JURNAL SISFOTENIKA
Vol. 10 No. 1, Januari 2020
p-ISSN: 2087-7897 ; e-ISSN : 2460-5344
DOI : 10.30700/jst.v10i1.948

Perancangan Perangkat Lunak Enkripsi SMS Menggunakan Algoritma RC6 Dan Rijndael Pada Smartphone

SMS Encryption Software Design Using RC6 and Rijndael Algorithms on Smartphones

Gusti Syarifudin, Benny Djoede Kristianto, Gat
STMIK Pontianak; Jln. Merdeka Barat No. 372 Pontianak, (0561)73555/(0561)737777
Jurusan Teknik Informatika, STMIK Pontianak
e-mail: **gus_wet@yahoo.com, bennydjoede87@gmail.com, gutsy1802@gmail.com**

Abstrak

Proses pengiriman pesan teks yang dilakukan pada perangkat smartphone pada dasarnya pengiriman pesan teks tersebut tanpa ada melakukan pengamanan terhadap isi pesan yang dikirim, sehingga ketika dilakukan penyadapan terhadap alur pengirimanya maka pesan teks yang disadap dapat langsung dibaca oleh penyadap. Untuk itu dibutuhkan perangkat lunak sebagai penunjang metode penyandian tertentu sehingga pesan terkirim tersebut menjadi lebih aman. Penelitian ini menggunakan bentuk penelitian studi literature dengan metode penelitian menggunakan Research & Development (R&D). Adapun teknik pengumpulan data menggunakan studi dokumentasi dan observasi untuk memperoleh teori algoritma rc6 dan algoritma rijndael. Sedangkan metode perancangan perangkat lunak menggunakan Rapid Application Development (RAD). Perancangan perangkat lunak menggunakan bahasa pemrograman java . Hasil perancangan ini menghasilkan sebuah perangkat lunak yang diberi nama "Enkripsi Sms" . Perangkat lunak enkripsi sms menggunakan algoritma rc6 dan rijndael telah dijalankan dan sesuai dengan yang diharapkan pengguna. Dengan adanya perangkat lunak ini, kerahasian dan keaslian informasi berupa pesan teks akan lebih terjaga.

Kata Kunci : Enkripsi Sms, Algoritma RC6, Algoritma Rijndael, Java, RAD.

Abstract

Sending text messages is done on a smartphone device is basically the text message delivery without doing a safeguard against the content of the messages sent, so that when it is done tapping against the Groove pengirimanya then intercepted text messages can be directly read by the tappers. For that it needs the software as a specific encoding method support so that the message sent is secure. This research uses the form of research studies, literature research method using Research & Development (R & D). As for the technique of data collection using the study documentation and observation to acquire the theory and algorithm rijndael rc6 algorithm. While the method of software design using Rapid Application Development (RAD). The design of software using the java programming language. The results of this design generates a software named "Sms Encryption". Encryption software sms using the rc6 algorithm and rijndael has been executed and in accordance with the expected user. With the

software, the confidentiality and authenticity of the information in the form of a text message will be more awake.

.

Keywords: Sms Encryption, RC6 Algorithms , Rijndael Algorithm, RC6, Java, RAD.

1. PENDAHULUAN

Perkembangan teknologi telekomunikasi yang ada pada saat ini mampu menciptakan berbagai macam perangkat keras yang dapat digunakan untuk mengirim atau menerima informasi dengan cepat dan mudah. Penggunaan *smartphone* sebagai device akses informasi telah berkembang pesat pada era ini. Terlebih lagi, banyak fitur-fitur aplikasi yang disediakan oleh android sebagai system operasi ponsel. Dari sekian banyak fitur yang dimiliki oleh android, salah satunya yang masih banyak digunakan yaitu SMS. Namun, seringkali pengguna kurang memperhatikan system keamanan data yang ada pada ponsel tersebut khususnya keamanan informasi yang ada di pesan singkat[1].

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama yang hanya boleh diketahui oleh pihak yang berhak saja. Layanan SMS yang menggunakan aplikasi SMS bawaan ponsel bukan merupakan jalur yang aman dalam pertukaran informasi. Pesan yang dikirim menggunakan aplikasi SMS bawaan ponsel masih berupa teks terbuka yang belum terproteksi selain itu pengiriman SMS yang dilakaukan tidak sampai secara langsung ke penerima, akan tetapi pengiriman SMS harus melewati *Short Message Service Center (SMSC)* yang berfungsi mencatat komunikasi yang terjadi antara pengirim dan penerima. Tersimpannya SMS pada SMSC, maka seorang operator mungkin pihak lain tidak berhak mengetahui informasi tersebut dapat memperoleh informasi atau membaca SMS didalam SMSC. Tersimpannya SMS pada SMSC, maka seorang operator mungkin pihak lain tidak berhak mengetahui informasi tersebut dapat memperoleh informasi atau membaca SMS didalam SMSC [2].

Ada beberapa metode yang bisa digunakan dalam keamanan informasi adalah kriftografi. Salah satu ilmu kriptografi yaitu algoritma simetris atau sering disebut algoritma kriptografi konvensional adalah algortima yang menggunakan kunci yang sama untuk proses enkripsi dan proses dekirpsi. Supaya pertukaran kunci simetrik aman pada jalur public maka dibutuhkan suatu protocol untuk pertukaran kunci. Supaya pertukaran kunci simetrik aman pada jalur public maka dibutuhkan suatu protocol untuk pertukaran kunci [3].

Pada penelitian ini menggunakan dua algoritma yang berbeda yaitu RC6 dan Rijndael yang digunakan dalam melakukan proses enkripsi maupn dekrispi serta ditambahkan informasi karakter yang terdapat pada pesan tersebut dengan format heksadesimal agar informasi lebih terbaca, perancangan *user interface* yang menarik serta penggunaan aplikasinya bisa diterapkan kedalam perangkat lunak *smartphone* dengan android versi 4.4 kitkat, fitur android kitkat yang cukup bannyak dan telah diperbaharui dari versi sebelumnya membuat android versi ini banyak digunakan, namun spesifikasi android kitkat dengan android lainya tidak jauh beda, hanya saja ada beberapa bug atau celah yang telah ditambal dan mendapat berbagai update baru, baik dari segi tampilan android kitkat itu sendiri hingga fitur-fitur dan fungsinya[4].

Penggunaan dua algortima RC6 dan Rijndael ini dilakukan demi memperkuat keamanan pesan teks, kedua algortima RC6 dan Rijndael termasuk kedalam algoritma blok cipher. Pada RC6 kode yang sangat pendek merupakan sebuah kemampuan tersendiri dari algoritma ini sangat sepadan apabila diimplementasikan kedalam

lingkungan smart card. Sedangkan pada Rijndael memiliki kemampuan untuk berkerja sangat baik untuk *platform* apapun. Ditambah dengan operasi yang menggunakan *table lookup* dan operasi XOR membuat prosesnya menjadi tidak terlalu rumit[5].

2. METODE PENELITIAN

Dalam penelitian ini penulis menggunakan metode penelitian *Research & Development* (R&D). R&D adalah "Metode penelitian yang digunakan untuk menghasilkan produk tertentu, dan menguji keefektifan produk tersebut". Produk tersebut tidak selalu berbentuk benda atau perangkat keras (*hardware*), seperti buku, alat tulis, dan alat pembelajaran lainnya. Akan tetapi dapat pula dalam bentuk perangkat lunak (*software*) seperti program pengolah data, pembelajaran di kelas, perpustakaan atau laboratorium, atau model – model pendidikan pembelajaran pelatihan, bimbingan, evaluasi, manajeman dan lain sebagainya [6].

2.1 Metode Pengumpulan Data

Adapun jenis data yang digunakan penulis dalam penelitian ini yaitu, sebagai berikut:

a.Data primer

merupakan sumber data yang diperoleh secara langsung dari sumber asli atau pihak pertama. Data primer secara khusus dikumpulkan oleh peneliti untuk menjawab pertanyaan riset atau penelitian. Data primer dapat berupa pendapat subjek riset (orang) baik secara individu maupun kelompok, hasil observasi terhadap suatu benda (fisik), kejadian, atau kegiatan, dan hasil pengujian.

b.Data sekunder

Data sekunder adalah data yang tidak didapatkan secara langsung dari objek penelitian, melainkan sumber data yang diperoleh peneliti secara tidak langsung melalui media perantara. Data sekunder pada umumnya berupa bukti, catatan, atau laporan historis yang telah tersusun dalam arsip, baik yang dipublikasikan dan yang tidak dipublikasikan. Data sekunder antaralain disajikan dalam bentuk tabel-tabel, diagram-diagram, atau mengenai topik penelitian.

2.2 Teknik Pengumpulan Data

Teknik pengumpulan data adalah cara-cara yang dilakukan untuk mencari, mengumpulkan dan memperoleh data untuk digunakan dalam melakukan penelitian, baik itu data yang diperoleh dengan servei langsung maupun dengan penggalian informasi. Teknik pengumpulan data merupakan langkah yang paling strategis dalam penelitian, karena tujuan utama dari penelitian ini adalah mendapatkan data. Untuk memperoleh data dan informasi dalam penelitian ini, penulis menggunakan teknik pengambilan data sebagai berikut :

a. Studi Dokumentasi

Teknik dokumentasi berupa studi keputusan dan kajian dari buku-buku, jurnal-jurnal pendukung (*hardcopy dan software*), literatur dari internet dan sejumlah dokmen mengenai data variabel yang perlukan.

b. Observasi

Pada penelitian ini observasi yang dilakukan dengan pengamatan langsung mengumpulkan data mengenai dokumentasi yang mengacu pada instrumen pengamatan yang berisi definisi-definisi dari item-item data. Melakukan kajian letretur yang berkaitan dengan penelitian yang dilakukan, pengumpulan data yang diperoleh dari sumber tertulis seperti: literatur artikel, berbagai websait, dan tulisan ilmiah yang dianggap terkait dan relevan dengan topik penelitian

2.3 Pengembangan Perangkat Lunak RAD

Penulis mengunakan metode perancangan RAD (*Rapid Application Developement*) karena peroses perkembangan perangkat lunak ini menekankan pada siklus perkembangan yang singkat dan pemanfaatan fungsi yang telah ada sebelumnya. Adapun langka-langkah yang dilakukan penulis yaitu[7]:

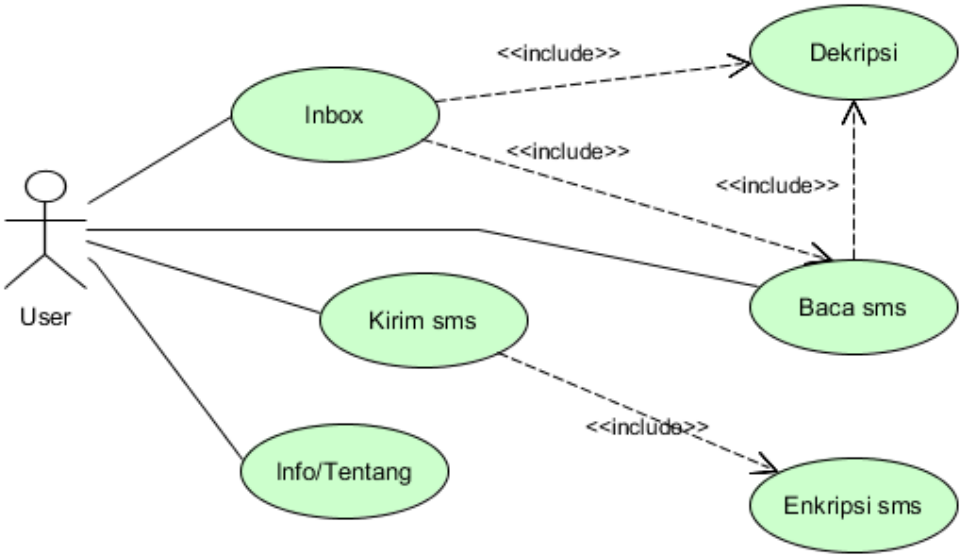
a. *Business Modeling*. Pada tahap ini, penulis mendaftarkan dan mendefinisikan fungis-fungsi yang akan dipakai dalam pembuatan aplikasi.
b. *Data modeling*. Penulis mengunakan informasi yang didapat dalam tahap diatas untuk menentukan banyaknya modul dan form yang akan digunakan dalam program tersebut. Jumlah komponen yang terdapat dalam setiap modul dan form akan ditentukan juga.
c. *Process Modeling*. Form dan modul yang sudah didefinisikan sebelumnya beserta komponennya disatukan untuk menentukan suatu program untuk. Hubungan antara modul dengan form juga didefinisikan oleh penulis.
d. *Application Generation.* Penulis membangun aplikasi enkripsi sms pengaman pesan teks dengan mengunakan algortima RC6 dan Rijndael ini mengunakan program *Eclipse*.
e. *Testing and turnover.* Setelah modul dirancang ke dalam program tersebut penulis melakukan testing pada form yang membuat modul tersbut. Setelah setiap modul dan form terbentuk dan diuji, semua modul dan form tersebut kemudian disatukan dan dilakukan pengujian kembali akan integritasnya, termasuk didalamnya pengujian validasi input tiap form.

2.4. Unified Modeling Language (UML)

Unified Modeling Language (UML) sebagai media untuk menampilkan grafik atau gambar untuk menvisualisasikan, menspesifikasikan, membangun dan pendokumentasian dari sebuah sistem pengembangan perangkat lunak[8].

2.4.1 Use Case Diagram

Use case diagram enkripsi SMS menceritakan tentang user yang menggunakan aplikasi ini secara optional bisa memilih untuk mengakses menu sesuai dengan yang diinginkan.

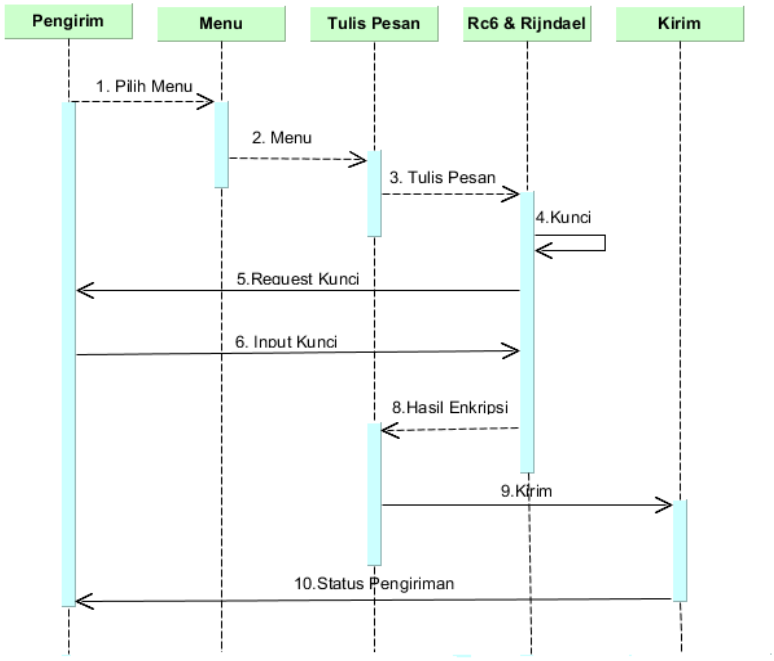


Gambar 1. Use Case Diagram

2.4.2 Sequence Diagram

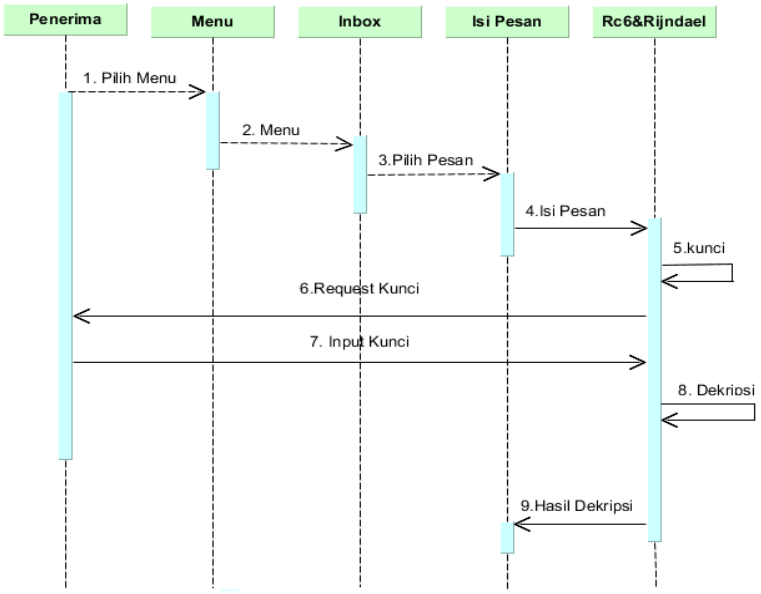
Diagram *Sequence* menggambarkan interaksi antar objek didalam dan disekitar sistem (termasuk *user*, display, dan sebagainya) berupan *message* yang digambarkan terhadap waktu. *Sequence* diagram terdiri antar dimensi vertical (waktu) dan dimensi horizontal (objek-objek terkait).

Gambar berikut ini terlihat pengirim memilih menu tulis pesan. Setelah menulis pesan dipilih sistem kemudian memanggil fungsi tulis pesan. Setelah pesan ditulis, proses selanjutnya adalah *user* diminta memasuki kunci enkripsi pada fungsi Rc6 dan Rijndael maka hasil enkripsi akan tampil pada fungsi tulis pesan pengiriman.



Gambar 2. Sequence Diagram Tulis Pesan

Sequence diagram baca sms di bawah ini penerima memilih menu inbox yang berisi pesan, kemudian dari inbox yang berisi pesan dibuka maka sistem meminta untuk *user* memasukan kunci yang sama dengan kunci enkripsi pada fungsi Rc6 dan Rijndael, setelah *user* memasukan kunci maka sistem melakukan proses dekripsi yang kemudian hasil pesan akan tampil pada fungsi isi pesan yang dapat dibaca oleh penerima.



Gambar 3. Sequence Diagram Baca Pesan

3. HASIL DAN PEMBAHASAN

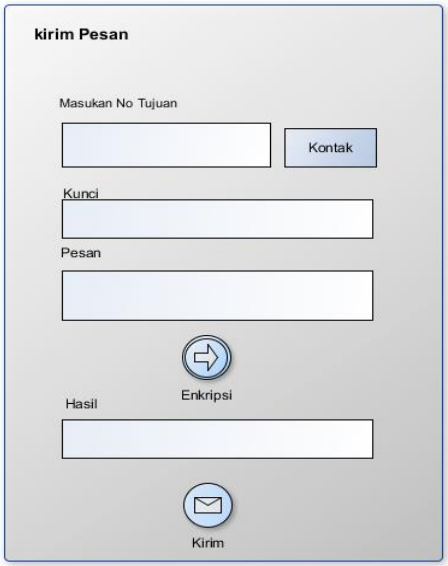
3.1 Perancangan Form Menu

Pada form menu ini terdapat tiga button yang memiliki fungsi masing-masing yaitu, button Tulis pesan berfungsi untuk menuju activity tulis pesan. button kotak masuk berfungsi menuju activity Inbox. Sedangkan button info berfungsi menuju activity info

Gambar 4. Perancangan Form Menu

3.2 Perancangan Form Kirim Pesan

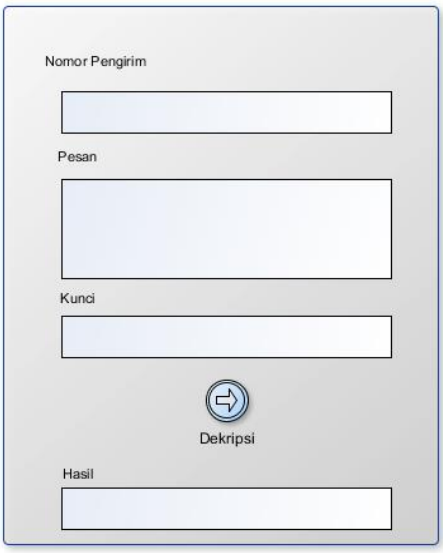
Rancangan interface yang ada pada form kirim pesan terdiri dari beberapa button yang memili fungsi melakukan import berdasarkan kontak yang ada pada smartphone yang digunakan, serta melakukan proses pengiriman pesan yang telah di enkripsi.



Gambar 5. Perancangan Form Kirim Pesan

3.3 Perancangan Form Pesan Masuk

Rancangan interface yang ada pada form pesan masuk terdiri dari button dekripsi yang memili fungsi melakukan proses membuka pesan yang di enkrpsi serta menampilkan hasil dari enkripsi pesan tersebut.



Gambar 6. Perancangan Form Pesan Masuk

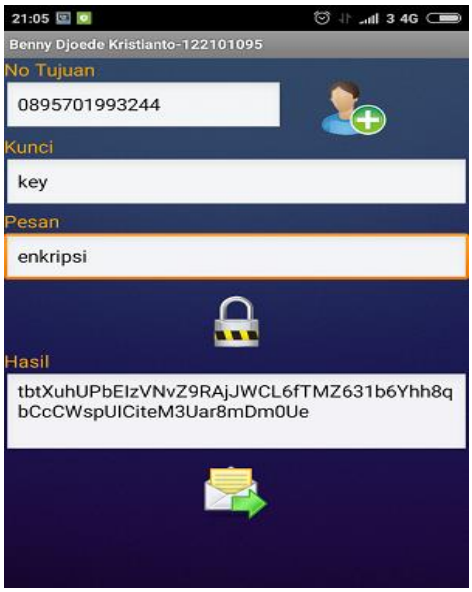
3.5 Tampilan Menu Utama

Dari tampilan menu utama dari perangkat lunak Enkripsi SMS ini terdapat beberapa button untuk masuk ke form lain. Menu Utama akan tampil pada saat pertama aplikasi dijalankan. Berikut merupakan tampilan dari form beranda

Gambar 7. Tampilan Menu Utama

3.6 Tampilan Menu Tulis Pesan/Enkripsi

Tampilan menu Tulis Pesan akan muncul, setelah user menekan button Tulis Pesan pada form Menu Utama, form Tulis Pesan berfungsi sebagai form untuk melakukan proses enkripsi sms serta melakukan pengiriman pesan. Berikut merupakan tampilan dari form Tulis Pesan.



Gambar 8. Tampilan Menu Tulis Pesan/Enkripsi

3.7 Tampilan Menu Baca Pesan/Dekripsi

Tampilan menu Baca Pesan akan tampil ketika user menekan button Baca Pesan pada form Menu Utama, form ini berfungsi untuk membaca pesan masuk dan melakukan proses dekripsi pesan. Berikut merupakan tampilan dari form Baca Pesan

.

Gambar 9. Tampilan Menu Baca Pesan/Dekripsi

3.8 Pengujian Pengujian Keamanan Berdasarkan *Avalanche Effect*

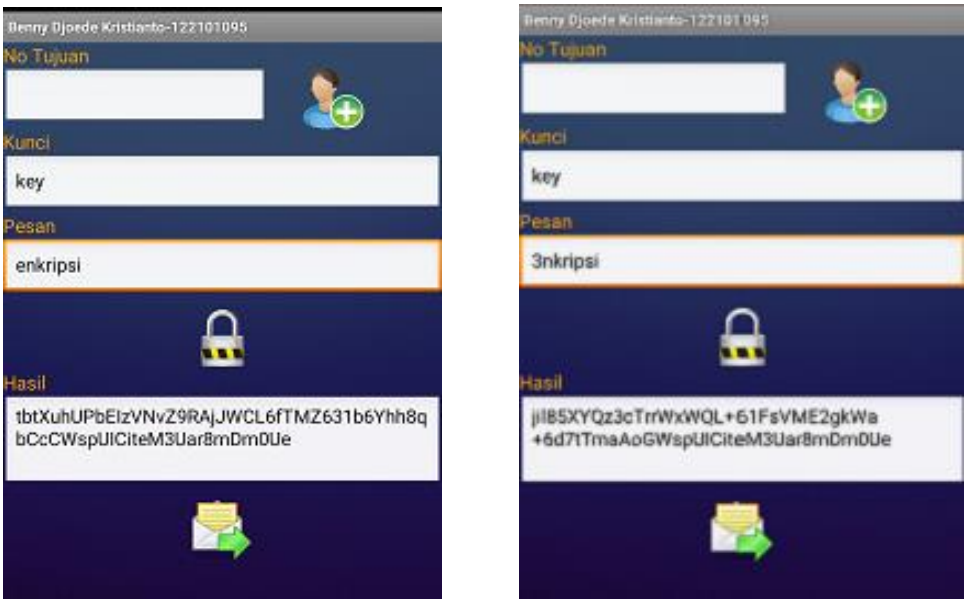
Salah satu karakteristik untuk menentukan baik atau tidaknya suatu algoritma kriptografi adalah dengan melihat avalanche effect-nya. Perubahan yang kecil pada *plainteks* maupun *key* akan menyebabkan perubahan yang signifikan terhadap cipherteks yang dihasilkan. Atau dengan kata lain, perubahan satu bit pada palintext maupun key akan menghasilkan perubahan banyak bit pada cipherteks.

Suatu avalanche effect dikatakan baik jika perubahan bit yang dihasilkan berkisar antara 45-60% (sekitar separuhnya, 50 % adalah hasil yang sangat baik). Hal ini dikarenakan perubahan tersebut berarti membuat perbedaan yang cukup sulit untuk kriptanalis melakukan serangan. Avalanche effect dihitung dengan rumus :

$$Avalanche\ effect = \frac{\text{Jumlah bit yang berubah}(Chipertext)}{\text{Jumlah Bit}(Chipertext)} \text{ x } 100\%$$

Pengujian dilakukan dengan evaluasi performa ke-1:

Pada langkah pertama dilakukan pengujian dengan menguji perubahan 1 bit pada *plaintext* yang digunakan adalah “enkripsi” dan “3nkripsi” dengan kunci sama yaitu “key” seperti tampak pada Gambar 3.5 berikut ini :



Gambar 10. Enkripsi Pengujian Evaluasi Pertama

Plaintext 1 : enkripsi
Plaintext 2 : 3nkripsi
Kunci : key
Ciphertext 1 :
tbtXuhUPbEIzVNvZ9RAjJWCL6fTMZ631b6Yhh8qbCcCWspUICiteM3Uar8mDm0Ue
Dalam biner adalah sebagai berikut :
1110100 1100010 1110100 1011000 1110101 1101000 1010101 1010000 100010 1000101 1101100 1111010 1010110 1001110 1110110 1011010 0111001 1010010 1100001 1101010

1001010 1010111 1000011 1001100 0110110 1110010 1010100 1001101 1011010 0110110 0110011 0110001 1000010 0110110 1011001 1101000 1101000 0111000 1010001 1000010 1000011 1100011 1000011 1010111 1110011 1110000 1010101 1101100 1000011 1101001 1110100 1100101 1001101 0110011 1010101 1100001 1110010 0111000 1101101 1100100 1101101 0110000 1010101 1100101

Ciphertext 2 :

jil85XYQz3cTrrWxWQL+61FsVME2gkWa+6d7tTmaAoGWspUICiteM3Uar8mDm0Ue.

Dalam biner dalah sebagai berikut :

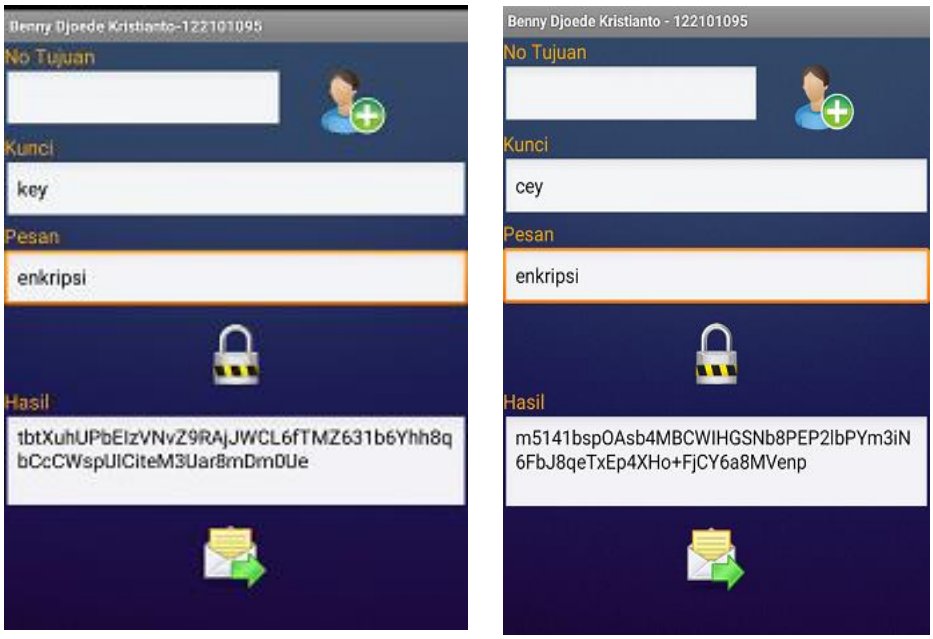
1101010 1101001 1101100 0111000 0110101 1011000 1011001 1010001 1111010 0110011 1100011 1010100 1110010 1110010 1010111 1111000 1010111 1010001 1001100 01010110110110 0110001 1110010 1110011 1010110 1001101 1000101 0110010 1100111 1101011 1010111 1100001 0101011 0110110 1100100 0110111 1110100 1010100 1101101 1100001 1000001 1101111 1000111 1010111 1110011 1110000 1010101 1101001 1000011 1101001 1110100 1100101 1001101 0110011 1010101 1100001 1110010 0111000 1101101 1100100 1101101 0110000 1010101 1100101

140/448*100%=31.25 %

Dari hasil penujian diatas tampak bahwa perbedaan kunci satu bit pada plaintext menghasilkan perbedaan bit sebesar 140 dari total 448 bit atau sekitar 31.25 %.

Pengujian dilakukan dengan evaluasi performa ke-2:

Pada langkah Kedua dilakukan pengujian dengan menguji perubahan 1 bit pada kunci pesan yang digunakan adalah plaintext “enkripsi” dengan kunci berbeda yaitu “key” dan “cey”seperti tampak pada Gambar 3.6 berikut ini.



Gambar 11. Enkripsi Pengujian Evaluasi ke Dua

Plaintext 1 : enkripsi
Kunci 1: key
Plaintext 2 : enkripsi

Kunci 2: cey
Ciphertext 1 :
tbtXuhUPbEIzVNvZ9RAjJWCL6fTMZ631b6Yhh8qbCcCWspUICiteM3Uar8mDm0Ue
Dalam biner adalah sebagai berikut:
1110100 1100010 1110100 1011000 1110101 1101000 1010101 1010000 100010 1000101
1101100 1111010 1010110 1001110 1110110 1011010 0111001 1010010 1100001 1101010
1001010 1010111 1000011 1001100 0110110 1110010 1010100 1001101 1011010 0110110
0110011 0110001 1000010 0110110 1011001 1101000 1101000 0111000 1010001 1000010
1000011 1100011 1000011 1010111 1110011 1110000 1010101 1101100 1000011 1101001
1110100 1100101 1001101 0110011 1010101 1100001 1110010 0111000 1101101 1100100
1101101 0110000 1010101 1100101
Ciphertext 2 :
m5141bspOAsb4MBCWIHGSNb8PEP2lbPYm3iN6FbJ8qeTxEp4XHo+FjCY6a8MVenp
Dalam biner adalah sebagai berikut :
1101101 0110101 0110001 0110100 0110001 1100010 1110011 1110000 1001111 1000001
1110011 1100010 0110100 1001101 1000010 1000011 1010111 1010111 1001000 1000111
1010011 1001110 1100010 0111000 1010000 1000101 1010000 0110010 1101100 1100010
1010000 1011001 1101101 0110011 1101001 1001110 0110110 1000110 1100010 1001010
0111000 1010001 1100101 1010100 1111000 1000101 1010000 0110100 1011000 1001000
1001111 0101011 1000110 1101010 1000011 1011001 0110110 1100001 0111000 1001101
1010110 1100101 1101110 1110000

232/448*100%= 51.78%

Dari hasil penujian diatas tampak bahwa perbedaan kunci satu bit pada kunci menghasilkan perbedaan bit sebesar 232 dari total 448 bit atau sekitar 51.78 %.

3.6 Pengujian *Heap Memory*

Heap memory merupakan porsi dari *memory* yang dialokasikan secara dinamis. Untuk menyediakan pengalaman user yang stabil, penting untuk aplikasi tidak begitu banyak mengambil porsi *memory* [7].

Gambar 13. Pengujian *Heap Memory* dengan *ADV*

4 KESIMPULAN

Setelah melalui proses penyelesaian skripsi yang berjudul "Perancangan dan Pengujian Perangkat Lunak Enkripsi SMS Menggunakan Algoritma RC6 Dan Rijndael Pada Smartphone Android", penulis menarik kesimpulan sebagai berikut :

a. Penggunaan kedua algoritma RC6 dan Rijndael sebagai algoritma enkripsi memperlihatkan sebuah avalanche effect yang baik. Hasil yang ditunjukan ini sesuai dengan parameter yang ditetapkan yaitu 50% dari besar blok penyandian.
b. Hasil enkripsi selalu sama dengan dekripsi walapun teks diinput dengan berbagai kombinasi karakter (huruf, angka, simbol).
c. Koneksi jaringan dibutuhkan pada perangkat lunak ini untuk dapat menjalankan fungsi pengiriman pesan yang sudah di enkripsi.
d. Penerapan algoritma kunci privat untuk enkripsi SMS pada smartphone dapat meningkatkan keamanan. Pesan yang terenkripsi tidak akan dapat dibaca jika tidak didekripsi dengan menggunakan kunci yang benar.

5 SARAN

Berdasarkan hasil pembahasan dan kesimpulan, maka dapat diambil beberapa saran sebagai berikut:

a. Meningkatkan nilai *avalanche effect* bisa dikembangkan lagi dengan menggunakan algoritma yang berbeda sehingga diperoleh nilai *avalanche effect* yang lebih tinggi lagi.
b. Perangkat lunak saat ini hanya mampu mengirimkan sms dengan sim *default* saja belum bisa digunakan untuk mengirimkan sms dengan mengunakan sim dua (pada *smartphone* dengan dua sim card)
c. Perangkat lunak belum dapat mengirimkan langsung kunci enkripsi dan kunci dekripsinya bersama pesan teksnya, diharapkan pada pengembangan selanjutnya perangkat dapat mengirimkan kunci bersamaan dengan pesan teksnya.
d. Dalam implementasi algoritma Rijndael ini hanya dalam cakupan kecil dan sangat mendasar dengan menggunakan bahasa pemrograman Java. Penyusun berharap agar kedepan dapat dikembangkan.

6 DAFTAR PUSTAKA

[1] Satriawan, I. W. D., Sasmita, I. G. M. A., & Bayupati, I. P. A. (2014). Aplikasi Enkripsi SMS dengan Metode RSA pada Smartphone Berbasis Android. *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*.

[2] Defni, D., & Rahmayuni, I. (2014). Enkripsi SMS (Short Message Service) pada telepon selular berbasis Android dengan metode RC6. *Jurnal Momentum*, *16*(1).

[3] Ariyus, D. (2008). *Pengantar ilmu kriptografi: teori analisis & implementasi*. Penerbit Andi.

[4] Irawan, R., & Ilhamsyah, Y. B. Aplikasi Enkripsi Dan Dekripsi Pesan Singkat Menggunakan Algoritma Knapsack Berbasis Android. *Coding Jurnal Komputer dan Aplikasi*, *3*(3).

[5] Azhar, R., & Kurniawan, K. (2016). Aplikasi Keamanan Sms Menggunakan Algoritma Rijndael. *MATRIK: Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, *16*(1), 105-112.