ANALISIS DAN IMPLEMENTASI ENKRIPSI DAN DEKRIPSI GANDA KOMBINASI ALGORITMA BLOWFISH DAN ALGORITMA TRIPLE DES UNTUK SMS PADA SMARTPHONE ANDROID

ANALYSIS AND IMPLEMENTATION OF DOUBLE COMBINATION ENCRYPTION AND DECRYPTION USING BLOWFISH AND TRIPLE DES ALGORITHM FOR SMS ON ANDROID SMARTPHONE

[1]Guntur Tri Wibowo **[2]R.Rumani M** **[3]Randy Erfa Saputra**

[1,2,3]Jurusan Sistem Komputer – Universitas Telkom
Jl. Telekomunikasi, Dayeuhkolot, Bandung 40257, Indonesia

[1]guntur.triwi@gmail.com [2]rumani@telkomuniversity.ac.id [3]resaputra@telkomuniversity.ac.id

Abstrak

SMS merupakan suatu jasa layanan yang sering digunakan masyarakat untuk berbagi informasi dari pengirim ke penerima melalui suatu provider. Dalam pengiriman suatu pesan dapat di sadap atau di manipulasi oleh hacker. Oleh karena dibutuhkan suatu sistem pengamanan pesan yang biasanya disebut kriptografi. Kriptografi itu untuk mengenkripsi pesan agar tidak di ketahui orang lain.

Dalam Tugas akhir ini dirancang suatu aplikasi SMS dengan menggunakan enkripsi dan dekripsi algoritma blowfish dan triple DES pada smartphone android. Pesan teks akan di enkripsi menggunakan algoritma blowfish kemudian pesan akan di enkripsi lagi dengan algoritma triple DES, dan SMS di kirim ke penerima.

Algoritma blowfish dan algoritma triple DES di implementasikan pada smartphone android diharapkan dapat mengenkripsi SMS sebelum dikirim dan mendekripsi sms ketika diterima. Dengan menggunakan enkripsi ganda keamanan SMS menjadi lebih terjamin dan waktu enkripsi dan dekripsi tidak memakan waktu yang lama serta nilai Avalanche Effect yang baik. Aplikasi ini dapat di manfaatkan untuk pengiriman pesan teks.

Kata kunci : ***SMS, kriptografi , android, algoritma blowfish, algoritma triple DES***

Abstract

SMS is a frequently used service society to share information from the sender to the receiver through a provider. In the delivery of a message can be in or near the manipulation by hackers. Because it takes a message security system which is usually called Cryptography. Cryptography to encrypt a message so that it is not in the know of others.

In this final project designed a SMS application by using encryption and decryption algorithms blowfish and triple DES in the android smartphone. A text message will be encrypted using the blowfish algorithm, then the message will be encrypted with thetriple DES algorithm, and send SMS to the recipient.

Blowfish and triple DES algorithm had implemented in on android smartphone is expected to encrypt SMS before. it is sent and decrypts sms when received. By using double encryption security SMS became more secured and encryption and decryption time does take a long time as well as the value of the Avalanche Effect is good. This application can be used to send the message text.

Keyword: SMS, cryptographic, android, blowfish algorithm, triple DES algorithm

1. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi dalam media komunikasi berkembang cepat. Dari komunikasi suara sampai komunikasi data. Dan sms merupakan jenis layanan komunikasi yang berkembang cepat karena biaya nya relatif murah. Tetapi seiring perkembangan teknologi, pengiriman pesan menjadi tidak aman, karena terdapat hacker yang mencuri data informasi penting. Masyarakat membutuhkan suatu privasi data agar tetap aman sehingga dibutuhkan kriptografi untuk menyembunyikan pesan.

Kriptografi merupakan suatu ilmu untuk untuk mengamankan pesan. Dalam kriptografi terdapat 2 konsep utama yaitu enkripsi dan dekripsi. Enkripsi digunakan mengubah informasi menjadi tidak di kenali dan dekripsi mengubah informasi yang tidak di kenali ke informasi awal. Untuk melakukan kriptografi dibutuhkan suatu algoritma.

Dalam tugas akhir ini akan mengimplementasikan kombinasi algoritma blowfish dan algoritma triple DES pada pesan teks. Pemilihan algotritma blowfish karena algoritma yang cepat dan tidak ada hak paten sedangkan algoritma triple DES merupakan algoritma yang memiliki keamanan yang cukup baik. Dengan mengkombinasikan algoritma tersebut di harapkan teks SMS menjadi lebih aman karena dua kali pengenkripsian dan pendekripsian walau berpengaruh terhadap waktu proses enkripsi dan dekripsi.

1.2 Rumusan Masalah

Permasalahan yang diangkat dalam pembuatan tugas akhir ini adalah bagaimana merancang aplikasi SMS yang dapat melindungi informasi dan privasi sehingga pengguna merasa aman dengan menggunakan metode algoritma *blowfish* dan *triple DES* pada *smartphone* android

1.3 Tujuan Penelitian

Tujuan dari pembuatan tugas akhir ini adalah Untuk merancang aplikasi yang dapat mengenkripsi dan mendekripsi pesan teks SMS pada smartphone dengan menggunakan kombinasi algoritma blowfish dan algoritma triple DES sehingga pesan SMS menjadi aman..

1.4 Batasan Masalah

Batasan masalah dalam penyusunan tugas akhir ini adalah sebagai berikut:

1. Data yang di enkripsi berupa teks, tidak berupa file, gambar atau video.
2. Tidak memperhitungkan biaya SMS.
3. Tidak membahas penyerangan jaringan pengiriman sms pada operator
4. Menggunakan minimal android 2.3 (gingerbread)
5. Pengujian algoritma terhadap waktu, memori dan avalanche effect.
6. Tidak membahas mode triple DES.
7. Kunci enkripsi dan dekripsi sesama User sudah saling mengetahui.

2. DASAR TEORI

2.1 SMS (*Short Message Service*)[7]

SMS merupakan suatu fasilitas untuk mengirimkan dan menerima suatu pesan singkat berupa teks melalui perangkat nirkabel yaitu perangkat komunikasi telepon seluler, dalam hal ini perangkat yang digunaka adalah telepon seluler. Panjang isi pesan pada sebuah paket SMS berukuran maksimal 160 karakter, dimana setiap karakter memiliki panjang 7 bit. Beberapa aplikasi standar telepon selular dapat mendukung panjang pesan dengan karakter sepanjang 8 bit (panjang pesan maksimum 140 karakter) dan karakter yang lebih panjang lainnya seperti 16 bit, namun karakter sepanjang 8 bit dan 16 bit ini tidak didukung oleh semua aplikasi standar telepon selular. Pada umumnya karakter sepanjang 8 bit dan 7 bit digunakan untuk menampilkan data seperti gambar dan simbol..

2.2 Android[1]

Android adalah suatu sistem operasi yang digunakan untuk perangkat *mobile* yang berbasis Linux yang mencakup system operasi, *middleware* dan aplikasi. Android juga menyediakan platform terbuka bagi para pengembang guna menciptakan aplikasi mereka sendiri untuk digunakan oleh bermacam peranti bergerak. Arsitektur Android secara garis besar terdiri dari :

1. *Linux Kernel*
   Linux merupakan sistem operasi terbuka yang handal dalam manajemen memori dan proses.
2. *Libraries*
   Android menggunakan beberapa paket pustaka yang terdapat pada C/C++ dengan standar *Berkeley Software Distribution* (BSD) hanya setengah dari yang aslinya untuk tertanam pada kernel Linux.
3. *Android runtime*
   Android Runtime merupakan mesin virtual yang membuat aplikasi Android menjadi lebih tangguh dengan paket pustaka yang telah ada.
4. *Application framework*
   Aplikasi menyediakan kelas-kelas yang dapat digunakan untuk mengembangkan aplikasi Android.
5. *Applications*
   Lapisan aplikasi merupakan lapisan yang paling tampak pada pengguna ketika menjalankan program.

2.3 Kriptografi [6]

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Kriptografi adalah ilmu pengetahuan dan seni menjaga message agar tetap aman. Tujuan penerapan kriptografi adalah untuk membuat sesuatu yang tersembunyi, dapat suatu pesan rahasia berupa teks, suara, gambar dan video. Di dalam sistem kriptografi terdapat 5 bagian yaitu

1. Plaintext adalah pesan atau data dalam bentuk aslinya teks yang dapat terbaca. Plaintext adalah masukan bagi algoritma enkripsi.
2. Secret Key adalah masukan bagi algoritma enkripsi merupakan nilai yang bebas terhadap teks asli dan menentukan hasil keluaran algoritma enkripsi.
3. Chipertext adalah keluaran algoritma enkripsi. Ciphertext dapat dianggap sebagai pesan tersembunyi yang akan terlihat acak.
4. Algoritma Enkripsi memiliki 2 masukan teks asli dan kunci rahasia. Algoritma enkripsi melakukan transpormasi terhadap teks asli sehingga menghasilkan teks sandi.
5. Algoritma Dekripsi memiliki 2 masukan yaitu teks sandi dan kunci rahasia. Algoritma dekripsi memulihkan kembali teks sandi menjadi teks asli bila kunci rahasia algoritma enkripsi sama dengan algoritma dekripsi.

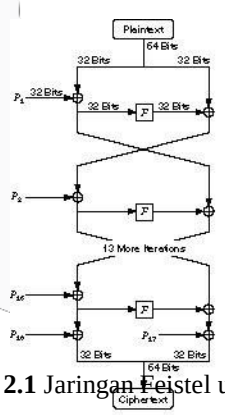
2.4 *Blowfish*[4]

Blowfish termasuk dalam enkripsi block Cipher 64-bit dengan panjang kunci yang bervariasi antara 32-bit sampai 448-bit. Algoritma Blowfish terdiri atas dua bagian yaitu Pembangkitan sub-kunci (Key-Expansion) dan Enkripsi Data. Enkripsi

Untuk alur algoritma enkripsi dengan metoda Blowfish dijelaskan sebagai berikut :

1. Array P terdiri dari delapan belas kunci 32-bit subkunci : P1,P2,…….,P18
2. Bentuk S-box sebanyak 4 buah masing-masing bernilai 32-bit yang memiliki masukan 256. Empat 32-bit S-box masing-masing mempunyai 256 entri.
3. Plainteks yang akan dienkripsi diasumsikan sebagai masukan, Plainteks tersebut diambil sebanyak 64-bit, dan apabila kurang dari 64-bit maka kita tambahkan bitnya, supaya dalam operasi nanti sesuai dengan datanya.
4. Hasil pengambilan tadi dibagi 2, 32-bit pertama disebut XL, 32-bit yang kedua disebut XR.
5. Selanjutnya lakukan operasi XL = XL xor Pi dan XR = F(XL) xor XR
6. Hasil dari operrasi diatas ditukar XL menjadi XR dan XR menjadi XL.
7. Lakukan sebanyak 16 kali, perulangan yang ke-16 lakukan lagi proses penukaran XL dan XR.
8. Pada proses ke-17 lakukan operasi untuk XR = XR xor P17 dan XL = XL xor P18.
9. Proses terakhir satukan kembali XL dan XR sehingga menjadi 64-bit kembali.

Blowfish menggunakan jaringan Feistel yang terdiri dari 16 buah putaran. Skema jaringan Feistel dapat dilihat di gambar ini.

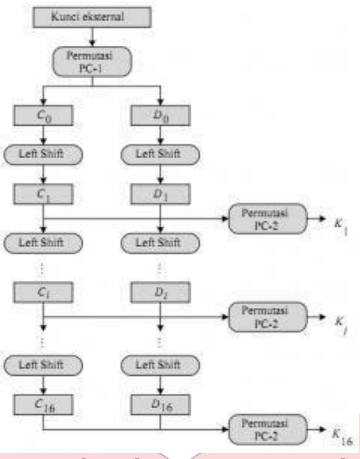


Gambar 2.1 Jaringan Feistel untuk Blowfish[4]

2.5 *Triple DES*[3]

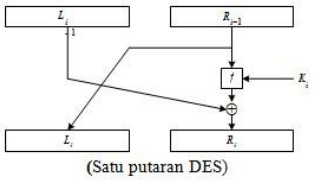
DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis cipher blok. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (internal key) atau upa-kunci (sub key). Kunci internal dibangkitkan dari kunci eksternal yang panjangnya 64 bit.

Pembangkitan Kunci Internal DES pada algoritma DES, dibutuhkan kunci internal sebanyak 16 buah, yaitu K1,K2,…,K16. Kunci-kunci internal ini dapat dibangkitkan sebelum proses enkripsi atau bersamaan dengan proses enkripsi. Kunci internal dibangkitkan dari kunci eksternal yang diberikan oleh pengguna. Kunci eksternal pada DES panjangnya 64-bit atau 8 karakter.



Gambar 2.2 Skema Pembangkitan Kunci Internal Algoritma *DES*[3]

Proses enkripsi terhadap blok plainteks dilakukan setelah permutasi awal. Setiap blok plainteks mengalami 16 kali putaran enkripsi. Untuk setiap putaran, digambarkan seperti gambar berikut:



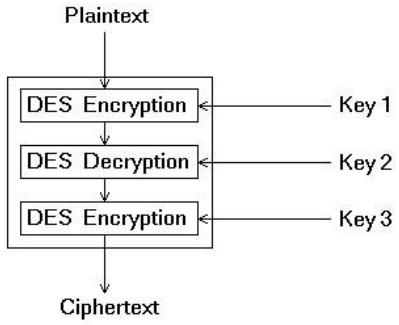
Gambar 2.3 Skema 1 putaran DES[3]

Setiap putaran enkripsi DES secara matematis dinyatakan sebagai :

$Li = R_{i-1}$ (2.2)

$Ri = L_{i-1} \oplus f(_{i-1}, K_i)$ (2.3)

Algoritma triple DES termasuk algoritma cipher blok berbasis kunci-simetris. 3DES (Triple Data Encryption Standard) atau biasa di sebut DESede atau juga Triple DES merupakan suatu algoritma pengembangan dari algoritma DES (Data Encryption Standard). Pada dasarnya algoritma yang digunakan sama, hanya pada 3DES dikembangkan dengan melakukan enkripsi dengan implementasi algoritma DES sebanyak tiga kali. 3DES memiliki tiga buah kunci yang berukuran 168-bit (tiga kali kunci 56-bit dari DES).



Gambar 2.4 Prosedure enkripsi pada *triple DES*[5]

3. PERANCANGAN DAN IPLEMENTASI SISTEM

3.1 Deskripsi Sistem

Sistem aplikasi ini memiliki nama Secret SMS, yang memiliki fungsi sebagai enkripsi dan dekripsi pesan *SMS*. Pada Aplikasi Secret SMS ini digunakan untuk mengirim pesan yang telah dienkripsi terlebih dahulu menggunakan 2 algoritma yaitu algortima *blowfish* dan *triple DES*, kemudian penerima akan menerima pesan dalam bentuk *chiper text*, agar dapat dibaca pesan tersebut di enkripsi dengan menggunakan kunci yang dimiliki. Aplikasi ini menggunakan dua algoritma yaitu *Blowfish* dan *triple DES*, kedua algoritma ini di kombinasikan sehingga menghasilkan pesan yang lebih aman dibandingkan dengan hanya menggunakan satu algoritma.

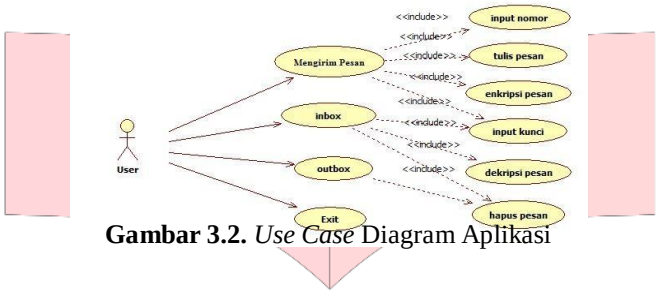
3.2 Gambaran Umum Sistem

Berikut ini merupakan gambaran umum aplikasi.

Gambar 3.1. Gambaran umum aplikasi

Gambaran umum aplikasi dimana user memasukan pesan yang akan dikirim. Untuk proses enkripsi pertama pesan diproses dengan menggunakan algoritma *blowfish* hasil proses tersebut, diproses lagi menggunakan algoritma *triple DES* maka keluaran dari proses terakhir dikirimkan ke penerima. Untuk proses dekripsi proses dibalik pertama menggunakan algoritma *triple DES* dan diproses lagi menggunakan *blowfish.*

Penggambaran interaksi antara user dengan sistem yang dibangun dapat dilihat pada *use case* berikut.



Gambar 3.2. *Use Case* Diagram Aplikasi

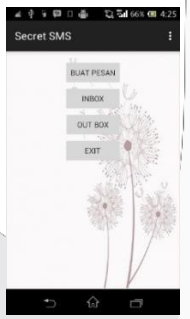
3.3 Implementasi

Implementasi *Interface* aplikasi pada telepon *smartphone sony Xperia m* dengan *Android version4.1(jellybean).* Implementasi antarmuka tiap menu diuji cobakan pada tahap pengujian *Inteface* yang diimplementasikan yaitu membuat pesan, *inbox dan outbox.*

Berikut ini adalah implementasi *interface* dari aplikasi *Secret SMS*

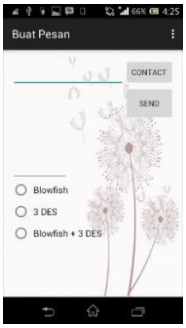
1. Halaman Utama

   Pada halaman *secret SMS* adalah *interface* untuk tampilan halaman utama yang berupa tampilan buat pesan, *inbox, outbox, exit.*

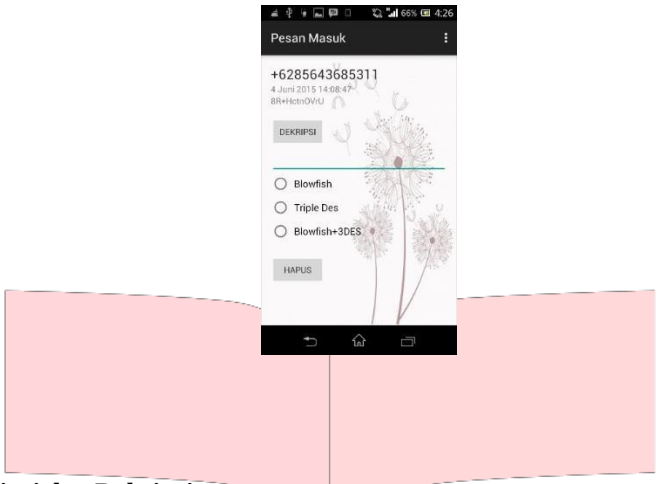


2. Buat Pesan

   pada halaman buat pesan menampilkan pengiriman pesan dengan memasukkan nomor tujuan, tulis pesan dan kunci adalah sebagai berikut :



3. Inbox Pesan
   pada halaman inbox pesan menampilkan semua list sms yang masuk. Kemudian pilih salah satu pesan untuk di dekripsi, masukkan kunci, terus pilih button radio dekripsi blowfish atau triple DES atau blowfish dan triple DES.



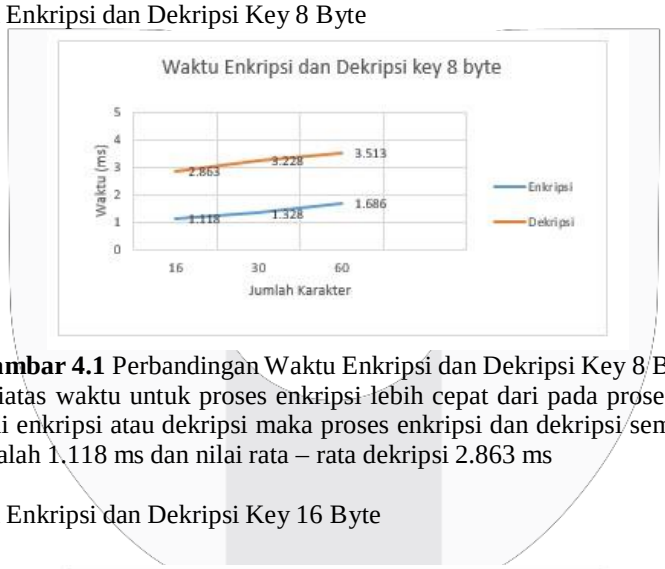
4. PENGUJIAN

4.1 Pengujian waktu enkripsi dan Dekripsi

Pengujian ini dilakukan dengan mengukur waktu proses ketika pesan dienkripsi sedangkan waktu proses dekripsi dilakukan ketika pesan didekripsi. Teknik perhitungan waktu dilakukan dengan panjang kunci 8 byte, 16 byte dan 24 byte serta panjang teks pesan 16, 30, 60 karakter.

Waktu proses enkripsi dan dekripsi adalah dengan menggunakan waktu millisecond.

4.1.1 Perbandingan Waktu Enkripsi dan Dekripsi Key 8 Byte



Gambar 4.1 Perbandingan Waktu Enkripsi dan Dekripsi Key 8 Byte

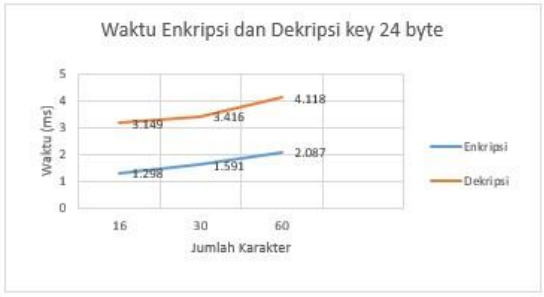
Terlihat dari gambar diatas waktu untuk proses enkripsi lebih cepat dari pada proses dekripsi. Semakin banyak jumlah karakter yang di enkripsi atau dekripsi maka proses enkripsi dan dekripsi semakin lama. Nilai rata – rata enkripsi 16 karakter adalah 1.118 ms dan nilai rata – rata dekripsi 2.863 ms

4.1.2 Perbandingan Waktu Enkripsi dan Dekripsi Key 16 Byte

Gambar 4.2 Perbandingan Waktu Enkripsi dan Dekripsi Key 16 Byte

Terlihat dari gambar diatas waktu untuk proses enkripsi lebih cepat dari pada proses dekripsi. Semakin banyak jumlah karakter yang di enkripsi atau dekripsi maka proses enkripsi dan dekripsi semakin lama. Nilai rata – rata enkripsi 16 karakter adalah 1.224 ms dan nilai rata – rata dekripsi 3.089 ms.

4.1.3 Perbandingan Waktu Enkripsi dan Dekripsi Key 24 Byte



Gambar 4.3 Perbandingan Waktu Enkripsi dan Dekripsi Key 24 Byte

Terlihat dari gambar diatas waktu untuk proses enkripsi lebih cepat dari pada proses dekripsi. Semakin banyak jumlah karakter yang di enkripsi atau dekripsi maka proses enkripsi dan dekripsi semakin lama. Nilai rata – rata enkripsi 16 karakter adalah 1.298 ms dan nilai rata – rata dekripsi 3.149 ms.

4.2 Pengujian *Avalanche effect*

Pada kriptografi, hasil yang diberikan sangat unik, berbeda dari data yang menjadi masukan dari proses tersebut. Sedikit perubahan pada data masukan dapat memberikan perubahan yang signifikan pada hasil proses kriptografi, dan perubahan tersebut dinamakan avalanche effect. Semakin besar perubahan yang terjadi, semakin baik performansi dari algoritma kriptografi tersebut

Tabel 4. 1 Pengujian *Avalanche Effect*

Plain Text	*Cipher Text*	*Avalanche Effect*
6B 75 6B 75	7134385739584f437a6d66437a6d664 378344575663651	44 % (67 perubahan bit)
6B 61 6B 75	46612b326848584a335553333864476 45347725754773d3d	43 % (83 perubahan bit)
73 61 70 75	49565070522f73446f5061665368387 142624e6935773d3d	48 % (93 perubahan bit)
73 61 70 61	773837625a7370673972354c526279 433161324172773d3d	45.8 % (88 perubahan bit)
6B 61 73 6B 75 73	706739426246455477616a55627379 625136493734413d3d	45% (89 perubahan bit)
6B 75 73 6B 75 73	3834715a45555a496835554d637547 305462637a43673d3d	45% (87 perubahan bit)

Dari hasil pengujian, terlihat bahwa perubahan satu bit pada masukan memberikan perubahan dengan rentang 67 bit – 93bit. Hasil ini menunjukkan penggabungan dari algoritma Blowfish dan Triple DES yang telah dibuat memiliki performa yang baik karena nilai Avalanche effect mendekati 50%. Suatu algoritma kriptografi akan sulit untuk dipecahkan ketika kunci yang digunakan tidak diketahui, dan hasil yang diberikan sangat unik.

4.3 Pengujian Alokasi Memori

Pengujian memori dilakukan untuk mengetahui seberapa besar memori yang dibutuhkan untuk menjalani aplikasi Secret SMS. Pengukuran memori dilakukan menggunakan DDMS (Dalvik Debug Monitor Server) yang terdapat pada android studio. Untuk skenario pengamatan dengan DDMS, aplikasi dijalankan kemudian membuka seluruh menu aplikasi dan mengukur total heap size dan allocated heap size yang terlihat.

Tabel 4. 2 Pengujian Memori

Percobaan	Total *Heap Size* (MB)	*Allocated Heap Size* (MB)
1	16.566	9.341
2	16.566	9.902
3	16.566	10.353
4	16.566	9.694
5	16.566	10.269
6	16.566	10.591
7	16.566	9.697
8	16.566	10.025
9	16.566	10.687
10	16.566	11.195
Dst....	.....	.....
Rata-Rata	16.566	10.138

Dari tabel 4.2 dapat dilihat data yang diperoleh dari hasil percobaan nilai total heap size adalah 16.566 MB. Sedangkan untuk allocated heap size, nilai maksimumnya 11.195 MB dan nilai minimumnya 9.341 MB.

Berdasarkan data yang diperoleh di atas dapat disimpulkan bahwa penggunaan memori allocated heap size aplikasi dari total memori heap size yang disediakan oleh perangkat android adalah 61.19% yang berarti aplikasi ini memakan memori sekitar 61.19% memori yang disediakan oleh device. Dengan begitu aplikasi akan berjalan dengan baik karena penggunaan memori tidak mencapai 100% karena jika mencapai 100% aplikasi tidak akan berjalan atau berhenti mendadak

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan implementasi dan pengujian yang telah dilakukan pada bab sebelumnya, maka dapat ditarik kesimpulan sebagai berikut

1. Waktu rata – rata proses enkripsi dengan panjang teks 16 karakter dan panjang kunci 8 byte adalah 1.118 ms
2. Waktu rata – rata proses dekripsi dengan panjang teks 16 karakter dan panjang kunci 8 byte adalah 2.863 ms
3. Algoritma kriptografi yang digunakan memiliki performa yang baik, dilihat dari nilai Avalanche effect yang berkisar antara 43 % - 48 %
4. Penggunaan memori heap size aplikasi Secret SMS dari total memori heap size yang disediakan oleh perangkat android adalah 61.19 %.

5.2 Saran

Saran untuk melakukan pengembangan pada aplikasi ini adalah sebagai berikut.

1. Dapat menggunakan algoritm yang lain selain triple DES dan blowfish
2. Interface dibuat lebih menarik lagi dan di tambah fitur-fitur nya..

DAFTAR PUSTAKA

[1] Hermawan, Stephanus. 2011. Mudah Membuat Aplikasi Android. Yogyakarta: Andi
[2] Khairunnisa, Sulasti. (2014). Analisis Performansi Enkripsi dan Dekripsi Algoritma RC6 dan RSA untuk inbox SMS pada Platform Android.
[3] Nurwahidin,Arif. 28 November 2011. "Pengembangan Algoritma Kriptografi DES dengan 112 kunci internal".
[4] Prasetyo, Kurniawan Nur. Januari 2014. Perancangan dan Implementasi Enkripsi Data dengan Algoritma Blowfish Berbasi FPGA.
[5] Rizal, Muhammad. Juli 2012. Analisa Perbandingan Metode Enkripsi RijnDael dan Triple DES untuk Pengamanan Data.
[6] Sadikin, Rifki. 2012. Kriptografi untuk Keamanan Jaringan. Yogyakarta: Andi
[7] Saskara, Gede Arna Jude . (2013). "Aplikasi Kriptografi untuk SMS Menggunakan Struktur Feistel Berbabis Android".
[8] Widodo, P.P., & Herlawati .2011. Menggunakan UML. Bandung : Informatika Bandung.