**Objetivo del prototipo**

Conocer el uso, funcionamiento e implementacion de herramientas de cifrado, hashing y generacion de CAPTCHAS, con el fin de conocer la integracion de estos modulos en diferentes lenguajes de programacion.

**Prototipo 1**

Se implemento un modulo de cifrado de mensajes de texto en lenguaje C++. Tratando de simular el proceso de cifrado del esquema que estamos usando.

La primera parte del proceso es abrir el mensaje para lo cual usamos las bibliotecas estándar stdio.h, posteriormente crearemos una palabra aleatoria de 10 caracteres usando una funcion Rand()%100 casteando el valor de salida a un char.

Al resultado se pasa por una funcion de hashing, esta funcion no es nativa de ninguna biblioteca estandart de C++ ni de C, por lo que se tuvo que conseguir una en internet y probar que efectivamente funcionara como lo necesitamos.

Posteriormente este hash se usara como llave para cifrar el mesaje que ya abrimos, para esto necesitaremos una funcion AES o DES, ninguna de estas es estandart de alguna biblioteca de C o C++, asi que tendremos que buscarlas 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 usaran, ya que no siempre estan funcionando correctamente, en algunos casos estan 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, encontrandonos con bibliotecas que cifraban mal ya que al meter la misma llave no descifraban e incluso bibliotecas que no logramos hacer que compilaran.

**Prototipo 2**

Se implemento un modulo de cifrado, descifrado y generacion de CAPTCHAS en Python, simulando el proceso antes del envio del correo y el que se hace despues de la recepcion de los correos electronicos.

Para este se uso el formato estandar del correo electronico especificado en el RFC 822, tambien se usaron bibliotecas ya estandarizadas de python para la implementacion de las funciones de hashing, funciones de cifrado y descifrado (AES o DES), funciones aleatorias y la generacion de los CAPTCHAS.

**Conclusión**

Se logro generar todo el proceso de envio y parte de el de recibimiento de mensajes. En cuanto a el envio se logro leer el mensaje, crear el strig a partir de funciones random, crear la llave con esa string y cifrar el correo exitosamente, ademas de esto se logro leer el archivo de mensaje de correo electronico y cifrar unicamente el mensaje que biene en este.

Por su parte el modulo de generacion de CAPTCHAS mostró muchos problemas para generarlos, ya que no logramos hacer que el interprete pudiera encontrar correctamente las funciones de la biblioteca de generacion CAPTCHAS por lo que al no poder generar un CAPTCHA la recuperacion no se puede realizar como se planteo, para verificar únicamente que las funciones sirven se implemento el descifrado del mensaje en el mismo metodo.