La comunicación por medio del Correo electrónico es atacada constantemente y por ellos 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 lee el contenido del correo y busca palabras específicas no necesitamos tantos servicios criptográficos para detener sus ataques a los correos electrónicos. Sería suficiente con tener un esquema de cifrado que nos 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 CAPTHCAS 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 nuestro adversario clasificador es un programa de cómputo, le es muy complicado encontrar la clave para descifrar el mensaje y poderlo clasificar correctamente.