PENERAPAN ALGORITMA SIMETRIS PADA APLIKASI KRIPTOGRAFI PESAN BERBASIS ANDROID

Tony Darmanto[1], Antonius[2], Edi Gunawan[3]
[1,2,3]Teknik Informatika, Fakultas Teknologi Informasi Universitas Widya Dharma, Pontianak
e-mail : [1]tony.darmanto@yahoo.com, [2]antoniusok@yahoo.com,[3]edig04@gmail.com

Abstract

Mobile device or known as smartphone have a role for human communication. Everyone can communicate even if they in long distance with using smartphone. But, the crime in digital communication keep happening. On of them is tapping. Tapping is a action to monitoring an information that sent by unauthorized people of that information. A way to solve tapping is do cryptography to informatin to be sent. Cryptography is generally devided into two things, that is encryption and decryption. Encryption is a process to convert a text into another format. Meanwhile, decryption is a process to convert back a information that has encrypt into original form. One of cryptography algorithm is symmetrical algorithm, which is an algorithm that uses the same key for the encryption and decryption process. Therefore, message cryptographic application are designed using symmetrical algorithm. The analytical technique used is Unified Modeling Language (UML) to modeling the system. In system designed, author using MySQL for database design dan using Android Studio as an Integrated Development Environment (IDE). From this entire research process, is expected can resolve tapping of the information that send by user.

Keyword: *application*, *cryptography*, *encryption*, *decryption*, *key*

Abstrak

Perangkat *mobile* atau yang dikenal dengan *smartphone* memiliki peran dalam komunikasi manusia. Setiap orang dapat melakukan komunikasi meskipun berada pada jarak yang jauh dengan menggunakan *smartphone*. Namun, kejahatan dalam dunia komunikasi *digital* tersebut terus terjadi. Salah satunya adalah penyadapan. Penyadapan merupakan kegiatan memantau informasi yang dikirim oleh orang yang tidak berhak atas informasi tersebut. Salah satu cara untuk mengatasi penyadapan adalah dengan melakukan kriptografi pada informasi yang akan dikirim. Kriptografi pada umumnya dibagi menjadi dua, yaitu enkripsi dan dekripsi. Proses enkripsi merupakan proses mengubah suatu teks ke dalam bentuk lain. Sedangkan dekripsi merupakan proses pengembalian pesan yang telah dienkripsi ke bentuk aslinya. Salah satu algoritma kriptografi adalah algoritma simetris, yaitu algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsinya. Oleh karena itu, dirancanglah aplikasi kriptografi pesan dengan menggunakan algoritma simetris. Teknik analisis yang digunakan adalah *Unified Modelling Language* (UML) untuk memodelkan sistem. Dalam melakukan perancangan, penulis menggunakan MySQL sebagai *database* dan menggunakan Android Studio sebagai *Integrated Development Environment* (IDE). Dari keseluruhan proses penelitian ini, diharapkan dengan adanya aplikasi kriptografi pesan ini, diharapkan dapat mengatasi penyadapan terhadap pesan yang akan dikirimkan oleh penggunanya.

Kata Kunci: aplikasi, kriptografi, enkripsi, dekripsi, kunci

1. PENDAHULUAN

Pengembangan terhadap teknologi terus dilakukan pada era modernisasi ini, baik dalam bentuk penemuan inovasi baru ataupun pembaharuan teknologi yang sudah ada. Salah satu pengembangan teknologi yang paling pesat adalah pengembangan teknologi perangkat *mobile*. Pada mulanya, perangkat *mobile* yang dikenal sebagai *handphone* hanya dapat digunakan untuk keperluan yang sangat terbatas, seperti untuk telepon dan pengiriman pesan singkat saja. Namun seiring perkembangannya, kini perangkat *mobile* tersebut sudah dikenal sebagai *smartphone*. Dikatakan *smartphone* atau telepon pintar, karena perangkat mobile tersebut dapat digunakan untuk keperluan yang lebih luas, seperti untuk *browsing*, sosial media dan *chatting*, mendengarkan musik hingga bermain *game*.

Salah satu pemanfaatan *smartphone* adalah sebagai media untuk melakukan *chatting.* Seperti diketahui, *chatting* adalah salah satu contoh komunikasi data secara digital yang sangat rawan terhadap kejahatan *digital,* seperti penyadapan. Penyadapan merupakan perbuatan untuk memantau informasi yang sedang dikomunikasikan secara rahasia oleh pihak ketiga atau pihak yang tidak memiliki wewenang atas informasi tersebut. Penyadapan

informasi secara digital dapat terjadi karena informasi dikirim melalui jaringan publik sehingga memungkinkan orang yang tidak berwenang dapat memperoleh atau mengakses informasi tersebut. Dampak dari penyadapan akan sangat luas, apalagi jika informasi yang disadap bersifat rahasia atau vital.

Untuk menangani kasus penyadapan, dapat dilakukan dengan beberapa cara. Salah satunya adalah dengan menggunakan kriptografi. Kriptografi merupakan ilmu menyandikan pesan ke dalam bentuk lain dengan menggunakan algoritma atau metode tertentu. Beberapa algoritma kriptografi biasanya menggunakan key atau kunci untuk menyandikan pesan ke bentuk lain dan mengembalikan pesan ke bentuk semula, sehingga key tersebut harus saling diketahui oleh pengirim dan penerima pesan. Jenis algoritma kriptografi tersebut dikenal sebagai algoritma simetris. Dengan melakukan kriptografi, meskipun informasi yang dikirim telah disadap, penyadap tidak akan mengetahui makna pesan tersebut karena tidak memiliki kunci kriptografi atas informasi tersebut. Beberapa contoh metode pada kriptografi dengan algoritma simetris yang biasa digunakan adalah *Scytale Cipher, Atbash Cipher, Caesar Cipher, Gronsfeld Cipher, Auto Key Vigenere Cipher, Running Key Vigenere Cipher, ROT13 Cipher* dan masih banyak lagi.

Berdasarkan uraikan permasalahan di atas, maka penulis tertarik untuk merancang suatu aplikasi kriptografi pesan berupa teks berbasis mobile, sehingga aplikasi ini dapat digunakan sebagai solusi untuk mengamankan pesan teks dalam komunikasi data digital. Perangkat mobile yang digunakan untuk membangun aplikasi kriptogrfi tersebut adalah berbasis Android. Penggunaan sistem operasi tersebut karena sistem operasi Android bersifat open source yang memudahkan para pengembang aplikasi untuk menciptakan, memodifikasi dan mengembangkan aplikasi atau fitur-fitur yang belum ada pada sistem operasi tersebut.

2. METODE PENELITIAN

2.1. Teknik Pengumpulan Data, Teknik Analisis Sistem, Teknik Perancangan Sistem

2.1.1. Teknik Pengumpulan Data

Adapun metode pengumpulan data yang digunakan adalah :

2.1.1.1. Studi Pustaka / *Study literature*

Studi Pustaka dilakukan untuk mencari dan mengumpulkan data yang dapat mendukung penulis dalam menyelesaikan skripsi ini. Data ini dapat berupa bahan-bahan pendukung seperti teori-teori, konsep-konsep yang berasal dari literatur-literatur .

2.1.2. Teknik Analisis Sistem

Teknik analisis sistem yang digunakan penulis dalam menganalisis dan merancang kriptografi pesan adalah teknik berorientasi objek dan menggunakan *Unified Modeling Language* (UML) sebagai *tool* untuk menvisualisasikan, dan mendokumentasikan aplikasi.

2.1.3. Teknik Perancangan Sistem

Dalam teknik perancangan aplikasi, penulis menggunakan *Android Studio* sebagai IDE (*Integrated Development Environment*), serta *database MySQL* untuk merancang sebuah aplikasi yang nantinya akan digunakan pada perangkat *mobile* bersistem operasi *Android*.

2.2. Landasan Teori

2.2.1. Analisis Sistem

Analisis sistem adalah istilah yang secara efektif mendeskripsikan fase-fase awal pengembangan sistem[1]. Analisis sistem adalah kegiatan untuk menguraikan sub-sub sistem dan melihat fungsi dari masing-masing sub sistem tersebut [2].

2.2.2. Perancangan Sistem

Perancangan sistem adalah proses menyusun atau mengembangkan sistem informasi yang baru[3]. Perancangan sistem akan membentuk sistem/ perangkat lunak dan menemukan bentuknya (termasuk arsitekturnya) yang mengatasi semua spesifikasi kebutuhan termasuk semua spesifikasi kebutuhan non-fungsional serta batasan-batasan lain yang dibuat daripadanya[4].

2.2.3. Kriptografi

Cikal bakal dari enkripsi dan deskripsi adalah berasal dari ilmu kriptografi. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematis yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data, serta autentifikasi data[5]. Kriptografi adalah sebuah teknik untuk memungkinkan transmisi informasi secara aman. Sederhananya, kriptografi mengubah informasi dari yang dapat dibaca secara jelas menjadi sebuah kode acak yang tidak masuk akal dan kemudian menyediakan sebuah perangkat untuk menguraikan pesan tersebut[6].

2.2.4. Android

Android adalah sistem operasi berbasis Linux yang dirancang untuk perangkat seluler layar sentuh seperti telepon pintar dan komputer tablet[7]. Android merupakan suatu sistem operasi yang berbasis Linux untuk telepon pintar (*smartphone*) ataupun pada komputer tablet. Android menyediakan *platform* terbuka bagi para pengembang dalam menciptakan aplikasi mereka sendiri untuk digunakan oleh bermacam piranti bergerak[8].

3. HASIL DAN PEMBAHASAN

3.1. Hasil Analisis

Kehidupan manusia sekarang ini tidak dapat lepas dari teknologi yang dapat membantu memudahkan segala aktivitas manusia. Salah satu teknologi tersebut adalah perangkat *mobile* atau yang dikenal sebagai *smartphone*. Hampir semua orang memerlukan smartphone untuk menunjang kehidupan, termasuk dalam hal komunikasi. Dengan menggunakan *smartphone*, setiap orang dapat melakukan komunikasi meskipun berada pada jarak yang jauh, bahkan hingga antar negara.

Namun, seiring perkembangan teknologi itulah, kejahatan dalam dunia digital terus bermunculan. Salah satunya adalah penyadapan. Penyadapan merupakan kegiatan memantau informasi yang sedang dikirimkan oleh orang yang tidak berhak atas informasi tersebut. Penyadapan dapat terjadi dikarenakan informasi dikirimkan melalui jaringan publik yang tidak aman karena setiap orang dapat melakukan kejahatan melalui jaringan publik tersebut. Untuk mengantisipasi penyadapan, dapat dilakukan kriptografi terhadap informasi yang akan dikirimkan sehingga meskipun terjadi penyadapan, penyadap tidak dapat mengetahui makna dari informasi tersebut karena ditelah diubah menjadi bentuk lain. Salah satu algoritma kriptografi yang umum digunakan adalah algoritma simetris, yang menggunakan kunci yang sama pada proses enkripsi dan dekripsinya. Enkripsi merupakan proses mengubah suatu pesan ke dalam bentuk lain, sedangkan dekripsi merupakan proses mengembalikan pesan yang telah dienkripsi ke bentuk aslinya. Oleh karena itu, dirancanglah aplikasi kriptografi pesan dengan menggunakan algoritma simetris yang diharapkan dapat membantu dalam pengamanan informasi pada saat melakukan komunikasi data.

3.2. Prosedur Pengoperasian Aplikasi

3.2.1. Prosedur Mendaftar User

Untuk melakukan pendaftaran, *user* dapat mengakses *menu* Daftar *User* yang terdapat pada *layout Login*. Setelah *layout* Daftar *User* ditampilkan, *user* diharuskan untuk menginputkan *username*, nama lengkap, *password* dan *retype* dari *password* yang diinputkan sebelumnya. Setelah penginputan data tersebut telah selesai dilakukan, *user* dapat mendaftarkan data tersebut dengan mengakses tombol Daftar. Jika *username* tersebut telah terdaftar, *user* diharuskan menginputkan *username* yang berbeda. Sedangkan jika *username* belum terdaftar, maka sistem akan mengecek kesesuaian *password* dan *retype password*. Jika *password* dan *retype password* sudah sesuai, maka data *user* tersebut akan tersimpan ke dalam *database*.

3.2.2. Prosedur Login

Untuk melakukan *login*, *user* harus meng-*input*-kan *username* dan *password* yang sudah pernah didaftarkan. Setelah *username* dan *password* telah terisi, *user* dapat melakukan *login* dengan mengakses tombol *Login* yang tersedia. Jika *username* dan *password* sesuai maka sistem akan menampilkan *layout Menu* Utama.

3.2.3. Prosedur Enkripsi

Untuk melakukan enkripsi, *user* dapat mengakses *menu Crypt Text* yang terdapat pada *layout Menu* Utama. Pada *layout Crypt Text*, *user* dapat memilih metode yang tersedia. *User* juga diharuskan untuk menginputkan teks yang akan dienkrip beserta kunci. Untuk melakukan enkripsi, *user* dapat mengakses tombol Enkripsi, kemudian hasil enkripsi akan ditampilkan pada *layout Crypt Result*. *User* dapat mengirimkan hasil enkripsi tersebut dengan mengakses tombol Kirim Hasil. Sedangkan jika *user* ingin menyalin hasil enkripsi tersebut, *user* dapat mengakses tombol Salin Hasil.

3.2.4. Prosedur Dekripsi

Untuk melakukan dekripsi, *user* dapat mengakses *menu Crypt Text* yang terdapat pada *layout Menu* Utama. Pada *layout Crypt Text*, *user* dapat memilih metode yang tersedia. *User* juga diharuskan untuk menginputkan teks yang akan didekripsikan beserta kunci. Untuk melakukan dekripsi, *user* dapat mengakses tombol Dekripsi, kemudian hasil dekripsi akan ditampilkan pada *layout Crypt Result*. Jika *user* ingin menyalin hasil enkripsi tersebut, *user* dapat mengakses tombol Salin Hasil.

3.2.5. Prosedur Tambah Teman

Untuk melakukan penambahan teman, *user* harus mengakses *menu* Daftar Pertemanan yang terdapat pada *layout Menu* Utama. Setelah itu, sistem akan menampilkan *layout* Daftar Pertemanan, kemudian *user* dapat mengakses tombol Tambah Teman dan sistem akan menampilkan *layout* Tambah Teman. Pada layout tersebut, user harus menginputkan *username* yang ingin ditambahkan sebagai teman. Jika *username* tersebut tidak terdaftar, maka *username* diharuskan untuk menginputkan kembali *username* lain.

3.2.6. Prosedur Ubah Password

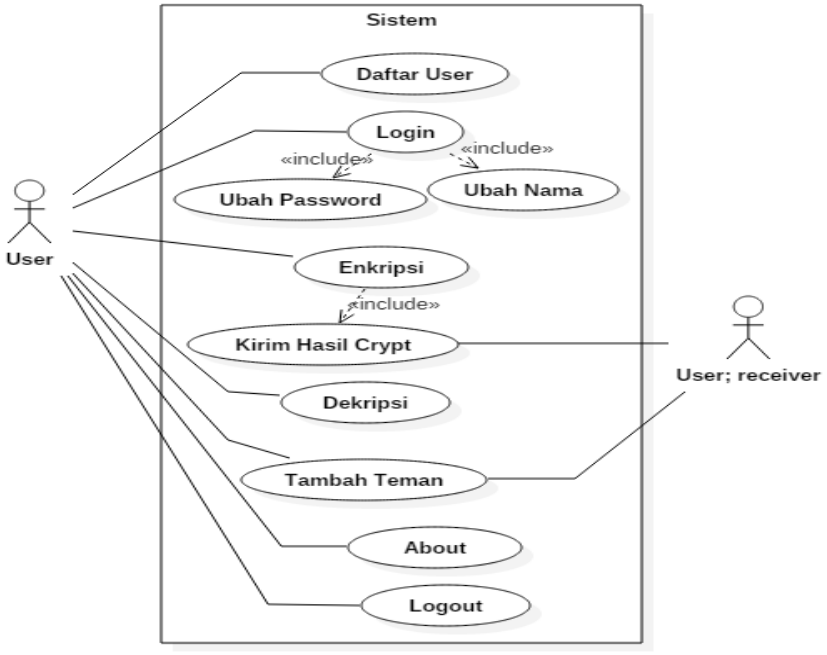
Untuk melakukan pengubahan *password*, *user* dapat mengakses *menu* Ubah *Password* yang terdapat pada *layout Menu* Utama dan sistem akan menampilkan *layout* Ubah *Password*. Pada *layout* Ubah *Password*, *user* diharuskan untuk menginputkan *password*, *password* baru dan *retype password* baru. Jika semua data tersebut telah diinputkan, *user* dapat menyimpan password tersebut dengan menekan tombol Simpan *Password* Baru. Jika *password* tidak sesuai, maka *user* diharuskan menginputkan *password* tersebut kembali. Sedangkan jika *password* baru dan *retype password* tidak cocok, user diminta untuk menginputkan ulang *retype password* tersebut. Setelah *password* telah sesuai serta *password* baru dan *retype password* baru sudah sama, maka *password* baru tersebut akan tersimpan ke dalam *database*.

3.2.7. Prosedur Ubah Nama

Untuk melakukan pengubahan nama, *user* dapat mengakses *menu* Ubah Nama yang terdapat pada *layout Menu* Utama. Setelah itu sistem akan menampilkan *layout* Ubah Nama dan *user* diharuskan untuk menginputkan nama barunya. Setelah itu *user* dapat menyimpan nama baru tersebut dengan menekan tombol Simpan Nama yang tersedia.

3.3. Gambaran Umum Rancangan Aplikasi Melalui Use Case Diagram

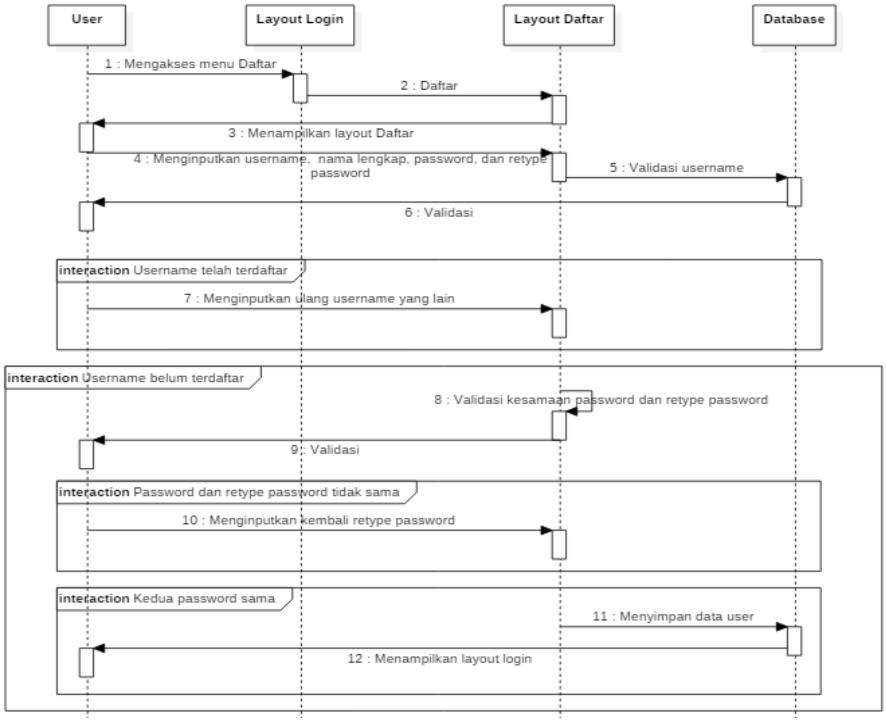
Diagram use case untuk perancangan aplikasi dapat dilihat pada gambar 1.



Gambar 1. Use Case Diagram

3.4. Diagram Urutan Perancangan Aplikasi

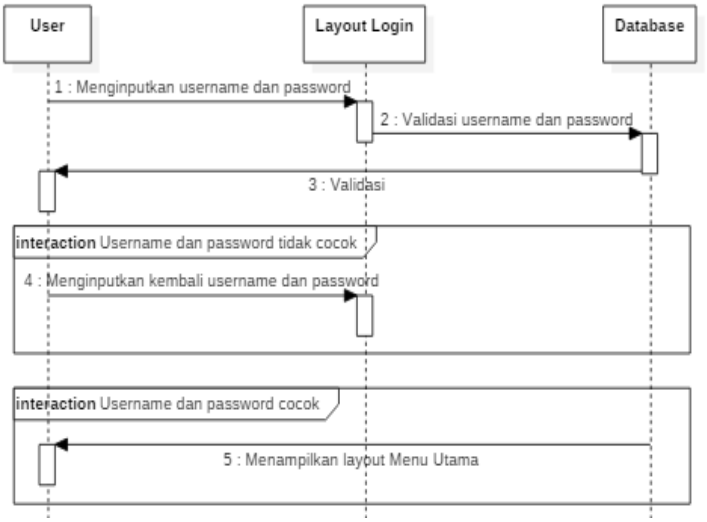
3.4.1. Diagram Urutan Daftar User



Gambar 2. Diagram Urutan Daftar User

Gambar 2 merupakan diagram urutan untuk melakukan daftar *user*. Untuk melakukan pendaftaran, *user* harus mengakses *menu* Daftar yang terdapat pada *layout Login*. Setelah itu sistem akan menampilkan *layout* Daftar. Pada *layout* tersebut, user harus melakukan penginputan *username*, nama lengkap, *password*, dan *retype password*. Untuk melakukan penyimpanan *user* tersebut, akan dilakukan validasi terhadap *username* dan *password*. Jika *username* belum terdaftar serta *password* dan *retype password* sama, maka data *user* tersebut dapat disimpan ke *database*.

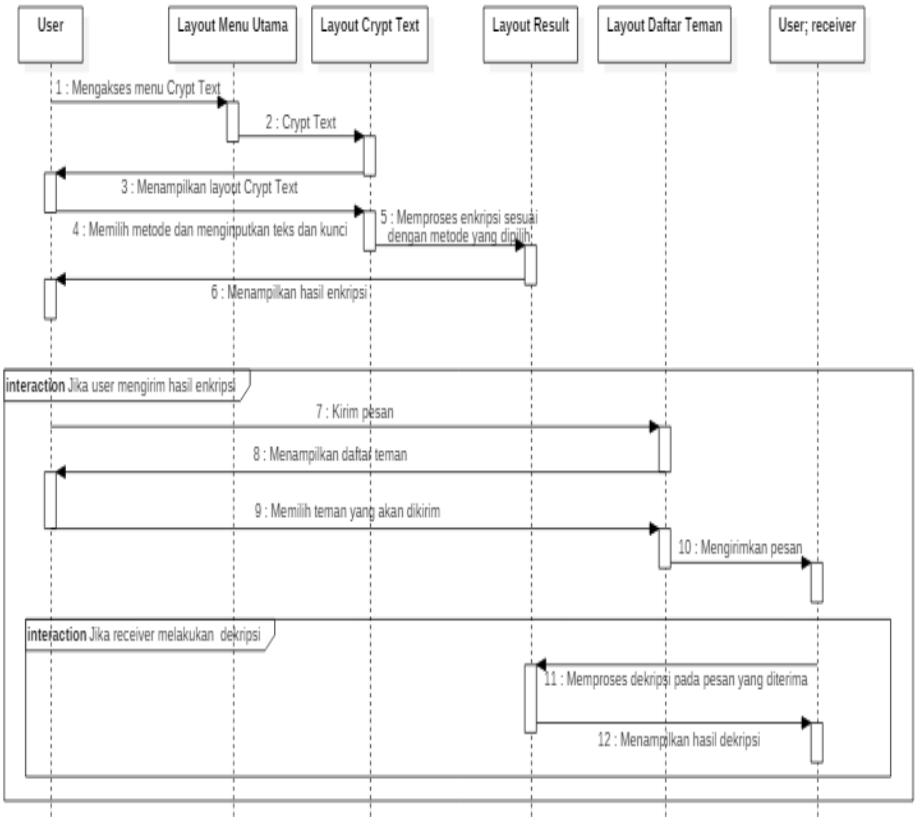
3.4.2. Diagram Urutan Login



Gambar 3. Diagram Urutan Login

Gambar 3 merupakan diagram urutan *login*. *User* dapat melakukan *login* dengan menginputkan *username* dan *password* pada *layout Login*. Setelah itu sistem akan melakukan validasi kesesuaian *username* dan *password* tersebut. Jika *username* dan *password* sesuai maka sistem akan menampilkan *layout Menu* Utama.

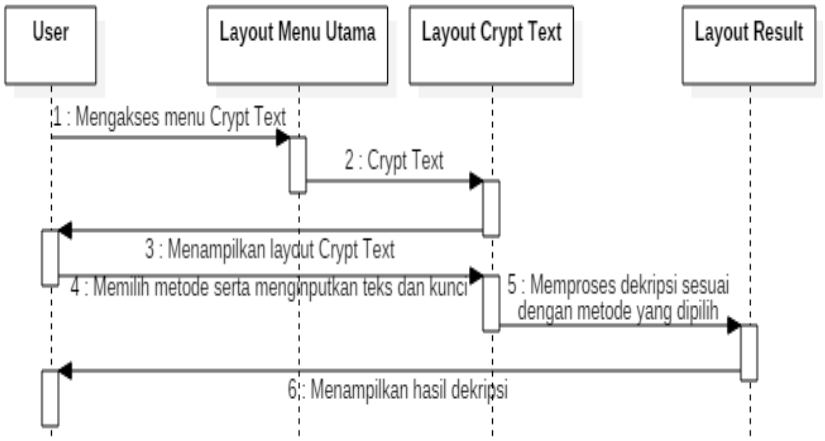
3.4.3. Diagram Urutan Enkripsi dan Kirim Pesan



Gambar 4. Diagram Urutan Enkripsi dan Kirim Pesan

Gambar 4 merupakan diagram urutan enkripsi dan kirim pesan. *User* dapat melakukan enkripsi dengan mengakses *menu Crypt Text* yang terdapat pada *layout Menu* Utama. Setelah *layout Crypt Text* ditampilkan, *user* diharuskan memilih metode serta menginputkan teks yang akan dienkrip dan kunci. Setelah itu sistem akan melakukan proses enkripsi dan hasil enkripsi akan ditampilkan pada *layout Crypt Result*. *User* dapat mengirimkan hasil enkripsi tersebut dengan mengakses tombol Kirim Hasil yang tersedia.

3.4.4. Diagram Urutan Dekripsi

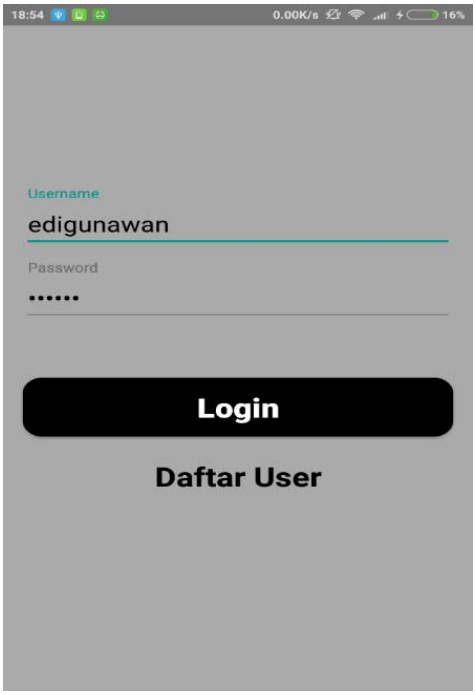


Gambar 5. Diagram Urutan Dekripsi

Gambar 5 merupakan diagram urutan untuk melakukan dekripsi. Sama halnya dengan proses enkripsi, untuk melakukan dekripsi, *user* dapat mengakses *menu Crypt Text* yang terdapat pada *layout Menu* Utama. Setelah *layout Crypt Text* dimunculkan, *user* diharuskan memilih metode yang diinginkan serta menginputkan teks yang akan didekripsikan serta menginputkan kunci untuk dekripsi. Setelah itu sistem akan melakukan proses dekripsi dan hasil dekripsi tersebut akan ditampilkan pada *layout Crypt Result*.

3.5. Tampilan Interface Aplikasi

3.5.1. Tampilan Interface Login

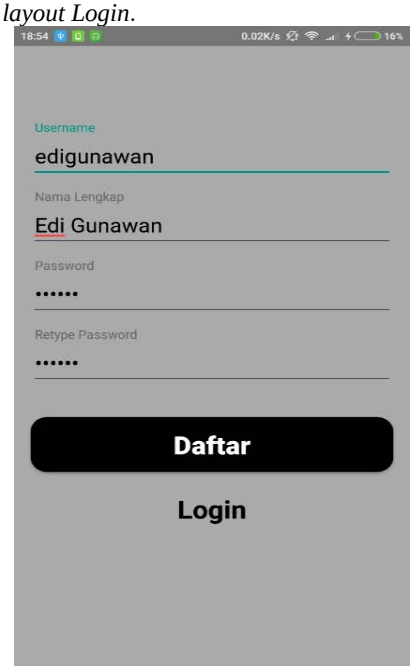


Gambar 6. Tampilan Interface Login

Gambar 6 merupakan tampilan dari *layout Login*. Pada *layout* ini terdapat dua buah *edittext* yang berfungsi untuk menerima *input*-an *username* dan *password*. Selain itu terdapat tombol *Login* untuk melakukan *login* berdasarkan *username* dan *password* yang diinputkan. Serta terdapat sebuah *textview* Daftar *User* yang berfungsi untuk menampilkan *layout* Daftar *User*.

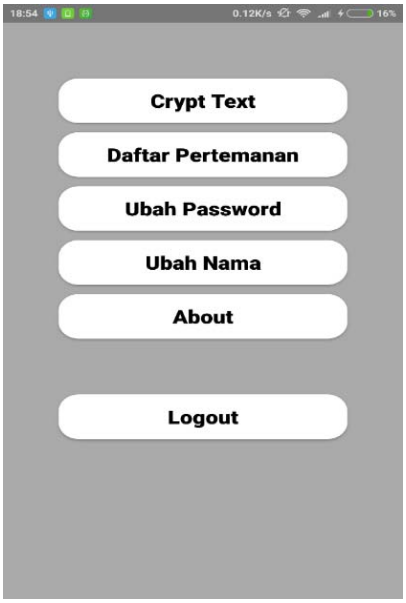
3.5.2. Tampilan Interface Daftar User

Gambar 7 di bawah ini merupakan tampilan dari *layout* Daftar *User*. Pada *layout* ini terdapat empat buah *edittext* yang berfungsi untuk menerimai *input*-an *username*, nama lengkap, *password* dan *retype password*. Terdapat sebuah tombol Daftar yang berfungsi untuk mendaftarkan data yang telah diinputkan serta sebuah *textview Login* untuk menampilkan *layout Login*.



Gambar 7. Tampilan Interface Daftar User

3.5.3. Tampilan Interface Menu Utama

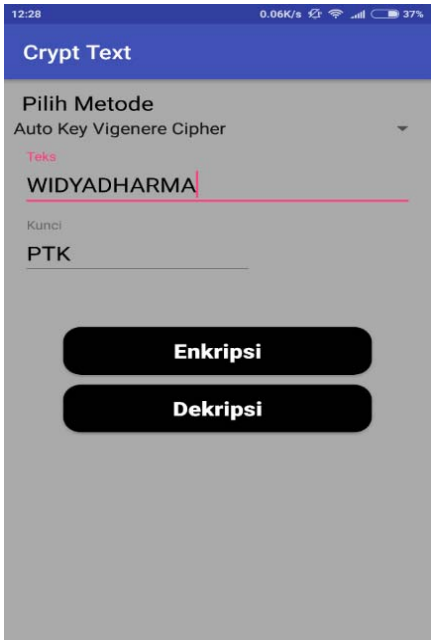


Gambar 8. Tampilan Interface Menu Utama

Gambar 8 merupakan tampilan dari *layout Menu* Utama. *Layout Menu* Utama ini akan ditampilkan saat *user* berhasil *login* ke dalam aplikasi. Pada *layout* ini, terdapat beberapa *menu* yang dapat diakses oleh *user*, diantaranya adalah *menu Crypt Text*, *menu* Daftar Pertemanan, *menu* Ubah *Password*, *menu* Ubah Nama, *menu About* dan *menu Logout*. *Menu Crypt Text* berfungsi untuk menampilkan *layout Crypt Text* yang dapat digunakan oleh *user* untuk melakukan proses enkripsi maupun dekripsi. Dari *layout* tersebut, proses enkripsi dan dekripsi akan diproses dan hasil enkripsi atau dekripsinya akan ditampilkan pada *layout Crypt Result*. *Menu* Daftar Pertemanan berfungsi untuk menampilkan *layout* Daftar Pertemanan, yang pada *layout* tersebut akan ditampilkan daftar *friend*, *pending* maupun *request* pertemanan yang masuk. Pada *layout* tersebut, juga terdapat sebuah tombol Tambah Teman yang berfungsi untuk menampilkan *layout* Tambah Teman untuk menambahkan teman sesuai

dengan *username* yang ditambahkan. *Menu* Ubah *Password* berfungsi untuk menampilkan *layout* Ubah *Password* yang dapat digunakan oleh *user* untuk mengganti passwordnya. Terdapat juga *menu* Ubah Nama yang dapat digunakan oleh user untuk mengganti nama daripada *username* tersebut. *Menu About* berfungsi untuk menampilkan *layout About*. Pada *layout About* akan ditampilkan beberapa informasi mengenai aplikasi kriptografi pesan ini. Selain itu terdapat juga sebuah *menu Logout* yang dapat digunakan oleh *user* untuk kembali ke *layout Login*.

3.5.4. Tampilan Interface Crypt Text



Gambar 9. Tampilan Interface Crypt Text

Gambar 9 merupakan tampilan dari *layout Crypt Text*. Pada *layout* ini, *user* dapat melakukan enkripsi ataupun dekripsi. *User* diharuskan untuk memilih metode yang akan digunakan, menginputkan teks dan kunci. Setelah semua masukan telah terisi, *user* dapat melakukan proses enkripsi dengan mengakses tombol Enkripsi yang tersedia ataupun jika *user* ingin melakukan proses dekripsi dapat dengan mengakses tombol Dekripsi yang tersedia.

Berikut merupakan hasil enkripsi dari beberapa metode yang tersedia:

Tabel 1. Tabel Hasil Enkripsi

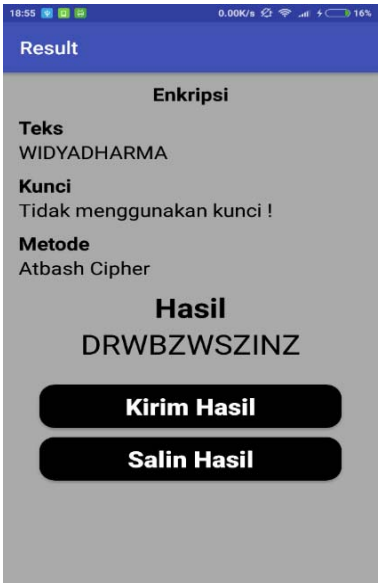
Teks	Kunci	Metode	Hasil
WIDYADHARMA	-	*Atbash Cipher*	DRWBZWSZINZ
WIDYADHARMA	PTK	*Auto Key Vigenere Cipher*	LBNUIGFAUTA
WIDYADHARMA	14	*Caesar Cipher*	KWRMORVOFAO
WIDYADHARMA	44512	*Gronsfeld Cipher*	AMIZCHLFSOE
WIDYADHARMA	-	*ROT13 Cipher*	JVQLNQUNEZN
WIDYADHARMA	PTK	*Running Key Vigenere Cipher*	LBNNTNWTBBT
WIDYADHARMA	3	*Scytale Cipher*	WYHMIAAADDR

Tabel 2. Tabel Hasil Dekripsi

Teks	KUNCI	Metode	Hasil
DRWBZWSZINZ	-	*Atbash Cipher*	WIDYADHARMA
LBNUIGFAUTA	PTK	*Auto Key Vigenere Cipher*	WIDYADHARMA
KWRMORVOFAO	14	*Caesar Cipher*	WIDYADHARMA
AMIZCHLFSOE	44512	*Gronsfeld Cipher*	WIDYADHARMA
JVQLNQUNEZN	-	*ROT13 Cipher*	WIDYADHARMA
LBNNTNWTBBT	PTK	*Running Key Vigenere Cipher*	WIDYADHARMA
WYHMIAAADDR	3	*Scytale Cipher*	WIDYADHARMA

3.5.5. Tampilan Interface Crypt Result

Gambar 10 di bawah ini merupakan tampilan dari *layout Crypt Result*. Pada *layout* ini akan ditampilkan hasil enkripsi ataupun dekripsi yang diproses pada *layout Crypt Text*. Terdapat dua buah tombol, yaitu tombol Kirim Hasil yang berfungsi untuk mengirimkan hasil enkripsi ataupun tombol Salin Hasil yang berfungsi untuk menyalin hasil enkripsi tersebut. Tabel hasil enkripsi dan dekripsi yang ditampilkan pada *layout Crypt Result* dapat dilihat pada Tabel 1 dan Tabel 2 di atas.



Gambar 10. Tampilan Interface Crypt Result

3.6. Pengujian Aplikasi

Pengujian dilakukan dengan menggunakan tiga *smartphone* yang berbeda. *Smartphone* pertama yaitu Asus Zenfone C dengan sistem operasi android 5.0 (*Lollipop*), yang kedua adalah Xiaomi Redmi Note 4 dengan sistem operasi android 7.0 (*Nougat*), yang terakhir adalah Vivo V7 dengan sistem operasi 8.0 (*Oreo*). Pengujian dilakukan pada *layout Login*, *layout* Daftar *User*, *menu-menu* yang terdapat pada *layout Menu* Utama, *layout Crypt Text*, *layout Crypt Result*, *layout* Daftar Teman, *layout* Daftar Pertemanan, *layout* Tambah Teman, *layout* Ubah *Password*, *layout* Ubah Nama, *layout About* dan *menu Logout*. Pengujian bertujuan untuk memastikan semua fitur yang terdapat pada setiap *layout* dapat berjalan dengan baik dan sesuai dengan rancangan aplikasi yang telah dibuat. Berikut adalah tabel pengujian:

Tabel 3. Tabel Pengujian Menu

No.	Layout	Keterangan
1	Layout Login	Berjalan dengan baik
2	Layout Daftar User	Berjalan dengan baik
3	Layout Menu Utama	Berjalan dengan baik
4	Layout Crypt Text	Berjalan dengan baik
5	Layout Crypt Result	Berjalan dengan baik
6	Layout Daftar Teman	Berjalan dengan baik
7	Layout Daftar Pertemanan	Berjalan dengan baik
8	Layout Tambah Teman	Berjalan dengan baik
9	Layout Ubah Password	Berjalan dengan baik
10	Layout Ubah Nama	Berjalan dengan baik
11	Layout About	Berjalan dengan baik
12	Logout	Berjalan dengan baik

Tabel 4. Tabel Pengujian Aplikasi

Smartphone	Versi Android	Keterangan	Catatan
Asus Zenfone C	5.0 (Lollipop)	Berjalan dengan baik	Semua fungsi berjalan dengan baik
Xiaomi Redmi Note 4	7.0 (Nougat)	Berjalan dengan baik	Semua fungsi berjalan dengan baik
Vivo V7	8.0 (Oreo)	Berjalan dengan baik	Semua fungsi berjalan dengan baik

4. KESIMPULAN

Berdasarkan implementasi dan evaluasi terhadap aplikasi kriptografi pesan berbasis *android* yang telah dijelaskan pada bab-bab sebelumnya, maka penulis dapat mengambil beberapa kesimpulan sebagai berikut:

a. Kriptografi dengan algoritma simetris akan menyebabkan penggunaan kunci yang sama dalam melakukan enkripsi dan deskripsi. Dengan demikian, kunci tersebut bersifat rahasia.
b. Pada algoritma kriptografi dengan menggunakan algoritma simetris, setiap susunan huruf masukan yang dienkripsi atau dekripsi memungkinkan untuk menghasilkan susunan huruf yang sama dengan huruf masukannya namun berbeda posisi. Jenis algoritma kriptografi ini disebut sebagai *transposition cipher*. Contoh *transposition cipher* yang ada pada aplikasi kriptografi pesan ini adalah *Scytale Cipher*. Selain *transposition cipher*, terdapat juga algoritma kriptografi yang disebut dengan *substitution cipher*, yaitu setiap huruf teks masukan akan mengalami pengubahan sesuai dengan kunci dan metode yang digunakan.
c. Melakukan proses enkripsi dengan menggunakan masukan teks dan kunci yang sama akan menghasilkan teks yang berbeda untuk setiap metodenya. Sama halnya dengan proses dekripsi.

5. SARAN

Setelah melakukan analisis pada hasil perancangan aplikasi kriptografi pesan ini, penulis menyadari bahwa perangkat lunak yang dihasilkan belum sempurna. Adapun beberapa saran dari penulis agar perangkat lunak ini dapat dikembangkan lebih jauh, antara lain:

a. Ditambahkannya algoritma-algoritma kriptografi yang memiliki proses enkripsi yang lebih rumit.
b. Ditambahkannya fitur *history* untuk menampung hasil-hasil enkripsi dan dekripsi.
c. Membangun kembali tampilan pesan yang lebih menarik.
d. Ditambahkannya fitur notifikasi pada saat terdapat pesan masuk ataupun saat ada permintaan pertemanan.

UCAPAN TERIMA KASIH

Dalam penyusunan skripsi ini, penulis telah banyak mendapat bantuan bimbingan, data, saran, dan dukungan moril dari berbagai pihak, pada kesempatan ini penulis ingin mengucapkan terimakasih kepada civitas akademika Sekolah Tinggi Manajemen Informatika dan Komputer Widya Dharma Pontianak, kepada pembimbing skripsi dan kepada pihak-pihak lain yang sudah sangat membantu penulis secara teknis dan moril dalam menyelesaikan penulisan skripsi ini.

DAFTAR PUSTAKA

[1] Muslihudin Muhamad dan Oktafianto. (2016). *Analisis dan Perancangan Sistem Informasi Menggunakan Model Terstruktur dari UML*. ANDI. Yogyakarta.
[2] Muharto dan Arisandy Ambarita. (2016). *Metode Penelitian Sistem Informasi: Mengatasi Kesulitan Mahasiswa dalam Menyusun Proposal Penelitian*. Deepublish. Yogyakarta.
[3] Muharto dan Arisandy Ambarita. (2016). *Metode Penelitian Sistem Informasi: Mengatasi Kesulitan Mahasiswa dalam Menyusun Proposal Penelitian*. Deepublish. Yogyakarta.
[4] Nugroho, Adit. (2010). *Rekayasa Perangkat Lunak Berorientasi Objek dengan Metode USDP*. ANDI. Yogyakarta.
[5] Wahana Komputer. (2010). *The Best Encryption Tools*. PT Elex Media Komputindo. Jakarta.
[6] Kelly, Brian. (2018). *The Bitcoin Big Bang: Bagaimana Mata Uang Alternatif Akan Mengubah Dunia.* PT Elex Media Komputindo. Jakarta.
[7] Jubile Enterprise. (2015). *Mengenal Dasar-Dasar Pemrograman Android.* PT Elex Media Komputindo. Jakarta.
[8] Amperiyanto, Tri. (2014). *Tips Ampuh Android: Cara Tepat dan Bijak Mendayagunakan Perangkat Android*. PT Elex Media Komputindo. Jakarta.