# EncriptApp: aplicación móvil Android para cifrar y descifrar archivos de texto

## Investigación en curso

Frank W. Santander

Programa de Ingeniería de Sistemas

fsantander@unab.edu.co

Universidad Autónoma de Bucaramanga

RESUMEN

La información es manejada actualmente por medio de dispositivos móviles, ya que garantiza la portabilidad del dispositivo y fácil acceso a la información, y debido a su gran popularidad, es un blanco importante para hackers. Por lo tanto, la información es fácil de obtener, y consecuentemente, ser manipulada por usuarios no autorizados. En este documento se presenta una investigación en curso sobre una aplicación móvil para Android que cifra y descifra archivos de texto.

ABSTRACT

Currently, the information is handled by mobile devices as this ensures device portability and easy access to the information, and due its great popularity, is an important target for hackers. Therefore, the information is easy to obtain, and consequently, be manipulated by unauthorised users. In this paper is presented an ongoing research about a mobile app that encrypt and decrypt text files.

Área de Conocimiento

Ingenierías.

Palabras Clave

Criptografía, MD5, SHA-1.

INTRODUCCIÓN

La criptografía es conocida como el estudio de la verificación y escondite de la información [1]. Por medio de la criptografía, los mensajes en archivos de texto recopilados pueden convertirse en código inentendible que garantiza que la información contenida no sea manipulada por usuarios no autorizados.

En este documento, es presentada una investigación en curso para el desarrollo de una aplicación móvil para Android que cifra y descifra y descifra archivos de texto plano, usando los algoritmos de cifrado MD5 y SHA-1. En la Sección 2, se presentan los objetivos del proyecto. La Sección 3 expone la metodología de investigación para la realización del proyecto. En la Sección 4 son presentados los referentes teóricos relacionados con Internet de las Cosas y seguridad. La Sección 5 corresponde al cronograma para el desarrollo de la investigación. La Sección 6 corresponde a los resultados esperados del proyecto. En la Sección 7 es presentada la identificación del proyecto. Finalmente, la Sección 8 presenta las referencias bibliográficas y electrónicas consultadas.

OBJETIVOS

Para el desarrollo del proyecto de investigación se han propuesto los siguientes objetivos:



Objetivo General

Implementar una aplicación móvil para cifrar y descifrar archivos de texto.

Objetivos Específicos

Elaborar un estado del arte sobre técnicas de cifrado/descifrado.

Realizar un estudio de mercados sobre la aplicación móvil para Android a desarrollar.

Desarrollar una aplicación para Android que cifre y descifre archivos de texto.

Implementar la aplicación móvil para Android para cifrado/descifrado de archivos de texto.

METODOLOGÍA DE LA INVESTIGACIÓN

Para el desarrollo del proyecto de investigación se han propuesto tres fases, que se relacionan directamente con los objetivos específicos de la propuesta de investigación (Ver Figura 10), las cuales se describen a continuación:

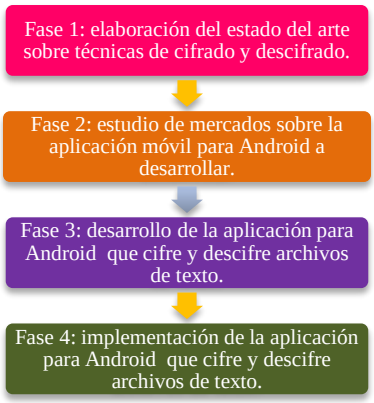


Figura 10. Fases del proceso investigativo.

Fuente. Elaboración propia.

Fase 1: Se realizó lo siguiente: (i) Búsqueda y revisión de la literatura; (ii) Lectura, análisis y clasificación.

Fase 2: Se realizó lo siguiente: (i) Diseño de los modelos de mercados; (ii) Encuesta sobre intereses por aplicaciones móviles que cifren y descifren archivos de texto.

Fase 3: Se está realizando lo siguiente: (i) Desarrollo de la aplicación móvil; (ii) Implementación de los algoritmos de cifrado.

Fase 4: Se está realizando lo siguiente: (i) Publicación de la aplicación móvil.

CRONOGRAMA POR DESARROLLAR

El cronograma de actividades para el desarrollo del proyecto, es presentado en la

Tabla 4.

Tabla 4. Cronograma de actividades

| ACTIVIDAD | | DURACIÓN (Meses) | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 1 | Búsqueda y revisión de la literatura | | | | | | | | | | | | |
| 2 | Lectura, análisis y clasificación | | | | | | | | | | | | |
| 3 | Diseño de los modelos de mercados | | | | | | | | | | | | |
| 4 | Encuesta sobre intereses por aplicaciones móviles que cifren y descifren archivos de texto. | | | | | | | | | | | | |
| 5 | Desarrollo de la aplicación móvil | | | | | | | | | | | | |
| 6 | Implementación de los algoritmos de cifrado | | | | | | | | | | | | |
| 7 | Publicación de la aplicación móvil | | | | | | | | | | | | |

REFERENTES TEÓRICOS

Saini y Mandall definen la criptografía como el estudio de la verificación y escondite de la información [1].

El algoritmo MD5 es definido por Shirey como una función criptográfica que produce un resultado *hash* de 128 bits, y diseñada por Ron Rivest para ser una versión mejorada del algoritmo MD4 [2].

El algoritmo SHA-1 es definido por Karkade y Joshi cono un algoritmo similar a MD5, pero produce un *digest* de 160 bits [3].

Gracias a la criptografía, la probabilidad de protección de información sensible o importante es mayor, haciendo más difícil su manipulación por parte de usuarios no autorizados.

En la criptografía existen retos para proteger la información como seleccionar los algoritmos correctos de cifrado y descifrado. También existen oportunidades como proyectar la protección de los datos de los usuarios por medio de una aplicación móvil para Android.

RESULTADOS PARCIALES

Con el desarrollo del presente proyecto de investigación se espera obtener los siguientes resultados:

Estado del arte sobre técnicas de cifrado/descifrado de texto.

Estudio de mercados realizado para la aplicación móvil desarrollada.

Una Aplicación móvil para Android que cifre y descifre archivos de texto (ver y Figura 11Figura 12).

Para el desarrollo del estudio de mercados, se tuvieron en cuenta los siguientes diseños: (i) Modelo PORTER, que señala los factores que pueden influir a la hora de ofrecer aplicaciones móviles de cifrado y descifrado; (ii) Modelo CANVAS, que destaca los factores utilizados al momento de ofrecer Encriptapp; encuesta que señale el interés de la población seleccionada por las aplicaciones móviles de cifrado y descifrado.

La aplicación móvil está desarrollándose en Android Studio, implementando los algoritmos de cifrado MD5 y SHA-1, y la subida de los archivos cifrados a plataformas de alojamiento de archivos como Google Drive y Dropbox. Posteriormente, se subirá a Google Play.


Figura 11. Captura de pantalla de inicio de EncriptApp. Elaboración propia.

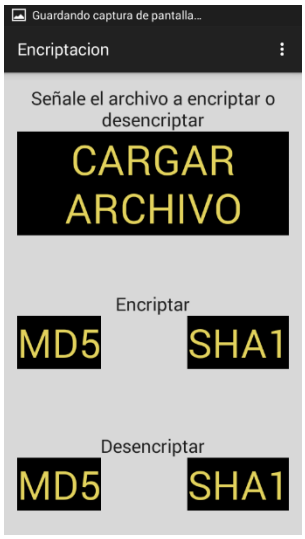


Figura 12. Captura de pantalla de opciones de cifrado y descifrado. Elaboración propia.

IDENTIFICACIÓN DEL PROYECTO

| | |
|---|---|
| Nombre del Semillero | Semillero de Investigación en Seguridad Informática (SI). |
| Tutor del Proyecto | Diana Teresa Parra Sánchez.<br>René Alejandro Lobo Quintero. |
| Grupo de Investigación | Grupo de Investigación en Tecnologías de Información (GTI). |
| Línea de Investigación | Línea de Investigación en Telemática.<br>Tecnología de la información. |
| Fecha de Presentación | Abril 21 de 2016 |

REFERENCIAS

[1] N. Saini y S. Mandal, «Review paper on cryptography. International Journal of Research [IJR],» p. 45, Mayo 2015.

[2] R. Shirey, «Request For Comments [RFC]: 4949 – Internet Security Glossary.,» Agosto 2007. [En línea]. Available: https://tools.ietf.org/html/rfc4949#page-188.

[3] R. A. Karkade y M. R. Joshi, «Network security with cryptography,» *International Journal of Computer Science and Mobile Computing*, p. 204, 2015.