APLIKASI PENGAMANAN DATA DENGAN METODE *INTERNATIONAL DATA ENCRYPTION ALGORITHM* BERBASIS ANDROID

Leonardo[1)], Yunus Fadilah Soleman[2)]

Program Studi Teknik Informatika
Institut Bisnis dan Informatika Kwik Kian Gie
Jl. Yos Sudarso Kav.87 Sunter Jakarta Utara 14350
[1] 55150166@student.kwikkiangie.ac.id, [2]yunus.fadilah@kwikkiangie.ac.id

ABSTRAK

Perkembangan teknologi pada era globalisasi ini membuat data semakin mudah untuk didapatkan. Dengan kemudahan dalam *sharing* data tersebut, maka data yang dimiliki menjadi rentan dan mudah didapatkan maupun digunakan oleh pihak yang tidak bertanggung jawab. Salah satu cara untuk mengamankan data yaitu dengan cara enkripsi data tersebut menggunakan kata sandi yang baik dan algoritma enkripsi data yang mendukung dengan menggunakan kata sandi dalam pengamananya. Banyak algoritma yang mendukung enkripsi dengan menggunakan kata sandi salah satunya dengan menggunakan metode *International Data Encryption Algorithm*. Penelitian ini akan dilakukan dengan metode observasi terhadap data dengan pendekatan kualitatif. Analisis data yang dilakukan dengan cara deskriptif, memaparkan hasil dari *experiment* dalam pengukuran data dalam bentuk tabel yang akan menginterpretasikan hasil dari observasi tersebut dengan menggunakan *Hash MD5* sebagai alat untuk melakukan verifikasi integritas data yang di enkripsi maupun didekripsi. Aplikasi enkripsi yang dihasilkan ini ditujukan untuk dapat memberikan solusi mengenai keamanan data yang menjadi pemasalahan yang ada. Aplikasi ini kiranya dapat membantu dalam mengamankan files yang penting pada Android dengan menggunakan kata sandi sebagai alat pengamananya.

Kata Kunci: Keamanan Data, *International Data Encryption Algorithm*, Java, Android, *Hash MD5*

ABSTRACT

The development of technology in this era of globalization make data easier to obtain. With the ease of sharing the data, the data that is owned becomes vulnerable and easily obtained or used by irresponsible parties. One way to secure data is by encrypting the data using a good password and supporting data encryption algorithms using passwords in the security. Many algorithms that support encryption by using a password, one of them is International Data Encryption Algorithm method. In addition, the IDEA algorithm is implemented into the Java framework for Android applications. This research was conducted by observing the data with a qualitative approach. Data analysis was carried out by descriptive method, describing the results of the experiment in measuring data in the form of tables that would interpret the results of these observations using MD5 Hash as a tool to verify the integrity of encrypted and decrypted data. The encryption application that is produced is intended to be able to provide solutions regarding the data security that is the problem that exists. This application can help in securing important files on Android by using a password as a security device.

***Keywords**: Data Security, International Data Encryption Algorithm, Java, Android, MD5 Hash*

PENDAHULUAN

Perkembangan Teknologi Informasi dan Komunikasi dalam kehidupan kita sehari-hari sekarang ini sangat pesat, baik mencari informasi maupun menerima informasi sehingga dapat membantu manusia memudahkan permasalahan yang sedang dihadapinya. Pada era Teknologi Informasi dan Komunikasi sekarang ini, perpindahan data merupakan hal yang sangat penting.

Namun perlu diingat, kemanan data dan informasi merupakan hal yang penting di era yang begitu pesatnya perkembangan teknologi informasi saat ini. Umumnya, setiap orang memliki data maupun dokumen penting yang hanya bisa diakses oleh orang orang tertentu

saja. Hanya yang menjadi permasalahanya adalah data tersebut belum diberikan kata sandi pada data. Banyaknya format file yang harus diamankan. Serta adanya penyadap yang bisa membuka atau membongkar data yang seharusnya hanya bisa di akses oleh orang tertentu, infrastruktur pengamanan data kurang baik, serta data yang dimiliki tidak dilindungi oleh kata sandi yang baik. Oleh karena itu, diperlukan metode untuk mengamankannya, salah satunya dengan menggunakan metode kriptografi.

Saat ini, kriptografi menjadi dasar bagi keamanan komputer dan jaringan karena yang menjadi pokok dari fungsi komputer dan jaringan adalah data ataupun informasi. Komputer dan jaringannya menjadi sarana bagi distribusi data dan informasi, maka data dan informasi tersebut harus diamankan agar hanya orang-orang yang berhak mengaksesnya yang dapat mengetahui maupun menggunakan data tersebut. Data-data tersebut diamankan dengan sedemikian rupa oleh pengirim sehingga orang lain tidak dapat mengenali data tersebut. Hal ini lebih dikenal dengan nama proses enkripsi.

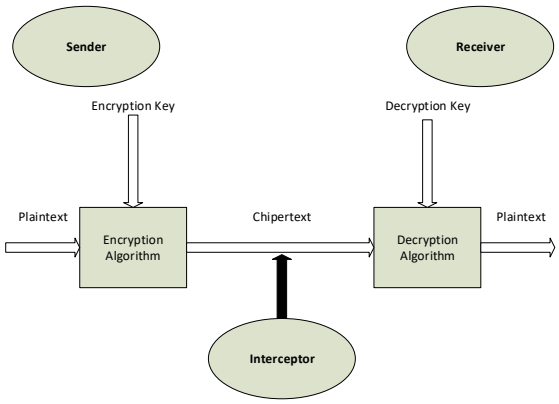
Dengan latar belakang yang demikian, maka penulis melakukan penelitian akhir kuliah dengan mengangkat topik "**Aplikasi Pengamanan Data Dengan Metode *International Data Encryption Algorithm* Berbasis Android"**

KRIPTOGRAFI

Kriptografi merupakan suatu ilmu yang menjelaskan bagaimana cara seseorang untuk mengirimkan sebuah pesan kepada seseorang yang dituju tanpa di interupsi dan hanya orang tersebut lah yang mengetahui *password* yang dikenakan pada pesan tersebut. (Chuck, 2016). Banyak dari kita yang sering mengartikan kriptografi merupakan hal yang sama dengan kriptologi. Kriptologi lebih komperhensif (formal) dan mencakup dari kriptografi dan kriptanalisis.

Ada beberapa istilah pada kriptografi seperti *Chiper, Chiper Text, Cryptanalysis, Dechiper, Enchiper,* dan *key. Chiper* merupakan sebuah algoritma yang digunakan untuk merubah sebuah teks biasa menjadi teks yang sudah dimodifikasi (*cipher text*). *Chiper Text*, merupakan hasil dari *cipher* yang merupakan teks yang sudah dimodifikasi. *Cryptanalysis* merupakan studi tentang prinsip dan metode yang mengartikan *cipher text* tanpa mengetahui kunci algoritma. *DeChiper* (*Decrypt*) merupakan cara yang digunakan untuk merubah teks yang telah dimodifikasi (*cipher text*) menjadi teks aslinya (p*lain text*). *Enchiper* (*Encrypt*) merupakan cara yang digunakan untuk merubah teks biasa (*plain text*) menjadi teks termodifikasi (*cipher text*). *Key*, merupakan kata kunci yang digunakan oleh algoritma Kriptografi dalam melakukan *encrypt* maupun *decrypt* data.

Berikut ini merupakan gambar yang menjelaskan kerja kriptografi secara umum:

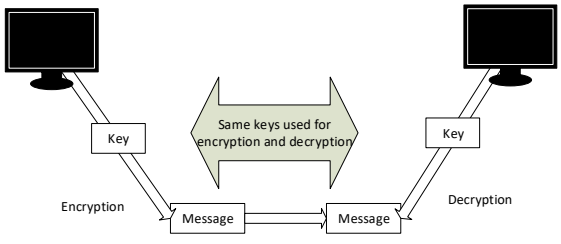


GAMBAR 1
MODEL *STANDARD* DARI *CRYPTOSYSTEM*

Terdapat dua teknik penguncian pada kriptografi yaitu:

Symmetric Keys (Kunci Simetris)

Kunci simetris merupakan kunci yang digunakan pada algoritma enkripsi dan dekripsi dimana kunci yang digunakan untuk enkripsi sama dengan kunci yang digunakan untuk dekripsi. Untuk lebih jelas dapat dilihat pada Gambar 2.



GAMBAR 1
DIAGRAM KUNCI SIMETRIS

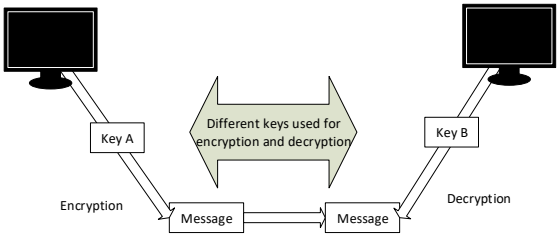
Kemanan dari model enkripsi ini tergantung dari pengguna untuk mengamankan *secret key*. Jika ada orang yang tidak

bertanggung jawab mendapatkan kunci, dia dapat membaca seluruh pesan yang sudah di enkripsi dengan cara mendekripsi pesan tersebut dengan kunci yang telah didapatkan.

Algoritma enkripsi yang menggunakan Kunci Simetris antara lain: *Data Encryption Standard* (DES) adalah sebuah algoritma enkripsi sandi blok kunci simetrik dengan ukuran blok 64-bit dan ukuran kunci 56-bit. DES untuk saat ini sudah dianggap tidak aman lagi. Penyebab utamanya adalah ukuran kuncinya yang sangat pendek (56-bit), *Advanced Encryption Standard* (AES) adalah lanjutan dari algoritma enkripsi standar DES (Data Encryption Standard) yang masa berlakunya dianggap telah usai karena faktor keamanan, *Blowfish* merupakan algoritma kunci simetrik cipher blok yang dirancang pada tahun 1993 oleh Bruce Schneier untuk menggantikan DES., *Twofish* merupakan algoritma kriptografi yang beroperasi dalam mode blok cipher berukuran 128 bit dengan ukuran kunci sebesar 256 bit, ukuran kunci yang besar ditujukan untuk meniadakan kemungkinan kunci lemah (weak-key)., *International Data Encryption Algorithm* (IDEA) algoritma enkripsi blok kunci yang aman dan rahasia yang dikembangkan oleh James Massey dan Xuejia Lai. Algoritma ini berkembang pada 1992 dari algoritma semula yang disebut dengan Proposed Encryption Standard and The Inproved Proposed Encryption Standard, *Rivest Cipher* (RC4) adalah algoritma cipher blok yang terkenal karena sederhana. Dirancang oleh Ronald Rivest pada tahun 1994.

Asymmetric Keys (Kunci tidak simetris)

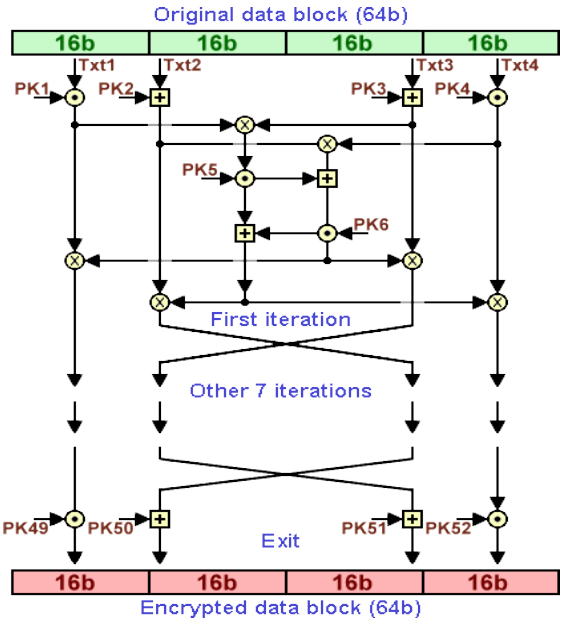
Pada *asymmetric keys* terdapat 2 kunci, yaitu kunci publik (Key A) yang biasa digunakan untuk enkripsi data dan kunci privat (Key B) untuk dekripsi data. Dapat dilihat pada Gambar 2.



GAMBAR 2
DIAGRAM KUNCI ASIMETRIS
Sumber: (Dunkerley, 2017)

Meskipun kunci secara matematis mirip, mereka tidak dapat diturunkan satu sama lain. Dua kunci dibuat untuk enkripsi dan tujuan dekripsi: satu kunci adalah kunci publik, yang diketahui semua pengguna, sedangkan kunci pribadi tetap rahasia dan diberikan kepada pengguna untuk menjaga privasi. Untuk menggunakan sistem ini, pengirim akan mengenkripsi sebuah pesan atau file dengan kunci publik penerima yang dimaksud. Untuk mendekripsi pesan ini, penerima akan menggunakan sebuah kunci pribadi yang hanya dia miliki. Tidak ada orang lain yang dapat mendekripsi pesan tanpa kunci privat ini. Publik kunci dapat dilewatkan secara langsung di antara pengguna atau ditemukan di direktori kunci publik. Kunci ketiga digunakan untuk mengenkripsi kunci pribadi, yang kemudian disimpan di lokasi yang aman. Kunci ketiga ini dapat digunakan untuk membuka kunci salinan terenkripsi kunci pribadi dalam kasus kehilangan atau pencurian kunci asli.

International Data Encryption Algorithm (IDEA)



GAMBAR 4
DIAGRAM KRIPTOGRAFI IDEA

International Data Encryption Algorithm (IDEA) merupakan algoritma *cipher block symmetric key* yang dirancang oleh Xuejia Lai dan James L. Massey dari ETH-Zürich dan pertama kali dideskripsikan pada tahun 1991. Ini adalah revisi minor dari *cipher*

sebelumnya, PES (*Proposed Encryption Standard*). IDEA pada awalnya disebut IPES (*Improved PES*). IDEA digunakan sebagai *cipher* simetris dalam versi awal dari kriptosistem privasi cukup baik. (Mandal, Kar, Das, & Panigrahi , 2015)

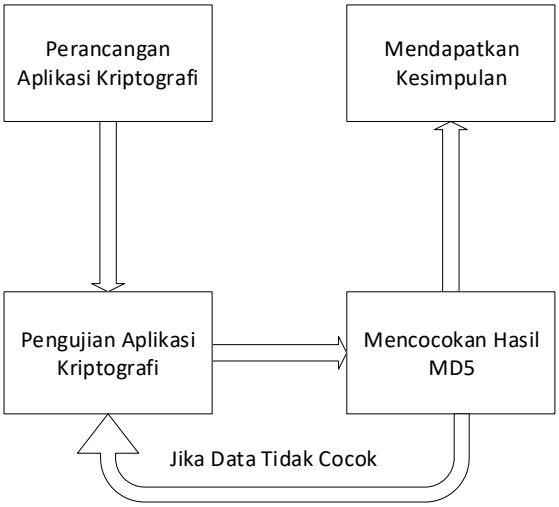
IDEA beroperasi pada blok 64-*bit* menggunakan kunci 128-*bit* dan terdiri dari seri delapan transformasi identik (putaran, lihat ilustrasi) dan output transformasi (setengah putaran). Proses untuk enkripsi dan dekripsi serupa. IDEA memperoleh banyak keamanannya dengan operasi *interleaving* dari grup yang berbeda, penambahan dan penggandaan modular, dan *bitwise eXclusive OR* (XOR) yang secara aljabar "tidak kompatibel" dalam arti tertentu. Lebih detail, operator ini, yang semuanya berhubungan dengan kuantitas 16-*bit*. (Schneier, 2015)

METODE PENELITIAN

Metodologi penelitian untuk menemukan solusi dari permasalahan keamanan data yaitu dengan metode eksperimen pada algoritma *International Data Encryption Algorithm.*

Metode Eksperimen

Metode eksperimen merupakan cara menguji suatu percobaan tentang suatu hal yang dihadapi. Disini akan dilakukan eksperimen berupa meakukan enkripsi maupun dekripsi sebanyak tiga kali terhadap data dengan menggunakan algoritma *International Data Encryption Algorithm* berbasis aplikasi android yang didesain dan dibuat.



Gambar 5 Tahapan Eksperimen yang Dilakukan

HASIL PENELITIAN DAN PEMBAHASAN

Aplikasi "Encrypt Your Files" Berbasis Android

Hasil dari rancangan software adalah sebuah aplikasi berbasis android yang diberi nama "Encrypt Your Files" dengan struktur menu sebagai berikut:

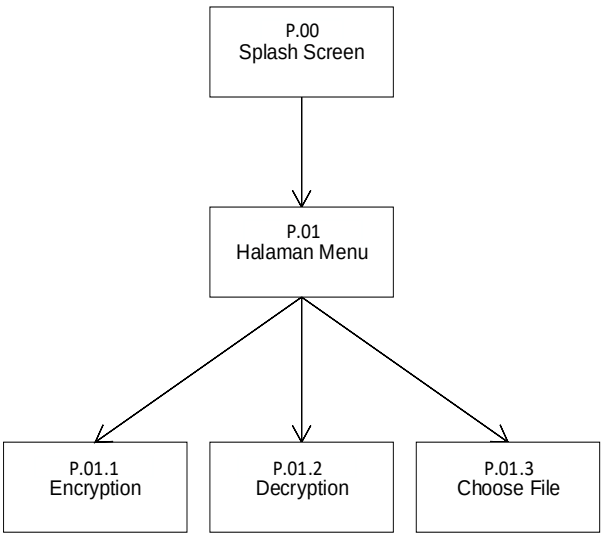
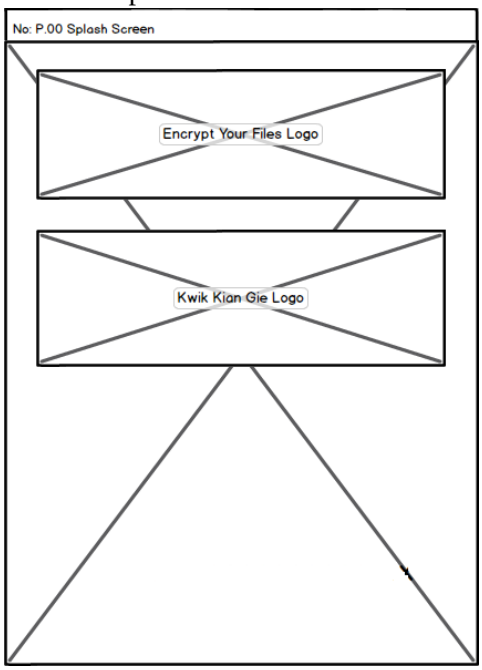


Diagram 1 Rancangan Aplikasi

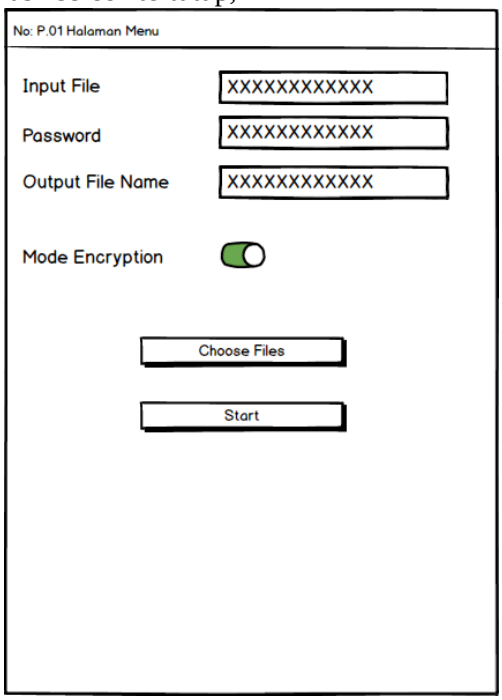
Keterangan:

P.00 merupakan halaman Splash Screen aplikasi saat aplikasi dibuka



Gambar P.00 Splash Screen

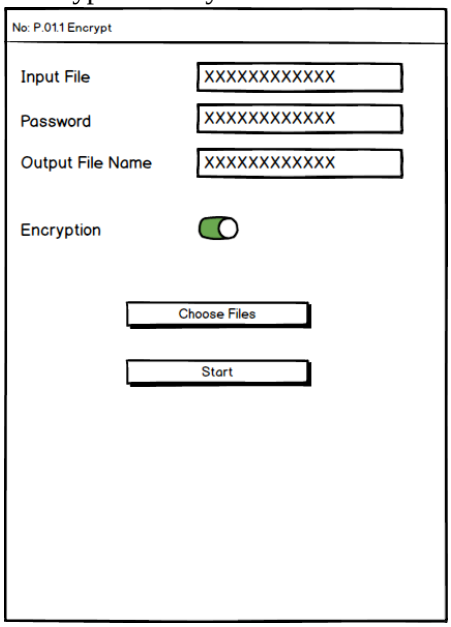
P.01 merupakan lanjutan setelah halaman splash screen tertutup,



Gambar P.01 Halaman Menu

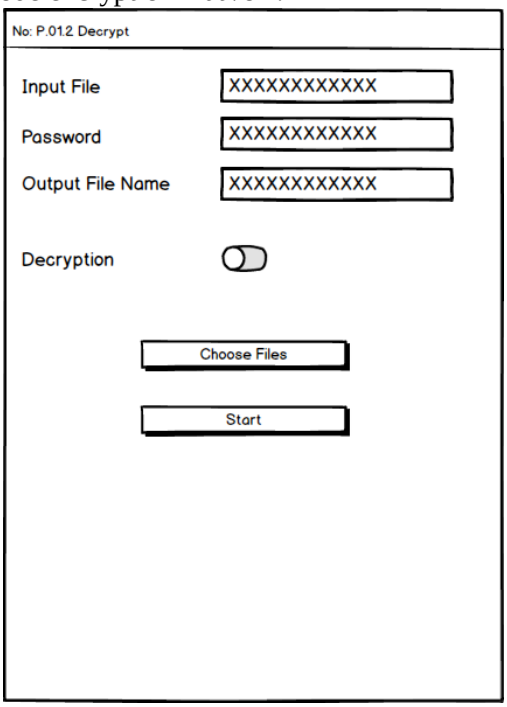
halaman menu menampilkan form input file, password, output file, mode encryption/decryption, button choose file, dan button start untuk melakukan kegiatan

P.01.1 merupakan halaman menu yang merupakan state Encryption. Ditandai dengan mode encryption menyala/on.



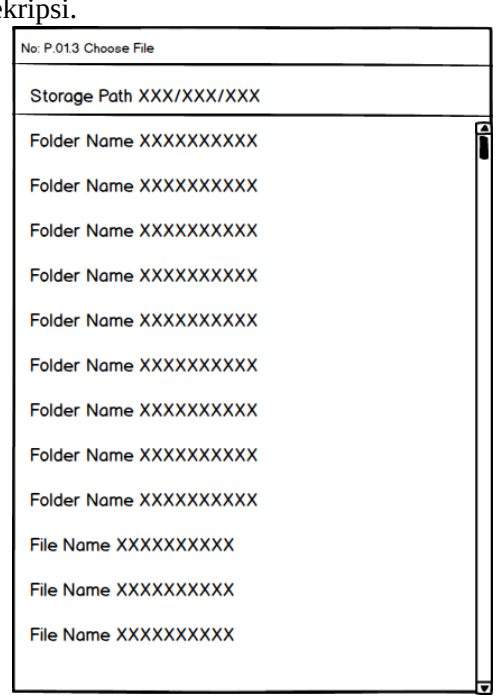
Gambar P.01.2

P.01.2 merupakan halaman menu yang merupakan state Decryption. Ditandai dengan mode encryption mati/off.



Gambar P.01.2 Decrypt

P.01.3 merupakan halaman choose file, untuk mengambil file yang akan di enkripsi atau dekripsi.



Gambar P.01.3 Choose File

Hasil Dari Metode Eksperimen Aplikasi "Encrypt Your Files" Dengan Menggunakan Algoritma IDEA

Tabel 1 Hasil Eksperimen Terhadap Aplikasi Algoritma *International Data Encryption Algorithm* Berbasis Android.

Format File	Encrypt	Decrpyt	Different
Ms. Word	✓	✓	×
Ms. Excel	✓	✓	×
PDF	✓	✓	×
Txt	✓	✓	×
Ms. Power Point	✓	✓	×
Ms. Access	✓	✓	✓

Keterangan Tabel 1:
Encrypt : File yang dapat di enkripsi
Decrypt : File yang dapat di dekripsi
Different : Perbedaan hasil MD5
✓ : Ya
× : Tidak

APLIKASI YANG DAPAT MENGAMANKAN DATA

Dengan hasil yang didapat dari eksperimen. Aplikasi "Encrypt Your Files" dapat melakukan pengamanan format file *Microsofr Word*, *Microsoft Excel*, *Microsoft Access*, *Microsoft Power Point*, *Portable Document Format*, serta *Text File*. Dengan tingkat pengembalian data 100% serupa dengan data sebelum diamankan. Hanya format file *Microsoft Access* yang menampilkan hasil MD5 yang berbeda tetapi tidak mempengaruhi isi data tersebut. Aplikasi yang dibuat membutuhkan *operating system* android minimal versi 8.0.0 (oreo) keatas dikarenakan membutuhkan modul yang baru tersedia pada *operating system* oreo.

KESIMPULAN

Beberapa kesimpulan yang dapat diambil dari penelitian ini adalah Aplikasi Android "*Encrypt Your Files*" yang didesain oleh penulis dapat mengamankan berbagai tipe files seperti *Word*, Berkas Naskah, *Persentation*, *Excell*, dan *Portable Document Format* dengan menggunakan *password* (kata sandi) sebagai alat pengaman data.Hasil Enkripsi untuk format File *Access* (.accdb) dapat di dekripsi seperti semula tetapi menghasilkan MD5 yang berbeda. Aplikasi Android "*Encrypt Your Files*" didesain hanya untuk melakukan enkripsi dan dekripsi files yang diinginkan oleh pengguna dan hasil enkripsi tidak dapat dibuka. Maka dari itu penyadap tidak dapat mengetahui isi daripada data yang terdapat pada file tersebut. Aplikasi Android "*Encrypt Your Files"* membutuhkan *operating system* minimal versi android 8.0.0 (Android Oreo) untuk dapat menjalankan aplikasi ini.

REFERENSI

Cardle, P. (2017). *Android App Development in Android Studio - Java plus Android edition for beginners.* Independently published.

Chuck, E. (2016). *Modern Cryptography : Applied Mathematics for Encryption and Information Security.* McGraw-Hill Education.

Ciampa, M. (2015). *Fundamentals, CompTIA Security+ Guide to Network Security.* Boston: CENGAGE L.

Cosmina, I. (2018). *Java for Absolute Beginners: Learn to Program the Fundamentals the Java 9+ Way.* Edinburgh: Apress.

DiMarzio, J. F. (2017). *Beginning Android Programming with Android Studio.* Indianapolis: Wrox.

Dunkerley, D. (2017). *Mike Meyers' CompTIA Security+ Certification passport, (Exam SY0-501).* McGraw-Hill Education.

Google LLC. (2018, Agustus 7). *Mengenal Android Studio.* Retrieved from Android Developer: https://developer.android.com/studio/intro/?hl=id

Horton, J. (2015). *Android Programming for Beginners.* Birmingham: Packt Publishing.

Horton, J. (2015). *Learning Java by Building Android Games.* Birmingham: Packt Publishing.

Jackson, W. (2017). *Android Apps for Absolute Beginners: Covering Android 7.* Apress.

Madria, S., & Hara, T. (2016). *Big Data Analytics and Knowledge Discovery: 18th International Conference, DaWaK 2016, Porto, Portugal, September 6-8, 2016, Proceedings.* Rolla, MO: Springer International Publishing.

Mandal, D., Kar, R., Das, S., & Panigrahi , B. K. (2015). *Intelligent Computing and Applications: Proceedings of the International Conference on ICA, 22-24 December 2014.* India: Springer .

Martin, K. (2017). *Everyday Cryptography: Fundamental Principles and Applications (2nd Edition).* United Kingdom: Oxford University Press.

Object Management Group. (2017, December). *About The Unified Modeling Language Specification Version 2.5.1.* Retrieved from Object Management Group: https://www.omg.org/spec/UML/#documents

Osis, J., & Donins, U. (2017). *Topological UML Modeling. An Improved Approach for Domain Modeling and Software Development. A volume in Computer Science Reviews and Trends.* Cambridge: Elsevier.

Schneier, B. (2015). *Applied Cryptography: Protocols, Algorithms and Source Code in C.* Wiley.

Seidl, M., Scholz, M., Huemer, C., & Gerti, K. (2015). *UML @ Classroom: An Introduction to Object-Oriented Modeling.* Heidelberg: Springer International Publishing.

Stewart, J. M., Chapple, M., & Gibson, D. (2015). *Certified Information System Security Professional, 7th Edition.* Sybex.

Yener, M., & Dundar, O. (2016). *Expert Android Studio.* Indianapolis: Wrox.

Zu, Q., & Hu, B. (2016). *Human Centered Computing: Second International Conference, HCC 2016, Colombo, Sri Lanka, January 7-9, 2016, Revised Selected Papers.* Springer International Publishing.