IMPLEMENTASI ALGORITMA ENKRIPSI RC5 UNTUK MENGAMANKAN GAMBAR PADA PERANGKAT ANDROID

I Nyoman Purnama

Sistem Informasi, STMIK Primakara

Jln. Tukad Badung 135 Denpasar, Indonesia
[1] pur182@yahoo.com

Abstract

Millions of people use social media to send pictures, messages, and other confidential information to friends and family members around the world. Sharing image through social media can be dangerous, if your private image accepted by other user. Image encryption is very necessary, so that your personal images are shared with the intended person. But complex encryption algorithms will consume a lot of resources owned by mobile devices. A lightweight encryption algorithm is needed so that the process of encryption and decryption need less time and computation. In this study the RC5 encryption algorithm is used to secure images to be shared on social media. RC5 is a fast symmetric block cipher encryption algorithm. The reason for using the RC5 algorithm is because its good security, besides the RC5 algorithm is also lightweight, fast and has good compatibility . From the results of the study obtained, RC5 has a variable word size, a variable number of rounds and a variable lengths secret key, that can be customized. In this experiment we analyse these RC5 paramaters to get a balance between security and speed in mobile devices. From the experiment shown that the average process for encryption for different key is 125.2ms and with different number of round the average time is 1352.2 ms .

Keywords : *RC5, encryption, decryption, image encryption, block cipher*

Abstrak

Jutaan orang menggunakan media sosial untuk mengirim gambar, pesan, dan informasi rahasia lainnya ke teman dan anggota keluarga di seluruh dunia. Berbagi gambar melalui media sosial bisa berbahaya, jika gambar pribadi Anda diterima oleh pengguna lain. Enkripsi gambar sangat diperlukan, sehingga gambar pribadi Anda dibagi dengan orang yang dituju. Tetapi algoritma enkripsi yang kompleks akan menghabiskan banyak sumber daya yang dimiliki oleh perangkat seluler. Algoritma enkripsi yang ringan diperlukan agar proses enkripsi dan dekripsi membutuhkan waktu dan komputasi yang lebih sedikit. Dalam penelitian ini algoritma enkripsi RC5 digunakan untuk mengamankan gambar untuk dibagikan di media sosial. RC5 adalah algoritma enkripsi cipher blok simetris cepat. Alasan menggunakan algoritma RC5 adalah karena keamanannya yang baik, selain itu algoritma RC5 juga ringan, cepat dan memiliki kompatibilitas yang baik. Dari hasil penelitian yang diperoleh, RC5 memiliki ukuran kata variabel, jumlah variabel putaran dan kunci rahasia panjang variabel, yang dapat dikustomisasi. Dari percobaan ditunjukkan bahwa proses rata-rata enkripsi untuk kunci yang berbeda adalah 125.2ms dan dengan jumlah putaran yang berbeda, waktu rata-rata adalah 1352.2 ms

Kata kunci : *RC5, enkripsi, dekripsi, enkripsi gambar, block cipher*

1. Pendahuluan

Perkembangan teknologi berkembang sangat cepat. Informasi dapat diakses di mana saja dan menyebar dengan sangat mudah. Salah satu teknologi yang memainkan peran penting dalam hal ini adalah Internet. Penggunaan internet memiliki hubungan dengan semakin banyaknya pengguna smartphone di dunia. Smartphone adalah perangkat yang memiliki tujuan utama sebagai telepon tetapi memiliki kemampuan seperti komputer. Kemampuan inilah yang menyebabkan smartphone juga bisa menggunakan fasilitas internet.

Salah satu kegunaan smartphone dan internet adalah untuk berhubungan sosial dengan orang lain. Satu dari cara untuk berhubungan secara sosial dengan orang lain adalah dengan menggunakan aplikasi yang disebut pesan social/Social media. Aplikasi ini adalah aplikasi yang terhubung dengan Internet dan dapat digunakan untuk mengirim pesan di smartphone baik itu chat baik teks maupun verbal. Penggunaan pesan sosial tentu saja harus menjaga privasi setiap orang yang menggunakannya.

Obrolan semua orang dengan orang lain tidak boleh dilihat oleh publik atau disadap oleh orang lain. Setiap aplikasi perpesanan sosial harus memiliki keamanan yang baik, untuk menjaga privasi masing-masing orang. Biasanya aplikasi pesan sosial sudah menyediakan enkripsi untuk dapat mengamankan obrolan penggunanya. Namun, aplikasi yang ada tidak memberikan keamanan untuk konten yang salah satunya ketika pengguna menggunakan aplikasi pesan sosial untuk berbagi gambar dengan teman. Di sini sebagian besar pesan sosial belum memiliki kemampuan untuk menjaga privasi gambar. Dengan semakin berkembangnya teknologi, para peretas juga semakin ahli dalam kemampuannya untuk menerobos server dari aplikasi social media yang memiliki keamanan lemah. Hal ini berimbas pada rentannya para peretas yang bisa membobol server dan menyebarkan gambar privasi yang dikirim via aplikasi social media

Hingga saat ini, berbagai algoritma enkripsi data telah diusulkan dan digunakan secara luas, seperti AES, RC5, RSA, atau IDEA, yang sebagian besar digunakan dalam teks atau data biner[2]. Sulit untuk menggunakannya secara langsung dalam data multimedia dan tidak efisien untuk enkripsi gambar berwarna karena tingginya korelasi antar piksel yang tinggi. Data multimedia seringkali memiliki redundansi tinggi, volume besar dan membutuhkan waktu pemrosesan yang lama. Enkripsi gambar dicapai melalui algoritma RC5 yang menggunakan operasi aritmatika sederhana dan rotasi bergantung pada jumlah data. Algoritma ini mengambil input dari dua kata dan menggunakannya sebanyak 16 set putaran. Parameter lain yang dipertimbangkan dalam algoritma RC5 yakni 'w' yang menunjukkan blok data, 'b' menunjukkan panjang kunci, 'r' menunjukkan jumlah putaran dan angka k 'menunjukkan nilai kunci yang digunakan. Parameter-parameter tadi dalam format terbalik digunakan untuk mendekripsi gambar, yang akhirnya memberikan output dalam bentuk aslinya.

Berdasarkan latar belakang ini, enkripsi RC5 akan digunakan untuk mengamankan gambar yang akan dibagikan kepada orang lain menggunakan perangkat smartphone Android. Smartphone Android telah dikenal secara luas dan digunakan oleh semua orang. Gambar yang disimpan di ponsel akan dienkripsi terlebih dahulu menggunakan parameter khusus RC5 sebelum gambar ini dibagikan melalui jaringan internet. Penelitian ini akan menganalisis waktu yang digunakan algoritma ini untuk mengenkripsi gambar, juga gambar keluaran akan diperiksa. Analisa ini akan mengukur kompleksitas algoritma RC5 berdasarkan jumlah waktu yang diperlukan untuk proses enkripsi dan dekripsi.

2. Tinjauan Pustaka dan Teori

A. Kriftografi

Kriptografi adalah ilmu mengenai teknik enkripsi dimana “naskah asli” (plaintext) diacak menggunakan suatu kunci enkripsi menjadi “naskah acak yang sulit dibaca” (ciphertext) oleh seseorang yang tidak memiliki kunci dekripsi[7]. Proses dekripsi menggunakan kunci dekripsi bisa mendapatkan kembali data asli. Probabilitas mendapat kembali naskah asli oleh seseorang yang tidak mempunyai kunci dekripsi dalam waktu yang tidak terlalu lama adalah sangat kecil.

Teknik enkripsi yang digunakan dalam kriptografi klasik adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi. Untuk public key cryptography, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif dibandingkan enkripsi simetris, karena enkripsi asimetris menggunakan bilangan – bilangan yang sangat besar[7].

Aspek Keamanan Kriptografi

Kriptografi memiliki beberapa aspek keamanan antara lain [8]:

1. Kerahasiaan (confidentiality), menjamin bahwa data-data tersebut hanya bisa diakses oleh pihak-pihak tertentu saja. Kerahasiaan bertujuan untuk melindungi suatu informasi dari semua pihak yang tidak berhak atas informasi tersebut.
2. Otentikasi (authentication), merupakan identifikasi yang dilakukan oleh masing – masing pihak yang saling berkomunikasi, maksudnya beberapa pihak yang berkomunikasi harus mengidentifikasi satu sama lainnya. Informasi yang didapat oleh suatu pihak dari pihak lain harus diidentifikasi untuk memastikan keaslian dari informasi yang diterima.
3. Integritas (integrity), menjamin setiap pesan yang dikirim pasti sampai pada penerimanya tanpa ada bagian dari pesan tersebut yang diganti, diduplikasi, dirusak, diubah urutannya, dan ditambahkan. Integritas data bertujuan untuk mencegah terjadinya pengubahan informasi oleh pihak-pihak yang tidak berhak atas informasi tersebut. Untuk menjamin integritas data ini pengguna harus mempunyai kemampuan untuk mendeteksi terjadinya manipulasi data oleh pihak-pihak yang tidak berkepentingan. Manipulasi data yang dimaksud di sini meliputi penyisipan, penghapusan, maupun penggantian data.
4. Nirpenyangkalan (Nonrepudiation), mencegah pengirim maupun penerima mengingkari bahwa mereka telah mengirimkan atau menerima suatu pesan. Jika sebuah pesan dikirim, penerima dapat membuktikan bahwa pesan tersebut memang dikirim oleh pengirim yang tertera. Sebaliknya, jika sebuah pesan diterima, pengirim dapat membuktikan bahwa pesannya telah diterima oleh pihak yang ditujunya.

B. RC5

Algoritma RC5 adalah algoritma block cipher yang dirancang oleh Profesor Ronald L. Rivest dari MIT dan dipublikasikan pertama pada Desember 1994. “RC” merupakan singkatan dari “Rivest Cipher” atau “Ron`s Code”. Sejak dipublikasikan, RC5 menarik perhatian banyak para ahli di dalam komunitas kriptographi dalam upaya memberikan akses keamanan secara akurat. Secara ringkas algoritma ini bekerja dengan penambahan modulus 2w,melakukan EX-OR dan melakukan rotasi x kekiri dengan jumlah y bit. RC-5 memiliki kelebihan dalam menentukan jumlah kata kunci yang digunakan, hal ini berarti akan memilih tingkat keamanan yang digunakan sesuai dengan aplikasinya[3].

Algoritma ini dirancang sedemikian rupa sehingga memenuhi syarat-syarat sebagai berikut :

- RC5 harus dirancang menjadi algoritma cipher simetri.
- RC5 harus cocok untuk digunakan pada hardware dan software. Hal ini berarti RC5 hanya boleh menggunakan primitif-primitif komputasi yang umum ditemukan pada mikroprosessor.
- RC5 harus berkecepatan tinggi. Berarti algoritma RC5 harus berorientasi word. Operasi-operasi RC5 harus dapat memproses 1 word penuh data
- RC5 harus dapat beradaptasi pada berbagai panjang word. Contohnya, pada prosessor terbaru 64-bit, panjang word-nya lebih panjang daripada prosessor 32-bit. RC5 harus dapat memanfaatkan ini, oleh karena itu RC5 memiliki parameter w yang menandakan panjang word
- RC5 harus dapat beroperasi dalam berbagai jumlah round. Jumlah round yang bervariasi memungkinkan pengguna untuk memanipulasi RC5 untuk menjadi lebih cepat atau lebih aman
- RC5 harus dapat beroperasi dalam berbagai panjang kunci. Hal ini mengakibatkan panjang kunci b menjadi parameter dalam algoritma RC5
- RC5 harus berstruktur sederhana. Struktur yang sederhana belum tentu menghasilkan keamanan yang rendah. Struktur yang sederhana akan memungkinkan analisis dan evaluasi yang cepat untuk menentukan kekuatan algoritma RC5
- RC5 harus hemat dalam pemakaian memori. Hal ini akan memungkinkan implementasi RC5 ke dalam smart-card atau perangkat lain yang memiliki keterbatasan memori
- RC5 harus mengimplementasikan metode data-dependent rotations. Metode ini adalah primitif kriptografi yang merupakan sasaran pengkajian RC5. Data-dependent rotations adalah suatu teknik yang merotasi data yang sekarang diproses secara sirkuler sebanyak N, di mana besarnya N tergantung data yang lain

a) Konsep Dasar RC-5

Algoritma RC-5 merupakan metode enkripsi menggunakan metode simetrik dan pengolahan dalam bentuk blok chiper, jadi kata kunci yang sama digunakan untuk proses enkripsi dan dekripsi. Parameter-parameter yang digunakan dalam RC-5 adalah sebagai berikut[3] :

- Jumlah putaran ini disimbolkan dengan r yang merupakan parameter untuk rotasi dengan nilai 0, 1, 2, …… 255.

- Jumlah word dalam bit disimbolkan dengan w. Nilai bit yang di support adalah 16 bit, 32 bit, dan 64 bit.
- Kata kunci (key word) Variable ini disimbolkan dengan b dengan range 0, 1, 2, …. 255. Key word ini dikembangkan menjadi array S yang digunakan sebagai key pada proses untuk enkripsi dan dekripsi.

Untuk memahami cara kerja RC-5, dapat dimulai dengan melihat konsep dasar bagaimana RC-5 ini bekerja. Hal ini dilakukan untuk memahami cara kerja algoritma ini lebih lanjut. RC-5 Menggunakan operasi dasar untuk proses enkripsi sebagai berikut[4] :

- Data yang akan dienkripsi dikembangkan menjadi 2 bagian bagian kiri dan bagian kanan dan dilakukan penjumlahan dengan key word yang yang telah diekspansi sebelumnya. Penjumlahan ditunjukan dengan tanda "+", dan disimpan di dua register A dan register B.
- Kemudian dilakukan operasi XOR, yang ditandai dengan tanda " ".
- Melakukan rotasi kekiri (shift left) sepanjang y terhadap x word yang ditandai dengan x<<< y. y merupakan interpretasi modulo w atau jumlah kata w dibagi 2. Dengan lg[w] ditentukan jumlah putaran yang dilakukan.
- Tahap akhir dilakukan penggabungan untuk mendapatkan data yang telah dienkripsi.

Proses dekripsi dilakukan dengan konsep dasar sebagai berikut :

- Data yang telah dienkripsi dikembangkan kembali menjadi 2 bagian dan disimpan di dua register A dan register B.
- Kemudian dilakukan rotasi ke kanan sejumlah r .
- Selanjutnya dilakukan operasi XOR yang ditandai dengan " ".
- Tahap akhir dilakukan pengurangan terhadap masing-masing register dengan key word yang ditunjukan dengan tanda "-", untuk mendapatkan plaintext.

b) Kelebihan dan Kekurangan RC-5

Adapun kelebihan dan kekurangan dari algoritma RC5 sebagai berikut [5]:

1. Kelebihan

- RC-5 menggunakan metode enkripsi simetrik, sehingga key yang sama digunakan untuk proses enkripsi dan dekripsi.
- RC-5 dapat diimplentasikan dengan hard ware ataupun soft ware, dimana RC-5 menggunakan dasar operasi komputasi yang biasa digunakan pada konsep dasar mikroprosesor.
- RC-5 mempunyai kemampuan proses enkripsi dan dekripsi yang cepat, besar nya kemampuan ini diperlihatkan dengan cara kerja beroreantasi pada kata (word).
- RC-5 dapat disesuaikan untuk bermacam-macam prosesor yang memiliki panjang bit data yang berbeda. Contohnya untuk prosesor 64 bit dapat dipakai untuk RC-5 dengan panjang kata yang diolah lebih panjang atau disesuaikan dengan kemampuan prosesor tersebut.
- RC-5 memiliki struktur yang iterative dengan variabel jumlah rotasi (putaran), sehingga pengguna secara eksplisit dapat memanipulasi trade off antara kecepatan dan tingkat keamanan.
- RC-5 mempunyai variabel panjang key word yang dapat divariasikan, sehingga pengguna dapat memilih tingkat keamanan yang dikehendaki sesuai dengan aplikasi yang digunakan.
- RC-5 sangat sedehana sehingga mudah untuk diimplementasikan dan membutuhkan memori yang kecil.

2. Kekurangan

- Semakin banyak jumlah kunci, maka semakin lama waktu yang dibutuhkan untuk memecahkan enkripsinya dan tingkat keamanan semakin tinggi.
- Semakin besar kapasitas file yang dienkripsi atau didekripsi maka semakin besar pula waktu proses enkripsi dan dekripsi

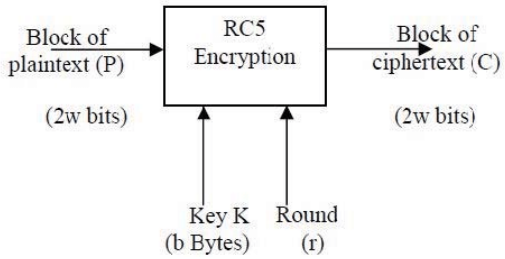
3. Metodologi Penelitian

Arsitektur Algoritma RC5

Seperti yang dijelaskan sebelumnya, algoritma RC5 adalah metode enkripsi yang menggunakan metode simetris dan pemrosesan dalam bentuk cipher blok, sehingga kata kunci yang sama digunakan untuk proses enkripsi dan dekripsi. Parameter yang digunakan dalam RC-5 adalah sebagai berikut:

1. Jumlah putaran(r) yang dilambangkan dengan r. Nilai yang digunakan sebesar 8,32 dan 64
2. Jumlah kata(w) dalam bit dilambangkan dengan w. Jumlah yang didukung adalah 16 bit, 32 bit, dan 64 bit.
3. Kata kunci (kata kunci) dilambangkan dengan b dengan jumlah 32 dan 64 bit

Di bawah arsitektur sederhana algoritma enkripsi RC5.



Gambar 1 Arsitektur algoritma enkripsi RC5

Ada 3 proses utama dalam RC5: ekspansi kunci, enkripsi dan dekripsi. Perluasan kunci adalah proses menghasilkan kunci secara internal dengan memanfaatkan komputasi rotasi kiri (<<<) dan rotasi kanan (>>>), panjang kunci tergantung pada jumlah round(r). Kunci internal kemudian digunakan dalam proses enkripsi dan dekripsi.

Proses enkripsi

Proses Enkripsi Diasumsikan bahwa ada dua blok input sama dengan w bit, A dan B. Dan itu diasumsikan juga bahwa kunci internal telah dibentuk, sehingga larik S [0 ... t-1] dihitung. Jadi pseudecode untuk proses enkripsi seperti di bawah ini:

```
A=A+S[0];
B=B+S[1];
for i=1 to r do
        A=((A ⊕B) <<< B) + S[2 * i];
        B=((B⊕A) <<< A) + S[2 * I + 1];
End for
```

Proses dekripsi

Proses dekripsi dilakukan oleh penerima data yang sudah dalam bentuk ciphertext. Proses ini dapat dilakukan dengan algoritma berikut:

```
for i= r downto 1 doB=((B – S [2 * i + 1]) >>> A) ⊕A;
        A=((A – S [2 * i]) >>> B) ⊕ B;
        End for
        B= B- S[1];
        A= A – S[0];
```

Data dari ciphertext diperluas menjadi dua bagian A dan B kemudian dikurangi dengan hasil ekspansi kunci dan diputar sebanyak r saat melakukan operasi XOR pada data. Tahap terakhir untuk mendapatkan plaintext adalah melakukan proses reduksi ke setiap bagian dengan hasil ekspansi kunci. Data-data ini kemudian digabungkan kembali untuk membentuk plaintext sesuai dengan pengirim atau data awal sebelum proses enkripsi.

Proses pembangkitan kata kunci

K [0-1] ... K [b] disalin ke tabel L [0-1] ... L [b] dengan aturan padding dengan karakter 0 hingga ukuran L [i] menjadi w / 2 bit.

Sebagai contoh:

K [0] = k L [0] = k000
K [1] = r L [1] = r000
K [2] = i L [2] = i000
K [3] = p L [3] = p000
K [4] = t L [4] = t000
K [5] = o L [5] = o000

Kemudian, inisialisasi tabel kunci internal KI dengan ukuran t = 2r + 2 sebagai berikut:

```
KI [0] ←P
for i ←1 to t - 1 do
KI [i] ←KI [i - 1]
Endfor
```

Algoritma pembentukan kunci internal menggunakan konstanta P dan Q yang diperoleh dari fungsi yang melibatkan bilangan irasional sebagai berikut:

P = Odd [(e - 2) 2w]
Q = Odd [(f - 1) 2w]

Catatan :

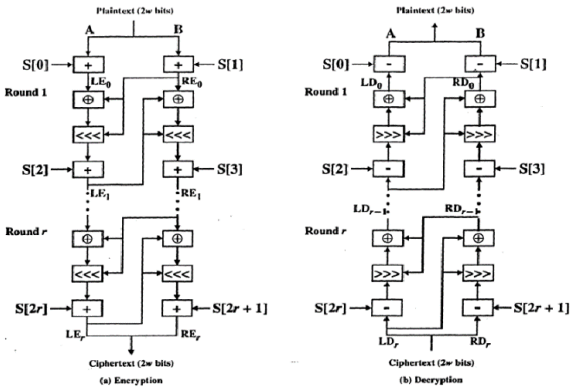
e = 2.718281828459.....
F = 1.618033988749.....

Kemudian L dan S dikombinasikan dengan algoritma berikut:

```
i ← 0
j ← 0
X ← 0
Y ← 0
n ← 3*max(r,c)
for k ← 1 to n do
        KI[i]←(KI[i] + X + Y)<<< 3
        X ← KI[i]
        i ← (i + 1) mod t
        L[j] ← (L[j] + X + Y)<<< 3
        Y ← L[j]
        j← (j + 1) mod c
endfor
```

catatan:

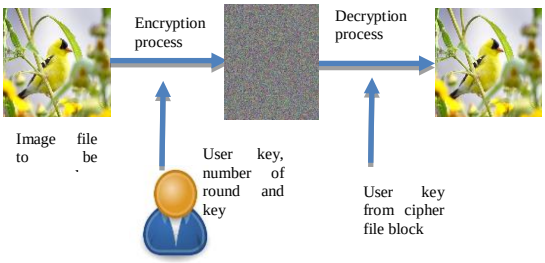
maks (r, c) adalah fungsi untuk menentukan jumlah terbesar antara r dan c. c adalah nilai maksimum panjang kunci b dibagi 4



Gambar 2 Diagram proses enkripsi dan dekripsi RC5

Desain sistem

Aplikasi yang dikembangkan menggunakan Android studio, pemrograman berbasis Java. Aplikasi akan berjalan di perangkat smartphone android. Pengguna akan menggunakan ponsel cerdas mereka untuk memasukkan gambar ke aplikasi. Pengguna juga memasukkan parameter RC5 seperti jumlah putaran dan jumlah kunci.



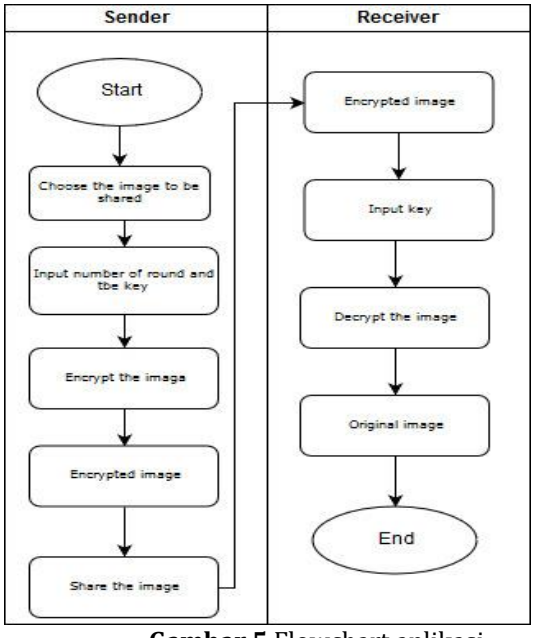
Gambar 3 Alur proses enkripsi dan dekripsi

Dalam fungsi file, proses diperlukan untuk membaca semua bit data gambar dan dikonversi ke blok data sesuai kebutuhan, sehingga algoritma RC5 dapat diimplementasikan untuk mengenkripsi dan mendekripsi file. Ada dua input ke fungsi enkripsi, yaitu gambar bit yang dikonversi untuk dienkripsi dan kunci rahasia yang diperluas. Kunci rahasia diperluas, diturunkan dari kunci rahasia yang disediakan pengguna pada proses pembuatan kata kunci.

6D	FA	82	C4	B4	CD	BF	1F	65	27	46	DA	1A	71	5A	23	17	03	B6	CC
BB	55	CD	7E	2D	6F	CB	AF	AC	48	28	9C	12	C6	3B	A8	D9	16	12	BB
1F	C0	D1	4A	E3	A3	15	48	AF	71	C5	83	90	FF	C4	0A	F8	E7	D9	EC
80	15	2B	AE	BA	1F	B3	57	CD	B4	CD	02	ED	02	1F	8C	89	60	D2	8B
4F	84	CE	86	1D	F2	CA	73	A8	43	83	5D	DC	0F	4A	67	D4	0A	8A	3B
A1	8F	CF	6A	21	7A	09	29	51	9D	AC	A9	FA	15	2B	B4	DB	F3	0F	71
1C	0E	31	B4	B9	48	B8	35	90	26	5B	BF	CA	44	A7	7B	2C	05	07	F6
2A	D4	29	26	CF	AF	4E	39	56	F8	B4	53	1E	45	78	84	FB	9F	67	A3

Gambar 4 Contoh nilai bit heksadesimal dalam gambar

Proses enkripsi dan dekripsi pada algoritma RC5 tidak dapat dipisahkan dari pembentukan kunci internal KI []. Kunci internal adalah kunci yang berbentuk tabel yang digunakan untuk melakukan proses enkripsi dan dekripsi. Kunci ini dibentuk dari pengguna yang diinput dan diubah menjadi bentuk array. Dalam pembentukan kunci diperlukan konstanta P32 = b7e15163 dan Q32 = 9e3779b9 dengan panjang kata 32 bit. Pembentukan tabel kunci dimulai dari tabel inisialisasi KI [] dan diakhiri dengan pencampuran dua array kunci. Hasil akhir dalam tabel KI [] adalah kunci internal untuk digunakan dalam proses enkripsi dan dekripsi. Di bawah ini adalah aliran dokumen dari sistem yang dikembangkan:



Gambar 5 Flowchart aplikasi

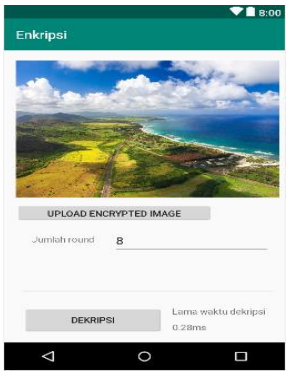
4. Hasil dan Pembahasan

Proses enkripsi mengambil gambar yang diunggah oleh pengguna sebagai input dan menghasilkan gambar sandi sebagai output.

Gambar pertama dikonversi ke nilai heksadesimal. Aliran data gambar dibagi menjadi 2 bit, di mana w adalah jumlah kata yang digunakan. Blok gambar 2w-bit pertama dimasukkan sebagai gambar biasa ke proses enkripsi algoritma RC5. Kemudian, blok gambar polos 2w-bit berikutnya mengikutinya, dan seterusnya dengan jalur pemindaian sampai akhir aliran bit data gambar. Proses ekspansi kunci, harus sudah proses sebelum enkripsi dapat dilakukan. Perluasan kunci ini juga digunakan dalam proses dekripsi. Kunci rahasia ini diterapkan secara terbalik. Kami menggunakan blok file sandi ini untuk mengirimkan melalui jaringan seluler:

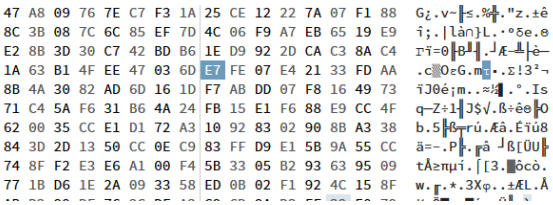
Gambar 6 Susunan blok file yang direncanakan

Hasil penelitian ini akan diuji menggunakan smartphone Android dengan spesifikasi Prosesor quad core 1.0Ghz, RAM 2 GB dan sistem operasi Android versi 5.1. Di bawah antarmuka pengguna aplikasi yang berjalan di smartphone android.



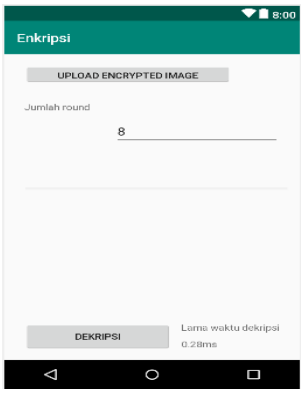
Gambar 7 Aplikasi enkripsi

Setelah proses enkripsi dijalankan, akan diperoleh hasil file enkripsi berupa nilai hexadesimal seperti berikut :



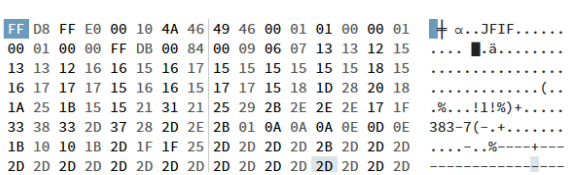
Gambar 8 Gambar asli dan hasil enkripsinya

Proses enkripsi dengan nilai round sebesar 16, sudah merubah struktur file gambar sehingga tidak bisa dikenali lagi. Tidak ada informasi visual yang diamati dalam gambar terenkripsi, dan gambar terenkripsi secara visual tidak dapat dibedakan bahkan dengan perbedaan besar sehubungan dengan gambar asli. Kesalahan dalam memasukkan kunci dalam proses enkripsi akan menyebabkan file menjadi rusak. Untuk mengembalikan file ke bentuk aslinya, proses dekripsi diperlukan yang merupakan kebalikan dari proses enkripsi, di mana proses akan mengembalikan nilai dan struktur bit data dalam file ke dalam bentuk aslinya. Proses mengembalikan data ke aplikasi keamanan data pada file memerlukan kunci yang tepat untuk dapat mengkonversi file ke bentuk aslinya.



Gambar 9 Aplikasi dekripsi

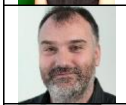
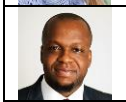
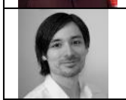
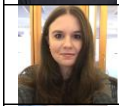
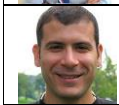
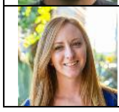
Setelah proses dekripsi dijalankan, akan diperoleh hasil file dekripsi berupa nilai hexadesimal file aslinya sebelum dilakukan proses enkripsi seperti berikut



Gambar 10 Nilai heksadesimal file hasil dekripsi

Berikut hasil lengkap percobaan yang dilakukan pada 20 gambar uji yang dimasukkan pada aplikasi mobile :

Tabel 1 Hasil percobaan enkripsi – dekripsi

Gambar asli	Hasil enkripsi	Hasil dekripsi/asli
	22 BF A7 5C 05 53 5F 98 E0 09 72 C7 63 8B FC FF 4C A5 BE EB B4 A6 FB 1A 8B E0 2F CB B2 53 13 3F BA 34 BB FA BF 1B 10 A1	49 46 00 01 01 01 00 48 α..JFIF.....H 45 78 69 66 00 00 49 49 .H.. ß.4Exif..II 98 82 02 00 10 00 00 00 52 6F 64 69 6E 20 45 63 ....Rodin.Ec 00 00 FF ED 00 5E 50 68 kenroth... φ.^Ph
	2C BA 84 64 A5 62 69 0D F8 05 F2 00 8C A2 8F 4C 58 0D 5E E7 CC B1 3C F5 B7 9F 67 CC 2D 99 7E D4 4E BA 3A 96	00 01 01 00 00 01 α..JFIF...... 45 41 54 4F 52 3A .... ..;CREATOR: 31 2E 30 20 28 75 .gd-jpeg.v1.0.(u 50 45 47 20 76 38 sing.IJG.JPEG.v8 79 20 3D 20 37 35 0),.quality.=.75 06 05 08 07 07 07 . .C..........
	[illegible]	[illegible]
	[illegible]	[illegible]
	[illegible]	[illegible]
	[illegible]	[illegible]
	[illegible]	[illegible]
	[illegible]	[illegible]
	[illegible]	[illegible]
	[illegible]	[illegible]
	[illegible]	[illegible]
	[illegible]	[illegible]
	[illegible]	[illegible]
	[illegible]	[illegible]
	[illegible]	[illegible]
	[illegible]	[illegible]
	[illegible]	[illegible]
	[illegible]	[illegible]
	[illegible]	[illegible]
	[illegible]	[illegible]

Dalam penelitian ini, kami juga mengukur kecepatan pemrosesan, selain keamanan gambar yang dihasilkan. Waktu yang diperlukan untuk melakukan proses enkripsi dan dekripsi tergantung pada nilai parameter RC5 (w / r / b) yang digunakan. Jika keamanan tambahan diinginkan dalam mengirim gambar tetapi tidak masalah dengan waktu pemrosesan enkripsi dari gambar, maka tidak masalah untuk memilih nilai dari setiap parameter yang cukup tinggi. Dalam proses enkripsi dengan jumlah kunci yang berubah nilainya, waktu rata-ratanya adalah 70 ms. Sedangkan proses enkripsi dengan nilai jumlah kunci bervariasi, rata-rata waktunya 125,2 ms. Dengan berbagai nilai putaran, dibutuhkan rata-rata 1352,2 ms.

5. Kesimpulan dan Saran

1. Kesimpulan

Penggunaan algoritma RC5 untuk mengenkripsi gambar pada telepon pintar adalah fitur yang baik. Implementasi algoritma enkripsi RC5 adalah algoritma enkripsi yang cukup aman dan memiliki kinerja tinggi, terbukti dari hasil file enkripsi yang sama sekali tidak bisa terbaca.

Berdasarkan hasil percobaan, penggunaan parameter pada algoritma RC5 benar-benar memberi pengguna fleksibilitas untuk memilih pertukaran antara kinerja dan keamanan. Parameterisasi juga memungkinkan RC5 menjadi lebih aman dengan meningkatkan jumlah nilai parameternya.

Algoritma RC5 dapat diimplementasikan dalam proses enkripsi bit data dalam file dengan

benar karena prosesnya ringan dan cepat sehingga akan menghemat waktu dan sumber daya, dalam mengenkripsi file yang memiliki ukuran data yang cukup besar.

Dari hasil percobaan terbukti bahwa kecepatan untuk mendapatkan keamanan yang lebih tinggi dengan merubah nilai putaran(round) pada enkripsi RC5 membutuhkan waktu enkripsi dan dekripsi dengan nilai rata-rata sebesar 1352,2 ms baik pada emulator maupun pada ponsel. Dimana nilai putaran menentukan tingkat kompleksitas algoritma RC5. Semakin tinggi nilai parameter putaran/w, maka semakin kompleks pula algoritmanya.

2. Saran

Adapun saran yang bisa disampaikan dari penelitian ini yaitu diperlukan penelitian lebih lanjut sehingga aplikasi ini dapat diadaptasi di Facebook atau Whatsapp melalui Application Programming Interface / API dari masing-masing aplikasi tersebut.

Daftar Pustaka:

1) Bambang Siswoyo, Benny kadarisman, "Analisis Dan Implementasi Sistem Keamanan Data Pada Pocket Pc Menggunakan Metode Enkripsi Algoritma Rc-4" . Jurnal Computech & Bisnis. Vol. 4, Juni 2010.
2) Ashwaq T. Hashim, Dr. Rasha Fahim Nathim, and Gaidaa Saeed Mahdi. "Modification of RC5 Algorithm for Image Encryption" IJCCCE Vol.14, No.2, 2014.
3) Sayekti Harits Suryawan, Hamdani, "Pengamanan Data File Dengan Menggunakan Algoritma Enkripsi Rivest Code 5," Jurnal Informatika Mulawarman Vol. 8 No. 2 Edisi Juli 2013 44.
4) Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, "Implementation of RC5 Block Cipher Algorithm for Image Cryptosystems", International Journal of Computer and Information Engineering Vol:1, No:8, 2007.
5) R.Sateesh Kumar, I.Navakanth, "Digital Image Encryption Based on the RC5 Block Cipher Algorithm", International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-6, June 2016.
6) Swathi Suresh, Mary Varghese and Aju D, "An Efficient and Optimized RC5 Image Encryption Algorithm for Secured Image Transmission", International Journal of Imaging and Robotics, Volume 15, Issue No. 3, Year 2015.
7) Imtihan, K., & Basri, M. H. (2019). SISTEM INFORMASI PEMBUATAN MANIFEST MUATAN KAPAL BERBASIS DEKSTOP DAN ANDROID. *Jurnal Manajemen Informatika dan Sistem Informasi*, *2*(2), 69-76.
8) Sentot Kromodimoeljo, "Teori dan Aplikasi Kriftografi", SPK IT Consulting, 2009.
9) Dwiky Andika, "Pengertian dan Sejarah Kriptografi", [Online]. Tersedia: https://www.it-jurnal.com/pengertian-dan-sejarah-kriptografi/ [Diakses 30 September 2019].
10) Agus Gunawan. "Analisis Penggunaan Algoritma RSA untuk Enkripsi Gambar dalam Aplikasi Social Messaging" Makalah IF2120 Matematika Diskrit ITB, 2016.