

**Laporan Tugas Akhir**  
**Mata Kuliah Pemrograman Mobile**



**Dosen Pengampu :**

Irzal Ahmad Sabilla, S.Kom, M.Kom.

Dwi Sunaryono, S.Kom , M.Kom.

Ridho Rahman Hariadi, S.Kom., M.Sc.

**Oleh Kelompok 9 :**

Widya Inayatul L (05311940000010)

Shavica Ihya Qurata Ayun L. (05311940000013)

Bryan Yehuda Mannuel (05311940000021)

# **BAB 1**

## **Deskripsi Singkat**

### **A. Latar Belakang Aplikasi**

Akhir-akhir ini ada berita viral mengenai maraknya instansi “Pinjol” atau pinjaman online yang ada di Indonesia, dimana setiap instansi “Pinjol” pasti meminta dokumen penting dan privat seperti KTP, NPWP, Foto Selfie, dan dokumen penting lainnya agar seseorang bisa dinilai layak untuk dipinjam uang. Dari berita ini, kelompok kami khawatir bahwa dokumen penting dan private ini dapat disalahgunakan apabila tidak dilakukan penjagaan dan penanganan data yang tepat.

Disini kelompok kami ingin membuat sebuah aplikasi yang bisa membantu orang-orang, tidak terbatas pada mereka yang ingin meminjam uang saja, untuk mengamankan dokumen mereka baik pada saat berada di device mereka, saat transit data, ataupun saat diterima oleh penerima yang diinginkan. Kelompok kami ingin membuat sebuah aplikasi Enkripsi dan Dekripsi dokumen yang bisa memudahkan setiap pengguna kami dalam melakukan penjagaan dan penanganan data mereka.

Pembuatan aplikasi ini akan memanfaatkan ilmu-ilmu yang sudah kami dapatkan selama 5 semester berkuliah di Departemen Teknologi Informasi seperti Enkripsi - Dekripsi, Algoritma AES, Algoritma DES, Algoritma RSA, Steganography, dan banyak algoritma Enkripsi - Dekripsi lainnya yang bisa dipilih. Nanti para user bisa mengupload dokumen mereka ke aplikasi kami secara local dan memilih algoritma yang ingin digunakan serta melakukan Enkripsi - Dekripsi secara mandiri terhadap data yang ingin mereka lindungi.

### **B. Target Aplikasi**

Target dari aplikasi ini adalah setiap orang yang sering melakukan transaksi data dan dokumen dalam keseharian hidup mereka. Orang-orang ini pasti membutuhkan suatu sistem perlindungan dan penjagaan terhadap dokumen mereka. Tanpa adanya perlindungan dan penjagaan, setiap data dan dokumen yang mereka transaksikan terancam untuk dicuri, disalahgunakan, dimanipulasi dan lain-lain. Kelompok kami menargetkan orang-orang seperti ini agar mereka bisa menggunakan aplikasi kami dalam menjaga keamanan data dan dokumen mereka.

### **C. Pemrograman Java**

Java adalah sebuah bahasa pemrograman komputer berbasis kepada Object Oriented Programming ( pemrograman berbasis objek ) yang sederhana dan tidak tergantung pada platform yang digunakan. Bahasa ini dikembangkan oleh Sun Microsystems dan memiliki banyak keunggulan, sederhana, ukurannya kecil, dan portable (dapat dipindah-pindahkan di antara bermacam platform dan sistem operasi).

### **D. Dasar Teori**

#### **1. Enkripsi**

Enkripsi adalah metode dimana informasi diubah menjadi kode rahasia yang menyembunyikan arti sebenarnya dari informasi tersebut. Enkripsi membantu dalam melindungi kerahasiaan data digital baik yang disimpan di sistem komputer atau dikirim melalui jaringan seperti internet.

## **2. Dekripsi**

Dekripsi adalah proses mengubah data yang telah dibuat tidak dapat dibaca melalui enkripsi kembali ke bentuk yang tidak terenkripsi. Dalam dekripsi, sistem mengekstrak dan mengubah data yang kacau dan mengubahnya menjadi teks dan gambar yang mudah dimengerti tidak hanya oleh pembaca tetapi juga oleh sistem.

## **3. Steganografi**

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada orangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Kata "steganografi" berasal dari bahasa Yunani steganos, yang artinya "tersembunyi atau terselubung", dan graphein, "menulis".

## **4. Algoritma AES**

Advanced Encryption Standard (AES) merupakan algoritma cryptographic yang dapat digunakan untuk mengamankan data. Algoritma AES adalah blok ciphertext simetrik yang dapat mengenkripsi (encipher) dan dekripsi (decipher) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut ciphertext; sebaliknya dekripsi adalah merubah ciphertext data menjadi bentuk semula yang kita kenal sebagai plaintext.

## **5. Algoritma DES**

DES (Data Encryption Standard) adalah algoritma cipher blok yang populer karena dijadikan standard algoritma enkripsi kunci-simetri, meskipun saat ini standard tersebut telah digantikan dengan algoritma yang baru, AES. DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis cipher blok. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit ciphertexts dengan menggunakan 56 bit kunci internal (internal key) atau upa-kunci (subkey). Kunci internal dibangkitkan dari kunci eksternal (external key) yang panjangnya 64 bit.

## **6. Algoritma RSA**

RSA adalah sebuah algoritma berdasarkan skema public-key cryptography. Pada umumnya algoritma yang satu ini digunakan untuk kepentingan autentikasi. Merupakan aspek dimana si penerima informasi dapat memastikan keaslian pesan, yakni dengan kata lain data dan informasi benar-benar berasal dari sumber yang benar. Oleh karena itulah kunci pada algoritma ini berbeda saat enkripsi dan dekripsinya.

## BAB 2

### Komponen Kerja

#### A. Material Aplikasi

Aplikasi ini akan membutuhkan Akses ke dalam File Storage milik user agar user bisa melakukan upload file dokumen atau data ke dalam aplikasi kami secara local. Akses ke dalam File Storage ini juga berguna bagi user ketika akan mengambil file dokumen atau data yang sudah dilakukan enkripsi ataupun dekripsi. Aplikasi ini juga akan membutuhkan Intent untuk melakukan pemilihan Algoritma Enkripsi ataupun Dekripsi yang sesuai dan juga untuk berganti layar Activity dalam Android. Begitu pula dibutuhkan Dialog Box dan juga Database CRUD sederhana untuk melakukan konfirmasi manipulasi Enkripsi ataupun Dekripsi terhadap dokumen yang diupload oleh user.

#### B. Pemanggilan Fungsi

Fungsi dalam Aplikasi ini akan terbagi menjadi 2 macam yaitu fungsi untuk fungsionalitas aplikasi dan juga fungsi untuk melakukan Dekripsi dan Enkripsi. Untuk fungsi fungsionalitas Aplikasi akan berguna dalam melakukan control Intent, control Dialog Box, control Database CRUD, pemilihan Algoritma Enkripsi atau Dekripsi, dan juga meminta ijin untuk mengakses File Storage. Sedangkan untuk fungsi Dekripsi dan Enkripsi, fungsi ini akan mengambil dokumen yang akan dilakukan manipulasi dan mengubahnya sesuai dengan Algoritma Enkripsi atau Dekripsi yang dipilih oleh user.

Untuk Fungsionalitas Aplikasi akan ada:

- Intent

*From "Main Page" if*

*Choose "Dekripsi Button" Then go to "Dekripsi Page"*

*From "Dekripsi Page" if*

*Choose "Algoritma A Button" Then go to "Algoritma A Page"*

*Choose "Algoritma B Button" Then go to "Algoritma B Page"*

*Choose "Algoritma C Button" Then go to "Algoritma C Page"*

*Choose "Enkripsi Button" Then go to "Enkripsi Page"*

*From "Enkripsi Page" if*

*Choose "Algoritma A Button" Then go to "Algoritma A Page"*

*Choose "Algoritma B Button" Then go to "Algoritma B Page"*

*Choose "Algoritma C Button" Then go to "Algoritma C Page"*

- Dialog Box – Dialog Box akan ditanyakan setiap kali user selesai menekan tombol "Lakukan Enkripsi" atau tombol "Lakukan Dekripsi" setelah selesai melakukan upload File. Jika ditekan "Ya" maka akan dijalankan prosesnya, tetapi jika ditekan "Tidak" maka tidak akan dijalankan prosesnya.
- Database CRUD – Database CRUD akan digunakan untuk melakukan penyimpanan sementara terhadap dokumen yang dilakukan upload kepada aplikasi kami agar aplikasi ini bisa berjalan secara local.

*Create New Database*

*Create New Table (File\_loc\_uploaded Varchar (200), File\_loc\_finished (200))*

*File\_loc\_uploaded = Get Uploaded Files*

*Select Table insert into File\_loc\_uploaded (File\_loc\_uploaded)*

*File\_loc\_finished = AlgoritmaEnkripsiPilihan(File\_loc\_uploaded)*

*Select Table insert into File\_loc\_finished (File\_loc\_finished)*

- Pemilihan Algoritma – Pemilihan Algoritma akan menggunakan Switch Case yang terhubung dengan Button yang dipilih oleh user.

*Switch Case AlgoritmaButton*

*If “1” Then “AlgoritmaA”*

*If “2” Then “AlgoritmaB”*

*If “3” Then “AlgoritmaC”*

- Meminta Ijin – Permintaan Ijin akan dilakukan di File Manifest Android dan accept atau tidaknya akan ditangkap di Main Activity. Bagian ini penting karena jika user tidak mengijinkan diaksesnya File Storage maka user tidak bisa melakukan upload dan download filenya sehingga aplikasi tidak akan bisa berjalan.

Untuk Algoritma Enkripsi dan Dekripsi akan digunakan berbagai macam algoritma yang sudah diajarkan dalam mata kuliah terdahulu mengenai Enkripsi dan Dekripsi yang ada di Departemen Teknologi Informasi. Sejauh ini kami akan menggunakan AES, DES, RSA. Nanti akan ditambahkan lagi selagi pembuatan proyek ini.

### C. Library

Aplikasi ini menggunakan library volley merupakan library yang berfokus untuk membantu koneksi ke API menjadi jauh lebih muda untuk fitur upload file dan upload image.

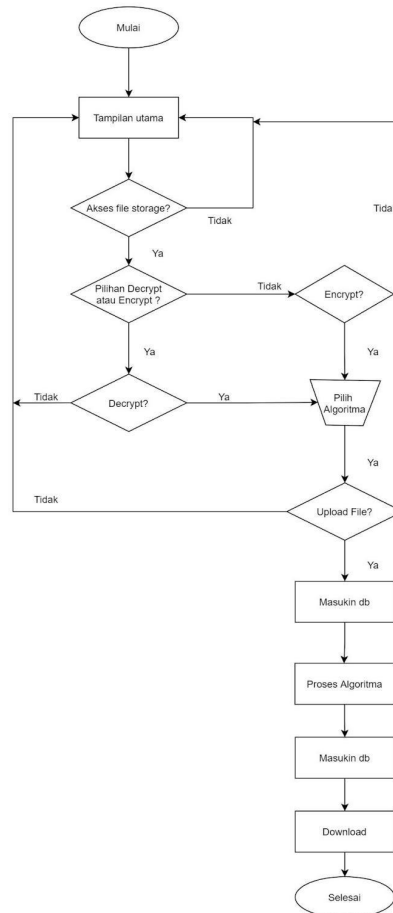
```
import com.android.volley.DefaultRetryPolicy;
import com.android.volley.Request;
import com.android.volley.RequestQueue;
import com.android.volley.toolbox.Volley;
```

## BAB 3

### Cara Kerja

#### A. Gambaran Umum Sistem

Secara umum sistem aplikasi yang akan kami buat terdiri atas fungsi encrypt dan decrypt dengan menggunakan algoritma dapat dilihat pada Gambar 1 berikut:



**Gambar 1. Gambaran Umum Sistem**

#### B. Implementasi Antarmuka

Pada implementasi antarmuka, aplikasi akan diuji menggunakan emulator dan handphone. Hal tersebut bertujuan untuk mengetahui apakah aplikasi telah berjalan sesuai dengan rancangan dan sasaran aplikasi. Pengujian pada emulator dilakukan untuk mempermudah dalam mendeteksi kesalahan saat program atau pengkodean dijalankan. Apabila pengujian emulator berhasil maka akan dilanjutkan pada tahap pengujian menggunakan handphone.

Pada halaman pertama aplikasi akan ditampilkan splash screen logo pembuka dari aplikasi DocGuard seperti gambar berikut.



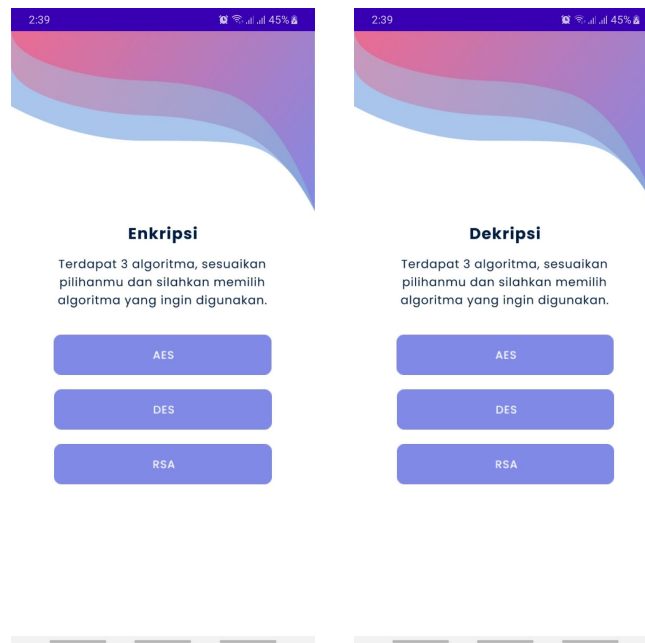
***Gambar 2. Splash Screen***

Selanjutnya akan diarahkan menuju halaman home yang menampilkan deskripsi singkat aplikasi serta terdapat tombol pilihan enkripsi dan dekripsi, nantinya pengguna akan memilih opsi untuk menggunakan fungsi enkripsi atau dekripsi.



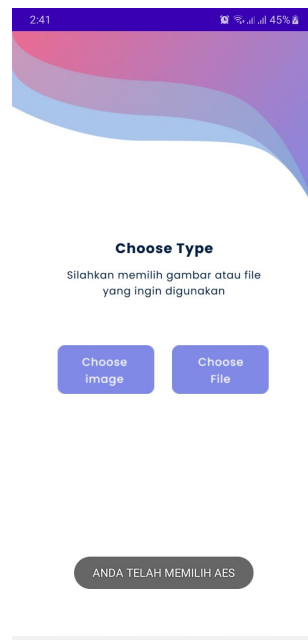
***Gambar 3. Menu Enkripsi Dekripsi***

Setelah memilih salah satu fungsi enkripsi atau dekripsi, pengguna akan diarahkan ke halaman enkripsi atau dekripsi sesuai yang dipilih oleh pengguna yang berisi tampilan pilihan algoritma yakni AES, DES, dan RSA. Nantinya pengguna akan memilih 1 dari 3 algoritma yang bisa digunakan. Terdapat 3 algoritma yang ditawarkan seperti gambar berikut.



***Gambar 4. Pilihan Algoritma***

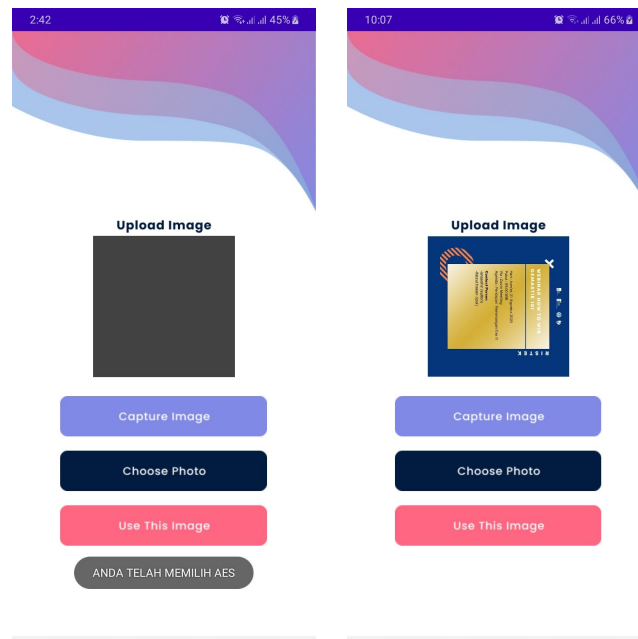
Setiap memilih algoritma AES, DES, ataupun RSA, selanjutnya akan diarahkan ke halaman yang berisi tampilan untuk memilih gambar atau file seperti gambar berikut ini.



***Gambar 5. Choose Type***

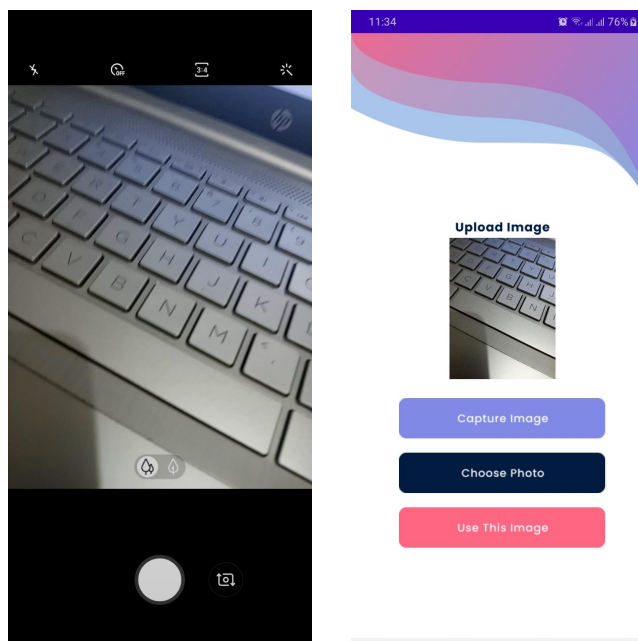


Jika pengguna menekan tombol *choose image* maka akan diarahkan ke halaman *upload image*. Pada halaman ini pengguna dapat *upload image* dari *capture camera* ataupun dari galeri *handphone* seperti gambar berikut.



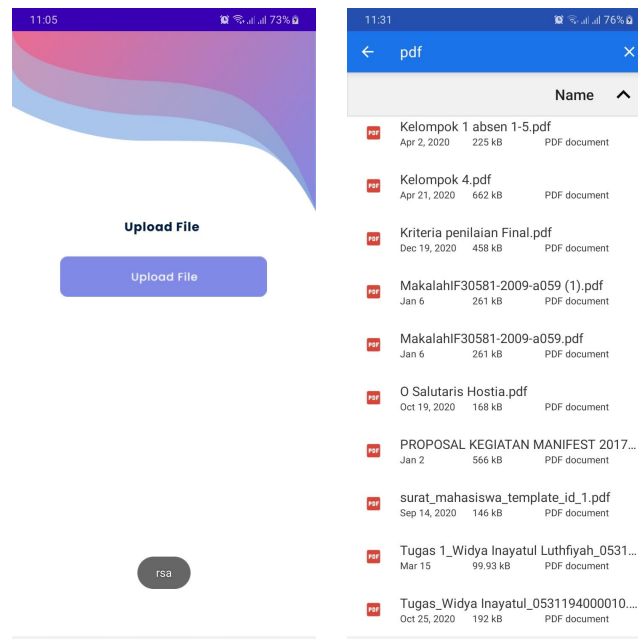
**Gambar 6. Upload Image Gallery**

Pengguna *upload image* melalui *capture camera* seperti gambar berikut.



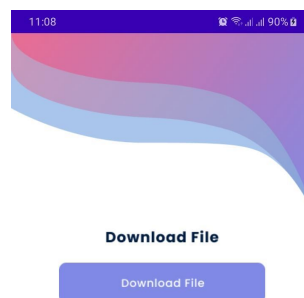
**Gambar 6. Upload Image Camera**

Jika pengguna menekan tombol *choose file* maka akan diarahkan ke halaman *upload file*. Pada halaman ini pengguna dapat upload file melalui *storage handphone* seperti gambar berikut ini.



**Gambar 7. Upload File**

Setelah *file* dan *image* diupload maka program akan dijalankan dan menghasilkan dokumen hasil enkripsi dan dekripsi berupa *file* dan *image* yang dapat di download seperti gambar berikut.



**Gambar 6. Download File**