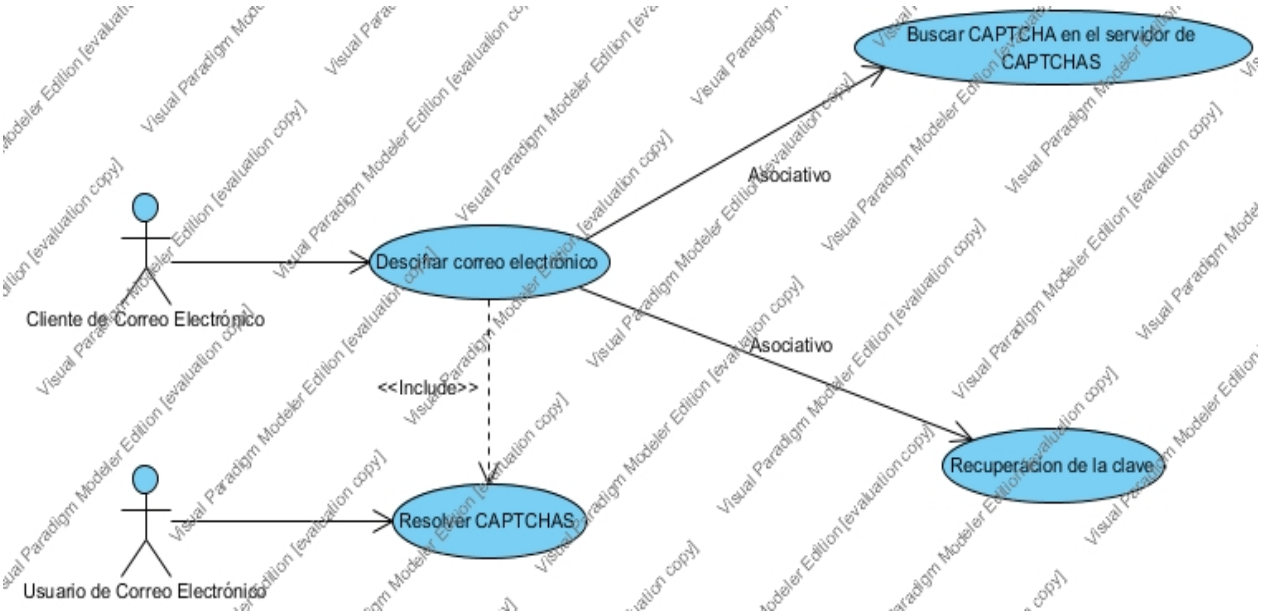

Figure 4.7: Diagrama de casos de uso CU6 Descifrar correo electrónico.

4.1.6 Diagrama de caos de uso CU7 Eliminar CAPTCHA del servidor.

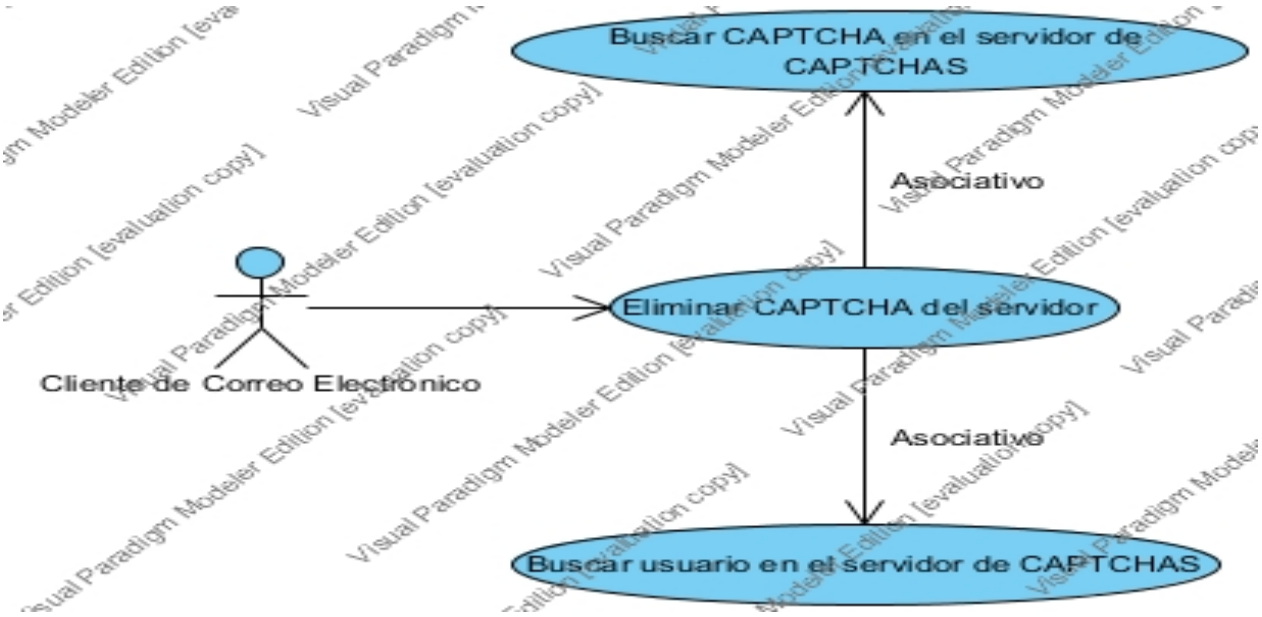

Figure 4.8: Diagrama de caos de uso CU7 Eliminar CAPTCHA del servidor.

Caso de Uso	CU7 Eliminar CAPTCHA del servidor.		
Actor	Actor 1. Cliente de correo electrónico.		
Descripción	Describe los pasos necesarios para eliminar los CAPTCHAS del servidor de CAPTCHAS.		
Pre-condiciones	1. Solicitar eliminar un mensaje de correo electrónico		
Post-condiciones			
Puntos de inclusión			
Puntos de extensión			
Flujo principal		Actor/Sistema	Acción a realizar
	1	Actor	Solicita eliminar CAPTCHA del servidor de CAPTCHAS
	2	Sistema	Busca al usuario y el CAPTCHA a eliminar en el servidor de CAPTCHAS
	3	Sistema	Elimina el CAPTCHA solicitado
	4	Sistema	Regresa la confirmación de que se eliminó el CAPTCHA.
			Fin del flujo principal.

Tabla 4.5: Descripcion CU7.

4.1.7 Diagrama de casos de uso CU8 Eliminar correo electrónico.

Caso de Uso	CU8 Eliminar correo electrónico.		
Actor	Actor 1. Usuario de correo electrónico.		
Descripción	Describe los pasos necesarios para eliminar un mensaje de correo electrónico.		
Pre-condiciones	1. Seleccionar un mensaje de correo electrónico		
Post-condiciones	Mensaje y CAPTCHA eliminados.		
Puntos de inclusión	1. Desempaquetar correo electrónico. 2. Eliminar correo electrónico del servidor		
Puntos de extensión	Eliminar CAPTCHA del servidor de CAPTCHAS		
Flujo principal		Actor/Sistema	Acción a realizar
	1	Actor	Selecciona un mensaje de correo electrónico a eliminar.
	2	Sistema	Desempaqueta el mensaje de correo electrónico
	3	Sistema	Valida si el mensaje esta timbrado. <FA01 - Mensaje no timbrado>
	4	Sistema	Invoca al caso de uso <CU Eliminar CAPTCHA del servidor>
	5	Sistema	Elimina el mensaje de correo electrónico y despliega el mensaje "El correo se ha eliminado correctamente"
			Fin del flujo principal.
	FA01 - Mensaje no timbrado.		
Flujo alternativo		Actor/Sistema	Acción a realizar
	1	Sistema	El sistema continúa a partir del paso 5 del flujo principal.
			Fin del flujo alternativo

Tabla 4.6: Descripcion CU8.

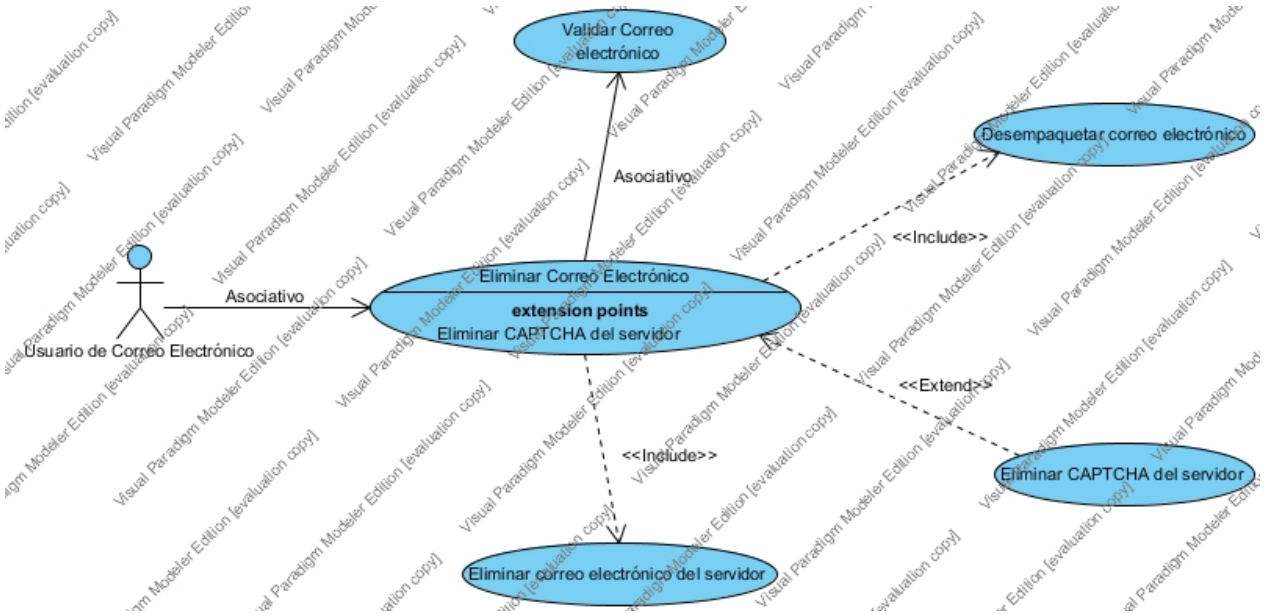

Figure 4.9: Diagrama de casos de uso CU8 Eliminar correo electrónico.

4.1.8 Diagrama de casos de uso CU9 Enviar CAPTCHAS

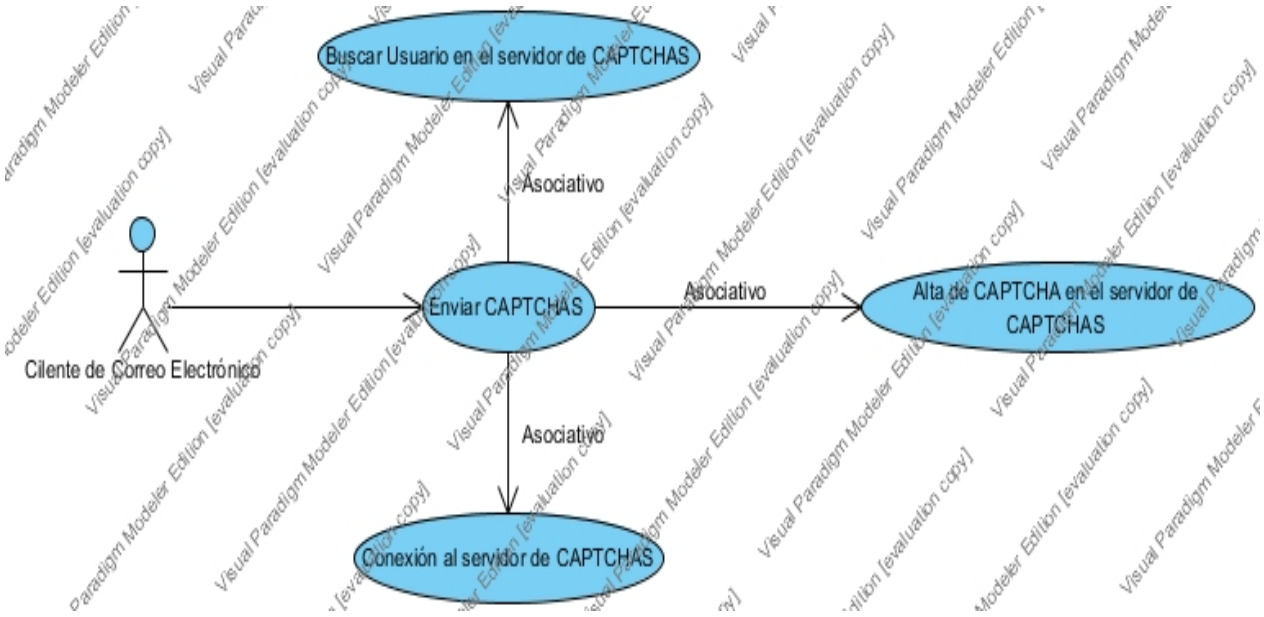

Figure 4.10: Diagrama de casos de uso CU9 Enviar CAPTCHAS

Caso de Uso	CU9 Enviar CAPTCHAS		
Actor	Actor 1. Cliente de correo electrónico.		
Descripción	Describe los pasos necesarios para enviar el CAPTCHA el servidor de CAPTCHAS		
Pre-condiciones	1. Solicitar el envió de un nuevo mensaje de correo electrónico.		
Post-condiciones	Envío del CAPTCHA al servidor de CAPTCHAS		
Puntos de inclusión			
Puntos de extensión			
Flujo principal		Actor/Sistema	Acción a realizar
	1	Actor	Solicita el envío de CAPTCHA al servidor
	2	Sistema	Abre la conexión y busca al usuario en el servidor de CAPTCHAS
	3	Sistema	Da de alta el CAPTCHA en el servidor asociándolo con el usuario.
	4	Sistema	Regresa la confirmación de que se dio de alta el CAPTCHA
			Fin del flujo principal.

Tabla 4.7: Descripcion CU9.

4.1.9 Diagrama de casos de uso CU10 Enviar correo electrónico.

Caso de Uso	CU10 Enviar correo electrónico.		
Actor	Actor 1. Usuario de correo electrónico.		
Descripción	Describe los pasos necesarios para enviar un mensaje de correo electrónico cifrado a otro usuario de correo electrónico.		
Pre-condiciones	1. El usuario tiene que redactar un mensaje de correo electrónico que contenga la dirección del destinatario.		
Post-condiciones	Envió de un mensaje cifrado al servidor de correo electrónico y el registro del CAPTCHA en el servidor de CAPTCHAS.		
Puntos de inclusión	1. Validar correo electrónico. 2. Empaquetar mensaje de correo electrónico SMTP.		
Puntos de extensión	Enviar CAPTCHA		
Flujo principal		Actor/Sistema	Acción a realizar
	1	Actor	Oprime el botón "Enviar"
	2	Sistema	Valida que el mensaje de correo electrónico contenga los datos mínimos.<FA01 - Campos no completados>
	3	Sistema	Genera una llave de cifrado
	4	Sistema	Con la llave generada genera el CAPTCHA y cifra el mensaje de correo electrónico.
	5	Sistema	Toma el mensaje cifrado y es empaquetado para enviarse al servidor de correo electrónico
	6	Sistema	Toma el CAPTCHA generado y se envía al caso de uso <CU Enviar CAPTCHA>
	7	Sistema	Despliega el mensaje de "envío satisfactorio"
			Fin del flujo principal.
	FA01 - Campos no completados.		
Flujo alternativo		Actor/Sistema	Acción a realizar
	1	Sistema	Notifica al usuario cuales campos mal proporcionado para poder enviar el mensaje correctamente
	2	Actor	Modifica los campos solicitados
	3		El flujo continua en el paso 1 del flujo principal
			Fin del flujo alternativo

Tabla 4.8: Descripcion CU10.

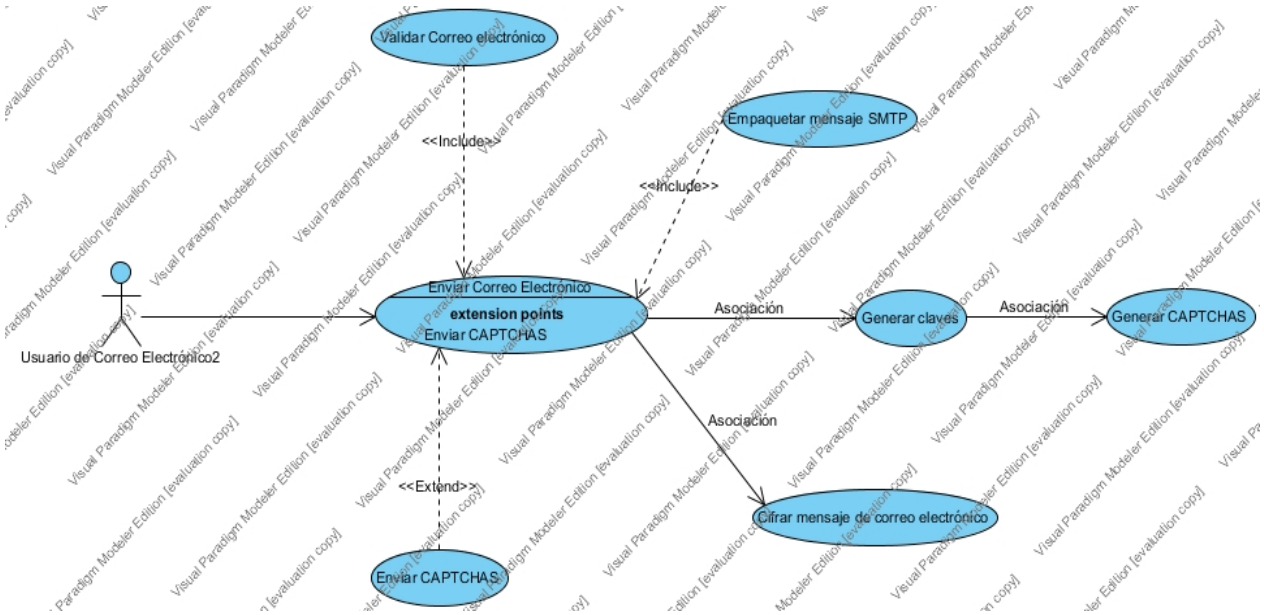

Figure 4.11: Diagrama de casos de uso CU10 Enviar correo electrónico.

4.2 Diagramas a bloques

Les presentaremos a continuación los diagramas a bloques, en donde mostramos cual es la secuencia de procesos a realizar. Esto nos ayuda a clarificar como se comunican los diferentes módulos de manera interna, cuales y como hacen los procesos.

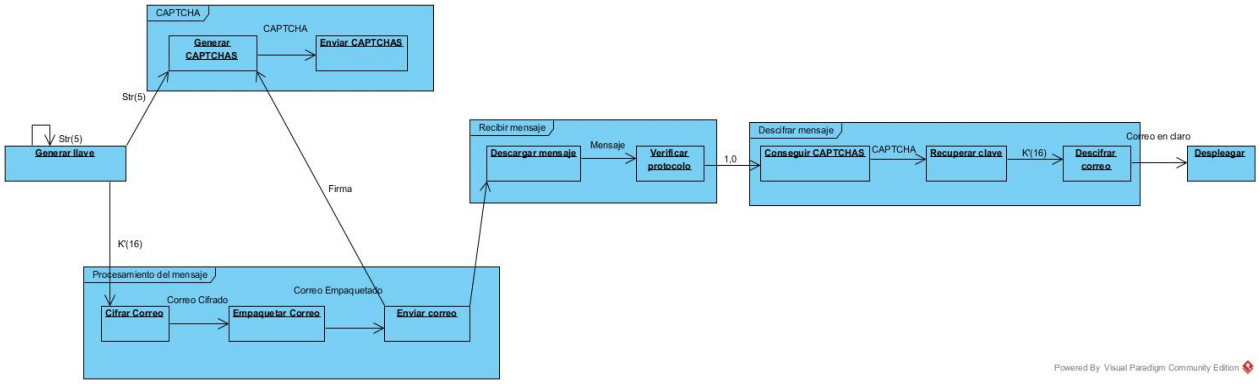

Figure 4.12: Diagrama a bloque 0 general del sistema

	Generar clave	**Generar CAPTCHA**	**Procesamiento del mensaje**	**Recibir mensaje**	**Descifrar mensaje**	**Desplegar**
Entradas	*Señal de activación	*Cadena de 5 caracteres: Str(5)	*Clave de 16 bytes: K'(16). *Mensaje de correo.	*Correo Cifrado	Verificación (1,0)	*Correo en claro
Salidas	*Cadena de 5 caracteres: Str(5) *Clave de 16 bytes: K'(16)	*Señal de envió	*Correo Cifrado	*Verificación (1,0)	*Correo en claro	
Descripción	Se activa el proceso generar clave, este crea una palabra de 5 caracteres (Str(5)), procesa la palabra Str(5) por medio de una función hash obteniendo una palabra de 256 caracteres (K(256)) y recorta esta clave a una palabra de 16 caracteres (K'(16)).	Toma la entrada Str(5) y la convierte en una imagen CAPTCHA, Posteriormente inicia una conexión con el servidor de CAPTCHAS para mandarlo a este.	Cifra el mensaje de correo con la clave K'(16), posteriormente lo firma y genera un timbre para saber que fue creado con este esquema y lo empaqueta para su envió.	El cliente hace una petición al servidor y descarga el mensaje de correo electrónico, lo des empaqueta verifica la firma y el timbrado para saber de quién viene y si está cifrado bajo este esquema.	Se hace una petición al servidor de CAPTCHAS, se descargan los CAPTCHAS asociados al correo, ya con el CAPTCHA este se resuelve y se recupera la cadena Str(5), esta se pasa por una función hash y se recupera K(256), esta se corta a K'(16), con esto se descifra el mensaje.	Se muestra el correo descifrado en la interfase del cliente de correo electrónico.

Tabla 4.9: Diagrama a bloques 0 general

Figure 4.13: Diagrama a bloques 1 Generar clave

	Generar Str(5)	**Aplicar Función Hash**	**Recortar Hash K'**
Entradas	*Llamada a Función	*Cadena de 5 caracteres: Str(5)	*Digesto K(128)
Salidas	*Cadena de 5 caracteres: Str(5)	*Digesto K(128)	*K'(16)
Descripción	Toma una función random módulo 67, para formar una palabra con 5 caracteres aleatorios tomados del siguiente conjunto.Anillo67-.,+*[a-z][A-Z]	Se pasa la cadena Str(5) por una función hash SHA-1 para obtener un digesto único de esta palabra.	Se copian a otro string lo primeros 16 caracteres del digesto K(128) para formar la clave K'(16)

Tabla 4.10: Diagrama a bloques 1 general clave

	Cifrar
Entradas	*Clave K'(16) *Mensaje de correo
Salidas	*Correo cifrado
Descripción	Se cifra el mensaje con un algoritmo de llave simétrica (AES o DES) usando una llave de 16bytes o 128bits.

Tabla 4.11: Diagrama a bloques 2 Cifrar Correo

Figure 4.14: Diagrama a bloques 3 Empaquetar Correo

	Empaquetamiento SMTP	**Timbrar Correo**
Entradas	*Mensaje Cifrado	*Correo Empaqueta
Salidas	*Correo Empaquetado	*Correo Timbrado
Descripción	Se toma el correo y se integra en el formato del correo marcado en el RFC822	Se timbra el mensaje colocando una marca después del final del mensaje. Para señalar que el correo enviado está cifrado bajo este protocolo.

Tabla 4.12: Diagrama a bloques 3 Empaquetar Correo

Figure 4.15: Diagrama a bloques 4 Enviar correo

	Abrir conexión SMTP	**Envió de Correo por SMTP**
Entradas	*Petición	*Correo empaquetado
Salidas	*Canal de comunicación	*Confirmación de envió
Descripción	Se genera una petición para conexión SMTP	Se manda el correo electrónico al servidor por medio del protocolo SMTP

Tabla 4.13: Diagrama a bloques 4 Enviar correo

Referencias

[1] Email, Internet: http://en.wikipedia.org/wiki/Email, Mayo, 2015

[2] Interactive Advertising Bureau, Marcelo Brodsky, "Reflexiones jurídicas sobre el e-marketing en Chile", Internet: http://www.iab.cl/reflexiones-juridicas-sobre-ele-marketing-en-chile.

[3] D. Jurafsky, Text Classification, Stanford University Natural Language Processing.

[4] S. Díaz Santiago y D. Chakraborty., "On Securing Communication from Profilers." Proceedings of International Conference on Security and Cryptography, Secrypt 2012, pp.154-162, Rome, Italy, 2012.

[5] Philippe Golle and Ayman Farahat. "Defending Email Communication Against Profiling Attacks" Proceedings of the 2004 ACM workshop on Privacy in the electronic society, ACM New York, NY, USA ©2004pp 39-40

[6] J. Klensin, "Simple Mail Transfer Protocol", Patent 5321, October 2008.

[7] J. Myers, "Post Office Protocol - Version 3", Patent 1939, May 1996.

[8] A. Gulbrandsen, "Internet Message Access Protocol (IMAP) - MOVE Extension", Patent 6851, January 2013.

[9] Ciphertext-only attack Internet: https://en.wikipedia.org/wiki/Ciphertext-only_attack,Noviembre2015.