Pemanfaatan Vigenere Cipher untuk Pengamanan Foto pada Sistem Operasi Android

Raka Mahesa - 13508074
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
the_legacy99@hotmail.com

***Abstrak*—Akhir-akhir ini sedang marak berita mengenai aplikasi *mobile* untuk Android ataupun iOS yang rupanya mengunggah data pribadi penggunanya ke server pembuat aplikasi tersebut. Hal ini merupakan salah satu contoh pelanggaran privasi karena mungkin saja terdapat berbagai data milik pengguna yang tidak boleh diketahui orang lain. Apalagi ponsel merupakan perangkat yang cukup personal sehingga besar kemungkinan terdapat data yang hanya boleh diketahui pemiliknya saja. Foto-foto merupakan salah satu contoh data yang mungkin cukup personal, apalagi ponsel zaman sekarang selalu dilengkapi dengan kamera. Karena itu penulis mencoba mengaplikasikan Vigenere *cipher*, sebuah metode kriptografi yang sederhana, untuk mengamankan berbagai foto atau gambar yang terdapat pada ponsel Android agar tidak jatuh ke tangan yang salah. Pada makalah ini akan digunakan Vigenere *cipher* yang sudah sedikit dimodifikasi agar dapat mengenkripsi sebuah gambar.**

***Kata Kunci*—Enkripsi gambar, Android, Metode Vigenere.**

I. PENDAHULUAN

Kriptografi merupakan sebuah ilmu tentang bagaimana cara menjaga agar data yang dikirimkan oleh pengirim dapat mencapai penerima pesan tanpa mendapat gangguan dari pihak ketiga.

Istilah kriptografi sendiri berasal dari dua buah kata dalam bahasa Yunani yaitu kata "cryptos" yang berarti rahasia dan kata "graphein" yang berarti tulisan. Dengan demikian, dari segi bahasa, kriptografi memiliki arti tulisan rahasia. Istilah tersebut amat tepat ketika kriptografi mulai digunakan, karena pada zaman-zaman tersebut pengiriman pesan dilakukan menggunakan tulisan sehingga untuk menjaga keamanannya, tulisan tersebut harus dirahasiakan. Dewasa ini, pesan atau data dapat memiliki berbagai wujud seperti tulisan, gambar, suara ataupun bentuk lainnya, sehingga kriptografi bukan hanya ilmu mengenai cara membuat tulisan rahasia saja tetapi juga ilmu menjaga kerahasiaan data dalam wujud lainnya.

Selain perubahan pada wujud pesan yang perlu dirahasiakan, saat ini kriptografi juga memiliki tujuan lain selain menjaga kerahasiaan pesan, yaitu menjaga kerahasiaan data pribadi. Kedatangan teknologi internet telat memudahkan manusia untuk mencari informasi mengenai orang lain, sehingga zaman sekarang ini, kerahasiaan diri merupakan suatu hal yang amat penting.

Seiring dengan berkembangnya zaman, berbagai macam tindak kejahatan baru yang memanfaatkan teknologi modern pun muncul. Salah satu tindak kejahatan yang muncul pada zaman modern ini dan menjadi marak ialah pencurian data pribadi. Data pribadi yang diincar biasanya merupakan data kartu kredit, password, ataupun alamat e-mail karena data tersebut mudah memberikan keuntungan bagi sang pencuri. Karena hal tersebut, kini data-data yang berharga itu biasanya sudah dienkripsi sehingga sulit untuk dicuri.

Di zaman *smartphone* ini, banyak orang yang menyimpan data pribadi pada perangkat seluler miliknya. Hal ini menjadikan *smartphone* sebagai barang incaran para pencuri data, apalagi masyarakat masih terbiasa dengan ponsel zaman dahulu yang tidak terhubung dengan internet dan lebih aman dari pencurian data pribadi. Selain itu ekosistem *smartphone* sekarang memungkinkan penggunanya untuk memasang berbagai aplikasi pada perangkat selulernya sehingga memudahkan pencuri data untuk mendistribusikan aplikasi jahat (*malware*) dengan tujuan mendapatkan data penggunanya. Bahkan kini aplikasi yang valid pun mengambil data pemakainya dan menggunggahnya ke server agar pembuat aplikasi tersebut dapat memahami konsumennya lebih jauh.

Dengan makalah ini, penulis mencoba untuk membantu menjaga kerahasiaan pemakai *smartphone*, khususnya *smartphone* Android, dengan meng-enkripsi berbagai gambar yang terdapat pada perangkat tersebut agar gambar tersebut tidak dimengerti oleh para pengambil data.

II. GAMBAR

Secara umum, gambar pada komputer terbagi menjadi dua jenis, yaitu gambar berbasis bitmap dan gambar berbasis vector. Gambar vector merupakan gambar yang terbuat dari kumpulan elemen yang didefinisikan dengan formula tertentu, misalnya elemen lingkaran, kurva dan lainnya. Sementara gambar bitmap terdiri dari kumpulan petak-petak berwarna yang disebut dengan nama pixel. Makalah ini hanya akan membahas mengenai gambar berbasis bitmap.

File berisi gambar bitmap dapat dibuat dengan berbagai tipe dan format. Ada gambar dengan format JPG, PNG, GIF, dan masih banyak format-format lain yang tidak umum seperti PSD atau TIF. Variasi gambar bukan hanya pada formatnya, bahkan sebuah file PNG dapat memiliki beberapa cara untuk menyimpan data gambarnya, misalnya PNG 16-bit, PNG 24-bit, ataupun PNG 32-bit yang memiliki jumlah kombinasi warna yang berbeda.

Meskipun gambar bitmap memiliki banyak format dan variasi, pada dasarnya gambar bitmap tetap merupakan kumpulan pixel berwarna. Warna pada pixel dapat direpresentasikan dengan berbagai cara, salah satu cara yang paling umum ialah dengan RGB. Representasi warna dengan RGB dilakukan dengan membagi warna menjadi tiga buah komponen, yaitu warna merah (R), hijau (G), dan biru (Blue) dimana kombinasi ketiga warna ini dapat menghasilkan hampir semua warna yang ada (terdapat lebih dari 16 juta kombinasi warna yang dapat dihasilkan dari ketiga komponen warna tersebut). Setiap komponen warna dapat memiliki nilai antara 0-255 dimana masing-masing komponen memiliki ukuran 8 bit.

III. Metode Vigenere

Vigenere *cipher* merupakan sebuah *cipher* substitusi polialfabetik yang diajukan oleh Blaise de Vigenere. Pada dasarnya, *cipher* Vigenere merupakan sebuah metode enkripsi yang terdiri dari beberapa Caesar *cipher* dengan nilai pergeseran yang berbeda-beda. Nilai pergeseran pada metode Vigenere berdasarkan pada sebuah kunci dan sebuah *tabula recta*, yaitu sebuah tabel alphabet dimana alphabet tiap barisnya digeser seperti pada gambar berikut:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 1. Sebuah *tabula recta*.

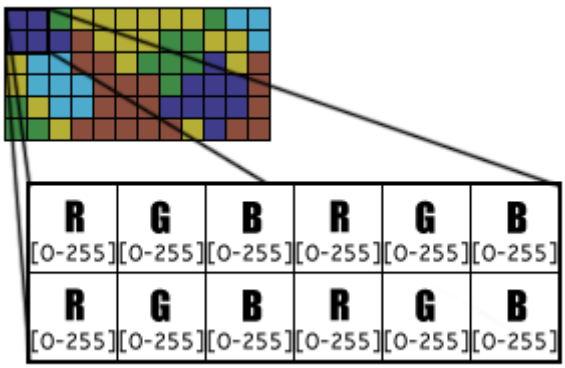
Bila teks "attackatdawn" akan dienkripsi menggunakan metode Vigenere dengan kunci "LEMON", maka pertama kunci harus diulang sampai sepanjang teks asli sehingga kini kunci menjadi "LEMONLEMONLE". Enkripsi dapat dilakukan dengan mengganti tiap huruf teks dengan huruf di tabula recta pada baris kunci dan kolom huruf teks. Misalnya huruf pertama pada teks, huruf "a" diganti dengan huruf pada tabula recta di baris L dan kolom A, yaitu huruf "A". Dilanjutkan dengan huruf berikutnya "T" diganti dengan huruf pada baris E dan kolom T, yaitu "X", lalu huruf "T" berikutnya diganti dengan huruf pada baris M dan kolom T, yaitu huruf "F" Langkah ini diulangin terus menerus sampai semua huruf terenkripsi dan didapatkan ciphertext-nya, "LXFOPVEFRNHR".

Sementara untuk mendekripsi teks yang dienkripsi menggunakan metode Vigenere, cukup dilakukan kebalikan dari aksi enkripsi tiap huruf. Misalnya untuk mendekripsi huruf "L", maka dicari kolom mana pada baris "L" yang memiliki huruf "A", yaitu kolom A, maka huruf pertama teks ialah "a". Berikutnya dicari kolom mana pada baris "E" yang memiliki huruf "X" dan kolom mana pada baris "M" yang memiliki huruf "F". Didapatkan kolom T dan kolom T, maka 3 huruf pertama dari teks orisinil ialah "att. Bila dilanjutkan terus untuk tiap huruf, akan didapatkan teks aslinya, yaitu "attackatdawn".

Metode Vigenere memanfaatkan *tabula recta* yang berisi pergeseran alfabet untuk melakukan enkripsi dan dekripsi. Meskipun begitu, *tabula recta* tidak harus tabel 26 x 26 yang berisi pergeseran alfabet, tabula recta dapat juga berupa tabel 10 x 10 yang berisi angka 0 sampai 9 ataupun tabel lainnya.

IV. Implementasi

Algoritma enkripsi Vigenere merupakan algoritma enkripsi yang ditujukan untuk meng-enkripsi teks yang merupakan rangkaian huruf alfabet. Oleh karena itu, algoritma Vigenere tidak dapat langsung digunakan untuk mengenkripsi gambar karena sebuah gambar dibentuk oleh sekumpulan pixel dan bukan huruf. Meskipun begitu, sebuah data gambar dapat direpresentasikan sebagai sederet nilai yang menggambarkan warna dari tiap pixel. Nilai warna tersebut dapat dipecah lebih jauh menjadi nilai komponen merah, hijau dan biru yang memiliki rentang nilai 0 sampai 255. Dengan begitu, didapatkan representasi dari sebuah gambar seperti pada gambar berikut



Gambar 2. Representasi sebuah gambar ke dalam deret komponen warnanya.

Setiap nilai pada representasi tersebut memiliki rentang sebesar 0 sampai 255, sehingga didapatkan sebuah alfabet dengan 256 huruf yang terdiri dari bilangan 0 sampai bilangan 255. Tabula recta dari alfabet 0-255 ini dapat dibangkitkan menggunakan algoritma berikut:

```
//Buat tabel
short[][] TABLE = new short[256][256];
for (int i = 0; i < 256; i++)
  for (int j = 0; j < 256; j++)
    TABLE[i][j] = (short) ((i + j) % 256);
```

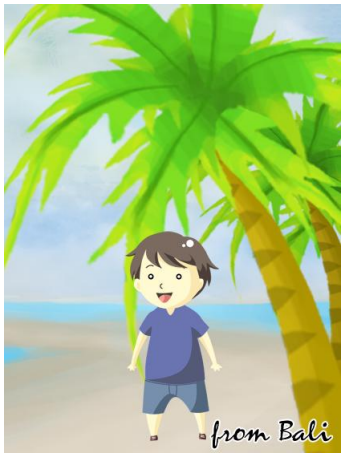
Pada Android, file gambar dapat dibaca dengan menggunakan kelas Bitmap, sementara data warna pixel gambar tersebut dapat diakses menggunakan fungsi getPixel(x, y) yang akan mengembalikan nilai warna dari pixel pada kolom x dan baris y. Nilai warna ini kemudian dipecah menjadi komponen RGB-nya dan disimpan pada sebuah deret agar kemudian dapat dienkripsi. Berikut implementasi cara mendapatkan array warna RGB dari sebuah gambar pada Android:

```
//Buat bitmap
Bitmap Bmp = BitmapFactory.decodeFile(Path);

//Buat array
short[] Colors = new short[Width * Height * 3];
for (int x = 0; x < Width; x++) {
 for (int y = 0; y < Height; y++) {
  int Index = [((x + (y * Width)) * 3);
  Colors[Index + 0] = Color.red(Bmp.getPixel(x,y));
  Colors[Index + 1] = Color.green(Bmp.getPixel(x,y));
  Colors[Index + 2] = Color.blue(Bmp.getPixel(x,y));
 }
}
```

Dengan mengimplementasikan enkripsi Vigenere pada deret tersebut, didapatkan sebuah deret baru yang berisi komponen warna yang sudah terenkripsi. Untuk melakukan enkripsi tersebut, digunakan kunci berupa deret bilangan yang terdiri dari bilangan antara 0 sampai 255. Bila deret sudah dienkripsi, maka deret tersebut perlu dikembalikan menjadi data warna setiap pixel agar dapat kembali membentuk gambar yang bisa dilihat namun tidak dapat dipahami. Berikut implementasi enkripsi vigenere dan pembentukan gambar tersebut.

```
//Enkripsi
short[] New= new short[Colors.length];
for (int i = 0; i < Colors.length; i++) {
  New[i] = TABLE[Key[i % Key.length]][Colors[i]];
}

//Buat warna dari komponen yang baru
int[] Pixels = new int[New.length / 3];
for (int i = 0; i < Pixels.length; i++) {
  Pixels[i] = Color.rgb(
    New[(i * 3) + 0],
    New[(i * 3) + 1],
    New[(i * 3) + 2]
  );
}

//Buat bitmap baru
Result = Bitmap.createBitmap(Pixels, Width, Height);
```

Terdapat dua buah gambar yang akan dienkripsi dengan algoritma Vigenere, gambar A merupakan sebuah gambar ilustrasi dan gambar B merupakan gambar foto yang diambil dengan kamera.



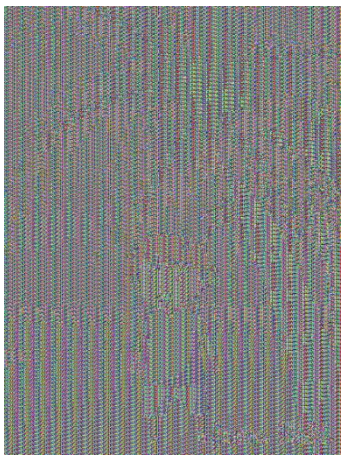
Gambar 3. Gambar A, gambar ilustrasi.

Gambar 4. Gambar B, gambar foto kota.

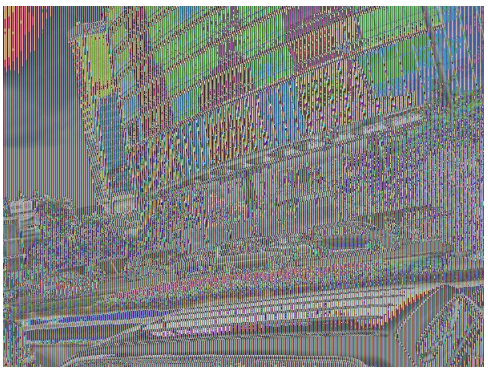
Berikut beberapa hasil enkripsi dengan kunci yang memiliki beragam panjang.

Gambar 5. Gambar A dienkripsi dengan panjang kunci 5.

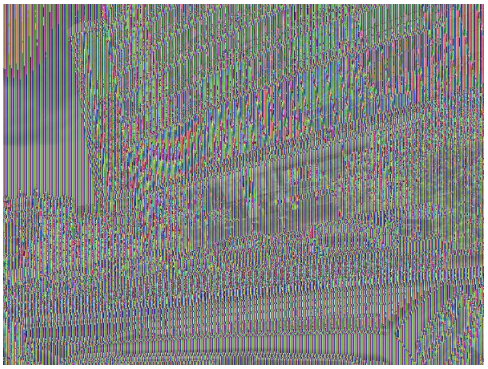
Gambar 6. Gambar A dienkripsi dengan panjang kunci 25.



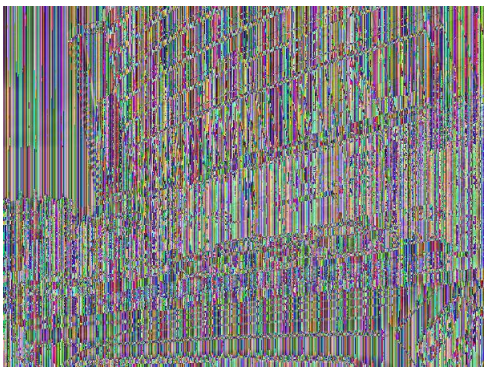
Gambar 7. Gambar A dienkripsi dengan panjang kunci 100.



Gambar 8. Gambar B dienkripsi dengan panjang kunci 5.



Gambar 9. Gambar B dienkripsi dengan panjang kunci 25.



Gambar 10. Gambar B dienkripsi dengan panjang kunci 100.

Secara umum, dapat dilihat bahwa semakin panjang kunci yang digunakan, enkripsi yang dilakukan akan semakin menyamarkan gambar asli. Meskipun begitu, dapat diamati bahwa tipe gambar juga menentukan seberapa tersamarnya suatu gambar setelah dienkripsi. Gambar B yang merupakan foto dengan komposisi dan warna yang lebih kompleks lebih mudah tersamarkan dibanding dengan gambar A yang merupakan gambar ilustrasi.

Gambar B sudah cukup tersamarkan bila dienkripsi menggunakan kunci dengan panjang 5, meskipun pola pada gambar masih dapat terlihat. Sementara ketika gambar A dienkripsi menggunakan kunci dengan panjang 5, bentuk gambar secara umum masih terlihat, meskipun warna pada gambar sudah berbeda jauh. Bahkan ketika dienkripsi menggunakan kunci yang memiliki panjang 100, pada gambar A masih terlihat pola yang memberi petunjuk mengenai gambar asli, meskipun kini objek pada gambar tersebut sudah tidak dapat dikenali.

Pada enkripsi gambar menggunakan metode Vigenere, dibutuhkan kunci yang panjang agar dapat menyamarkan gambar dengan baik. Misalnya bila kunci dengan panjang 5 digunakan, maka pergeseran nilai warna akan berulang setiap tiga buah pixel, sehingga mengakibatkan pola yang berulang. Selain itu, metode Vigenere juga lemah pada gambar yang memiliki lebar kelipatan 3 (gambar A dan gambar B memiliki lebar 420 dan 600 pixel) karena akan membuat pergeseran berulang pada setiap baris pixel, akibatnya perubahan warna pada gambar akan terjadi per kolom sehingga lebih mudah dimengerti manusia.

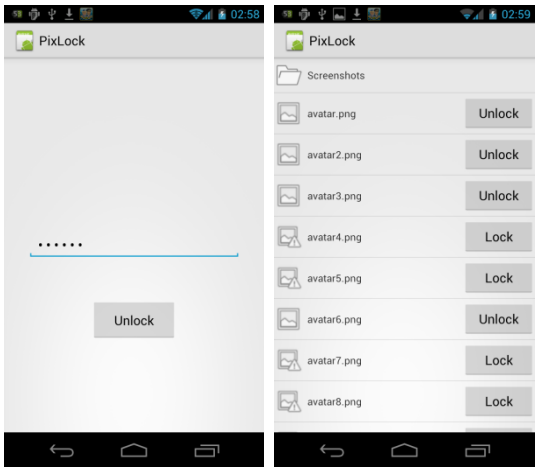
Selain itu, agar pemilik smartphone dapat melihat gambar yang sudah dirahasiakan, diperlukan cara untuk mendekripsi gambar yang sudah dienkripsi. Proses dekripsi gambar mirip dengan proses enkripsi gambar, hanya berbeda. Dekripsi dilakukan dengan mendapatkan deret komponen warna tiap pixel dari gambar, mengembalikannya ke deret komponen warna yang asli, dan mengembalikannya ke dalam bentuk gambar. Berikut implementasi proses dekripsi gambar:

```
//Buat bitmap
Bitmap Bmp = BitmapFactory.decodeFile(Path);

//Buat array
short[] Colors = new short[Width * Height * 3];
for (int x = 0; x < Width; x++) {
```

```
 for (int y = 0; y < Height; y++) {
  //Get color
  int Index = [((x + (y * Width)) * 3);
  Colors[Index + 0] = Color.red(Bmp.getPixel(x,y));
  Colors[Index + 1] = Color.green(Bmp.getPixel(x,y));
  Colors[Index + 2] = Color.blue(Bmp.getPixel(x,y));
 }
}

//Dekripsi
short[] New = new short[Colors.length];
for (int i = 0; i < Colors.length; i++) {
  New[i]= (New[i] - Key[i % Key.length] + 256) % 256;
}

//Buat warna dari komponen yang baru
int[] Pixels = new int[New.length / 3];
for (int i = 0; i < Pixels.length; i++) {
  Pixels[i] = Color.rgb(
    New[(i * 3) + 0],
    New[(i * 3) + 1],
    New[(i * 3) + 2]
  );
}

//Buat bitmap baru
Result = Bitmap.createBitmap(Pixels, Width, Height);
```

Kunci yang digunakan untuk melakukan enkripsi akan dibangkitkan ketika pengguna pertama kali memakai aplikasi. Kunci dibangkitkan secara acak, sehingga seorang pengguna aplikasi tidak dapat mendekripsi gambar orang lain yang dienkripsi dengan kunci yang berbeda.

Berikut tampilan-tampilan lain dari aplikasi Android yang sudah dibuat:



Gambar 11. Tampilan aplikasi.

V. KESIMPULAN

Terdapat beberapa hal yang dapat disimpulkan dari pengaplikasian Vigenere *cipher* pada *file* gambar di Android.

Yang pertama ialah bahwa metode enkripsi sederhana seperti Vigenere *cipher*, dapat dimanfaatkan untuk menyamarkan gambar meskipun dibutuhkan kunci yang panjang agar gambar dapat tersamarkan dengan baik. Dan bila digunakan dengan benar, hasil enkripsi masih dapat dibuka oleh aplikasi Android, meskipun kini pengguna tidak dapat mengenali objek pada gambar.

Hal lain yang dapat disimpulkan ialah bahwa tingkat keamanan dari Vigenere *cipher* sebanding dengan panjangnya kunci yang dipakai untuk melakukan enkripsi. Dari gambar 8 sampai gambar 10 dapat dilihat bahwa gambar dengan kunci yang lebih panjang dapat disamarkan dengan lebih baik.

Hal terakhir yang dapat disimpulkan ialah bahwa tipe gambar berpengaruh terhadap seberapa efektif metode Vigenere dalam menyambarkan gambar. Gambar dengan warna yang lebih sederhana seperti gambar ilustrasi akan lebih sulit disamarkan karena pola pada gambar akan lebih mudah terlihat.

REFERENCES

[1] http://www.mustek.com.tw/Class/bit_vec.html
[2] http://www.cs.trincoll.edu/~crypto/historical/vigenere.html.
[3] http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher.
[4] http://developer.android.com/reference/android/graphics/Bitmap.html.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 19 Maret 2012

ttd

Raka Mahesa
13508074