Guatemala 05 de octubre de 2020

Avances en el Proyecto #2

Cifrado de Información

Juan Fernando De León 17822
Jose Amado Garcia 181469
Edgar Andree Toledo 18439
Ricardo Antonio Valenzuela 18762
Sara Zavala 18893

Introducción

En la actualidad diversos países cuentan regulaciones y legislaciones en las cuales permiten a los proveedores de servicios de internet registrar el tráfico en línea de cada usuario. Esta es una de las razones por la cual la mensajería segura y encriptada se ha vuelto de suma importancia. Si se utiliza el sistema de mensajería SMS estándar y no cifrados estos están abiertos para que proveedores de servicios de telefonía, el gobierno y piratas informáticos vean la información que se maneja en estas aplicaciones.

La mensajería cifrada brinda una encriptación *peer to peer,* esto quiere decir que tanto la persona que envía el mensaje y la persona que lo recibe cuentan con una comunicación segura. La mensajería encriptada evita que la información enviada y recibida permanezca secreta e integra. El cifrado de información es un proceso de codificación para evitar que cualquier persona que no sea el destinatario previsto vea el mensaje enviado. En el cifrado de información moderno se utilizan algoritmos donde la información cifrada es ilegible para cualquier persona que no tenga acceso a una clave que se utiliza para descifrar el texto. Dos métodos modernos de cifrado son la clave pública (asimétrica) y la clave privada (simétrica).

Materiales y métodos

Para la realización de este chat se utilizarán ciertas herramientas de programación relacionadas con el lenguaje JavaScript y Python.

- Visual Studio Code: es un editor de código fuente desarrollado por Microsoft para Windows , Linux y macOS. Incluye soporte para la depuración, control integrado de Git, resaltado de sintaxis, finalización inteligente de código, fragmentos y refactorización de código

  En este editor se realizará todo el código que construye la estructura de nuestro proyecto

- Django: es un framework de desarrollo web de código abierto. Este se utilizará para el manejo de base de datos y el mantenimiento de un API con el cual se controlará las entradas y salidas con un servidor

  Metodología:
  El proyecto se llevará a cabo por medio de react, javascript y Django. Se creará un proyecto de react donde se manejan los componentes principales para nuestro chat web. Ya teniendo creados cada uno de los componentes, de los cuales están
  - página principal
  - Interfaz de primer usuario
  - interfaz de segundo usuario
  - Manejo de permisos

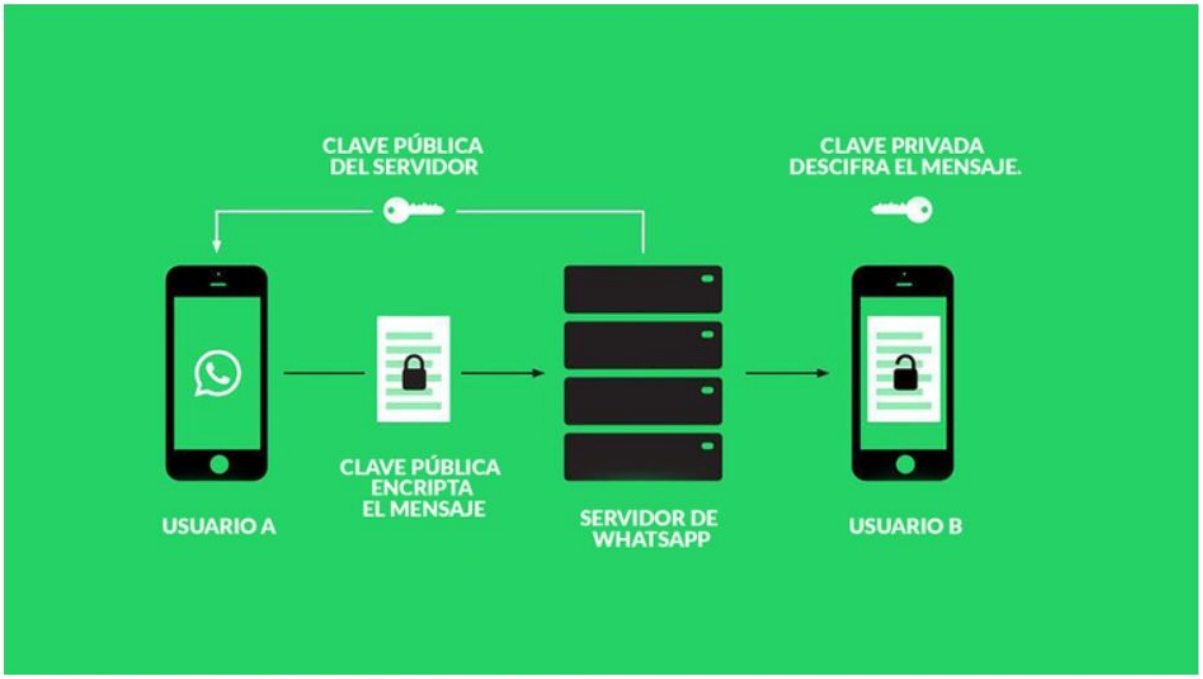
Teniendo implementados los componentes, pasaremos a la creación de un API propio y/o implementación de uno ya existente. Con esto podremos hacer todas las llamadas necesarias, extracción, y almacenamiento de datos.

Teniendo el chat ya estructurado y con el manejo de información estable, podremos comenzar la implementación del cifrado y descifrado de los mensajes y datos enviados por medio de nuestro chat. Para esto se utilizara el lenguaje Python

INVESTIGACIÓN

Hace poco más de dos años, a principios de abril de 2016, WhatsApp anunciaba la encriptación de extremo a extremo (end-to-end) en las comunicaciones. Esto significa que la información de las conversaciones, en vez de estar almacenadas en los servidores centralizados y gestionados por WhatsApp, son guardadas a través de claves de cifrado en el dispositivo del usuario.

"Este protocolo de cifrado extremo a extremo está diseñado para evitar que terceras partes y WhatsApp tengan acceso al texto plano de las llamadas o los mensajes. Y lo que es más, incluso si las claves de cifrado de un dispositivo de usuario se ven comprometidas físicamente, no podrán ser usadas para volver atrás en el tiempo y descifrar mensajes transmitidos con anterioridad."



El funcionamiento del cifrado de extremo a extremo.

Así, en este proceso, existen claves (keys) de cifrado públicas y privadas. Pero, ¿es WhatsApp un sistema 100% seguro?

"Es casi perfecto ya que su seguridad ha sido comprometida en lo que va del año por una investigación realizada por el Perito Informático Marcelo Romero. Encontró un falla en las claves para vulnerar este protocolo de cifrado de extremo a extremo, en la versión web y móvil", señala Emiliano Zárate, investigador digital e instructor en Informática Forense y Seguridad de la Información.

De todos modos, en general, los expertos en ciberseguridad consideran que WhatsApp no es fácil de hackear sin acceso al teléfono.