CrApp: aplicación móvil Android para encriptar y desencriptar archivos e información

DOI: 10.46932/sfjdv2n1-082

Received in: November 1st, 2020
Accepted in: December 30th, 2020

Miguel Fernando Martinez
Programa de Ingeniería de Sistemas
Universidad Autónoma de Bucaramanga
E-mail: mmartinez887@unab.edu.co

RESUMEN
La información que almacenamos en los smartphones y tablets es más importante de lo que nos podemos imaginar y si cae en malas manos, puede afectar a nuestra vida social, laboral y familiar. Por eso, es muy importante proteger correctamente nuestros dispositivos móviles para que, en caso de que lo perdamos, nos lo roben o lo tomen "prestado" temporalmente sin nuestro consentimiento, impidamos que puedan acceder a dicha información evitando así problemas de privacidad y seguridad.

Palabras Clave: Criptografía, AES 256 bytes.

1 INTRODUCCIÓN

La criptografía se ha definido como una serie de técnicas de codificación o cifrado con el fin de modificar representación lingüísticas de ciertos lenguajes o información con el fin de hacerlos ilegibles para mantener la confidencialidad y evitar su lectura por parte de terceros.

Este material es presentado al *VI Encuentro Institucional de Semilleros de Investigación UNAB*, una actividad de carácter formativo. La Universidad Autónoma de Bucaramanga se reserva los derechos de divulgación con fines académicos, respetando en todo caso los derechos morales de los autores y bajo discrecionalidad del grupo de investigación que respalda cada trabajo para definir los derechos de autor. Conserve esta información

En este documento, es presentada una investigación en curso para el desarrollo de una aplicación móvil para Android que cifra y descifra documentos, fotos, videos y todo tipo de información, utilizando el algoritmo de cifrado AES de 256 bytes. En la Sección 2, se presentan los objetivos del proyecto. La Sección 3

proyecto. La Sección 4 corresponde al cronograma para el desarrollo de la investigación. En la Sección 5 se presenta el estado del arte con la criptografía y seguridad.. La Sección 6 corresponde a los resultados esperados del proyecto. En la Sección 7 se presentan los resultados parciales .La sección 8 presenta las referencias bibliográficas y electrónicas consultadas.

2 OBJETIVOS

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

2.1 OBJETIVO GENERAL

Implementar una aplicación móvil para encriptar y desencriptar documentos, fotos, videos y todo tipo de archivos.

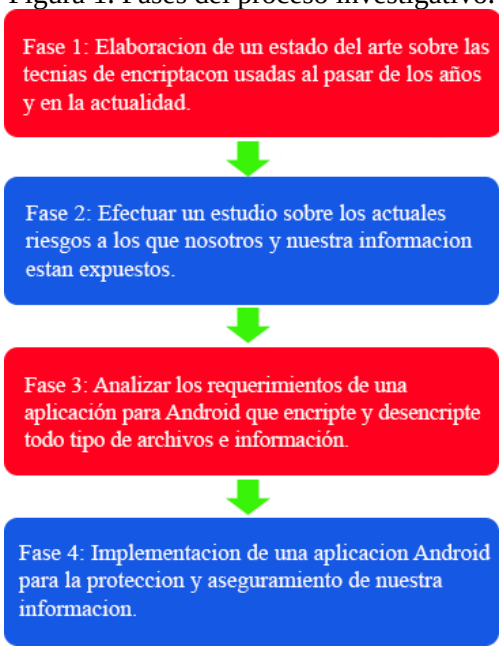
2.2 OBJETIVOS ESPECÍFICOS

- Elaborar un estado del arte sobre técnicas de cifrado/descifrado.
- Realizar un estudio de riesgos actuales a lo que podemos ser víctimas por medio de nuestros dispositivos móviles.
- Analizar los requerimientos de una aplicación para Android que encripte y desencripte todo tipo de archivos e información.
- Implementar la aplicación móvil Android para encriptar/desencriptar información.

3 METODOLOGÍA DE LA INVESTIGACIÓN

Para el desarrollo del proyecto de investigación se ha utilizado una metodología de desarrollo en cascada con cuatro fases, que se relacionan directamente con los objetivos específicos de la propuesta de investigación (Ver Figura 1), las cuales se describen a continuación:

Figura 1. 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) Estudio sobre riesgos de nuestrainformación; Fase 3: Se está realizando lo siguiente: (i) Desarrollode la aplicación móvil; (ii) Implementación de los algoritmos de encriptación Fase 4: Se está realizando lo siguiente: (i) Publicación de la aplicación móvil.

4 CRONOGRAMA PORDESARROLLAR

El cronograma de actividades para el desarrollo del proyecto, es presentado en la Tabla 1.

Tabla 1. Cronograma de actividades

ACTIVIDAD		DURACIÓN (Meses)			
		1	2	3	4
1	Búsqueda y revisión de la literatura.	x			
2	Lectura, análisis y clasificación.	x			
3	Diseño de técnicas y algoritmos.		x		
4	Pruebas y mejoras de la app y susalgoritmos.			x	
5	Implementación de la aplicación paraasegurar nuestros datos.				x

5 ESTADO DEL ARTE

Algoritmo	Descripción/Características
Clave simétrica	utilizan las mismas claves criptográficastanto para el cifrado del texto plano como para el descifrado del texto cifrado. Las claves pueden ser idénticas o puede haber una simple transformación para ir entre las dos claves.
RSA	Los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto, conocido, de dos números primos grandes elegidos al azar y mantenidos en secreto. Actualmente estos primos son del ordende 10^200.
AES	El algoritmo se basa en varias sustituciones, permutaciones y transformaciones lineales, cada unaejecutada en bloques de datos de 16 bytes - por lo tanto el término blockcipher. Esas operaciones se repiten varias veces, llamadas "rondas".
Cifrado Cesar	Es un tipo de cifrado por sustitución enel que una letra en el texto original es reemplazada por otra letra que se encuentra un número fijo de posiciones más adelante en el alfabeto

6 REFERENTES TEÓRICOS

La criptografía es una técnica, o más bien un conjunto de técnicas, que originalmente tratan sobre la protección o el ocultamiento de la información frente a observadores no autorizados.[1].

RSA es uno de los sistemas de cifrado asimétricos más exitosos de la actualidad. Originalmente descubierto en 1973 por la agencia de inteligencia británica GCHQ, recibió la clasificación "top secret". Debemos agradecer a los criptologos Rivest, Shamir y Adleman por su redescubrimiento civil en 1977. Ellos tropezaron con él durante un intento de resolver otro problema criptográfico.
[2].

Dentro de los sistemas simétricos se encuentra el algoritmo Advanced Encryption Standard (AES), que es uno de los algoritmos más utilizados en la actualidad, considerado por el gobierno de los Estados Unidos como un algoritmo seguro para protección nacional de información y del cual, aún no se conocen ataques eficientes que lo puedan vulnerar.[3].

Una de las amenazas más relevantes es el software malicioso desarrollado de forma específica para esta plataforma. La cantidad, complejidad y diversidad del malware que se genera para Android ha crecido de manera considerable en los últimos años.

Nuevas familias de códigos maliciosos y sus variantes se desarrollan con distintos objetivos. Entre estos se encuentran troyanos SMS que suscriben al usuario a servicios de mensajería premium sin su consentimiento, botnets que buscan convertir en zombi al dispositivo móvil al tiempo que roban información, adware para el envío de publicidad no deseada o ransomware que cifra la información y solicita un pago como rescate para que el usuario pueda recuperar sus datos.

De acuerdo con el documento "Tendencias 2014: el desafío de la privacidad en Internet" de ESET Latinoamérica, en donde se estudiaron los registros de detección de software malicioso, en el año 2010 se identificaron solo tres familias de malware para Android, para 2011 fueron 51, a finales de 2012 se detectaron 63, mientras que en 2013 ya se habían identificado 79 familias.[4]

7 RESULTADOS PARCIALES

Siguiendo los pasos anteriormente mencionados se espera llegar a los siguientes resultados:

- Estado del arte, algoritmos de encriptación actualmente usados.
- Estudio sobre amenazas a nuestra información almacenada en dispositivos móviles.
- Una Aplicación móvil para Android que encripte y desencripte todo tipo de archivos(ver Figura 2 y Figura 3).

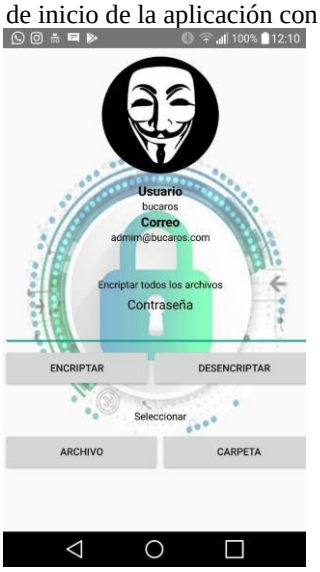
La aplicación móvil está desarrollándose en Android Studio, implementando el algoritmo de

cifrado de archivos AES de 2156 bytes con una llave de 32 bytes de largo, y la elección del tipo de archivo a encriptar así como un cliente web para poder encriptar el móvil desde cualquier lugar.

Figura 2. Captura de pantalla del login de CrApp.

Elaboración propia.

Figura 3. Captura de pantalla de inicio de la aplicación con lasopciones de criptografía.



Elaboración propia.

8 IDENTIFICACIÓN DEL PROYECTO

Nombre del Semillero	Semillero de Desarrollo de Aplicaciones Móviles.
Tutor del Proyecto	René Alejandro Lobo Quintero.
Grupo de Investigación	Grupo PRISMA.
Línea de Investigación	Línea de Investigación en tecnología y sociedad
Fecha de Presentación	Octubre 06 de 2017

REFERENCIAS

[1] Escuela Técnica Superior de Ingenieros Informáticos «Introducción a la criptografía». Octubre 2017. Available: http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_ discreta/web/aritmetica_modular/criptografia.html

[2] Boxcryptor.com «Cifrado AES y RSA» Octubre 2017. [En línea]. Available: https://www.boxcryptor.com/es/encryption/

[3] Lic. Adrián Pousa «Algoritmo de cifrado AES, aceleración detiempo de cómputo sobre arquitecturas multicore» Octubre 2017. Available:

[4] http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes_y_Seguridad/Trabajos_Finales/Pousa_Adrian.pdf

[5] Revista seguridad UNAM «Riesgos de seguridad en Android» Octubre 2017. Available: https://revista.seguridad.unam.mx/print/221